On cyber

The utility of military cyber operations during armed conflict

van Haaster, J.

ON CYBER

Jelle van Haaster

On Cyber

Jelle van Haaster

ISBN: 9789493124011

On Cyber

The Utility of Military Cyber Operations During Armed Conflict

Jelle van Haaster

Cover: Jelle van Haaster

Typography and design: Merel de Hart, Bureau Multimedia NLDA

Printed: Reprografie FBD Breda

ISBN: 9789493124011

This dissertation was financially and factually supported by the Royal Netherlands Army, Netherlands Defence Academy and the Netherlands Defence Cyber Command. The views and opinions in this dissertation are and remain solely the responsibility of the author and do not necessarily reflect those of the Ministry of Defence.

On Cyber

The Utility of Military Cyber Operations During Armed Conflict

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor
aan de Universiteit van Amsterdam
op gezag van de Rector Magnificus

prof. dr. ir. K.I.J. Maex

ten overstaan van een door het College voor Promoties ingestelde commissie,
in het openbaar te verdedigen in de Aula der Universiteit
op vrijdag 5 juli 2019, te 13.00 uur

door Jelle van Haaster

geboren te Dongeradeel

Promotiecommissie

Promotores

prof. dr. P.A.L. Ducheine	Universiteit van Amsterdam
prof. dr. T.D. Gill	Universiteit van Amsterdam

Co-promotores

prof. dr. F.P.B. Osinga	Nederlandse Defensie Academie

Overige leden

prof. dr. N.A.N.M. van Eijk	Universiteit van Amsterdam
prof. mr. C.E. du Perron	Universiteit van Amsterdam
prof. dr. D.W.J. Broeders	Erasmus Universiteit Rotterdam
dr. S.J.G. Reyn	Ministerie van Defensie
dr. M.C. Zwanenburg	Ministerie van Buitenlandse Zaken
prof. mr. dr. H.G. van der Wilt	Universiteit van Amsterdam

Faculteit der Rechtsgeleerdheid

For Siri

Table of contents

Table of contents

1

Introduction

1 Introduction

1.1 Introduction

"Ours is the age of the network."[1]

We live in an increasingly connected society;[2] national business and social networks are intertwined with other national and international networks. The free flow of data and unhindered functioning of our network structures have become vital for States, companies and individuals.[3] States can influence and inform citizens in unprecedented ways. Corporations can bind, influence and inform customers and employees like never before using new digital means and methods. Individuals enjoy rapid data-exchange through social networks like Facebook and Twitter, enabling them to share every aspect of their personal and professional life.[4] We have committed ourselves to life on the Internet and have become dependent on the unobstructed flow of data and functioning of our network infrastructures.[5] Comfort and user friendliness have prevailed over online security and safety.

In recent years we have witnessed the dangers of connecting virtually everything to the Internet – from power plants to the thermostat of the heating system in our houses.[6] It has become clearer than ever that connecting everything to the Internet does not necessarily yield a wholesome effect. The media daily reports 'cyber attacks', ranging from a 'mere' leaked document to a fully-fledged, service crippling, distributed denial of service attack.[7] A

[1] Antoine Bousquet, "Chaoplexic Warfare or the Future of Military Organisation," *International Affairs*, no. No. 84 (2008), 915-929. p. 915.

[2] See for example: European Commission, Digital Economy and Society Index (Brussels: European Commission, 2017). International Telecommunication Union (ITU), Measuring Hte Information Society Report, Vol. 1 (Geneva: International Telecommunication Union, 2017). pp. 2-22.

[3] For instance, the telecommunication and the information and communication sectors have been earmarked to be vital to the functioning of the Dutch government, see: The Hague Security Delta. (2015). Securing Critical Infrastructures in the Netherlands. The Hague: The Hague Security Delta. p. 9; See also: Ahmad Kamal, *The Law of Cyber-Space an Invitation to the Table of Negotiations*, 1st ed. (Geneva: United Nations Institute for Training and Research, 2005). p. 17.

[4] For instance, we share 684.478 Facebook posts, 10.000 Tweets, 3.600 Instagram photos and 48 hours of video per minute. Source: Neil Spencer, "How Much Data is Created Every Minute," visualnews.com/2012/06/19/how-much-data-created-every-minute/ (accessed October 30, 2013).

[5] Aelita Skarzauskiene and Marius Kalinauskas, "The Future Potential of Internet of Things," *Social Technologies*, no. 2(1) (2012), 102-113.pp. 103-104.

[6] Alina Selyukh and Jim Finkle, "Some U.S. Utilities Say They're Under Constant Cyber Attack," reuters.com/article/2013/05/21/us-cybersecurity-utilities-idUSBRE94K18V20130521?feedType=RSS&feedName=technologyNews&utm_source=feedly (accessed October 30, 2013); See for instance: Evan Osnos, "Hacking with Chinese Characteristics," newyorker.com/online/blogs/evanosnos/2013/01/hacking-with-chinese-characteristics.html (accessed October 30, 2013).

[7] See for instance: Eduard Kovacs, "DDOS Attack on DigiD Impacts 10 Million Dutch Users," news.softpedia.com/news/DDOS-Attack-on-DigiD-Impacts-10-Million-Dutch-Users-348791.shtml (accessed October 30, 2013). See also: Paul A. L. Ducheine, "The Notion of Cyber Operations," in Research Handbook on International Law and Cyberspace, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar Publisching, 2015), 211-232. pp. 211-213.

wide variety of actors are engaging in these types of harmful 'cyber'[8] activities, from non-State actors to States.[9] The motive of an individual behind these activities can range from recreation ("I was bored and thought it would be fun"[10]) to hacktivism and personal gain.[11] Private IT-security firms are contracted by States to secure systems, but also to exploit systems belonging to other States and corporations.[12] Apart from corporations, terrorists and organised criminal organisations seek to exploit unsuspecting States, companies and individuals.[13] We are witnessing the largest bank robberies in our history, for instance 45 million dollars was stolen from ATM-machines in less than ten hours using cyber means and methods,[14] and the 'SWIFT system' mediating bank transactions was misused resulting in 60 and 80 million dollars being stolen.[15]

Apart from the non-State entities, States are also engaging in harmful cyber activities by unleashing high-end malware on the Internet to achieve geopolitical and military goals.[16] The media have widely covered the use of Stuxnet, but that was relatively low-level compared to the malware currently wreaking havoc on the Internet.[17] Flame-malware, which was discovered on Iranian State-owned systems, was considered such complex code that it was deemed to take up to a year to analyse; it "redefines the notion of cyber war and cyber espionage" in a technical sense.[18] Since Flame is already old (it has been circulating online over six years now), it gives us a rather grim view on what malware we have yet to discover.[19]

[8] The author will devote considerable attention to describing and defining the meaning of the elusive prefix 'cyber' in chapter three of this thesis. For the purpose of this chapter it suffices to define the meaning of 'cyber' as 'relating to the cyberspace construct' (of which the Internet is a part).

[9] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques and Tools for Security Practitioners*, 1st ed. (Waltham: Syngress, 2011).

[10] Translated from Dutch, the answer of a 17-year old hacker to the question why he crippled one of the biggest Dutch Internet Service Providers. Source: Security.nl, "17-Jarige KPN-Hacker Bekent Schuld," security.nl/posting/35861/17-jarige+KPN-hacker+bekent+schuld (accessed October 30, 2013).

[11] Andress and Winterfeld, Cyber Warfare: Techniques and Tools for Security Practitioners p. 198.

[12] Ibid.

[13] Ibid. pp. 198-201.

[14] Colleen Long, "Feds in NYC: Hackers Stole $45M in ATM Card Breach," washingtontimes.com/news/2013/may/9/feds-nyc-hackers-stole-45m-atm-card-breach/?page=all (accessed October 30, 2013).

[15] "Here's how Hackers Stole $80 Million from Bangladesh Bank," The Hacker News, last modified March 14, 2016, accessed February 14, 2018, thehackernews.com/2016/03/bank-hacking-malware.html.; "Hackers Steal $60 Million from Taiwanese Bank; Two Suspects Arrested," The Hacker News, last modified October 11, 2017, accessed February 14, 2018, thehackernews.com/2017/10/swift-bank-hacking.html.

[16] See for example: Netherlands Coordinator for Security and Counterterrorism, Cyber Security Assessment Netherlands 2017 (The Hague: Netherlands Coordinator for Security and Counterterrorism, 2017). pp. 11-18.

[17] For an overview on Stuxnet documentation see: Tofino Security, "Stuxnet Central," tofinosecurity.com/stuxnet-central (accessed October 30, 2013).

[18] A. Gostev, "The Flame: Questions and Answers," securelist.com/en/blog/208193522/ (accessed October 30, 2013).

[19] Neil Rubenking J., "Flame Malware: Cybergeddon Or Old News?" securitywatch.pcmag.com/security-spyware/298405-flame-malware-cybergeddon-or-old-news (accessed October 30, 2013).

High-end malware only represents one side of the spectrum of cyber means and methods. These ‘hard power’ cyber capabilities are increasingly supplemented with ‘soft power’ cyber capabilities such as social-media and traditional capabilities to systematically influence target audiences.[20] The disruptive effectiveness of the systematic use of traditional and new capabilities was demonstrated in the information campaign before, during and in the wake of the 2016 U.S. elections.[21] The ominous campaign involved, amongst other, the coordinated use of social-media, conventional media and cyber operations to achieve policy objectives.[22]

Thus, States are able, in principle, to conduct a vast range of cyber operations. Therefore, cyber operations are widely heralded as force-multiplying weapon in the arsenal of both State and non-State actors.[23] The consideration and use of cyber means and methods in the light of Western politico-military debate regarding action in Libya and Syria evidences this notion.[24] Their use hitherto, however, is often seemingly swiftly cast aside as a viable modus operandi.[25] One of the issues leading to dismissal of ‘the cyber option’ is our limited understanding of the effects and implications of using cyber means and methods. Understanding means and methods is imperative for adequate appreciation of their value. State actors undoubtedly have the technological proficiency to cause effects through cyberspace, however, most still seem to lack understanding of the utility of (military) cyber operations. The negligence towards ‘the cyber option’ evidences that our technical proficiency in cyberspace far exceeds our understanding of cyber means and methods.

[20] “’I made Steve Bannon’s Psychological Warfare Tool’: Meet the Data War Whistleblower,” The Guardian, accessed June 30, 2018, theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[21] See for example: United States Office of the Director of National Intelligence. Background to “Assessing Russian Activities and Intentions in Recent US Elections”: The Analytic Process and Cyber Incident Attribution. Washington, D.C.: United States Office of the Director of National Intelligence, 2017.

[22] See for instance: “How Russia Pulled Off the Biggest Election Hack in U.S. History,” Esquire, ac-cessed February 8, 2017 <esquire.com/news-politics/a49791/russian-dnc-emails-hacked/>; “Did Putin Direct Russian Hacking? and Other Big Questions,” The Atlantic, accessed January 6, 2017, <theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/>; “’Kompromat’ and the Danger of Doubt and Confusion in a Democracy,” The New York Times, accessed Febru-ary 8, 2017, <nytimes.com/2017/01/15/world/europe/kompromat-donald-trump-russia-democracy.html>.

[23] Current developments in the creation of military doctrine supports this notion, see for instance: Dutch Ministry of Defence, *The Defence Cyber Strategy* (The Hague: Dutch Ministry of Defence, 2012); Ministry of Defence of the Russian Federation, *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space*, trans. NATO Cooperative Cyber Defence Centre of Excellence, 2011); United States Department of Defense, *Strategy for Operating in Cyberspace*, 2011).

[24] Eric Schmitt and Thom Shanker, “U.S. Debated Cyberwarfare in Attack Plan on Libya,” nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0 (accessed October 30, 2013); Paul McLeary, “Dempsey Lays Out various US Military Options in Syria,” defensenews.com/article/20130722/DEFREG02/307220026/Dempsey-Lays-Out-Various-US-Military-Options-Syria (accessed 30 October, 2013); Amber Corrin, “The Other Syria Debate: Cyber Weapons,” fcw.com/articles/2013/09/04/cyber-weapons-syria.aspx (accessed 30 October, 2013).

[25] Schmitt and Shanker, “U.S. Debated Cyberwarfare in Attack Plan on Libya,”

1.2 Framing the problem

There are many different cyber means and methods used in the world today by a wide variety of State and non-State actors, many of which are benign 'routine uses' of information and communication technologies for social or professional purposes. The Internet is most prominently used for sending and receiving mails, text or instant messaging, reading online news, using customer services and participating in social networks.[26] In other words, the harmful activities described above only represent a portion of the activities conducted on the Internet. Notwithstanding its benign use, the Internet is also used for harmful activities such as crime,[27] espionage,[28] sabotage[29] and more generally: forwarding one's interest to the detriment of another's.[30] Cyber means and methods have become one of the many ways of forwarding or protecting one's interests. This notion has made its way into the armed forces from the late 1990s to the 2000s.[31] Many armed forces have organised themselves for utilising cyber means and methods in military cyber operations and some have used these operations in conflict.[32] Although armed forces are conducting military cyber operations, there is a lack of understanding regarding the utility of military cyber operations.

[26] "Living Online: What the Internet is used For," Eurostat, 2017, accessed February 15, 2018, ec.europa.eu/eurostat/cache/infographs/ict/bloc-1b.html; "Most Popular Online Activities of Adult Users in the Unites States 2015," 2015, accessed February 15, 2018, statista.com/statistics/183910/internet-activities-of-us-users/; "Email 'most Common Internet Activity' in Britain," BBC, 2017 , accessed February 15, 2018, bbc.com/news/technology-40812692.

[27] See for instance: "The Relentless Growth of Cybercrime," Europol, 2016, accessed February 15, 2018, europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime.

[28] See: "Snowden Archive," The Intercept, 2017, accessed February 15, 2018, theintercept.com/snowden-sidtoday/.

[29] See Stuxnet for instance: Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32. Stuxnet Dossier," Symantec Security Response (2011).; "Stuxnet Central," 2012, accessed October 30, 2013, tofinosecurity.com/stuxnet-central.

[30] See for example: "BlackEnergy Trojan Strikes again: Attack Ukrainian Electric Power Industry," ESET, 2016, accessed February 10, 2017, welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/; "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, 2016, accessed February 10, 2017, wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. "Inside Kremlin Propaganda Machine: Russian Blogger Exposes Russia's Internet Troll Factory," , accessed February 27, 2016, youtube.com/watch?v=L5w3Ib1cyJM; "How Russia Pulled Off the Biggest Election Hack in U.S. History," Esquire, accessed February 8, 2017, esquire.com/news-politics/a49791/russian-dnc-emails-hacked/; United States Office of the Director of National Intelligence, Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution (Washington, D.C.: United States Office of the Director of National Intelligence,[2017]); "The Podesta Emails," WikiLeaks, 2016, accessed February 8, 2017, wikileaks.org/podesta-emails/; "Hillary Clinton Email Archive," WikiLeaks, 2016, accessed February 8, 2017, wikileaks.org/clinton-emails/; M. Donner, "Cyberassault on Estonia," IEEE Security and Privacy 5, no. 4 (2007), 4.; Peter Finn, Cyber Assaults on Estonia Typify a New Battle Tactic, 2007), A01.

[31] See for example: The White House, Securing America's Cyberspace, National Plan for Information Systems Protection: An Invitation to a Dialogue (Washington, DC: The White House, 2000).; U S Department of Defense, "Joint Task Force on Computer Network Defense Now Operational," Office of the Assistant Secretary of Defense (Public Affairs), no. 658-98 (December 30, 1998).; North Atlantic Council, The Prague Summit and NATO's Transformation: A Reader's Guide (Brussels: NATO Public Diplomacy Division, 2003).; Harry D. Raduege, "Future Defense Department Cybersecurity Builds on the Past," Signal (February 01, 2008).

[32] See: Center for Strategic and International Studies (CSIS), The Cyber Index: Interantional Security Trends and Realities (Geneva: United Nations Institute for Disarmament Research (UNIDIR),[2013]).pp. 9-109.

Armed forces use the following categorisation of the different levels involved in military operations: strategic (with the political and military components), operational and tactical.[33] The national strategic or political-strategic level involves "applying the full range of national resources, across all instruments of power, to achieve policy objectives."[34] The military-strategic level is aimed at the "coordinated, systematic development use of the military" to achieve the specified policy objectives.[35] The operational level within the military consequently focuses on planning, conducting and sustaining "campaigns and major [military] operations [...] within theatres or areas of operations."[36] The operational level links strategic objectives (i.e. those derived from policy objectives) to concrete military activities in areas of operations. [37] These concrete military activities are conducted at the tactical level where "activities, battles and engagements are planned and executed" to contribute to achieving a military objective.[38]

The problem of ill understanding of the utility of cyber means and methods presents itself at all levels of warfighting, the strategic, operational and tactical. First, at the strategic level, it is unclear to what extent military cyber operations by the military power instrument could be used, for what purposes and how it contributes to State power or strategic interests (e.g. anticipation, prevention, protection, deterrence, intervention, stabilisation or normalisation). As a consequence, States rather resort to traditional means and methods than to relatively new capabilities, as it is unclear how these can contribute to a State's interests. These factors lead to military cyber operations not being used to the full extend at the strategic level and this impacts the use of cyber means and methods at the lower levels (i.e. operational and tactical).

Secondly, at the operational level a similar unfamiliarity with cyber means and methods results in military cyber operations not being used to their full extent. Commanders are reluctant to employ cyber operations as it is unclear what effects these can achieve in theatre and at what risk. The latter are primarily caused by gaps in knowledge regarding the effectiveness and legal framework enveloping the use of military cyber operations. Many unfounded assumptions as to the effectiveness and legitimacy of cyber means and methods, and general unfamiliarity, impede the willingness of commanders to resort to cyber operations. As a consequence, the operational level is reluctant in employing cyber operations, which in turn impacts the strategic and tactical levels.

[33] The Netherlands Defence Doctrine adds the political-strategic and the technical level to the levels of military activity (see: Dutch Ministry of Defence, Netherlands Defence Doctrine (Den Haag: Ministerie van Defensie, 2013). pp. 92-97) this thesis will use NATO's three level standard.

[34] North Atlantic Treaty Organisation, Allied Joint Publication 1(D): Allied Joint Doctrine (Brussels: Nato Standardization Agency, 2017). p. 1-8.

[35] Dutch Ministry of Defence, Netherlands Defence Doctrine (Den Haag: Ministerie van Defensie, 2013). p. 93.

[36] North Atlantic Treaty Organisation, Allied Joint Publication 1(D): Allied Joint Doctrine (Brussels: NATO Standardization Agency, 2017). p. 1-10.

[37] Ibid. p. 1-10.

[38] Ibid. p. 1-11.

As third, at the tactical level, where the activities are actually conducted that may contribute to achieving operational and/or strategic objectives, there is also much to be desired in the realm of cyber activities. Those conducting military cyber operations may receive little guidance or assignments as the knowledge required to give guidance only slowly enters the operational and strategic levels, which results in little opportunities to apply skills in real life and affects morale. As a consequence of reluctance in employing military cyber operations, non-cyber units at the tactical level may lack supporting cyber activities that may function as force-multiplier and/or generally make their operations more effective.

Thus, the problem of lack of understanding presents itself at all levels within the military, however, all levels of warfighting also contribute to the problem. Ideally, all relevant persons at the various of warfighting understand the utility of military cyber operations. As mentioned above, however, understanding is lacking. This problem could be solved in various ways; one way is by creating awareness at the strategic level as to cyber capabilities and effects. This top-down approach would eventually permeate the operational and tactical levels of warfighting and lead to the integration of cyber capabilities in the firmament of armed forces. An alternative would be a bottom-up approach, involving the tactical and operational levels 'selling' the merits of cyber capabilities to the strategic level. That would, however, require a certain pedigree of cyber operations' effectiveness. This thesis will hold that neither the top-down or bottom-up approach is satisfactory, a multi-faceted and multilevel approach will be necessary to create understanding at all levels of warfighting and facilitate the true integration of cyber operations within the armed forces.

1.3 Goal of this thesis

The goal of this research is to contribute to a more comprehensive understanding of the utility of military cyber operations. Before States can adequately employ cyber means and methods, a thorough understanding is required of the strategic, societal, technological, military and legal context wherein these operations are conducted. For instance, at the strategic level decision-makers need to know how military cyber operations can contribute to State interests, at the operational level a military commander needs to know what the relations are between traditional military operations and military cyber operations. Before being able to employ these means at all, technical personnel and materiel is needed to prepare and execute the cyber operation. Apart from that, these cyber activities have to be conducted in conformity with the applicable legal frameworks. This research will envelop these issues by expanding on the following research question:
What is the utility of military cyber operations during armed conflict?

1.4 Research methodology

In order to answer the research question, this thesis will utilise the interdisciplinary research process (IRP).[39] In other words, this thesis is interdisciplinary, which can best be summarised as an approach "to address a compelling problem that defies explanation by a single discipline".[40] Interdisciplinarity is not a research methodology; it "is a matter of manner rather than of method, requiring a sensitivity to nuance and context, a flexibility of mind, and an adeptness at navigating and translating concepts."[41] There is "no one 'best' way to conduct [interdisciplinary] research, but instead there are multiple options, each with advantages and disadvantages".[42] One of the 'early' (2008) and better-developed interdisciplinary processes is the IRP,[43] which "while being controversial' presents a "complete step-by-step interdisciplinary process. [44] This thesis will base itself on the IRP.

The IRP encompasses certain steps, namely: (1) state research question; (2) justify using an interdisciplinary approach; (3) identify relevant disciplines; (4) conduct literature research; (5) develop adequacy in each relevant discipline; (6) analyse the problem and evaluate each insight or theory; (7) identify conflict between insights and their sources; (8) create common ground between insights; (9) construct a more comprehensive understanding; (10) reflect on, test, and communicate the understanding.[45] Steps one to six are aimed at drawing on disciplinary insights, steps seven to ten focus on integrating the disciplinary insights into a synthesis. Step one has been covered in section 1.5, the following paragraphs will focus on steps two and three. Steps four to six will be conducted in chapters two to six. Steps seven to ten will be conducted in chapter seven.

First, as any choice for a specific way of conducting research, the choice has to be justified, as epitomised in step two of the IRP. Interdisciplinarity is used to integrate disciplinary insights in order to research complex problems, that is, problems too complex to be handled by a single discipline. This thesis requires such an approach, as the complexity of the utility of military cyber operations cannot be captured by a single discipline. Doing monodisciplinary research would result in a single-faceted answer to the research question, this monolithic view on military cyber operations is one of the main issues contributing to the problematic state of 'cyber'. For instance, a technical view (e.g. computer sciences) of cyber operations will rule out the strategic consequences involved, the strategic view

[39] See: Allen F. Repko and Rick Szostak, *Interdisciplinary Research: Process and Theory*, 3rd ed. (Thousands Oaks: Sage, 2017).

[40] Daniel C. Mack and Craig Gibson, eds., *Interdisciplinarity and Academic Libraries* (Chicago: Association of College and Research Libraries, 2012). p. 168.

[41] Robert Frodeman et al., ed., *The Oxford Handbook of Interdisciplinarity* (New York: Oxford University Press, 2010). p. xxxi.

[42] Gabriele Bammer, Disciplining Interdisciplinarity: Integration and Implementation Sciences for Researching Complex Real-World Problems (Canberra: Australian National University E Press, 2013). p. 5.

[43] See: Allen F. Repko and Rick Szostak, Interdisciplinary Research: Process and Theory.

[44] Frodeman et al., ed., The Oxford Handbook of Interdisciplinarity. p. 367.

[45] Allen F. Repko and Rick Szostak, Interdisciplinary Research: Process and Theory. p. 78.

(e.g. international relations) in turn omits many of the technical intricalities of cyber operations. Taking a military view (e.g. war studies) of cyber operations will omit many non-military cyber capabilities that may prove useful in military cyber operations, taking a non-military view (e.g. sociological) will fail to acknowledge many of the complexities involved in military organisation and operations. A legal perspective (e.g. public international law) to military cyber operations will not sufficiently address certain aspects of the military and technical fields involved in utilising cyber operations. Thus, there is no single discipline that can capture all the intricalities of the utility of military cyber operations, as mentioned before, utility is complex and depends on various factors, for example strategic, societal, technological, military and legal. Therefore, this thesis will use interdisciplinarity and the IRP as this mind-set and process force a researcher to incorporate and facilitate multiple disciplines.

Step three of the interdisciplinary research process is aimed at identifying disciplines relevant to or involved in answering the research question. This paragraph will briefly highlight the disciplines needed to discuss the utility of military cyber operations. Chapter two, 'On Power', will incorporate relevant portions of political science, more specifically international relations theory regarding power. Chapter three, 'On Society', will utilise concepts from sociology as the subject is informationised society. Chapter four, 'On Technology, will use insights from computer sciences (history), computer security, political science (conflict and peace studies), and military doctrine in order to discuss 'cyberspace' and 'cyber capabilities'. Chapter five, 'On Fighting', uses insights from military doctrine to discuss the military's ability to incorporate cyber operations. Chapter six, 'On Law', self-evidently utilises law as discipline and as it focuses on conflict, it concentrates on international humanitarian law as part of public international law.

Steps four to ten will be conducted in the various chapters of this thesis. Step five, developing adequacy in each relevant discipline, commands a brief explanation beforehand. Step five might seem as if mastery in all disciplines is required, fortunately "scholars of interdisciplinary studies agree that no individual can attain mastery of all relevant disciplines". [46] The IRP involves developing adequacy and not mastery; mastery involves "learning a discipline thoroughly in order to practice it" and adequacy "merely comprehending how that discipline characteristically looks at the world in terms of its perspective, assumptions, epistemology, concepts, theories and methods".[47] The aim of the chapters is adequacy, deriving the relevant portions of specific disciplines needed to answer the sub-questions as listed in the following section.

[46] Mack and Gibson, eds., Interdisciplinarity and Academic Libraries. p. 172.

[47] Allen F. Repko, *Interdisciplinary Research: Process and Theory*, 1st ed. (London: Sage, 2008). p. 43.

1.5 Structure

Utility involves "fitness to some purpose or worth to some end",[48] thus a certain desired purpose or end is required when assessing utility. Apart from that, the context must be understood, as without context statements on utility would be general and serve little purpose.[49] In other words, in order to provide an answer to the potential utility of military cyber operations a sense of purpose and context is required. This sense of purpose and context will be created by addressing five perspectives as depicted in Figure 1, each with a specific sub-question.

First, to understand how the military instrument can be employed, to what end, and how cyber capabilities can contribute to achieving this end, the notion of 'power' needs to be addressed. Actors seek to promote their interests using all instruments at their disposal, whether or not they succeed depends on complex workings of power. Before being able to forward what the utility of cyber capabilities is, the utility of the military has to be understood as instrument of power. This understanding can be created by placing the military instrument in the broader context of other instruments of State power and from that, derive their respective role in achieving State interests. By doing so one can appreciate the utility of the instruments of power – including the military instrument. Chapter two will do so by answering the sub-question:
What are the main theoretical viewpoints on power, how is power manifested and to what end and through which means?

After having examined the interests sought after on a strategic level, chapter three will place the cyber capabilities in their societal context. The *raison d'être* of 'all things cyber', increasing attention for 'cyber', and the rising use and potential of cyber capabilities is informationised society. Chapter three will illustrate that this society offers both new ways for influencing other actors but in turn opens up opportunities for other actors to influence us as well. Our reliance on information technology has brought open up new opportunities but in turn has made us vulnerable to myriads of new threats. One of the new means and methods for influencing each other in contemporary society is 'cyber', however, the scope, nature and meaning of 'cyber' is very ambiguous. Chapter three will discuss the effect of informatisation, the consequent increasing potential of cyber capabilities, and clarify meaning of 'cyber'. It will do so by answering the following sub-question:
What is the impact of informationised society and cyber on power?

[48] Merriam-Webster Dictionary, "Definition of Utility," Merriam-Webster, merriam-webster.com/dictionary/utility (accessed March 8, 2017).

[49] See for instance: Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred A. Knopf, 2007). p. 719.

Chapter four will aim to clarify the 'realm' where actors seek to influence each other with cyber capabilities ('cyberspace') and list the capabilities with which they seek to do so ('cyber capabilities'). This understanding of the realm and the capabilities used therein is instrumental for assessing the potential utility of cyber capabilities to the military. Chapter four will address these issues by answering the following sub-question:
How are cyber capabilities conceptualised and utilised by State and non-State actors?

Before being able to provide an answer as to the utility of military cyber operations, the question should be answered whether the military is able to integrate the cyber capabilities within the different levels of warfighting. As by integrating these capabilities, the military can organise them into a form allowing the cyber capabilities to be wielded. This form is known as a military operation, or in this specific context: a military cyber operation. As cyber capabilities are relatively new, chapter five will discuss how armed forces are conceptually and doctrinally organised and what the place of cyber capabilities is within that organisation. Chapter five will do so by addressing the following question:
What is the conceptual place of cyber capabilities within military organisation and how are cyber capabilities integrated in the armed forces?

Should the military succeed in integrating cyber capabilities and use these in military cyber operations there are certain limits on using them. A legal framework governs military cyber operations in peacetime and during conflict.[50] The contents and application of this legal framework have been much debated. In academic circles debate has surpassed the stage of whether or not international humanitarian law applies to cyber operations; instead, academic debate now centres on how to best apply the legal framework. In policy circles, however, there is still much debate as to which rules apply to cyber operations in peacetime and during conflict.[51] The legal framework may limit the ways military cyber operations are used and consequently impact their utility, hence chapter six will seek to answer the following question:
What is the international humanitarian law legal framework for employing military cyber operations above the threshold of attack during armed conflict?

[50] See for example: Katharina Ziolkowski, Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy (Tallinn: NATO CCD COE Publications, 2013); Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017).

[51] "UN GGE on Cybersecurity: The End of an Era?" The Diplomat, 2017, accessed February 20, 2018, thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

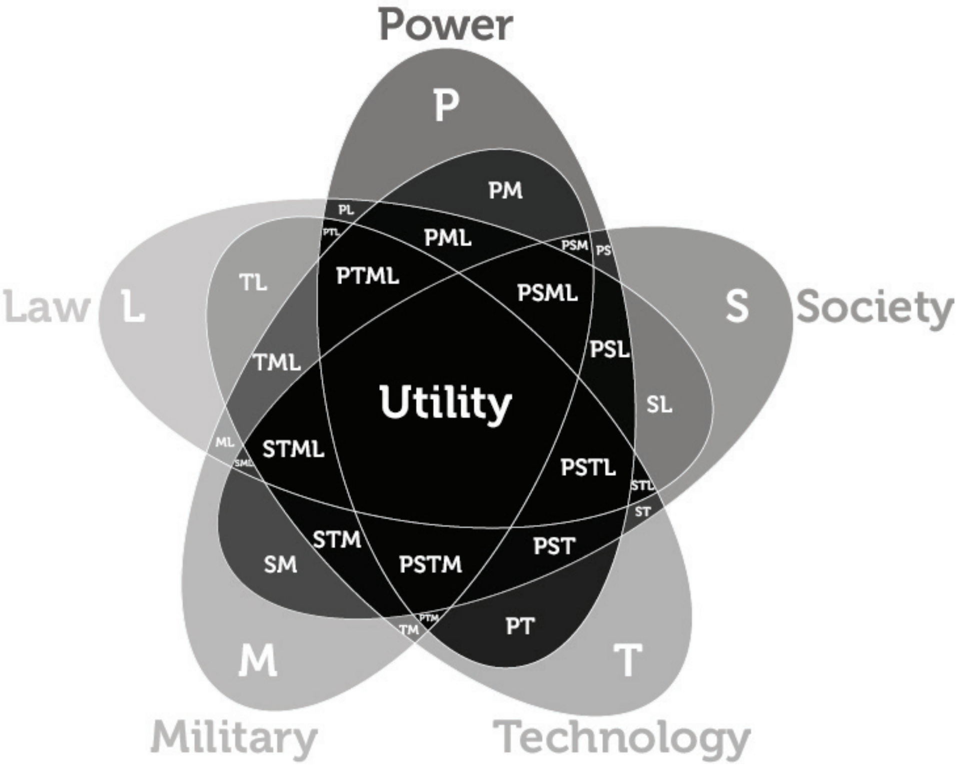

Figure 1 Structure of this research where five perspectives will be adjoined in order to enhance understanding of the utility of military cyber operations.

2
On Power

2 On Power

2.1 Introduction

Within international relations the concept of power, or its absence is one of the most contested issues.[1] Even though "weighty books have analysed and elaborated the concept",[2] much is unsettled apart from a notion that the issue requires attention.[3] It especially requires attention in the context of this thesis that seeks to present what the utility is of military cyber operations. Military cyber operations, from a State perspective, are conducted by its armed forces. Or in power instruments parlance, military cyber operations are conducted by the military instrument of power. The use of the military instrument serves the Clausewitzian notion of a "continuation of policy by other means".[4] In other words, the military instrument – including military cyber capabilities – serves to fulfil a political goal. Seldom, however, the military instrument is used stand-alone. Often the military is employed within a broader, more comprehensive, context also including other capabilities or power instruments at a State's disposal. The ability of a State to achieve its political goals using these instruments is often expressed in power; a powerful State is more likely to accomplish its goals than a less powerful State. The discussion on the concept of power has resulted, amongst other, in the notion that the likelihood of a State achieving a political goal depends on a wide range of factors.

2.1.1 Goal of this chapter

As mentioned in chapter one, utility involves fitness to some purpose or end – statements on utility without a specified purpose are trivial. States conduct activities to some end, namely promoting their interests. In their international relations actors may resort to military activities such as military cyber operations. In order to assess the utility of military cyber operations, the purpose of the military instrument in international relations has to be understood. The context of the military instrument, its purpose, potential ends, and factors impacting potential successfulness are included in the power discussion of the 20th century. Therefore, to create understanding of the context wherein military cyber operations are utilised from an international relations perspective this chapter will discuss the power debate by answering the following research question: *What are the main theoretical viewpoints on power, how is power manifested, to what end and through which means?*

[1] David A. Baldwin, "Power and International Relations," in *Handbook of International Relations*, eds. Walter Carlsnaes, Thomas Risse and Beth A. Simmons (London: Sage, 2002), 177-191. p. 177.

[2] Robert Gilpin, *War and Change in World Politics* (Cambridge: Cambridge University Press, 1983). p. 13

[3] Ronen Palan, *Global Political Economy: Contemporary Theories* (London: Routledge, 2000). pp. 53-54.

[4] Carl von Clausewitz, *On War, Translated and Edited by Michael Howard and Peter Paret* (Princeton: Princeton University Press, 1976). p. 28.

2.1.2 Structure

This chapter is structured as follows: the first section will distinguish two approaches to understanding power, the 'power as resource' and 'relational power' approach (section 2.2). The latter will provide the theoretical basis for the remainder of this chapter, it must, however, be considered in the light of the former ('power as resource'). After having discussed the approaches and resulting factors to be taken into account when discussing and appreciating power in section 2.2, this chapter will focus on the mechanisms involved in conveying power. It will do so by describing the four faces of power and the more modern 'power concepts' in section 2.3. The power concept involved impacts potential successfulness of an activity and consequently the utility. After that, section 2.4 will discuss to what *ends* power can be used. This sense of purpose on a strategic level, as mentioned before, is integral to the notion of utility of military cyber operations but to any other activity as well. Section 2.5 will discuss the *means* through which power is conveyed by States, as the means selected, similar to the power concept involved, impacts the effectiveness of an activity and consequently the utility. This chapter will conclude with a model specifying the factors to be taken into account when discussing power, the concepts through which power is conveyed, the means used therein and the ends sought after. By doing so it will uncover factors to be taken into account when assessing the utility of military cyber operations.

2.2 Approaches to power

The power of States was deemed to be easily measurable in the eighteenth century:[5] factors to be taken into account where "territory, wealth, armies and navies".[6] Such a quantification of power is well suited for decision makers in matters of foreign politics – including war. Since by using this approach, a decision maker operates under the assumption of having empirical basis for making decisions on waging war and potential outcomes. In the beginning of the twentieth century, however, scholars argued "that only the Great Powers, by reason of their disproportionate strength, can invest their national policies with real international importance". [7] The great powers were conceived to be the only States with the military means to back up their foreign policy.[8] International politics were depicted as "a sort of game played by superpersons around a supergameboard".[9] The eighteenth-century concept, however, still played a prominent role throughout the twentieth century. It was believed that a State's power position could be derived from its

[5] Baldwin, "Power and International Relations." pp. 177-178.

[6] Ibid.

[7] Frank H. Simonds and Brooks Emeny, The Great Powers in World Politics: International Relations and Economic Nationalism (New York: American Book Company, 1937).

[8] Baldwin, "Power and International Relations." p. 177.

[9] Harold Hance Sprout and Margaret Tuttle Sprout, *Foundations of International Politics* (New Jersey: Van Nostrand, 1962). p. 237.

sources of power; Morgenthau further developed this ‘power as resource approach’ with his influential writings on balance of power that places strong emphasis on power resources.[10]

This ‘power as resource approach’ was challenged in 1950 by the ‘relational power approach’.[11] Power was conceived to be not only possession of particular resources or elements; instead, power should be defined relationally.[12] There is a triadic relation, “power over whom is not yet a complete specification: there must be added, in such and such particulars (the scope of power)”.[13] For instance, “A and B may each have power over C, but with regard to different areas of C’s behaviour, determining policies which C is to pursue in different fields; more simply, A and B may have power with respect to different values of C’s”.[14] The relation power approach does not discard the idea of sources of power entirely, but it stresses that the context of application of power or influence is crucial in determining the outcome. Power is conceived to be “an actual or potential relationship between two or more actors (persons, states, groups, etc.) rather than a property of any one of them”.[15]

This section will further describe the development of these two approaches, first the ‘power as resource approach’ will be discussed (sub-section 2.2.1) and secondly the ‘relational power approach’ (sub-section 2.2.2). After that, the differences and common grounds between the approaches will be highlighted in a model for assessing power (sub-section 2.2.3). In doing so this section will seek to answer the first part of this chapter’s sub-question: *What are the main theoretical viewpoints on assessing power?*

2.2.1 Power as resource

This sub-section will discuss the ‘power as resource approach’, which is also known as the ‘elements of national power approach’ or ‘power as entity’.[16] The modern take on ‘power as resource’ is epitomised in the concept of ‘balance of power’.[17] ‘Balance of power’, in all its different meanings,[18] has enjoyed variable popularity. Sometimes it has “been highly regarded and sometimes not”, “it had its heyday in the eighteenth and nineteenth

[10] Hans J. Morgenthau, *Politics among Nations: The Struggle for Power and Peace* (New York: Alfred A. Knopf, 1948).

[11] Baldwin, “Power and International Relations.” p. 178.

[12] Harold D. Laswell and Abraham Kaplan, *Power and Society: A Framework for Political Inquiry* (New Haven: Yale University Press, 1950). p. 75.

[13] Ibid.

[14] Ibid. p. 76.

[15] Baldwin, “Power and International Relations.” p. 178.

[16] David A. Baldwin, “Power and International Relations,” in *Handbook of International Relations*, eds. Walter Carlsnaes, Thomas Risse-Kappen and Beth A. Simmons, 2nd ed. (Los Angeles: SAGE, 2013), 273-297. p. 287; Janice Bially Mattern, “The Concept of Power and the (Un)Discipline of International Relations,” in *The Oxford Handbook of International Relations*, eds. Christian Reus-Smit and Duncan Snidal, 2008b), 691-697. p. 692.

[17] See for instance: Morgenthau, *Politics among Nations: The Struggle for Power and Peace*. p.178; John J. Mearsheimer, *The Tragedy of Great Power Politics* (New York: WW Norton & Company, 2001).

[18] Inis L. Claude, *Power and International Relations* (New York: Random House, 1962). pp. 12-13; Baldwin, “Power and International Relations.” p. 244.

centuries, [...] it suffered disrepute during the greater part of the first half of the twentieth century, and [...] It has recently [i.e.1962] made a most impressive comeback".[19] Within that concept "States were depicted as seeking to maximise power relative to each other, thus producing a 'balance of power' or as seeking to produce a balance of power".[20] The concept 'balance of power' "implies that changes in power distribution can be observed an measured.[21]

The 'balance of power' can imply equilibrium or disequilibrium and epitomises the basic lust and consecutive struggle for power in a (neo-)realist tradition. Power, resulting in a balance, is achieved either (semi-) automatically, as it is deemed to be the default situation of international relations, or manually as a by-product of intrinsic human motivations. Disregarding its mode of operation, a question rises with regard to what it is that is being compared within 'balance of power'. The purpose of exemplifying the factors being measured in determining the power distribution is to provide a contrast to the 'relational power approach' in sub-section 2.2.2. This sub-section will use Morgenthau's 1948 factors for assessing power distribution as illustration since these have proven most influential throughout power as resource publications.[22]

In 1948 Morgenthau stated the factors involved in determining power: geography, natural resources, industrial capacity, military preparedness, population, national character, national morale and quality of diplomacy.[23] Morgenthau considers some of these to be "more or less stable" and others to be constantly changing.[24] He illustrates how these can qualitatively be employed as general measuring rod. Considering the factor geography for instance, he deems the geographically isolated position of the United States to be a 'fundamental factor' impacting its foreign relations.[25]

Morgenthau considers it to be the task of the analyst of international relations to compare "one power factor in one country with the same or another power factor in another country [...]" this analysis concerns "the relative weight of changes in the individual components of the power of different nations for the over-all power relations of these different nations".[26] This control over resources approach is the most widely used and accepted approach to the

[19] Claude, Power and International Relations p. 12.

[20] Baldwin, "Power and International Relations." p. 274.

[21] Quincy Wright, *A Study of War: Volume II* (Chicago: The University of Chicago Press, 1942). p. 743.

[22] Mattern, "The Concept of Power and the (Un)Discipline of International Relations," in , 691-697. p. 692.

[23] Morgenthau, Politics among Nations: The Struggle for Power and Peace pp. 80-108.

[24] Ibid. p. 80.

[25] Ibid. p. 80.

[26] Ibid. p. 110.

study of national power.[27] Other scholars have followed the qualitative approach taken by Morgenthau, but have supplied it with an empirical basis.[28]

The main problems with Morgenthau's approach are: "(1) it is not always certain that actors will be able to use resources which are nominally under their control; (2) it is not always clear what types of resources should be included in a general measure of power, and one suspects that for different types of conflicts different combinations of resources will be needed to explain the outcomes of conflicts; (3) some types of resources, such as the will to use force, are extremely difficult to measure; (4) the focus on national power precludes the consideration of the role of non-state actors in determining the outcome of conflicts; and (5) it is not clear how one is to deal with interdependence, coalition and collective action".[29] Although there are some problematic issues with Morgenthau's approach, it was and still is an influential approach to measuring power.[30] The following sub-section will discuss the challenger of the 'power as resource approach' known as the 'relational power approach'.

2.2.2 Relational power

The 'relational power approach' conceives power and its measurability different from the 'power as resource approach'. As mentioned before, proponents of this approach argue that power should be defined relationally: It "does not reside in a resource but stems from the particular relation in which abilities are actualised".[31] Power is only meaningful "if its control is seen to be valued by other actors in the interaction […]".[32] Power resources are considered to constitute *actual power* within the 'power as resource approach' whilst they are only one of the many facets of *potential power* within the 'relational power approach'. Whether or not *potential power* can be turned into *actual power* depends on the actors and their relations. There are three key-elements in the 'relational power approach', power is deemed: non-fungible (2.2.2.1),[33] multidimensional[34] (2.2.2.2) and dependent of the context or "specific policy-contingency frameworks" (2.2.2.3).[35] This section will briefly describe the ratio behind these three interlinking elements.

[27] Jeffrey Hart, "Three Approaches to the Measurement of Power in International Relations," *International Organisation* 30, no. 2 (1976), 289-305. p. 289.

[28] See for instance: J. D. Singer and Melvin Small, "The Composition and Status Ordering of the International System: 1815-1940," *World Politics* 18, no. 2 (1966), 236-282.

[29] Hart, "Three Approaches to the Measurement of Power in International Relations." p. 290.

[30] Mattern, "The Concept of Power and the (Un)Discipline of International Relations," in , 691-697. pp. 692-694.

[31] Stefano Guzzini, "On the Measure of Power and the Power of Measure in International Relations," *DIIS Working Paper*, no. 28 (2009). p. 7.

[32] Stefano Guzzini, "Structural Power: The Limits of Neorealist Power Analysis," *International Organisation* 47, no. 3 (1993), 443-478. pp. 452-453.

[33] Baldwin, "Power and International Relations." p. 180.

[34] Ibid. p. 178.

[35] Guzzini, "Structural Power: The Limits of Neorealist Power Analysis." p. 453.

2.2.2.1 Fungibility

The first issue is fungibility, which refers to "the ease with which power resources useful in one issue-area can be used in other issue-areas".[36] Money is the prime example of a highly fungible resource, money "can be used to buy a car, a meal, a haircut, or a book."[37] Some scholars conceive power to be "the currency of great-power politics [...] what money is to economics, power is to international relations".[38] Power is, however, not as fungible as money or "time and information".[39] Money functions as "the real world measure of wealth",[40] but "there is no equivalent currency with which to measure power" within the relational power approach.[41] Power, being deemed (relatively) non-fungible, is considered to be multidimensional; a statement about power can only be made if provided with context.[42] Since "we cannot say that an actor 'has power' without specifying power to 'to do what'",[43] it is necessary to specify dimensions of power.

2.2.2.2 Multidimensional

Power is multidimensional, it consists – at least – of the dimensions scope and domain.[44] Less accepted domains are dimensions such as weight, costs and means.[45] The scope of power is understood to comprise objectives and the affected issue areas.[46] Domain "refers to the [...] actors subject to [the] influence [attempt]"[47] or simply "the target[s]".[48] The weight relates to the (potential) effectiveness of power, that is, the likelihood that "B's behaviour is or could be affected by A".[49] Costs indicate both the cost to actor A and the costs to B, for instance "is it costly or cheap for A to influence B? Is it costly or cheap for B to comply with A's demands?"[50] Means refer to the various instruments "of exercising influence"; there are

[36] Baldwin, "Power and International Relations." p. 180.

[37] Baldwin, "Power and International Relations." p. 180.

[38] Mearsheimer, The Tragedy of Great Power Politics. p. 59.

[39] Baldwin, "Power and International Relations." p. 180.

[40] Guzzini, "On the Measure of Power and the Power of Measure in International Relations." p. 7.

[41] Guzzini, "On the Measure of Power and the Power of Measure in International Relations." p. 7.

[42] Guzzini, "Structural Power: The Limits of Neorealist Power Analysis." p. 454.

[43] Joseph S. Nye, *Cyber Power* (Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, 2010). p. 2.

[44] Laswell and Kaplan, *Power and Society: A Framework for Political Inquiry*. p. 74; Baldwin, "Power and International Relations." p. 179; Joseph S. Nye, *The Future of Power*, 1st ed. (New York: Public Affairs, 2011). p. 6; Robert A. Dahl, "The Concept of Power," *Behavioral Science* 2, no. 3 (1957). p. 203.

[45] Baldwin, "Power and International Relations." p. 178; See also: Laswell and Kaplan, *Power and Society: A Framework for Political Inquiry*. p. 74. They describe the dimensions domain, scope, weight and coerciveness; Dahl, "The Concept of Power." p. 203. He describes the dimensions of base/domain, means/instruments, amount/extent and range/scope.

[46] Nye, *The Future of Power*. p. 6; Baldwin, "Power and International Relations." p. 180; Guzzini, "Structural Power: The Limits of Neorealist Power Analysis." p. 453.

[47] Baldwin, "Power and International Relations." p. 180.

[48] Guzzini, "Structural Power: The Limits of Neorealist Power Analysis". p. 453.

[49] Baldwin, "Power and International Relations." p. 180; Guzzini, "Structural Power: The Limits of Neorealist Power Analysis," , 443-478. pp. 453-454; See also: Dahl, "The Concept of Power." p. 203. He refers to weight simply as the amount or extent an actor has power over another actor.

[50] Baldwin, "Power and International Relations." p. 178.

"many ways to categorise such means", which will be discussed later in this chapter.[51]

2.2.2.3 *Contextual*

Any statement about power would be meaningless without "the specification of the situation", which is called the policy-contingency framework.[52] Specifying the situation is an "important step in capability analysis" and basically entails "establishing who is trying to get whom to do what" and in what situation.[53] Some power resources may be useless in one policy-contingency framework or situation whilst being extremely influential in others, "the only way to determine whether something is a power resource or not is to place it in the context of a real or hypothetical policy-contingency framework".[54] Such a framework requires contextual analysis consisting of the historical and societal background.[55]

Thus, the relational approach to power conceives power and its measurement in a broader context than the 'power as resource approach'. Adding factors and dimensions increases the difficulty of measuring power; it is "difficult to add up the various dimensions in order to arrive at some overall estimate of an actor's power".[56] Hence, any estimate of an actors' overall power is "likely to be controversial".[57]

2.2.3 Sub-conclusion

This section has sought to answer the following sub-question: *What are the main theoretical viewpoints on assessing power?* This section has covered two theoretical viewpoints on assessing power: the 'power as resource' (see 2.2.1) and 'relational power' approaches (see 2.2.2). Although the theoretical foundations differ with regard to the possession of power and its measurability, the approaches have common grounds, or more precise, they are not entirely irreconcilable. The method forwarded within the 'relational power approach' is general in nature; every meaningful statement about power would include some of the power dimensions, including statements derived from the 'power as resource approach'. The difference lies in focus, for instance the 'power as resource approach' focuses almost exclusively on the dimension 'means'. Focus on a single or particular set of dimensions could result in tunnel vision, ruling out other dimensions that may be equally important. Thus, as a matter of approach, the relational power approach seems to be able to incorporate the various aspects of power more adequately. As this approach offers a comprehensive framework for making statements on power and is able of incorporating

[51] Baldwin, "Power and International Relations."pp. 178-179.

[52] Guzzini, "Structural Power: The Limits of Neorealist Power Analysis," , 443-478. p. 454.

[53] David A. Baldwin, *Economic Statecraft* (New Jersey: Princeton University Press, 1985). p. 149.

[54] David A. Baldwin, "Power Analysis and World Politics: New Trends Versus Old Tendencies," *World Politics* 31, no. 2 (1979), 161-194. p. 165.

[55] Guzzini, "Structural Power: The Limits of Neorealist Power Analysis," , 443-478. p. 454.

[56] Baldwin, "Power and International Relations." p. 179.

[57] Ibid. p. 179.

other viewpoints as well, this chapter will use the ‘relational power approach’ to structure the notion of power.

An aggregation of the potential elements to be taken into account when adopting the ‘relational power approach’ is depicted in Figure 2 and will be briefly specified here. First, whether or not an actor is powerful depends on the (hypothetical) policy-contingency framework or context (see Figure 2 grey square). An actor’s (in)action in this specific context may have different consequences in another (see 2.2.2.3). Apart from that, power in this context may not necessarily constitute overall power; it depends on the situation at hand whether or not an actor is powerful. In some cases, a target actor may not be receptive for the influence attempt made by State A because it simply is not interested or entirely non-receptive, for instance if State A would enforce import controls for State B which does not import goods to State A.

Besides context, the dimensions of power can aid in making statements on power. The most accepted dimensions are scope and domain (see 2.2.2.2). The scope of the (in)action includes the objectives are sought after or the issue areas affected. The domain involves assessing the actors subjected to the (in)action. Although not considered a ‘most accepted dimension’, it would be irrational to omit the ‘power as resource approach’ by not including the means used in the (in)action – as this is still a very influential approach (see 2.2.1). Other dimensions which could be included are weight (how likely is it that the target’s behaviour is or could be affected) and costs (how costly is it to influence the target and how costly is it for the target to comply).

Some elements depicted in the framework in Figure 2 have been covered in other discussions within the power debate or can be further specified by looking at State practice. Whereas actors’ interaction is depicted as simple red and blue arrows in Figure 2, there is a distinct discussion within the power debate specifying the ways through which actors create relations. Also, there are generalised overviews of the scope of State activities and the means States have at their disposal. The remainder of this chapter will seek to further specify these elements: the mechanisms of interaction in the context of power will be discussed in section 2.3, the scope in section 2.4 and the means in section 2.5.

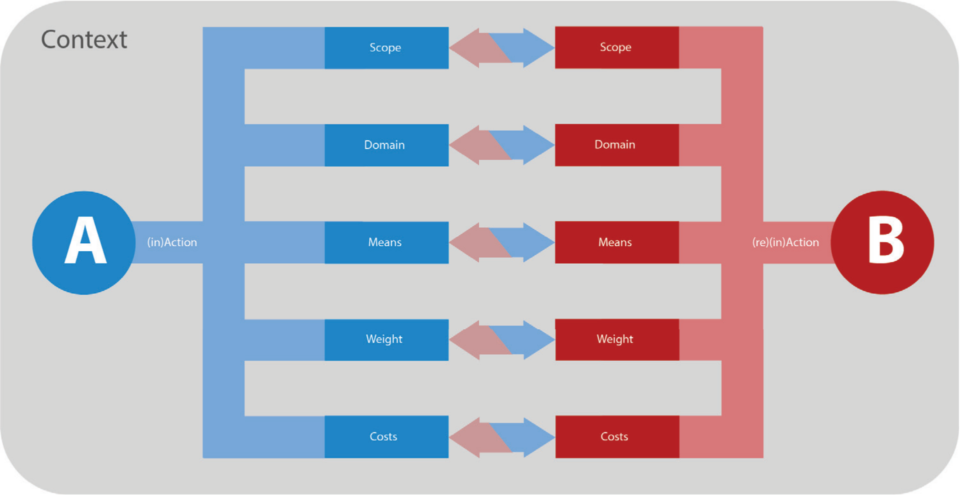

Figure 2 Power framework

2.3 Power's manifestation

This section will seek to further specify the various power mechanisms through which actors manifest power by answering the following sub-question: *How is power manifested?* Debate regarding this question has been going on from the sixties until now in the form of the 'faces of power' discussion and has quite recently resulted in the more modern 'taxonomy of power concepts framework'. Many elements within the 'taxonomy of power concepts framework' are derived from the faces discussion, as such the 'faces of power' discussion must be understood in order to be able to appreciate the more modern power concepts framework. The 'faces of power' discussion and 'power concepts' framework revolve around the questions of and what constitutes power and how power is manifested.

In order to answer the sub-question this section will first describe the outline of the faces of power discussion by describing the four faces of power (see sub-section 2.3.1.1 to 2.3.1.4) and then reflect on the value of the faces discussion (see sub-section 2.3.1.5). After that this section will describe a more modern, also deemed "analytically more systematic and precise",[58] approach to power as advanced by Michael Barnett and Raymond Duvall in their taxonomy of power concepts (see sub-section 2.3.2).[59] Lastly, this section will conclude with reflecting on the relation of the taxonomy of power framework and faces of power discussion, consequently the framework and discussion will be integrated into the conceptual power framework (see Figure 2) in section 2.3.3.

[58] Michael Barnett and Raymond Duvall, "Power in International Politics," *International Organisation* 59, no. 1 (2005), 39-75. p. 43. Note 13.

[59] Ibid.

2.3.1 Faces of power

The faces of power discussion started after realisation set upon certain scholars "that there are two faces of power, neither of which the sociologist see and only one of which the political scientist sees".[60] The discussion offers "three alternative ways of conceiving of power as a relationship of influence, each of which [goes] beyond that first face".[61] The following sub-sections will provide an overview of the four faces of power.

2.3.1.1 *First face of power*

The first face of power is the classical conception of power, with a strong focus "on observable behaviour", making identifying "decision-making [...] their central task".[62] Power can only be analysed after "careful examination of series of concrete decisions".[63] Hence, identifying "who prevails in decision-making [seems] the best way to determine which individuals and groups have more power in social life, because direct conflict between actors presents a situation most closely approximating an experimental test of their capacities to affect outcomes".[64] Who prevails in decision-making and their preferences in specific issue-areas – so-called interests – can only be derived from situations "in which the preferences of the hypothetical ruling elite run counter to those of any other likely group that might be suggested" in other words, during conflict.[65] From the first face of power viewpoint one can derive that power is about influencing the decision-making process in situations of concrete conflict or "in activity bearing directly upon"[66] decision-making. Therefore power, under the first face, is deemed to operate by influencing decision-making and/or the decision-making process. Those with the greatest influence upon decision-making are deemed most powerful.

2.3.1.2 *Second face of power*

The second face of power entails "decision-making and nondecision-making" in both overt and covert conflicts and was most prominently forwarded by Peter Bachrach and Morton Baratz.[67] It is grounded upon the notion that "some person or association could limit decision-making to relatively non-controversial matters, by influencing community values and political procedures and rituals", overlooking these more or less covert processes would be overlooking "the less apparent, but nonetheless extremely important, [second]

[60] Peter Bachrach and Morton S. Baratz, "Two Faces of Power," *The American Politcal Science Review* 56, no. 4 (1962), 947-952. p. 947.

[61] Janice Bially Mattern, The Concept of Power and the (Un) Discipline of International RelationsOxford University Press, 2008a). p. 693.

[62] Steven Lukes, *Power: A Radical View* (Hong Kong: MacMillan Education Ltd, 1974). p. 12.

[63] Robert A. Dahl, "A Critique of the Ruling Elite Model," *The American Political Science Review* 52, no. 2 (1958). p. 466.

[64] Nelson W. Polsby, *Community Power and Political Theory* (New Haven: Yale University Press, 1963). Cited in Lukes, Power: A Radical View. p. 13.

[65] Dahl, "A Critique of the Ruling Elite Model." p. 466.

[66] Bachrach and Baratz, "Two Faces of Power." p. 948.

[67] Lukes, Power: A Radical View. p. 18.

face of power".[68] Through the process of nondecision-making, "demands for change in the existing allocation of benefits and privileges in the community can be suffocated before they are even voiced; or kept covert; or killed before they gain access to the relevant decision-making arena; or, failing all these things, maimed or destroyed in the decision-implementing stage of the policy process".[69] Proponents of power's second face also focus on observable conflict, if there is no conflict one must assume "that there is consensus on the prevailing allocation of values, in which case nondecision-making is impossible".[70] Thus the second face of power adds control over (political) agenda's and exclusion of potential issues from the decision-making spheres to the ambit of exerting power.

2.3.1.3 *Third face of power*

The third face of power is forwarded by Steven Lukes, who states, "it is highly unsatisfactory to suppose that power is only in situation of [...] conflict".[71] Perhaps the "supreme exercise of power [is] to get another or others to have the desires you want them to have – that is, to secure their compliance by controlling their thoughts and desires".[72] Nondecision-making power within the second-face can be distinguished on the basis of a conflict or a grievance, without conflict, it is believed that there is consensus. Lukes' critique is that it is not clear what constitutes a conflict or grievance and secondly that would be "the supreme and most insidious exercise of power to prevent people, to whatever degree, from having grievances by shaping their perceptions, cognitions and preferences",[73] the first two faces of power are blind to these forms of power.[74]

The third face of power, as opposed to the first and second, allows consideration of the "many ways in which potential issues are kept out of politics, whether through the operation of social forces and institutional practices or through individuals' decisions".[75] In other words, power is deemed to function much broader, also by "supressing latent conflicts within society", [76] for instance through control of information, mass media, socialisation and indoctrination at schools.[77]

2.3.1.4 *Fourth face of power*

Peter Digeser' fourth face of power or 'power4' draws heavily on Foucault's writings and differs from the other faces "in how it deals with subjects, where it is found and how it is

[68] Bachrach and Baratz, "Two Faces of Power." p. 949.

[69] Lukes, *Power: A Radical View.* p. 19; Peter Bachrach and Morton S. Baratz, "Decisions and Nondecisions: An Analytical Framework," *The American Political Science Review* 57, no. 3 (1963), 632-642. pp. 641-642.

[70] Lukes, Power: A Radical View. p. 19.

[71] Ibid. p. 23.

[72] Lukes, Power: A Radical View. p. 23.

[73] Ibid. p. 24.

[74] Peter Digeser, "The Fourth Face of Power," *The Journal of Politics* 54, no. 4 (1992), 977-1007. p. 979.

[75] Lukes, Power: A Radical View

[76] Ibid. p. 57.

[77] Ibid. p. 23.

exercised, studied, and manifested".[78] The fourth face of power involves "the [...] formation of our dispositions, desires, and intentions",[79] also called (human) agency, i.e., the human capacity of choice making. The fourth face of power revolves around "enabling or disabling of agency, i.e., the ability to have desires, form goals, and act freely".[80] The other faces of power take the autonomous choice of a subject to act freely or making choices for granted, often autonomy is derived from concepts such as "rationality, intentionality, responsibility, mutuality, interest, etc."[81] and analysed through domains such as "psyche, subjectivity, personality, consciousness, etc.".[82] In other words, subjects make choices based on (contingent) values, but power4 conceives it differently; power4 tampers our most basic ability to freely make choices and having the notion that we are able to choose.

Thus power4 shapes and lies at the bottom of our core values, as such its workings are hard to distinguish. Lying at the heart of fundamental subjectivity (i.e. the state of being subject), power4 also "lies at the bottom of all our social practices: politics, medicine, religion, psychiatry, work".[83] In other words, power is everywhere, "power is co-extensive with the social body; there are no spaces of primal liberty between the meshes of the network".[84] The fourth face of power focuses "not on the effects of biases on issues or on the violation of true interests, but rather on the sources and effects of the norms and values regardless of their bias or truth".[85]

The vehicles of power are both A and B – dichotomies which in turn also produce a particular power perception – which can entail individuals, groups or States. Through their "practices and interactions" power is conveyed and it is "put into operation when [they] participate in discourse and norms".[86] Power is possessed by neither of them and its exercise can only be taken "in a weak sense" since the fourth face of power presupposes that there are "no essential interests, no enduring set of true desires and wants that are part of our natures [...] subjects do not choose to exercise power4".[87] Power is not about the subjects, but the relations and circumstances that shaped the subjects, for instance through "institutional and cultural practices".[88] As a consequence, "the exercise of the fourth face

[78] Digeser, "The Fourth Face of Power," , 977-1007. p. 979.

[79] Ibid. p. 980.

[80] Ibid. p. 980.

[81] Stephen K. White, "Foucault's Challenge to Critical Theory," *The American Political Science Review* 80, no. 2 (1986), 419-432. p. 419.

[82] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, 2nd ed. (New York: Random House, 1995). pp. 29-30.

[83] Digeser, "The Fourth Face of Power." p. 980.

[84] Michel Foucault, "Power and Strategies." In *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, edited by Colin Gordon. New York: Pantheon. Cited in Digeser, *The Fourth Face of Power*. p. 981.

[85] Ibid. p. 982.

[86] Michel Foucault, "Power and Strategies." In *Power/Knowledge: Selected Interviews and Other Writings 1972-1977*, edited by Colin Gordon. New York: Pantheon. Cited in Digeser, *The Fourth Face of Power*. p. 982.

[87] Ibid.

[88] Jana Sawicki, *Disciplining Foucault: Feminism, Power, and the Body* (New York: Routledge, 1991). pp. 21-22.

of power is revealed only in an examination of the myriad and infinitesimal mechanisms of our social practices and discourses".[89]

Illusive and omnipresent as power4 is, it does not mean that it works without constraints or produces indefinitely pliable subjects.[90] Subjects resist to power, since they are not "predesigned to be rational, responsible, self-disciplined individuals", but that does not necessarily mean, "that we are predesigned to be something else".[91] Therefore, within the fourth face of power, "complete success in any attempt to forge a particular kind of subjectivity is impossible".[92]

2.3.1.5 *Value of the faces debate*

The faces of power discussion envelopes the question how power may be utilised and what qualifies as power and what does not. The previous sub-sections have discussed the four faces of power in order to distil how power is deemed to operate. Though seemingly the easiest way out of a stalemate of conflicting views, each and every aspect of power's operation is a valid way of influencing. Thus, taking the different faces into account, the following non-limitative list of means and methods are deemed to be forms of influence: Influencing decision-making, controlling (political) agenda's, exclusion of potential issues, control of information, control over mass media, socialisation, indoctrination through schools and all phenomena associated with power4.

The faces of power are a very conceptual approach of analysing the mechanisms of exerting power or influence. Although expressing how power is used and how it is deemed to function, it offers no systematic overview of different ways of conveying power. Barnett and Duvall have forwarded a more modern taxonomy of power concepts, which they argue to be "analytically more systematic and precise, and conceptually more general", contrary to the "gaps and absences" within the faces debate.[93] The following sub-section will provide an overview of the taxonomy of power concepts.

2.3.2 Taxonomy of power concepts

Power is an essentially contested subject.[94] Barnett and Duvall argue that there is a way out of the stalemate and such a way out is necessary, since "the failure to develop alternative conceptualisations of power limits the ability of international relations scholars to understand how global outcomes are produced and how actors are differentially enabled

[89] Digeser, "The Fourth Face of Power." p. 985.

[90] Ibid; See also: William E. Connolly, "Taylor, Foucault, and Otherness," *Political Theory* 13, no. 3 (1985), 365-376. p. 371.

[91] Digeser, "The Fourth Face of Power." pp. 977-1007

[92] Ibid.

[93] Barnett and Duvall, "Power in International Politics," , 39-75. p. 43. Note 13.

[94] Baldwin, "Power and International Relations." pp. 177-178.

and constrained to determine their fates".[95] They distinguish four types of power: (1) Compulsory, epitomising "power as relations of interaction of direct control by one actor over another"; (2) institutional, considering "the control actors exercise indirectly over others through diffuse relations of interaction"; (3) structural, expressing "the constitution of subjects' capacities in direct structural relation to one another"; and (4) productive, entailing the "socially diffuse production of subjectivity in systems of meaning and signification".[96] The following sub-sections will further describe these four power concepts.

2.3.2.1 *Compulsory power*

Compulsory power follows the Dahlian definition of power, "the ability of A to get B to do what B otherwise would not have done";[97] it is very similar to the first face of power and hinges on intentionality, conflict and successfulness of A (see sub-section 2.3.1.1).[98] Barnett and Duvall depart from intentionality as perquisite for exercising power, "even if unintentionally [...]" power is present "whenever A's actions control B's action or circumstances", as is the case when unintentional or collateral damage is caused for instance.[99] Both State and non-State actors can exert compulsory power, "multinational corporations can use their control over capital to shape the foreign [and global] economies" and "nonstate networks and groups sometimes [...] terrorise entire populations".[100] Compulsory power does not require material resources; "it also entails symbolic and normative resources",[101] for instance appealing to normative values in order to compel an actor to do something.[102]

2.3.2.2 *Institutional power*

Institutional power involves an "actors' control of others in indirect ways", "the conceptual focus here is on the formal and informal institutions that mediate between A and B, as A, working through the rules and procedures that define those institutions, guides, steers, and constraints the action (or nonactions) and conditions of existence of others".[103] In such a scenario, A does not exercise power directly over B, "A cannot necessarily be said to 'possess' the institutions that constraints and shapes B", but A could be the dominant actor "that maintains total control over an institution".[104] Barnett and Duvall reckon that,

[95] Baldwin, "Power and International Relations." p. 41.

[96] Ibid. p. 43.

[97] Dahl, "The Concept of Power." pp. 202-203.pp. 202-203.

[98] Barnett and Duvall, "Power in International Politics." p. 49.

[99] Ibid. pp. 49-50; See also: Baldwin, "Power and International Relations." pp.

[100] Barnett and Duvall, "Power in International Politics." p. 50.

[101] Ibid. p. 50.

[102] See for example: Amnesty International, "Reports Israeli government plans to retaliate against Amnesty International over settlements campaign," amnesty.nl/actueel/reports-israeli-government-plans-to-retaliate-against-amnesty-international-over-settlements-campaign (accessed April 18, 2018).

[103] Barnett and Duvall, "Power in International Politics." p. 51.

[104] Ibid. p. 51.

in such a case, arguably, the institution would be “an instrument of compulsory power”.[105] Institutions serve as geospatial and temporal link between actors and can serve to affect “the behavior or conditions of others only through institutional arrangements (such as decisional rules, formalised lines of responsibility, divisions of labor, and structures of dispersed dependence)”.[106] Examples of institutions mediating actors relations are the United Nations, the North Atlantic Treaty Organisation, the European Union, the World Trade Organisation etc. An example of dominant actors within institutions are the permanent five in the United Nations Security Council who have the ‘power of veto’, contrary to other members.[107]

2.3.2.3 *Structural power*

Structural power hints towards Steven Lukes’ third face of power (see sub-section 2.3.1.3), it “concerns the structures – or, more precisely, the co-constitutive internal relations of structural positions – that define what kinds of social being actors are”.[108] More concretely, structural power “concerns the determination of social capacities and interests” of actors, based upon the notion “that the structural position, A, exists only by virtue of its relation to structural position, B”.[109] Even more specific, it “is the production and reproduction of internally related positions of super- and subordination, or domination, that actors occupy”.[110] Structural power “works to maintain the structures in which all actors are located and which [...] permit or constrain the action they may wish to take with respect to others with whom they are directly connected”.[111] Structural power is best characterised by Steven Lukes statement that it is “the supreme and most insidious exercise of power” to prevent or permit actors from arising within societies or structures.[112] Classical examples of structural power are the master-slave and capital-labour relations, where “the social relational capacities, subjectivities, and interests of actors are directly shaped by the social positions that they occupy.”[113] In other words, capital and labour accept their positions in the structure resulting in lack of conflict, nonetheless their structural positions produce a clear power relation (i.e. labour subjugated to capital).

2.3.2.4 *Productive power*

Productive power is based on more or less “generalised and diffuse social processes”, contrary to structural power which is based on a direct structural relations.[114] Productive

[105] Ibid. p. 51.

[106] Ibid. p. 51.d

[107] See: article 27 (3) UN Charter.

[108] Barnett and Duvall, “Power in International Politics.” pp. 52-53.

[109] Ibid. p. 53.

[110] Ibid. p. 55.

[111] David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power* (London: Routledge, 2011). p. 48.

[112] Digeser, “The Fourth Face of Power,” , 977-1007. p. 979; Barnett and Duvall, “Power in International Politics,” , 39-75. p. 53.

[113] Barnett and Duvall, “Power in International Politics.” pp. 52-53.

[114] Ibid. p. 55.

power “is the constitution of all social subjects with various social powers through systems of knowledge and discursive practices of broad and general scope”.[115] This differs from structural power; the focus is not on structures, but on “systems of signification and meaning (which are structured, but not themselves structures), and to networks of social forces perpetually shaping one another”.[116] In other words, productive power looks beyond structures, it is concerned with “the social processes and the systems of knowledge through which meaning is produces, fixed, lived, experienced and transformed”,[117] but also how discursive processes and practices produce social identities and capacities”.[118] Examples of productive power refer “to the discursive production of the subjects” by using categories of classification such as “civilised, rogue, European, unstable, Western, and democratic states”.[119] As such it shares conceptual foundations of the fourth face of power as to the constitution of the subject (see sub-section 2.3.1.4).

2.3.2.5 *Value of the power concepts*

The four power concepts taxonomy is promoted as a way out of the stalemate within the power debate in international relations. It is beyond doubt that the taxonomy presents more concrete and systematic footholds for researchers. This is only logical considering the fact that it is presented in a single publication rather than four separate publications over a time-span of nearly fifty years – as is the case with the faces discussion. The value of the four power concepts is that it enables the use of the faces’ theoretical foundations and actualising it in a systematic analytical framework. As such it is more useful than the faces of power discussion in unveiling how power manifests itself in relations of actors.

2.3.3 Sub-conclusion

This section has outlined the faces of power discussion (see sub-section 2.3.1) and the taxonomy of power concepts framework (see sub-section 2.3.2). The faces of power discussion is very abstract and as such not suited for making concrete statements on power (see sub-section 2.3.1.5). The taxonomy of power concepts framework, whilst building on the faces discussion, describes the concrete mechanisms through which power is manifested and as such is more useful here in answering the sub-question:
How is power manifested?

The compulsory, institutional, procedural and structural power concepts clarify how actors interact as depicted in Figure 3, or in other words: how power is manifested. The power concepts serve to illuminate the power mechanisms through which actors interact when seeking to influence each other. The effectiveness of an (in)action and the usefulness specific capabilities depends, in part, on the power concept involved. For example, the

[115] Ibid.

[116] Ibid.

[117] Ibid.

[118] Ibid.

[119] Ibid.

use of institutions might prove useful when the other actor is represented within that institution or when it has interest in the institution's issue area. Whereas an actor not bound or affected by the institution nor represented therein, is not likely to be affected by an influence attempt via institutions. Thus, the power concept or mechanism involved impacts potential successfulness of an activity and consequently may also impact the utility of any capability assisting in achieving the goal of an activity.

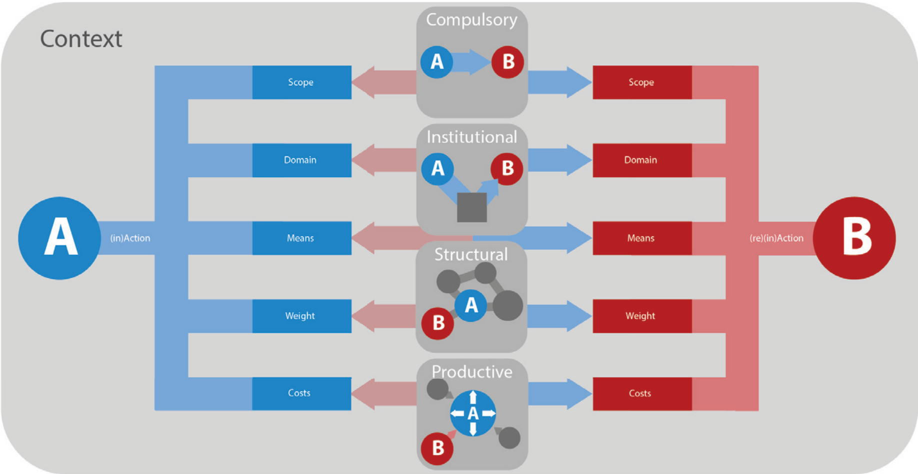

Figure 3 Power concepts integrated in the relational power framework

2.4 Scope of power

One of the accepted dimensions of power is 'scope', which entails the objectives or ends sought after (see sub-section 2.2.2). For delineating utility, the scope is essential – as utility was defined as comprising 'some purpose or worth to some end' (see Chapter One). This section will seek to derive the scope of power in international relations, in other words, the ends of State uses of power. This section will do so by answering the following sub-question: *To what end is power used?*

In inter-state affairs there are various ends or objectives sought after at a strategic level. Unfortunately, there is no generalised overview of these objectives. As an illustration of potential objectives, this section will use the seven strategic functions described by the Dutch government in the context of security, namely: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation. These functions were designed to "clarify how the government provides for the security of the country and [consequently] what the role of the Armed Forces is in that broader context."[120] Thus, although being used to distinguish the role of the Armed Forces, the strategic functions are broader

[120] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions* (The Hague: Ministry of Defence, 2010). p. 14.

and encompass other departments within States as well. They are, however, primarily concerned with 'security' as State interest and less with other interests such as promoting prosperity[121] and other values. In other words, for the subject at hand, delineating the utility of the military instrument and consequently military cyber operations, the strategic functions are adequate. For other, non-security issues the strategic functions may be less suited.

The following sub-sections will discuss the seven strategic functions by conducting a theoretical literature review. The literature review will start with examining the definition of the strategic function as forwarded in the Dutch White Papers.[122] After that, French, United Kingdom and United States policy documents in the realm of strategic goals will be analysed in order to come to a generalised understanding of the strategic function from a State perspective. As there is a considerable gap between the conception of the content and viability of certain strategic functions between policymakers and academia, the State perspective will be adjoined with the academic perspective on the strategic function. This will result in a generalised overview of the strategic functions in sub-section 2.4.8 and their potential viability and/or effectiveness.

2.4.1 Anticipation

Anticipation is defined as function to prepare "for foreseen and unforeseen developments and incidents that may affect [State] interests".[123] The strategic function anticipation originates in the French White Paper of 2008, this paper and subsequent publications describe this function as *"connaître et anticiper"* (knowledge and anticipation).[124] Knowledge and anticipation is considered the basis for assessing situations and making decisions, the function "spans five major areas: intelligence, knowledge of theatres of operations, diplomacy, forward planning [including horizon scanning] and knowledge management."[125] The Netherlands conception of anticipation and areas overlaps entirely with the French function knowledge and anticipation, which in turn are similar to anticipation within the United Kingdom and United States security strategies.[126]

[121] Cabinet Office United Kingdom, *A Strong Britain in an Age of Uncertainty: The National Security Strategy* (London: The Stationary Office, 2010). p. 9.

[122] Ministry of Defence (Netherlands), Future Policy Survey: Summary and Conclusions; Netherlands Ministry of Defence, [Dutch] Eindrapport Verkenningen: Houvast Voor De Krijgsmacht Van De Toekomst (Den Haag: Ministerie van Defensie,[2010]).

[123] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[124] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security* (New York: Odile Jacob Publishing Corp., 2008). p. 62.

[125] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 62.

[126] See for instance: Netherlands Ministry of Defence, *[Dutch] Eindrapport Verkenningen: Houvast Voor De Krijgsmacht Van De Toekomst*. p. 196; Ministry of Foreign Affairs Security Policy Department, "A Secure Netherlands in a Secure World," Government of the Netherlands, government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html (accessed June 23, 2014). p. 13; Cabinet Office United Kingdom, *A Strong*

Anticipation is also firmly rooted in international relations, primarily in literature concerning anticipation of change, a mechanism for handling uncertainty and in the context of foresight.[127] There are, however, limits to foresight and/or anticipation, after an extensive evaluation of "the performance of 284 expert political forecasters in the assessments of more than 80,000 predictions over a 20 year period",[128] the evaluation concluded: "humanity barely bests the chimp" in forecasting political issues.[129] In other words, humans are not performing well in foreseeing events; as such technical political forecasting arose. Instead of human forecasting, algorithms are better suited to forecast situations since the algorithms prove to be equally or more accurate than human forecasting.[130] As the aforementioned evaluation noted: "it is impossible to find any domain in which humans clearly outperformed crude extrapolation algorithms, less still sophisticated statistical ones".[131] At present, however, "there is very little likelihood that human punditry, particularly the opinionated self-assurance so valued in the popular media, will be completely replaced by the unblinking assessments of computer programs".[132] In other words, for the time being, human forecasting will drive forecasting and anticipation, as such it will be flawed.

2.4.2 Prevention

Prevention is characterised as taking "active steps intended to prevent a threat occurring to the interests of the [State]".[133] The rationale for doing so is that "one of the best ways to guarantee security in the face of risks of conflict or crisis is to prevent the occurrence, by acting on their causes in a timely fashion".[134] The French security strategy emphasises three pillars, prevention before (acting on origins and resolve disputes peacefully), during (limit

Britain in an Age of Uncertainty: The National Security Strategy. p. 34; Barack Obama, *National Security Strategy of the United States* (Darby: Diane Publishing Co., 2010). p. 11.

[127] Charles A. McClelland, "The Anticipation of International Crises: Prospects for Theory and Research," *International Studies Quarterly* 21, no. 1 (1977), 15-38; Colin S. Gray, *War, Peace and International Relations: An Introduction to Strategic History* (Oxford: Routledge, 2007). pp. 25; Gerald Schneider, Nils Petter Gleditch and Sabine Carey, "Forecasting in International Relations," *Conflict Management and Peace Science* 28 (2011), 5-14.

[128] Philip A. Schrodt, James Yonamine and Benjamin E. Bagozzi, "Data-Based Computational Approaches to Forecasting Political Violence," in *Handbook of Computational Approaches to Counterterrorism* (New York: Springer, 2013), 129-162. p. 131.

[129] Philip E. Tetlock, *Expert Political Judgment: How Good is it? how can we Know?* (Princeton: Princeton University Press, 2005). p. 51.

[130] Schrodt, Yonamine and Bagozzi, "Data-Based Computational Approaches to Forecasting Political Violence," in , 129-162. pp. 130-131.

[131] Tetlock, Expert Political Judgment: How Good is it? how can we Know?. p. 54.

[132] Schrodt, Yonamine and Bagozzi, "Data-Based Computational Approaches to Forecasting Political Violence," in , 129-162. p. 155.

[133] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[134] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 62.

effects of conflict) and at the end of conflict (supporting stabilisation or reconciliation).[135] The United Kingdom strategy stresses integrating "diplomatic, intelligence, defence and other capabilities" in order to prevent crisis in any of its stages.[136] The United States strategy places emphasis on prevention in the context of inter-State (e.g. conflicts between States) and intra-State (e.g. terrorism) affairs. [137] In sum, prevention is firmly rooted in the security strategies of selected States. In academia it is less settled and much more debated.

Prevention as a strategic function relates to the academic debate of the feasibility and viability of conflict prevention, primarily within international relations. Emerging in the 1990s,[138] the debate regarding conflict prevention is out of its infancy, although "scholars and policymakers still struggle with conceptual and policy issues, preventing conflict has become broadly accepted among regional and international actors, even if only on a rhetorical level."[139] Questions within the conflict prevention debate revolve around issues such as: "should conflict prevention be limited only to the early and non-escalatory stages of conflict, or also encompass the escalation and post-conflict stages of conflict" (so-called operational versus structural or deep prevention); the feasibility of conflict analysis and early warning; and enhancing the effectiveness of conflict prevention ("how to design preventative action plans and strategies that accomplish the stated objectives and desired preventive outcome").[140] Thus there are considerable overlaps in the prevention function in security strategies and the academic debate of conflict prevention. Issues nowadays do not revolve around whether there is such a thing as conflict prevention, instead the focus is how to best achieve it – if at all.[141]

2.4.3 Deterrence

Deterrence is defined as "discouraging activities that conflict with the interests of the [State] or the international rule of law by holding out the prospect of retaliatory measures."[142] Deterrence is derived from the French security strategy, where emphasis is places upon nuclear deterrence.[143] In the United Kingdom deterrence is listed as a relevant

[135] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 62.

[136] Cabinet Office United Kingdom, A Strong Britain in an Age of Uncertainty: The National Security Strategy. p. 34.

[137] Barack Obama, *National Security Strategy of the United States* (Darby: Diane Publishing Co., 2015). pp. 7-14.

[138] John Hopkins School of Advanced International Studies, "Conflict Prevention," John Hopkins School of Advanced International Studies, sais-jhu.edu/content/conflict-prevention (accessed May 4, 2017).

[139] Alice Ackermann, "The Idea and Practice of Conflict Prevention," *Journal of Peace Research* 40, no. 3 (2003), 339-347. p. 341.

[140] Ibid. pp. 341-344.

[141] See for instance: David Carment and Albrecht Schnabel, eds., *Conflict Prevention: Path to Peace Or Grand Illusion?* (New York: United Nations University Press, 2003).

[142] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[143] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. pp. 64-65.

activity in various non-nuclear contexts and only "ultimately" in a nuclear context.[144] This is very similar to the U.S. security strategy where deterrence is referred to in various non-nuclear and nuclear contexts.[145] In other words, in national security strategies deterrence is settled as an activity/function to be pursued by States, contrary to academia where the utility of nuclear and non-nuclear deterrence is highly debated.

Deterrence is not new, holding out the prospect of adverse consequences is an established way of advancing State interests throughout history.[146] With the advent of nuclear weapons deterrence rested "on the threat of pain and extinction, not just on the threat of military defeat."[147] Whether or not deterrence via nuclear weapons was effective during the Cold War is contested in academia: On one side deterrence theory is "being premised on a litany of unwarranted assumptions, improvable assertions and logical contradictions"[148] on the other side "nuclear deterrence might in practice nevertheless have prevented the war nobody wanted".[149] The end of the Cold War and the 9/11 terrorist attacks resulted in deterrence as a strategic approach "falling out of favor".[150] Nuclear weapons and deterrence "went hand in hand and were reliable partners" during the Cold War, however, "the end of the Cold War decoupled the two."[151] Lacking a "post-Cold War school of thought" in the field of deterrence theory, "deterrence is receiving woefully inadequate consideration as a potential approach to the defence of [State] interests".[152] Whilst nuclear deterrence will remain a pillar of many security strategies, see for instance the British, French and U.S. security strategies, the debate has moved to non-nuclear deterrence, requiring "thinking in terms of weapons of 'mass effect' rather than weapons of mass destruction".[153]

[144] Cabinet Office United Kingdom, A Strong Britain in an Age of Uncertainty: The National Security Strategy. pp. 22 and 30.

[145] Obama, National Security Strategy of the United States. pp. 10-13; Obama, National Security Strategy of the United States. p. 48.

[146] Thomas C. Schelling, *Arms and Influence: With a New Preface and Afterword* (Yale: New Haven and London Yale University Press, 2008). pp. 1-34.

[147] Thomas C. Schelling, Arms and Influence: With a New Preface and Afterword. p. 23.

[148] Lee Butler, "At the End of the Journey: The Risks of Cold War Thinking in a New Era," *International Affairs (Royal Institute of International Affairs 1944-)* 82, no. 4 (2006), 763-769. p. 766.

[149] Frank Sauer, *Atomic Anxiety: Deterrence, Taboo and the Non-use of U.S. Nuclear Weapons* (New York: Palgrave Macmillan, 2015). pp. 15. Referring to:; George H. Quester, "Crises and the Unexpected," *The Journal of Interdisciplinary History* 18, no. 4 (1988), 701-719;
See also: Stephen Peter Rosen, "After Proliferation: What to do if More States Go Nuclear," Foreign Affairs 85, no. 5 (2006), 9.; Francis J. Gavin, "Same as it Ever was: Nuclear Alarmism, Proliferation, and the Cold War," International Security 34, no. 3 (2009), 7-37.; Robert S. Mcnamara, "Apocalypse Soon," Foreign Policy, no. 148 (2005), 29-35.; Wade L. Huntley, "Rebels without a Cause: North Korea, Iran and the NPT," International Affairs 82, no. 4 (2006), 723-742.

[150] Adam B. Lowther, Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century (New York: Palgrave MacMillan, 2012). p. 2.

[151] Ibid. pp. 4-5.

[152] Ibid. p. 3.

[153] Ibid. pp. 4-5.

Instead of focusing primarily on nuclear weapons, the deterrence focus is broadening to other means. Various authors seek to reappraise the conceptual components of the 20th century deterrence debate (e.g. assured destruction/retaliation, countervalue versus counterforce, strategic stability, crisis stability, competitive strategy and extended deterrence) in the light of 'new' means and methods.[154] One development is receiving considerable attention in the context of deterrence, namely: cyber means and methods (which will be discussed in chapter three).[155] The debate on new means and methods to deter is far from settled, however, the basic premise is clear: "deterring current and future adversaries will require an expanded set of tools that rely more on the diplomatic, informational and economic elements of national power."[156] Thus deterrence is firmly rooted in governmental publications and in academia, however, the latter is currently reconsidering the value of deterrence in the 21st century.

2.4.4 Protection

In the Dutch context, protection is defined as "protecting and, if necessary, defending the territory and residents of the [State]".[157] The French national security lists the two types of risk the function should address: intentional aggression "such as acts of terrorism, major cyber attacks"; and unintentional risks "such as highly lethal health crises, natural disasters [and] technological disasters".[158] In order to do so, protection should encompass "training of personnel, preparation of businesses and public communication, with a view to enhancing the global resilience of French society".[159] The United Kingdom security strategy, similar to the French strategy, lists protection and resilience in the face of natural and man-made emergencies.[160] The United States security strategy remarks that it has "no greater responsibility than protecting the American people"; [161] protection similarly envelops different fields, from countering terrorism and armed violence to ecological and economical risks.[162] All publications list a variety of intentional/unintentional and internal/

[154] Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar.(Navigating Deterrence: Law, Strategy, and Security in the Twenty-First Century)," *New York University Journal of International Law and Politics* 47, no. 2 (2015), 327-355. pp. 344-345.

[155] See for instance: Ben Buchanan, "Cyber Deterrence Isn'T MAD; it's Mosaic," *Georgetown Journal of International Affairs* (2014), 130-140; Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security* 7, no. 1 (2014), 54-67; Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND Corporation, 2009); Uri Tor, "'Cumulative Deterrence' as a New Paradigm for Cyber Deterrence," *Journal of Strategic Studies* (2015), 1-26.

[156] Lowther, Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century. p. 8.

[157] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[158] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 66.

[159] Ibid. p. 66.

[160] Cabinet Office United Kingdom, A Strong Britain in an Age of Uncertainty: The National Security Strategy. p. 22.

[161] Obama, National Security Strategy of the United States. p. 7.

[162] Ibid. pp. 7-13.

external threats, the goal is to protect against these threats and/or create resilience to stave of its adverse consequences.

It is difficult to couple an academic debate to the strategic function protection, as the latter is very broad and could relate to various debates. The question needing an answer is protection from what? In the context of terrorism this could relate to the debate regarding countering terrorism. When concerning ecological disasters, it could relate to environmental protection or disaster response. In the case of intra-State armed violence protection could relate to the consequences of armed conflict to the law of armed conflict. In a more general sense, however, protection could be considered to relate to the broader concept of "national security", as protection is aimed at preventing loss or degradation of security.

Security, similar to protection, "may be defined not merely as a goal but as a consequence – this means that we may not realise what it is or how important it is until we are threatened with losing it."[163] In other words, "security is defined and valorised by the threats which challenge it".[164] Security involves "in an objective sense, [...] the absence of threats to acquired values, in an subjective sense, the absence of fear that such values will be attacked."[165] In a more general sense, as absence of threats is quite difficult in the case of earthquakes or other environmental threats, national security is characterised as "a low probability of damage to acquired values."[166] For national security to be useful, "one could specify security with respect to the actor whose values are to be secured, the values concerned, the degree of security, the kinds of threats, the means for coping with such threats, the costs of doing so, and the relevant time period."[167] In the contemporary context, the values that security covers for example are "human rights, economics, the environment, drug traffic, epidemics, crime, or social injustice, in addition to the traditional concern with security from external military threats."[168] In other words, the concept of security has been reconceptualised to include a broad range of issues in addition to the 'traditional' national security.[169]

[163] Richard H. (Richard Henry) Ullman, "Redefining Security," *International Security* 8, no. 1 (1983), 129-153. p. 133.

[164] Ibid. p. 133.

[165] Arnold Wolfers, "" National Security" as an Ambiguous Symbol," *Political Science Quarterly : PSQ ; the Journal Public and International Affairs* 67, no. 4 (1952), 481-502. p. 485.

[166] David A. Baldwin, "The Concept of Security," *Review of International Studies; Rev.Int.Stud.* 23, no. 1 (1997), 5-26. p. 13.

[167] Ibid. p. 17.

[168] Ibid. p. 5.

[169] See: Barry Buzan and Lene Hansen, The Evolution of International Security Studies (Cambridge: Cambridge University Press, 2009). p. 189; Ralph Pettman, "Human Security as Global Security: Reconceptualising Strategic Studies," Cambridge Review of International Affairs 18, no. 1 (2005), 137-150.

In sum, protection has a function in various governmental policies; however, it is on a different level of abstraction than other strategic functions. All strategic functions serve protection to some extent and protection serves all strategic functions since it creates the freedom of action required to conduct the activities. Hence protection is a requirement for and a product of other functions. Indicative of protection being on a different abstraction level is that the States' description of protection as a notion of State interest is not found within a distinct academic debate. It relates most to the general debate on 'national security' or 'security' within academia, this debate does give a theoretical basis for the scope of protection and the dimensions that could be considered (e.g. values protected, degree of security, threats, etc.). The focus of protection is primarily territorial, notwithstanding that it depends on both national and international factors.[170]

2.4.5 Intervention

Intervention in defined as "enforcing a change in the behaviour of one or more parties that threaten the interests of the [State]".[171] The French national security strategy stresses intervention as "an essential mode of action for our armed forces, especially outside the national territory".[172] The primary of which "is to put an end to overt hostilities, reduce the level of tension, provide a sufficiently safe environment for local and international actors to operate without threat or hindrance."[173] The United Kingdom strategy mentions intervention less explicitly, however, it does note the option of military intervention, humanitarian intervention and intervention overseas.[174] The same goes for the United States strategy, it does list various activities outside its border, amongst other use of the military, but it does not explicitly mention intervention as the Dutch and French strategies. The activities do, however, implicitly resemble each other. As such there is no doubt that all documents acknowledge the use of 'intervention' as function to promote or secure State interests.

In academia 'intervention' as an activity by States is much debated, primarily within international relations and its sub-field of security studies in the second part of the 20th century. This is in stark contrast to politics and/or policy where it is assumed that contemporary interventions are 'obviously' effective.[175] Throughout history intervention has served different purposes, "the [political purpose of intervention] that decision makers

[170] See for instance: Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 61.

[171] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[172] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 67.

[173] Ibid. p. 207.

[174] Cabinet Office United Kingdom, A Strong Britain in an Age of Uncertainty: The National Security Strategy. pp. 30-33.

[175] Martha Finnemore, *The Purpose of Intervention: Changing Beliefs about the use of Force* (London: Cornell University Press, 2004). p. 4.

view as desirable in one period may not be valued by decision makers at another period."[176] For instance "interventions in failed, strategically unimportant states, which policy makers felt obliged to make at the close of the twentieth century, would have been condemned as sovereignty violations in the 1960s or wasteful folly in earlier periods."[177] Thus there is no 'obvious' use of interventions as this is highly contextual and its use or function changes throughout time.

Some of the key factors impacting the success of intervention are the feasibility, legality and perceived legitimacy by States and domestic publics. The feasibility of intervention is "always about judging the required means to achieve a particular end" and how, how long and by whom intervention "will be implemented".[178] Legality is typically understood as being "[specified by article 2 and 51 of the UN Charter] which firmly defend the sovereign equality for all member states, while sanctioning war only in the case [of] self-defense and threats to international peace and security".[179] The third factor, legitimacy, "connotes whether an intervention is regarded as acceptable and/or 'right' – be it morally, or otherwise justified".[180] In some cases "legal authorisation may create legitimacy", however, "the two are not synonymous".[181] There are also two perspectives to legitimacy, the first is an empirical perspective and the second a normative one. The empirical or descriptive perspective is "concerned with the attitudes and beliefs of citizens towards their government" (or in this case vis-à-vis the intervening actor).[182] The other normative or prescriptive is "concerned with the actual moral properties of a political order", [183] that is, "whether or not a particular political action can be considered legitimate according to some moral or ethical standard."[184] Obtaining a degree of legitimacy is difficult as intervention is often seen "as progressive principle that prevents dictators from freely abusing their own populations or as a repressive tool used by big powers to impose their rule on other nations."[185]

In other words, in the academic debate on intervention, contrary to security policies, it is not obvious that it is effective, intervention is highly contested and contextual as evidences by States understanding "different goals to be important and different actions to be effective or legitimate at different times."[186] Thus, in the security strategies intervention is an

[176] Ibid. p. 140

[177] Martha Finnemore, The Purpose of Intervention: Changing Beliefs about the use of Force. p. 140.

[178] David Held and Kyle McNally, eds., *Lessons from Intervention in the 21st Century: Legality, Feasibility and Legitimacy* (Chichester: Global Policy Journal, 2015). p. 6.

[179] Ibid. p. 6.

[180] Ibid. p. 82.

[181] Ibid. p. 82.

[182] Cord Schmelze, "Evaluating Governance: Effectiveness and Legitimacy in Areas of Limited Statehood," *SFB-Governance Working Paper Series* 26 (2011). p. 7.

[183] Ibid. p. 7.

[184] Held and McNally, eds., Lessons from Intervention in the 21st Century: Legality, Feasibility and Legitimacy. p. 75.

[185] Pascal Boniface, "What Justifies Regime Change?" *The Washington Quarterly* 26, no. 3 (2003), 59-71. p. 63.

[186] Finnemore, The Purpose of Intervention: Changing Belifes about the use of Force. p. 95.

instrument to induce a change in behaviour, most likely outside a State's territory, involving the armed forces and/or other capacities. The use of intervention and effectiveness is not discussed, at least, not in the selected governmental publications. Academics look at intervention differently; the use and effectiveness of intervention is seen as contextual and subject to many dynamics.

2.4.6 Stabilisation

The Dutch strategic function of stabilisation encompasses activities aimed at "establishing security in a current or former conflict zone to achieve political stability and economic and social development."[187] In the French white paper on national security stabilisation is incorporated in the third pillar of the strategic function prevention, specifying the need for 'economic, diplomatic means and co-operation' in stabilisation and reconciliation and under the function intervention where stabilisation operations are highlighted.[188] The British national security strategy similarly notes the use of diplomatic action and adds strategic intelligence in preventative and stabilisation activities.[189] The United States security strategy does not specifically refer to stabilisation as an activity, however, the term is used copiously throughout the document as a goal to achieve, for instance in the context of national defense, combatting terrorism, weapons of mass destruction and economy.[190] Thus the Dutch strategic function stabilisation is not considered a separate function in the French, British and United States publications, however, it receives due attention.

The concept of stabilisation is contested in academia,[191] it is was "once criticised as a passing fad in the wake of US-led military interventions in Afghanistan and Iraq", however, it showed "remarkable staying power" and now the question is asked whether stabilisation is "still relevant in a world revolutionised by new information technologies, cyber-security threats, transnational extremist groups, spreading criminal violence and climate change?"[192] In other words, as the future of stabilisation is anticipated it is safe to assume that it will remain a concept here to stay for the time being. There are, however, certain issues with the concept. The basic concept of stabilisation utilised by States operates on the assumption that (1) the problem is fragility, (2) stability is the solution and (3) stabilisation

[187] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[188] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 62.

[189] Cabinet Office United Kingdom, A Strong Britain in an Age of Uncertainty: The National Security Strategy. p. 30.

[190] Obama, National Security Strategy of the United States. p. 7, 9, 11 and 15.

[191] See for instance: Roger Mac Ginty, "Against Stabilisation," *Stability: International Journal of Security & Development* 1, no. 1 (2012); Christian Dennys, "For Stabilisation," *Stability: International Journal of Security & Development* 2, no. 1 (2013).

[192] S. A. Zyck and M., "Preparing Stabilisation for 21st Century Security Challenges," *Stability: International Journal of Security & Development* 4, no. 1 (2015). p. 2.

"the path to be taken".[193] This notion is "widely seen as problematic by [...] academics and practitioners".[194]

One of the issues is the goal of stabilisation, since whether or not stabilisation is effective depends on the definition of the goal, in this case: stability. There are two generalised views as to the objective of stabilisation resulting in stability: in the broad vision "stabilisation is expected to build lasting peace, security, stability and prosperity"; in the narrower, more modern vision stabilisation "is no more than the absence of acute crises", it is "the exceptional toolkit to defuse acute crises in which resilience breaks down".[195] The broad notion of stabilisation is seen as virtually impossible to achieve and the narrow notion as less unlikely to achieve.[196] Although whether stability is achievable at all is also contested, considering that stabilisation is conducted in post-conflict zones, stability "in such diverse, frenetic, contested contexts is a non-definable, unachievable, immeasurable, and elastic concept that possesses no inherent value."[197]

A second illustrative issue is the stabilizing States' overambitious goals coupled with overestimation of knowledge and power over the internal workings of the 'fragile' destabilised State, whilst in most situations the "local elites – whose extensive 'ownership' often sparked the crisis in the first place – [...] regional and global economic relationships hold the largest sway over the course of events".[198] Apart from that there are myriads of other issues with stabilisation that are too detailed to discuss in depth here.[199] A general conclusion that can be drawn from these issues is that States should accept that "international attempts at stabilisation can only influence at the margins".[200]

In conclusion, States have acknowledged stabilisation as a goal sought after (US, UK and France) and/or a distinct activity (Netherlands). In academia, stabilisation is highly contested, both the basic premise of intervening in another State expecting to improve the situation and the mechanisms used in doing so. It is beyond doubt, however, that stabilisation is an activity States seek after on the international stage.

[193] Philipp Rotmann and Léa Steinacker, Stabilisation: Doctrine, Organisation and Practice Lessons from Canada, the Netherlands, the United Kingdom and the United States (The Hague: Global Public Policy Institute,[2013]). p. 36.

[194] Ibid. p. 37.

[195] Philipp Rotmann, "Toward a Realistic and Responsible Idea of Stabilisation," *Stability: International Journal of Security & Development* 5, no. 1 (2016). pp. 5-6.

[196] Ibid. p. 6.

[197] Mark Knight, "Reversing the Stabilisation Paradigm: Towards an Alternative Approach," *Stability: International Journal of Security & Development* 5, no. 1 (2016). p. 2.

[198] Rotmann, "Toward a Realistic and Responsible Idea of Stabilisation." p. 6.

[199] See for an overview: Roland Paris and Timothy D. Sisk, eds., The Dilemmas of Statebuilding: Confronting the Contradiction of Postwar Peace Operations (New York: Routledge, 2009). pp. 1-18; Roland Paris, At War's End: Building Peace After Civil Conflict (Cambridge: Cambridge University Press, 2004). pp. 40-51.

[200] Ibid. p. 6.

2.4.7 Normalisation

The normalisation function is defined as "restoring normal living conditions after a conflict or disaster"[201] and is characterised as a primarily civilian endeavour, although in some cases the armed forces may provide support.[202] It includes international humanitarian help, rebuilding former conflict zones and/or capacity building in post-conflict zones. The French national security strategy does not use the term normalisation nor does it adopt it as a strategic function. The elements included under normalisation, however, do appear in the French strategy. After stabilisation, via armed forces, the strategy earmarks a "predominantly civilian operation involving reconstruction, re-establishing public institutions and restoring basic economic capacities."[203] The United Kingdom and United States strategies do not mention normalisation or reconstruction. Thus normalisation is only found explicitly in the Netherlands as a strategic function.

In academia normalisation is not found as a separate function, instead, it belongs to a broader framework of post-conflict reconstruction.[204] The path to post-conflict reconstruction has three stages, initial response, transformation and fostering sustainability.[205] The ultimate goal being normalisation, which is achieved when: "1) extraordinary outside intervention is no longer needed; 2) the processes of governance and economic activity largely function on a self-determined and self-sustaining basis; and 3) internal an external relations are conducted according to generally accepted norm of behaviour."[206] Post-conflict reconstruction is conducted in failed States with an exogenous entity intervening to reconstruct the failed State, the intervening entity's goal being to "transform a failed state into a normal state, according to the western liberal understanding of the term."[207] Thus understood, normalisation within the framework of post-conflict reconstruction relates to achieving the end-state of a normal State. In other words, as with stabilisation, the problem is the 'abnormality' of failed or fragile States according to the Western perspective, normality is the goal sought after and normalisation is the path to be taken.

[201] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[202] Netherlands Ministry of Defence, [Dutch] Eindrapport Verkenningen: Houvast Voor De Krijgsmacht Van De Toekomst. pp. 199-200.

[203] Commission du Livre Blanc sur la Défense et la Sécurité Nationale, *The French White Paper on Defence and National Security*. p. 203.

[204] Association of the U. S. Army (AUSA) and Center for Strategic and International Studies (CSIS), *Post-Conflict Reconstruction: Task Framework* (Washington, D.C.: CSIS,[2002]).

[205] Ibid. p. 4.

[206] Ibid. p. 2.

[207] Yosef Jabareen, "Conceptualizing " Post- Conflict Reconstruction" and " Ongoing Conflict Reconstruction" of Failed States," *International Journal of Politics, Culture, and Society* 26, no. 2 (2013), 107-125. p. 122.

Similar to stabilisation, normalisation is complex and myriads of difficulties arise. One of the most critical issues is that "postwar reconstruction is an essentially neo-liberal enterprise and an openly political project, and raises complex questions about state sovereignty and legitimacy, self-determination, democracy (local and national), and social, economic and political justice" and whilst the language of reconstruction is full of democratic values, "affected countries appear to not have the right to break with macroeconomic orthodoxy, challenge imbalances in global power and resource distribution, and chart their own paths towards rebuilding their societies and economies."[208] In other words, the agenda for normalizing States is criticised in academia as seeking to transform "war-shattered states into 'liberal market democracies' as quickly as possible".[209]

Apart from this issue with the general idea normalisation there are many issues in implementing social and economic changes in order to normalize a fragile or failed State. The relief and reconstruction complex for instance, composed of external private corporations and non-governmental organisations, it supplants local authorities and "as a result, most foreign aid [does] not reach the local population [in places such as Afghanistan, Bosnia, Cambodia, East Timor and Iraq]".[210] Apart from that, these large, international reconstruction missions generate "distortions to the local economies and [contributes] to the appearance of [the] Dutch disease".[211] Similar to issues with normalisation, "the critical role of local populations in post conflict reconstruction is often overshadowed by the arrival of major international actors" whilst "reconstruction is largely determined by the commitment and capacities of local populations".[212]

Thus the feasibility and efficacy of normalisation is much debated in academia. Normalisation is characterised as an outside intervention aiming to transform a failed or fragile State into a normal State in the perspective of the entity wishing to normalize the failed or fragile State. These attempts have rarely resulted in a sustainable peace or a liberal market democracy and hence it is clear that the feasibility of normalisation as strategic function is highly contested.[213]

2.4.8 Sub-conclusion

This section has sought to answer the following sub-question: To what end is power used? In order to answer the question a theoretical literature review was conducted covering

[208] Shalmali Guttal, "The Politics of Post- War/ Post- Conflict Reconstruction," *Development* 48, no. 3 (2005), 73. p. 80.

[209] Roland Paris, *At War's End* (Cambridge: Cambridge University Press, 2004). p. 5.

[210] Nikolaos Tzifakis, "Post-Conflict Economic Reconstruction," Princeton, pesd.princeton.edu/?q=node/260 (accessed May 21, 2017).

[211] Nikolaos Tzifakis, "Post-Conflict Economic Reconstruction".

[212] Sanam Naraghi Anderlini and Judy El-Bushra, "Post-Conflict Reconstruction," *Inclusive Security, Sustainable Peace: A Toolkit for Advocacy and Action* (2004), 51-68. p. 51.

[213] Paris, *At War's End*. pp. 55-148.

the scope of power in international relations. As an example of the 'ends' this section has used the Dutch strategic functions: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation. In order to come to a generalised understanding of these functions, selected U.S., U.K. and French policy documents were analysed. This analysis has shown that the seven Dutch strategic functions are not universally applicable, however, they do resonate within the selected policy documents. In the French documents five of the seven functions are found, which is logical as the Dutch functions are based on the French. In the U.S. and U.K. documents the functions are not found nor explicitly recognised as strategic function, the terms are used, however, throughout the texts. Thus the strategic functions do not enjoy broad application besides France and the Netherlands, on the other hand they can be seen as illustrative for the scope of power as they are terms that States use to describe the goals they seek to achieve.

After assessing the usage of strategic functions in selected policy documents, the sub-sections have reflected on the status of the strategic functions in academia. Most strategic functions relate to an academic debate, protection is the only function that has no clear equivalent in academia. As was noted, protection seems to be on a higher conceptual level than the other functions, all functions serve protection or security (see sub-section 2.4.4). All seven strategic functions are accepted concepts (or issue areas) in academia, many in the field of international relations or its sub-fields such as conflict, security or peace studies (see Table 1). The functions anticipation, prevention, deterrence, protection and intervention are established and debate focuses on engaging in these activities most effectively. The functions stabilisation and normalisation are highly contested in academia and are considered overambitious, unsuccessful and ineffective in attaining their desired purpose.

In other words, in academia, five of the seven strategic functions can be seen as feasible and the others as unachievable in their current context. This notion has a great impact upon utility of cyber capabilities and capabilities in general. If the goal of normalisation and stabilisation as used by States is simply unachievable, the utility of any capability to achieving that goal is greatly reduced. If the goal is deemed more achievable, as is the case in anticipation, prevention, deterrence, protection and intervention, then the capabilities may be more easily proven useful in attaining the goal. As such the scope of an action greatly influences the potential utility of a specific capacity.

Strategic function	France	US	UK	Academic debate	Academic status
Anticipation	Explicit	Implicit (not a strategic function)	Implicit (not a strategic function)	Forecasting in IR	Concept is accepted Human forecasting flawed Computational forecasting more effective
Prevention	Explicit	Implicit	Implicit	Conflict prevention	Concept is accepted Most effective application contested
Deterrence (non-nuclear)	Explicit (nuclear)	Implicit (nuclear and non-nuclear)	Implicit (nuclear and non-nuclear)	Deterrence in IR	Nuclear deterrence as concept accepted Non-nuclear deterrence concept is evaluated
Protection	Explicit (intentional and unintentional)	Implicit (intentional and unintentional)	Implicit (natural and man-made)	National security	Concept is accepted Security is contextual and depends on value protected
Intervention	Explicit	Implicit	Implicit	Intervention in IR	Concept is accepted Effectiveness depending of perceived legitimacy
Stabilisation	Subsumed under prevention	Implicit	Implicit	Stabilisation in IR	Concept is accepted Effectiveness highly contested
Normalisation	Subsumed under prevention	Implicit	Implicit	Post-conflict reconstruction	Concept is accepted Effectiveness highly contested

Table 1 Overview of Dutch strategic functions, their status in French, American and British policy documents, corresponding academic debate and academic status

2.5 Power instruments

This section will discuss the ‘means’ dimension of power as part of the relational power framework (see Figure 2). Although not included in the list of ‘most accepted dimensions of power’ (see sub-section 2.2.2.2), the means dimension is still the focal point of many seeking to assess power, for instance in the power as resource approach, and as such it would be illogical not to include this dimension. As does the scope of an action, the means used to influence impacts the potential successfulness of the (in)action. Therefore, this section will seek to create a generalised overview of the means used to influence actors by answering the following sub-question: Through which means is power manifested?

The means used in international relations relate to the instruments of power (also known as ‘State instruments of power’ or ‘instruments of Statecraft’) and although thinking in terms of ‘instruments’ may sound as relatively concrete – as opposed to the conceptual approaches to power and power mechanisms – “the notion of instruments of national power is an abstraction".[214] The concept of 'instruments' is less subject to debate than approaches to power or power mechanisms. Although they are not subject to debate, the "terminology in this domain is not widely agreed upon".[215] This section will discuss the instruments of power in academia and in the realm of military policy- and decision-making by analysing the gaps and overlaps between Carr's, Mann's, DIME and DIMEFIL categorisations of power instruments.

Carr's 1946 "The Twenty-Years' Crisis" serves as the starting point for most writings on instruments of State power. Carr divided political power, "for the purpose of discussion",[216] into three categories: "(a) military power, (b) economic power [and] (c) power over opinion".[217] A more modern, historical sociological, account of sources of power comes from Michael Mann.[218] Michael Mann's IEMP-model is derived from his *magnum opus* "The Sources of Social Power" (1986),[219] in which he attempts to develop a "grand theory on human societies in general from a firm empirical base".[220] The acronym stands for ideological, economical, military and political sources, which are deemed sources of (social) power. The DIME-acronym, short for the diplomatic, informational, military and economical instruments, gained momentum during the Cold War,[221] it draws heavily on the 'power as resource' approach (see 2.2.1) and primarily serves policy makers in structuring interagency cooperation within the government. DIMEFIL proponents in the 'Post 9/11' decade suggested that the financial, intelligence and law enforcement instrument should be added to the DIME acronym in order to be comprehensive.[222] Carr's and Mann's instruments "support strategic thought at the highest levels" whereas DIME and MIDLIFE are better suited "as a guide to organizing government and allocating resources".[223] Instead of describing the various approaches in depth, this section aims to analyse the gaps and overlaps and present a harmonised overview.

[214] Robert D. Worley, Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System (Raleigh: Lulu Press, 2012). p. 181.

[215] Ibid.

[216] Edward H. Carr, The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations, 2nd ed. (London: MacMillan & Co. Ltd., 1946). p. 108.

[217] Ibid.

[218] Michael Mann, "Authoritarian and Liberal Militarism: A Contribution from Comparitative and Historical Sociology," in *International Theory: Positivism and Beyond*, eds. Steve Smith, Ken Booth and Marysia Zalewski (Cambridge: Cambridge University Press, 1996), 221-239. p. 221.

[219] Michael Mann, The Sources of Social Power: A History of Power from the Beginning to A.D. 1760, Vol. I (Cambridge: Cambridge University Press, 1986); Michael Mann, The Sources of Social Power: The Rise of Classes and Nation-States 1760-1914, Vol. II (Cambridge: Cambridge University Press, 1993); Michael Mann, The Sources of Social Power: Global Empires and Revolution 1890-1945, Vol. III (Cambridge: Cambridge University Press, 2012); Michael Mann, The Sources of Social Power: Globalizations 1945-2011, Vol. IV (Cambridge: Cambridge University Press, 2013a).

[220] Michael Mann, "The Sources of My Sources," *Contemporary Sociology: A Journal of Reviews* 42, no. 4 (2013b), 499-502. p. 499.

[221] Worley, Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System. p. 182.

[222] Ibid. p. 181; See also: Security Council of the Russian Federation, "The Military Doctrine of the Russian Federation," scrf.gov.ru/documents/33.html (accessed June 23, 2014). p. 1; CDU/CSU Parliamentary Group, "A Security Strategy for Germany Presented at the CDU/CSU Security Conference". p. 11.

[223] Ibid. p. 191.

2.5.1 Gaps and overlaps

2.5.1.1 *Diplomatic/political instrument*

Every categorisation recognises the value of the diplomatic or political instrument, Carr, however, deems political power to overarch other instruments and does not specifically distinguish it.[224] Since the more modern approaches (IEMP, DIME and DIMEFIL) generally agree on the existence of this instrument, the diplomatic or political instrument can be deemed a separate instrument.[225]

The question then arises with regard to semantics, is it the political instrument as forwarded by Carr and Mann or the diplomatic instrumented forwarded in DIME(FIL) doctrine? Semantically speaking, the proponents of DIME(FIL) err in naming the instrument. The adjective 'diplomatic' refers to the "the work of maintaining good relations between the governments of different countries [or] not causing bad feelings".[226] Whereas 'political' entails the more general notion "of or relating to politics or government"[227] in which politics comprises the "activities that relate to influencing the actions and policies of a government or getting and keeping power in a government".[228] Diplomacy is an integral part of politics, but the latter comprises more than only diplomacy as the DIME(FIL) categorisation expresses.[229] Diplomacy, according to advocates of DIME(FIL), is not only about keeping good relations; it is generally about forwarding values, interests, objectives; not necessarily to keep relations 'good'. Hence, taking into account what DIME(FIL) tries to capture in the scope of the diplomatic instrument, the *political* instrument would be semantically more correct.

As to the activities included under the ambit of the political instrument, the IEMP and DIME(FIL) models both recognise outward facing geopolitical diplomacy, however, DIME(FIL) does not capture Mann's 'inward facing' political power. The notion of inward facing power is, however, integral to political power whether foreign or domestically. Inward facing power is about the capacity of politics to actually penetrate society and implement decisions; these decisions can bear directly upon domestic and foreign affairs. Hence, Mann's inward facing power should be added to the scope of the political instrument.

[224] Carr, The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations. p. 102.

[225] Mann, The Sources of My Sources. p. 502; Ralph Schroeder, "An Anatomy of Power: The Social Theory of Michael Mann," in , eds. John A. Hall and Ralph Schroeder (Cambridge: Cambridge University Press, 2005), 1-16. p. 2; Ministry of Defence, Joint Doctrine Publication 0-01: British Defence Doctrine. p. 1-6; Joint Chiefs of Staff, Joint Publication 1: Doctrine for the Armed Forces of the United States. I-12.

[226] Merriam-Webster Dictionary, "Diplomatic," merriam-webster.com/dictionary/diplomatic (accessed July 22, 2014).

[227] Merriam-Webster Dictionary, "Political," merriam-webster.com/dictionary/diplomatic (accessed July 22, 2014).

[228] Merriam-Webster Dictionary, "Politics," merriam-webster.com/dictionary/diplomatic (accessed July 22, 2014).

[229] Ministry of Defence, Joint Doctrine Publication 0-01: British Defence Doctrine. p. 1-6; Joint Chiefs of Staff, Joint Publication 1: Doctrine for the Armed Forces of the United States. I-12; Dutch Ministry of Defence, Netherlands Defence Doctrine. p. 20; North Atlantic Treaty Organisation, Allied Joint Publication 1(D): Allied Joint Doctrine. p. 1-2.

2.5.1.2 *Informational instrument*

The informational instrument or ideological power is understood in different ways by the authors, however, these views are not irreconcilable as will be demonstrated. Carr describes 'power over opinion',[230] which could be considered a result of using the informational instrument within the DIME(FIL) categorisation.[231] DIME(FIL) categorises activities such as the controlled release of information and protecting own information under the informational instrument.[232] Therefore, incorporation of 'power over opinion' under the ambit of informational instrument seems most logical, this instrument generally incorporates the instrumental usage of information whereas gaining 'power over opinion' is a very specific effect of employing information. Contrary to Carr, relating Mann's ideological power to the informational instrument is more difficult, it is less instrumental than DIME(FIL) and power over opinion. Mann describes underlying factors such as meaning, norms and aesthetic and ritual practices, although important in understanding the effects of using information, they have less instrumental value.[233] In sum, the informational instrument includes activities such as gaining power over opinion (Carr); unifying meaning, norms and aesthetic and ritual practices (Mann); controlled release of information (DIME(FIL)); and protecting own information (DIME(FIL)).

2.5.1.3 *Military instrument*

The value and use of the military instrument is uncontested by Carr and Mann, as well as by DIME- and DIMEFIL-proponents. Carr specifies the military instrument as the ultimate power instrument that could be used as an extension of foreign policy.[234] Although the statement on the supremacy of the military instrument may have rung true in the interbellum and during the Cold War, nowadays it seems an out-dated statement. Most contemporary military doctrines recognise the value of other instruments and interagency cooperation as exemplified by the DIME(FIL) approach, in other words, the military contributes equally to State power as other instruments. Thus, it is still important and unique in some regards, however, it is not the only nor the ultimate instrument of power.[235]

[230] Carr, The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations. p. 234.

[231] North Atlantic Treaty Organisation, Allied Joint Publication 1(D): Allied Joint Doctrine. p. 1-3; Joint Chiefs of Staff, Joint Publication 1: Doctrine for the Armed Forces of the United States. I-12.

[232] North Atlantic Treaty Organisation, Allied Joint Publication 1(D): Allied Joint Doctrine. p. 1-3; Joint Chiefs of Staff, Joint Publication 1: Doctrine for the Armed Forces of the United States. I-12; Dutch Ministry of Defence, Netherlands Defence Doctrine. p. 22.

[233] Michael Mann, "The Sources of My Sources," *Contemporary Sociology: A Journal of Reviews* 42, no. 4 (2013b), 499-502. P. 499.

[234] Carr, The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations. p. 108.

[235] See also: Juan Emilio Cheyre, "Defence Diplomacy," in *The Oxford Handbook of Modern Diplomacy*, eds. Andrew F. Cooper, Jorge Heine and Ramesh Thakur (Oxford: Oxford University Press, 2013). p. 373; Joseph S. Nye, *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2004). p. 5; Organisation for Economic Co-operation and Development, *Policy Coherence and Whole Government Approaches in Fragile States* (Paris: OECD, 2005). p. 2; D. Kavanagh and D. Richards, "Departmentalism and Joined-Up Government," *Parliamentary Affairs* 54, no. 1 (2001), 1-18; Andrew Leslie, Peter Gizewski and Michael Rostek, "Developing a Comprehensive Approach to Canadian Forces Operations," *Canadian Military Journal* 9, no. 1 (2007). p. 14.

Mann uses a more conceptual approach and argues that the military can lead to intensive power over a limited space and extensive power over a larger space.[236] The DIME(FIL)-proponents approach mirrors Mann's, intensive power resembles hard coercive power and extensive power that of soft attractive power. Mann, however, describes it on a more theoretical and fundamental level than DIME(FIL)-proponents. Mann's and DIME(FIL)-proponents' viewpoints express certain uses of the military instrument, these viewpoints differ but are complementary, as such all following viewpoints will be considered as ways of utilising the military instrument: extending foreign policy, intensive and extensive power, and hard coercive and soft attractive power.

2.5.1.4 *Economical instrument*

The economical instrument is not contested either, it is considered to be a powerful instrument at a State's disposal. As with the informational instrument, Carr has specified the use of economical power most specifically, Mann has pinpointed over- or underlying sociological factors of a fundamental nature and DIME(FIL) proponents have made the most general statement about economical power. Carr describes two ways of utilising economical power: (1) autarky and (2) to acquire influence abroad.[237] Mann unveils the mechanism behind harnessing economical power consisting of (1) the formation of groups amongst production, distribution, exchange, and consumption of goods and (2) monopolisation of control over these groups to gain economical power.[238] DIME(FIL) proponents first generally describe the economical instrument as an enabler to improve one's economical position or to decrease that of others and secondly they sketch various possible actions.[239] As a matter of categorisation, defining the various economical courses of actions and phenomena under the umbrella of economical instrument seems most logical as it is the most general term. As with Mann's ideological sources of power, his economical sources are somewhat harder to grasp than Carr's or those of DIME(FIL) proponents. The easiest way out, again, is to see Mann's sources as targets and effects of wielding the economical instrument.

2.5.1.5 *Financial instrument*

The addition of financial, intelligence and law enforcement instruments to DIME in United States' governmental papers is relatively recent. As mentioned before, these policy papers are produced in the wake of the 'war on terror' where a 'whole of government' approach against terrorism was advocated.[240] Although they are primarily used in a contra-terrorism setting, even during regular – non-terrorism related – affairs the financial, intelligence and

[236] Mann, The Sources of Social Power: A History of Power from the Beginning to A.D. 1760. p. 26.

[237] Carr, The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations. p. 120 and pp. 123-124.

[238] Schroeder, An Anatomy of Power: The Social Theory of Michael Mann. p. 7; Mann, The Sources of Social Power: A History of Power from the Beginning to A.D. 1760. p. 24.

[239] Dutch Ministry of Defence, Netherlands Defence Doctrine. p. 21; Joint Chiefs of Staff, Joint Publication 1: Doctrine for the Armed Forces of the United States. p. I-13; North Atlantic Treaty Organisation, Allied Joint Publication 1(D): Allied Joint Doctrine. p. I-3.

[240] The Chairman of the Joint Chiefs of Staff, National Military Strategic Plan for the War on Terrorism (Washington, D.C.: The Joint Chiefs of Staff, 2006).; Bush, The National Security Strategy of the United States of America.

law enforcement instruments play an important role. Their place as full-fledged separate instruments, however, seems to be analytically incorrect, though understandable from a policy perspective, i.e. the 'war' on terror. The modes of operation suggested under the guise of the financial instrument are somewhat similar to those suggested under the ambit of the economical instrument, namely: "disrupt the financing of terrorism" by identifying and blocking "the sources of funding for terrorism, freeze the assets of terrorists and those who support them, deny terrorists access to the international financial system, protect legitimate charities from being abused by terrorists, and prevent the movement of terrorists' assets through alternative financial networks".[241] Therefore, considering the financial instrument as an exemplification of different operating methods vis-à-vis non-state actors under the economical instrument seems more logical.

2.5.1.6 *Intelligence instrument*

Intelligence is deemed to be "the first line of defense against terrorists and [...] hostile States".[242] Within the DIME categorisation intelligence was "subsumed under the information instrument",[243] whereas DIMEFIL deems it to be a separate instrument. Intelligence fulfils a role in every State activity,[244] from military to economical intelligence, all instruments utilise intelligence in some form. Yet again the creation of a separate 'intelligence instrument' seems to be a political statement signifying its importance during contra-terrorism, it does not appear to be analytically correct. Intelligence agencies are often dedicated military or non-military and related to some part of the political, military, economical or law-enforcement establishment. Military agencies (such as the national security agency) make up an integral part of the military instrument; economical agencies (for instance the Criminal Investigation Unit of the Internal Revenue Service) make up a part of the economical instrument; law-enforcement agencies belong to civil capacities; and agencies aimed at gathering information about foreign States, organisations and individuals could be considered a part of the political instrument (such as the non-military parts of the Central Intelligence Agency). Consequently, this section will consider intelligence to be an integral part of other instruments and not as separate instrument.

2.5.1.7 *Law-enforcement instrument*

The law-enforcement instrument can be wielded to great effect domestically and abroad, the latter being the focus in post-9/11 governmental papers.[245] The law-enforcement instrument is considered to fulfil a role in stabilising volatile governments and regions.[246] As various governmental publications recognise, there are various other civil capacities

[241] The Chairman of the Joint Chiefs of Staff, National Military Strategic Plan for the War on Terrorism. p. 6.

[242] Bush, The National Security Strategy of the United States of America. p. 30.

[243] Worley, Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System. p. 184.

[244] The Joint Chiefs of Staff, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (Washington, D.C.: The Joint Chiefs of Staff, 2014). pp. 130-131.

[245] Worley, Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System. pp. 184-186.

[246] Ibid. p. 187.

that fulfil a similar stabilizing role in a different manner (see 2.4.6). These civil capacities reside "outside government control or [are] unable to make a direct impact outside national territory"[247], such as "legal power, police force, administrative organisations, education, health care, media and utility companies".[248] Although they are not under direct governmental control (e.g. utility companies) or are not specifically tailored to being deployed outside national territory (e.g. law-enforcement), they can contribute to projecting power, that is, if a government is able to mobilise these capacities. The DIMEFIL-construct of a 'law-enforcement instrument' would have a more logical place under the general scope of 'civil capacities'.

2.5.2 Sub-conclusion

This section has sought to create a generalised overview of the means dimension of the power to by answering the following sub-question: Through which means is power manifested? The means dimension of power relates to publications regarding 'instruments of power' or 'sources of power'. This section has sought to create a more comprehensive overview of the concept and description of instruments of power.

The categorisations of Carr, Mann, DIME and DIMEFIL are largely complementary in nature. Carr describes power most conceptually, Mann most theoretically and DIME(FIL)-proponents most instrumentally. By integrating the insights, an illustrative overview of instruments of power is created and thus an answer to the question through which means power is manifested (see Table 2). Although the means in Table 2 may seem to express favouritism towards DIME nomenclature, the instruments are to be understood as the broadest categories for classifying different means at a State's disposal. They are etymologically similar to DIME, but differ content-wise; DIME reflects a primarily security or military take on the means dimension whereas Table 2 gives a more comprehensive view – including academic insights of Carr and Mann.

[247] Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p. 22.

[248] Ibid. p. 22.

Means	Content
Political instrument	Wield other instruments (Carr) Internal politics (Mann) Geopolitical diplomacy (Mann) Achieving foreign policy objectives (DIME)
Informational instrument	Gain power over opinion (Carr) Unify meaning, norms and aesthetic and ritual practices (Mann) Controlled release of information (DIME) Protecting own information (DIME) Collect information (DIMEFIL)
Economical instrument	Gain autarky (Carr) Influence abroad (Carr) Monopolise control over classes (Mann) Support or combat other actors (DIME) Disrupt finance of other actors (DIMEFIL)
Military instrument	Extending foreign policy (Carr) Intensive power over limited space (Mann) Extensive power over larger space (Mann) Hard coercive power (DIME) Soft attractive power (DIME)
Civil capacities	Legal power (DIME) Law enforcement (DIMEFIL) Administrative organisations (DIME) Education (DIME) Utility companies (DIME) Etc.

Table 2 Generalised overview of means

2.6 Conclusion

This thesis seeks to describe what the utility of military cyber operations is during conflict. Utility encompasses fitness to some purpose or end; the power debate as discussed in this chapter is pivotal in deriving this purpose or end of the military instrument in general and military cyber operations in specific. This chapter has highlighted different aspects of the power debate by answering the following research question: *What are the main theoretical viewpoints on assessing power, how is power manifested, to what end and through which means?*

Section 2.2 has discussed the 'power as resource' and 'relational power' approaches and answered the first part of the research question: *What are the main theoretical viewpoints on assessing power?* The main viewpoints are best summarised as the 'power as resource' and 'relational power' approaches. The 'power as resource' approach classically expresses that power is measurable and quantifiable by 'simply' adding up various resources at an actor's disposal. The actor with most resources is more likely to forward its interests and hence more powerful, whereas a weaker actor is less likely to be able to achieve its goals. The relational power approach advances a more nuanced notion of power, supplements it with an analytical framework whilst at the same time does not rule out the influence of power resources. An actor does not possess power; it manifests itself only in the relation between actors in a specific setting. Any statement on a power situation is considered to be contextual, if supplemented with enough information along predefined dimensions; then it may hold enough information to be become a valid statement on a particular power configuration in a specific setting. This chapter has adopted the 'relational power' approach and derived an analytical framework (see Figure 2). The accepted dimensions scope, domain and means of an (in)action taken by actor A should be weighed against the receptiveness of actor B to the (in)action of actor, potentially adjoined with the dimensions of weight and costs.

Section 2.3 focused on the sub-question: *How is power manifested?* In order to answer the sub-question, the faces of power and the more modern 'taxonomy of power concepts' were discussed. The latter builds on the faces of power and clarifies best how power is manifested, namely through the compulsory, institutional, procedural and structural power concepts (see Figure 3). These concepts illuminate the mechanisms through which actors interact when seeking to influence each other. The effectiveness of an action and the utility of specific capabilities depends, amongst other, on the power concept involved.

Section 2.4 discussed the scope dimension of power and by doing so focused on the third part of the research question: *To what end is power manifested?* Section 2.4 has used the Dutch strategic functions as illustration of potential ends: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation. In order to come to a generalised understanding of these functions, selected U.S., U.K. and French policy documents were adjoined with insights from academia. This analysis has shown that the seven Dutch strategic functions are not universally applicable and that the viability of some is contested in academia. The strategic functions are useful, however, as an example of the ends of manifesting power, or in other words, the 'scope' dimension of the power framework.

Section 2.5 has answered the last part of the research question: *Through which means is power manifested?* There are various ways to categorise the means through which power can be conveyed. Section 2.5 has described the academically accepted categorisations by Carr and Mann and the military/security approaches of DIME and DIMEFIL. Although the categorisations differ on theoretical and conceptual level, they provide useful insight in the means at a State's disposal to project power. By integrating the academic and policy insights a more comprehensive overview of the concept and description of instruments of power was created. The means at a State's disposal comprise of the political, economical, informational and military instruments and civil capacities.

The answer to the research question is reflected in Figure 4. This research has selected the 'relational power' approach as the best developed approach to assessing power, whilst acknowledging the means focus from the 'power as resource' approach. The theoretical viewpoints from the 'relational power' approach are reflected in the power dimensions:

scope, domain, means, weight and costs. These dimensions should be placed in their appropriate context in order to make statements about a specific power configuration. The scope dimension of power could include ends such as the Dutch strategic functions: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation. The means dimension could involve instruments and capacities such as the political, informational, economical, military and civil. The domain, weight and costs dimensions are too contextual to provide an in-depth overview in advance. For instance, the domain (the actors subjected to the (in)action) is highly contextual and the weight (potential successfulness) and costs (cost to comply or resist) highly depend on scope, domain and means. Also impacting the successfulness of an actor to influence others is the power mechanism involved, influence can manifest through the following power concepts: compulsory, institutional, structural and productive.

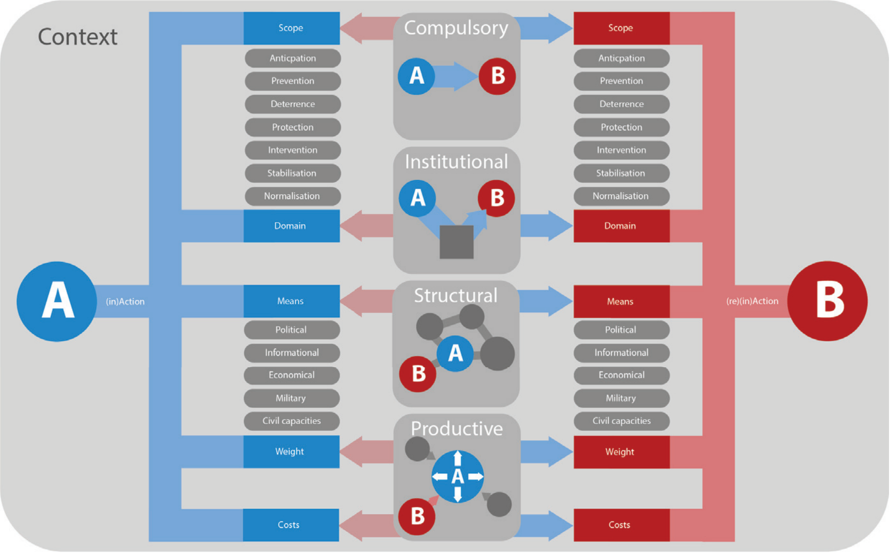

Figure 4 Integrating approaches, mechanisms, and dimensions

2.6.1 Relevance

The insights from this chapter serve to highlight the elements which impact the utility of activities conducted in international relations, including the use of military cyber operations. This chapter's insights serve to highlight, for example, for what purposes activities can be used to influence, through which power concepts they can operate, by whom they can be used, and against whom. The framework advanced in this chapter is general in scope, it encompasses all activities, it is not specific to the use of military cyber operations. The elements reflected the power framework are, however, essential to the research question of this thesis, as all elements impact the potential utility of military cyber operations.

The context, power dimensions and power concepts affect the utility of military cyber operations. As power was deemed non-fungible, what is useful in one context cannot directly be said to be useful in another situation. This translates to military cyber operations, their utility in one context does not automatically imply that they serve a purpose in another situations. For instance, should a military cyber operation prove to be very useful in deterring non-State adversaries, this does not necessarily mean that they are equally suited for deterring State actors.

The power dimensions also affect the utility of military cyber operations, without a specified purpose (scope dimension), the utility of these operations will be marginal as it is unclear to what end they are employed. Scope matters in determining the utility of military cyber operations as they could be better suited for attaining specific goals. For instance, they could be suited for intervening abroad, whilst being less suited for deterring other actors. It is beyond doubt that before being able to engage in military cyber operations the actor should have the means to do so (means dimension) and use them vis-à-vis another actor (domain dimension). As to the power concept involved, results may vary when military cyber operations are used to directly compel another actor into doing something (compulsory power concept) or when they are used to shape the perceptions of an actor (productive power concept).

Thus, the power perspective advanced in this chapter forms the strategic context wherein military cyber operations are used. The strategic functions in the power framework give concrete footholds regarding the sense of purpose required to assess utility. Besides that, the framework highlights factors impacting the effectivity of activities in achieving strategic functions. As such the power perspective is instrumental to this research (see Figure 5).

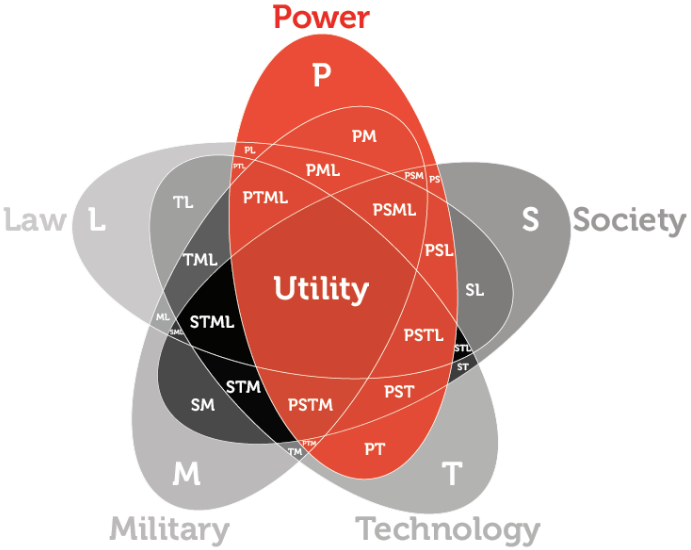

Figure 5 The 'power' or international relations perspective to utility

3

On Society

3 On Society

3.1 Introduction

Information is integral to contemporary society, we are increasingly connected. These technological, social and cultural advancements leading to and constituting our networked society are considered to be a potent medium for conveying power. Societies are under constant pressure of disruptive and less disruptive technological, cultural, societal and economical changes. In some cases, new 'types' of societies emerge. The most general historical-sociological approach to societies is that we have seen three overlapping forms of societies or ages: Pre-industrial (hunter-gathering, pastoral, horticultural, agrarian and feudal), industrial and informational (or post-industrial).[1] These societies have resulted in different forms of conveying power, the current society has, amongst other, resulted in the emergence of military cyber operations.

3.1.1 Goal of this chapter

The context of 'all things cyber', increasing attention for 'cyber', and the rising use and potential of cyber capabilities is informationised society. This society is the basis for the utility of cyber capabilities and it is the context wherein these capabilities are used. The power framework in chapter two, however, is technology agnostic due to its general character. In order to evaluate the impact of informatisation on the power framework this chapter will confront the framework described in chapter two with developments in contemporary society by answering the following sub-question: *What is the impact of informationised society and cyber on power?*

3.1.2 Structure

In order to describe the impact of informationised society on power this chapter will confront the various parts of the power framework with the consequences of informationised society and 'cyber'. In order to do so, this chapter will first describe informationised society by discussing the sociological accords of this societal development (section 3.2). Secondly, this chapter will discuss the rise of 'cyber' within informationised society (section 3.3). Third, this chapter will confront the power concepts (compulsory, institutional, structural and productive) and the accepted power dimensions (scope, domain and means) with informatisation and cyber (section 3.4). Lastly, this chapter will conclude by answering the sub-question (section 3.5).

[1] Manuel Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture (Chichester: Wiley-Blackwell, 2010a). p. 14.

3.2 Informatisation

The omnipresence of information is considered normal nowadays. Although hard to imagine for the progenies of the information age, this was not always the case. Technological, cultural, societal, and economical progress has transformed society into a networked or information society. Being emerged in the *zeitgeist* of the information age, it is not always clear how the availability of information permeates the fabric of society. In order to be able to assess the impact of informationised society on the power framework (see chapter two) the concept has to be further specified, this section will do so by answering the sub-question: *What is information society and how can it be characterised?*

The discussions regarding informationised society are plagued by technological determinism[2] or cyber-utopianism.[3] Although technology is often seen as defining element of our current society, there are other factors to be taken into account. In order to facilitate a broad approach this section will use Frank Webster's five perspectives on informationised society, namely: technological (3.2.1), economic (3.2.2), occupational (3.2.3), spatial (3.2.4) and cultural (3.2.5).[4] After describing the characteristics of informatisation via the five perspectives, this section will reflect on the 'revolutionary' character of these developments (3.2.6). The perspectives on informationised society and reflection on their revolutionary character are used to answer the sub-question in sub-section 3.2.7.

3.2.1 Technological

Many consider the watershed between the industrial and post-industrial age to have occurred after World War Two.[5] Major technological breakthroughs constituting the information revolution – such as "[...] the first programmable computer, [...] the transistor",[6] integrated circuits and micro processing – laid the basis for an 'information age'. It took until the 1970s, however, for "information technologies [to] diffuse widely, accelerating their synergistic developments and converging into a new paradigm".[7] Drivers behind the diffusion of information technologies are developments in the fields of "micro-electronics, computers and telecommunications".[8] These resulted in one of the most iconic innovations of the networked society, namely: The Internet. Although being iconic, the idea of connecting devices is not revolutionary, it stems from a long lineage of networking efforts.

[2] Christian Christensen, "Discourses of Technology and Liberation: State Aid to Net Activists in an Era of " Twitter Revolutions"," *The Communication Review* 14, no. 3 (2011), 233-253. p. 250.

[3] Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011). p. xiii.

[4] Frank Webster, *Theories of the Information Society*, 4th ed. (London: Routledge, 2014). pp. 10-11.

[5] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 39.

[6] Ibid. pp. 39-44.

[7] Ibid. p. 39.

[8] Ibid. p. 39.

From Morse's efforts "to build a network of telegraph offices" in 1845,[9] Bell's nineteenth and early twentieth century efforts to create telephone networks,[10] mid-twentieth century radio broadcasting networks,[11] broadcast satellites[12] and cable television[13] we arrived at computer networks in the last quarter of the twentieth century. The foundation of the Internet is "the existence of computers and the use of machine code compilers – languages – as a basis of communicating with them" and crucial to its development was "the existence of telecommunication networks".[14] The universality of "digital language and the pure networking logic of the communication system created the technological conditions for horizontal, global communication."[15]

The Internet has facilitated unprecedented interconnection via the world-wide web (www), laptops and cellular phones in the 1990s; digital cameras, webcams, digital television, broadband, wireless networking and GPS in the 2000s; tablets, smartphones, smartwatches, smart glasses and smart-everything in 2010s. The information (r)evolution influences the way we work, socialize and spend our pastime.

This sub-section will briefly describe technological trends lying at the heart of society's informatisation. It will not focus on specific technical phenomena such as the rise of semiconductors, integrated circuits, microprocessors and microcomputers and the Internet's foundations.[16] Also it will not focus on the trends captured in 'singularity literature' in which technology may or may not comport to certain 'laws' or models – be

[9] Ibid. p. 244.

[10] Ibid. pp. 248-260.

[11] Ibid. pp. 261-275.

[12] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. pp. 295-304.

[13] Ibid. pp. 305-320.

[14] Ibid. p. 321.

[15] Ibid. p. 45.

[16] See: M. Riordan, "The Lost History of the Transistor," *IEEE Spectrum* 41, no. 5 (2004), 44-49. p. 46; Computer History Museum, "Fairchild's Approach: The Planar Process," computerhistory.org/revolution/digital-logic/12/329, (accessed October 6, 2014); Christophe Lécuyer, "The Planar Process," Nobelprize.org: The Official Web site of the Nobel Prize, nobelprize.org/nobel_prizes/themes/physics/lecuyer/planar.html (accessed October 6, 2014); J. A. Hoerni, "Method of Manufacturing Semiconductor Devices (U. S. Patent no. 3,025,589)," *IEEE Solid-State Circuits Newsletter* 12, no. 2 (2007), 41-42; Brian Winston, Media, Technology and Society, a History: From the Telegraph to the Internet (London: Routledge, 1998). p. 222; Michael R. Betker, John S. Fernando and Shaun P. Whalen, "The History of the Microprocessor," Bell Labs Technical Journal 2, no. 4 (1997), 29-56. p. 29; Winston, Media, Technology and Society, a History: From the Telegraph to the Internet. pp. 235-236.

it Moore's law,[17] Kryder's law, [18] or the Logistic[19], Bass,[20] Gompertz,[21] Gupta,[22] Tobit II[23] or SAW models.[24] Instead, it will focus on the increasing use of information technologies by humans to illustrate society's informatisation from a technological perspective. This sub-section will first briefly discuss changes in information storage, communication, and computational power available per capita (3.2.1.1).[25] After that, this sub-section will reflect on the discussion regarding the revolutionary character of these technological developments (3.2.1.2), as this is distinct from the discussion regarding the revolutionary character of informationised society as a whole (see 3.2.6).

3.2.1.1 Storage, communication and computation

Storage is defined as "the capacity to maintain information over a considerable amount of time" for later retrieval.[26] Storage comes in analogue (e.g. video, photo print, audio cassette, cine movie film, vinyl, LP, books, etc.) and digital format (e.g. PC hard-disk, DVD, Blu-Ray, server hard-disks, CDs, portable hard disk, portable media players, memory cards, videogames, floppy disk, chipcards, etc.).[27] Before 2000, information was primarily stored on analogue storage, from 2000 onwards digital storage started making "a significant contribution to our technological memory [i.e. 25 percent of total storage]".[28] The amount of storage available per person has increased from 0.5 gigabyte (GB) in 1986, 3.9 GB in 1993, 12.1 GB in 2000, 60.3 GB in 2007, to 685 GB in 2014 (see Figure 6). In other words, information and communication technologies have resulted in humankind exponentially hoarding "information in its personal technological memories".[29]

[17] G. E. Moore, "Cramming More Components Onto Integrated Circuits," *Proceedings of the IEEE* 86, no. 1 (1998), 82-85.

[18] Chip Walter, "Kryder's Law," *Scientific American* 293, no. 2 (2005), 32.

[19] Richard N. Foster, *Innovation: The Attacker's Advantage* (London: MacMillan, 1986).

[20] Frank M. Bass, "A New Product Growth for Model Consumer Durables," *Management Science* 50, no. 12 (2004), 1825-1832; Frank M. Bass, "A New Product Growth for Model Consumer Durables," *Management Science* 15, no. 5 (1969), 215-227.

[21] Peg Young and J. K. Ord, "Model Selection and Estimation for Technological Growth Curves," *International Journal of Forecasting* 5, no. 4 (1989), 501-513.

[22] Sunil Gupta, "Impact of Sales Promotions on when, what, and how Much to Buy," *Journal of Marketing Research : JMR* 25, no. 4 (1988), 342-355.

[23] Ashish Sood et al., "Predicting the Path of Technological Innovation: SAW Vs. Moore, Bass, Gompertz, and Kryder," *Marketing Science* 31, no. 6 (2012), 964-979.

[24] Kurzweil, R. (2005). *The Singularity is Near: When Humans Transcend Biology*. London: Viking Penguin. pp. 35-106.

[25] Based on: Martin Hilbert and Priscila López, "The World's Technological Capacity to Store, Communicate, and Compute Information," *Science* 332, no. 6025 (2011), 60.; M. Hilbert and P. Lopez, "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part I: Results and Scope," *International Journal of Communication* 6 (2012a), 956-979.; M. Hilbert and P. Lopez, "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part II: Measurement Unit and Conclusions," *International Journal of Communication* 6 (2012b), 936-955.

[26] M. Hilbert and P. Lopez, "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part I: Results and Scope." p. 964.

[27] Martin Hilbert and Priscila López, "The World's Technological Capacity to Store, Communicate, and Compute Information." p. 3.

[28] Ibid.

[29] M. Hilbert and P. Lopez, "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part I: Results and Scope. p. 960.

Communication capacity is defined as "the capacity to receive or send information, while being transmitted over a considerable distance outside the local area".[30] Two types of communication are distinguished: broadcasting (one-way transmission) and telecommunication (two-way transmission).[31] Examples of broadcasting are cable, personal navigation devices, satellite and terrestrial television; radio; newspapers; and paper advertisement.[32] Telecommunication, for instance, includes phone, Internet, and mobile phone.[33]Broadcasting of information in general increased from 432 exabytes (EB)[34] in 1986, 715 EB in 1993, 1200 EB in 2000, to 1900 EB in 2007. Telecommunication of information per person has increased from 0.05 GB in 1986, 0.08 GB in 1993, 0.35 GB in 2000, to 9.7 GB in 2007 (see Figure 6).

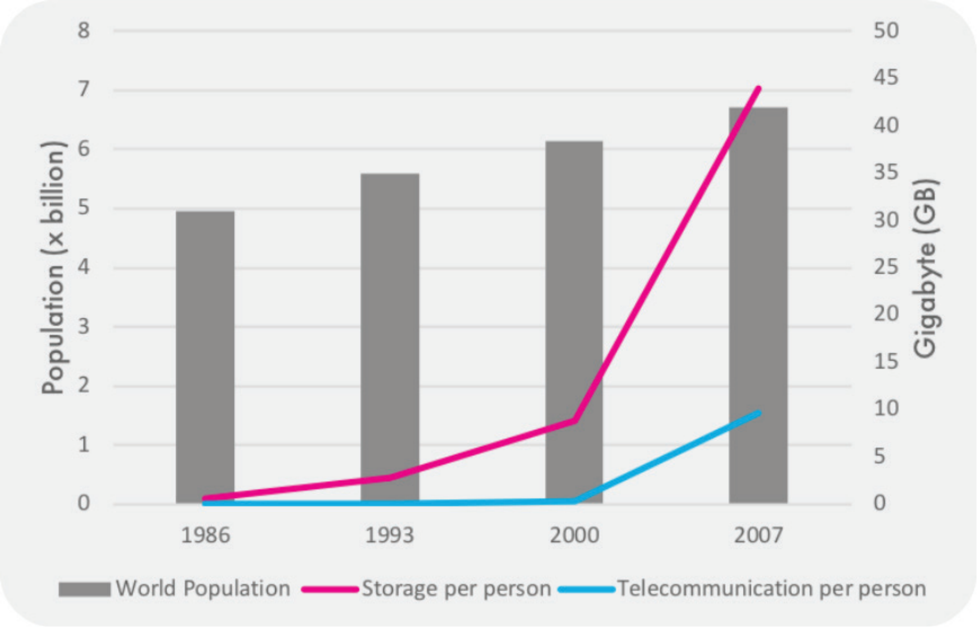

Figure 6 World population and storage per person.[35]

[30] Ibid. p. 964.

[31] Ibid.

[32] Ibid.

[33] M. Hilbert and P. Lopez, "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part I: Results and Scope. p. 964. .

[34] One exabyte contains one billion (1.000.000.000) gigabytes.

[35] Based on: Martin Hilbert and Priscila López, "The World's Technological Capacity to Store, Communicate, and Compute Information," S2cience 332, no. 6025 (2011); Martin Hilbert, Quantifying the Data Deluge and the Data Drought: Background Note for the World Development Report 2016 (Washington D.C.: World Bank,[2015]) and United Nations Department of Economic and Social Affairs, World Population Prospects: The 2017 Revision (New York: United Nations,[2017]).

Computing capacity is the capacity to meaningfully transform "information according to a set of instructions".[36] Computing capacity consists of two types of processing, general-purpose (e.g. personal computers, videogame consoles, servers, supercomputers, pocket calculators, mobile phones) and application-specific (e.g. digital signal processors such CD, DVD players, fixed phone, mobile phone, printer, fax, camcorders, etc.).[37] Computing capacity is relatively hard to capture in a generalised unit (e.g. a GB or EB), Hilbert and Lopez have chosen the unit million instructions per second (MIPS) as a unit for assessing increases in computing power. In 1986 the processing power available to a person was 0.06 MIPS, in 1993 0.8 MIPS, in 2000 47.2 MIPS and in 2007 954 MIPS (see Figure 7).[38]

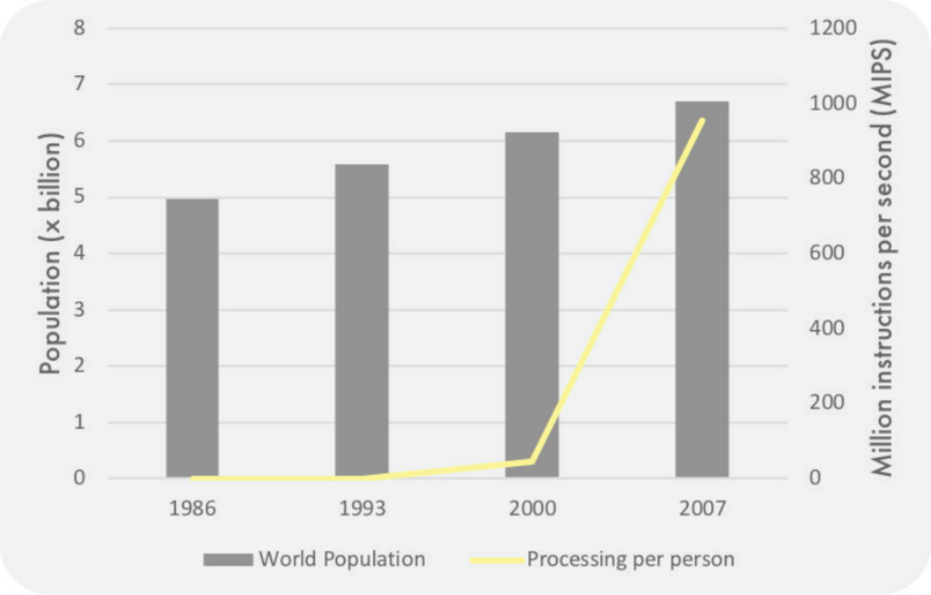

Figure 7 Available MIPS per capita. [39]

The trends in storage capacity, communications capacity and processing power illustrate that Humankind is exponentially storing, communicating, and computing information. The developments in the past decades are best characterised as 'accelerating'. Expressed in the frame of 'Moore's law' (time it takes to double capacity): storage capacity has doubled every 40 months, communication capacity every 34 months, and computing capacity

[36] M. Hilbert and P. Lopez, "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part I: Results and Scope. p. 964.

[37] Ibid.

[38] Martin Hilbert and Priscila López, "The World's Technological Capacity to Store, Communicate, and Compute Information". p. 63.

[39] Based on: Martin Hilbert and Priscila López, "The World's Technological Capacity to Store, Communicate, and Compute Information," Science 332, no. 6025 (2011) and United Nations Department of Economic and Social Affairs, World Population Prospects: The 2017 Revision (New York: United Nations,[2017]).

every 14 months.[40] Although affirming that society is undergoing rapid informatisation, the figures alone are relatively useless in characterising our contemporary society. The following sub-section will cover the claims as to the revolutionary character of technological informatisation.

3.2.1.2 Revolutionary technology

There are "two periods during which the claim was made that new technologies were of such consequence that they were thought to be bringing about systematic social change": the early-1980s and the mid-1990s.[41] The first, early-1980s herald of information society is "the world's leading futurist Alvin Toffler"; he considered the world to be shaped "by three waves of technological innovation".[42] The waves consisted of a First Wave "agricultural phase, a Second Wave industrial phase, and a Third Wave phase now [1980] beginning".[43] Toffler recognizes "a powerful tide [...] surging across much of the world today, creating a new, often bizarre, environment in which to work, play, marry, raise children or retire [...] in this bewildering context, businessmen swim against highly erratic economic currents; politicians see their ratings bob wildly up and down; universities, hospitals, and other institutions battle desperately against inflation [...] value systems splinter and crash, while the lifeboats of family, church, and state are hurled madly about."[44] That third wave "is the information revolution that is engulfing us now and which presages a new way of living".[45]

The second, mid 1990s heralds of impending societal change consider "merging of information and communication technologies (ICTs)" and the "rapid growth of the Internet" to foretell a new society.[46] A "transition from an industrial age to a post-industrial or information age" was witnessed,[47] 1995 marked the entrance to "this new era".[48] The industrial age was based on manufacturing and "exchange of atoms" (tangible, physical products), the new age on exchange and "manufacturing of bits".[49] ICTs and the Internet were deemed to promote "economic success, education and the democratic process".[50] Amidst of the enthusiasts there are others who counter the 1995 heralds of change, some consider the "Internet hucksters" to be wrong in assessing the potency of the Internet.[51] They urge to "discount the fawning techno-burble about virtual communities [...] a poor substitute it is, this virtual reality where frustration is legion and where -- in the holy names

[40] Ibid. p. 64.
[41] Webster, Theories of the Information Society. p. 9.
[42] Ibid. p. 9.
[43] Alvin Toffler, *The Third Wave: The Classic Study of Tomorrow* (New York: Bantam Books, 1980). p. 4.
[44] Ibid. p. 4.
[45] Webster, Theories of the Information Society. p. 9.
[46] Webster, Theories of the Information Society. p. 10.
[47] Nicholas Negroponte, *Being Digital* (London: Hodder & Stoughton, 1995). p. 163.
[48] Bill Gates, *The Internet Tidal Wave* (Redmond: Microsoft, 1995). p. 7.
[49] Negroponte, *Being Digital*. p. 163.
[50] Webster, Theories of the Information Society. p. 10.
[51] Christopher Stoll, "The Internet? Bah!" *Newsweek* 125, no. 9 (1995), 41. p. 41.

of Education and Progress -- important aspects of human interactions are relentlessly devalued."[52] Although the author of the statement later said that of his "many mistakes, flubs, and howlers, few have been as public as my 1995 howler",[53] he uncovers a tendency for technological determinism within information age proponents.

In all of the accounts of an impending information age "technology [...] is privileged above all else, hence it comes to identify an entire social world [...]".[54] Some deem this approach to be wrong, "technology does not determine society",[55] however, this "technological determinism [...] has a prominent place in the culture of modernity".[56] The problem of technological determinism is, however, not insurmountable. Technological advancements have to be placed in a nuanced context, "a technological system can be both a cause and an effect; it can shape or be shaped by society", the impact of technologies increases "as they grow larger and more complex, systems tend to be more shaping of society and less shaped by it."[57] Thus the accelerating trends described and depicted in sub-section 3.2.1.1 are relevant in pointing to increasing informatisation and potentially society being shaped by informatisation. It is without doubt that a society "cannot be understood or represented without its technological tools",[58] however, technology should be considered as an integral part of society. Hence innovative technology constituting the information age is influential, but not revolutionary by itself. Adaption of technology in series of interlinking societal processes may result in a new way of living, but the mere existence of new technology does not suffice to constitute a new age. Therefore, sub-sections 3.2.2 to 3.2.5 will discuss the other factors to be taken into account (economic, occupational, spatial and cultural) and reflect on the revolutionary character as an integral whole (in sub-section 3.2.7).

3.2.2 Economic

Webster's second perspective for describing information society is 'economic', which is an approach to information society that "charts the growth in economic worth of informational activities." [59] The economical perspective on information society involves the notion that a new economy has emerged in the last quarter of the twentieth century, it

[52] Ibid. p. 41.

[53] Ziad Muhmood Kane, "Newsweek in 1995: Why the Internet Will Fail." thenextweb.com/shareables/2010/02/27/newsweek-1995-buy-books-newspapers-straight-intenet-uh/ (accessed October 9, 2014).

[54] Webster, Theories of the Information Society. p. 11.

[55] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 5.

[56] Merrit Roe Smith and Leo Marx, *Does Technology Drive History? the Dilemma of Technological Determinism*, 4th ed. (Cambridge: Massachusetts Institute of Technology, 1994). p. xi.

[57] Thomas P. Hughes, "Technological Momentum," in *Does Technology Drive History? the Dilemma of Technological Determinism*, eds. Merrit Roe Smith and Leo Marx, 4th ed. (Cambridge: Massachusetts Institute of Technology, 1994), 101-114. p. 113.

[58] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 5.

[59] Webster, Theories of the Information Society. p. 15.

is characterised by the terms “informational, global and networked”.[60] The new economy is distinct from previous societies, in pre-industrial societies “the labor force is engaged overwhelmingly in the extractive industries: mining, fishing, forestry, agriculture”.[61] Life in those societies “is primarily a game against nature [...] one works with raw muscle power, in inherited ways, and one’s sense of the world is conditioned by dependence on the elements”.[62] In industrial society “the machine predominates [...] energy has replaced raw muscle and provides the basis of productivity [...] and is responsible for the mass output of goods which characterizes industrial society.”[63] The rhythm of life in the industrial society is “mechanically paced: time is chronological, methodological, evenly spaced”, catchphrases are “maximisation and optimisation”.[64] The new, post-industrial society “is based on services [...] it is a game between persons”.[65] Decisive is not raw muscle power or energy, but knowledge, “the central person is the professional, for he is equipped, by his education and training, to provide the kinds of skill which are increasingly demanded”.[66] This sub-section will briefly discuss two illustrative features of this ‘new economy’: resources and weightless economy.

Central to the information age is information or knowledge, which includes “data, information, images, symbols, culture, ideology and values”.[67] Knowledge is considered to be the main resource in information age economies; hence this new economy was dubbed the informational or the knowledge economy.[68] Important to recognise is that knowledge “has always been a factor in the economy”,[69] although the informational economy “is distinct from the industrial economy, it does not oppose its logic”.[70] The informational economy subsumes the industrial economy “through technological deepening, embodying knowledge and information in all processes of material production and distribution”.[71] Proper knowledge input “can reduce labour requirements, cut inventory, save energy, save raw materials, and reduce the time, space, and money needed for production”.[72] New industries, based on “new and different technologies [...], different science, different logic,

[60] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 77.

[61] Daniel Bell, The Coming of Post-Industrial Society: A Venture in Social Forecasting (New York: Basic Books, 1973). p. 463.

[62] Ibid. p. 464.

[63] Daniel Bell, The Coming of Post-Industrial Society: A Venture in Social Forecasting. p. 465.

[64] Ibid. pp. 465-467.

[65] Ibid. p. 467.

[66] Daniel Bell, The Coming of Post-Industrial Society: A Venture in Social Forecasting. pp. 467-468. See also: Zygmunt Bauman, *Liquid Modernity* (Cambridge: Polity Press, 2006). pp. 58-59.

[67] Alvin Toffler and Heidi Toffler, *War and Anti-War* (London: Little, Brown and Company Limited, 1993). p. 58.

[68] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 100; Peter Ferdinand Drucker, The Age of Discontinuity: Guidelines to our Changing Society, 3rd ed. (London: Transaction Publishers, 2000). p. 263.

[69] John Arquilla and David Ronfeldt, *In Athena’s Camp: Preparing for Conflict in the Information Age* (Washington, D.C.: Rand corporation, 1997). p. xiv.

[70] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 100.

[71] Ibid. p. 100.

[72] Toffler and Toffler, *War and Anti-War*. p. 58.

and different perception", require a different workforce: "they demand knowledge workers rather than manual workers."[73]

Contrary to 'industrial' companies, net-worth of information age companies can hardly be measured "in terms of its hard assets like buildings, machines, stocks, and inventory".[74] Knowledge industries "produce and distribute ideas and information rather than goods and services";[75] their value "depends on ideas, insights, and information in the heads of their employees and in the data banks and patents these companies control".[76] Examples include the software and video gaming industry where the product is primarily in an intangible digitised format.[77] Apart from that, due to "an accelerated commodification of the informational realm", the brand of a product is increasingly significant, the product still matters, but its intangible properties such "as a 'name' [carries] economic weight beyond the actual technical capabilities".[78] These developments are reflected in the top-listed companies according to market capitalisation (see Table 1). In 1996 the list was spearheaded by various, rather traditional companies (e.g. oil, gas, beverage, telephone), whereas in 2017 the top listings are entirely occupied by technology companies.

1996 (Q4)	**2003 (Q4)**	**2010 (Q4)**	**2017 (Q4)**
General Electric	General Electric	Petrochina	Apple Inc.
Royal Dutch Shell	Royal Dutch Shell	Exxon Mobile	Alphabet Inc.
The Coca Cola Company	Microsoft	General Electric	Microsoft
Nippon Telegraph and Telephone	Exxon Mobil	China Mobile	Amazon.com
Exxon Mobil	The Coca-Cola Company	Industrial and Commercial Bank of China	Facebook

Table 1 Top five companies by market capitalisation (a value created by multiplying the total number of shares by the share price).[79]

Thus, contrary to industrial companies, "capital itself [...] is increasingly based on intangibles".[80] This 'weightless economy', best described as "the trade in intangible

[73] Drucker, The Age of Discontinuity: Guidelines to our Changing Society. p. 12.

[74] Toffler and Toffler, *War and Anti-War*. p. 59.

[75] Drucker, The Age of Discontinuity: Guidelines to our Changing Society. p. 263.

[76] Toffler and Toffler, *War and Anti-War*. p. 59.

[77] See also: "Economics A-Z," The Economist, 2004, accessed May 7, 2018, economist.com/economics-a-to-z/w.

[78] Webster, Theories of the Information Society. p. 144.

[79] Based on: Financial Times, *FT Global 500* (London: Financial Times,[2017]).; Financial Times, *FT Global 500* (London: Financial Times,[1996]).; Financial Times, *FT Global 500* (London: Financial Times,[2003]).; Financial Times, *FT Global 500* (London: Financial Times,[2010]).

[80] Toffler and Toffler, *War and Anti-War*. p. 59.

information, services, and intellectual property rather than physical goods", however, "is [only] a small fraction of the manufacturing economy".[81] There are still many pre-industrial, industrial and a variety of mixed form economies, "knowledge work does not lead to a disappearance of work".[82] Thus, there is a new form of economy, focussed on information and resulting in weightless economy. This is considered to be a watershed with industrial economies and a defining feature of the economic perspective on information society.

3.2.3 Occupational

Webster's third perspective on information society is 'occupational', which involves the suggestion "that we have achieved an Information Society when the preponderance of occupations is found in information work".[83] An often-used example signifying changing society is the shift from blue-collar to white-collar work in the United States. 'Information workers' do white-collar work;[84] they make "computers, software, and related goods and services",[85] whereas blue-collar workers are employed in the manufacturing industries. In 1900 the group white-collar occupations made up about 17.6 percent of the workforce, by 1980 it accounted 50,8 percent of all employed workers.[86] In 2006, over 70 per cent of the workforce is found in the service sector in Western Europe, Japan and North America.[87]Assuming white-collar work is, amongst other, knowledge or information work, one might step to conclude that we live in an information age.

It is necessary, however, to exercise caution in ascertaining the existence of information society by looking at quantitative aspects, such as number of information workers.[88] Quantitative measuring does not indicate "the hierarchies – and associated variations in power and esteem of [information workers]", "it disguises the possibility that the growth of certain types of information occupation may have particularly important consequences for social life".[89] For instance, computing and telecommunications engineers could prove most influential due to their driving function in technological innovation, or scientific researchers due to their contribution "in bringing about innovation, conversely, social workers handling "problems of an ageing populations, increased family dislocation and juvenile delinquency may have little to do with an information society, though undoubtedly social workers would

[81] Chris Anderson, *Makers : The New Industrial Revolution*, 1st ed. (New York: Crown Business, 2012). pp. 95-96.

[82] Drucker, The Age of Discontinuity: Guidelines to our Changing Society. p. 251.

[83] Webster, Theories of the Information Society. p. 17.

[84] Anderson, Makers : The New Industrial Revolution. p. 120.

[85] Arquilla and Ronfeldt, In Athena's Camp: Preparing for Conflict in the Information Age. p. xv.

[86] Bell, The Coming of Post-Industrial Society: A Venture in Social Forecasting. p. 483.

[87] Webster, Theories of the Information Society. p. 14.

[88] Merriam-Webster Dictionary, "Willingness," merriam-webster.com/dictionary/willingness (accessed November 14, 2013). p. 15.

[89] Webster, Theories of the Information Society. p. 16.

be classified with ICT engineers as 'information workers'.[90] There are no clear-cut answers as to the decisiveness of particular occupations in determining the dawn of information society; signalling these factors, however, illustrates the shortcomings of a single quantitative, occupational argument for information society. Although being inconclusive itself, "the process of work is at the core of social structure",[91] hence looking at the way we work does yield indications regarding the informatisation of society.

3.2.4 Spatial

The fourth perspective on information society is 'spatial', where "the major emphasis is on information networks which connect locations and, in consequence, can have profound effects on the organisation of time and space".[92] Notions of time and space have changed due to technological innovation. The prime example is the global economy, which is now a "spatially dispersed, yet globally integrated organisation of economic activity."[93] One of the most appealing examples is customer service of major software companies such as Microsoft and Hewlett-Packard, who now outsource services to (semi-) periphery States.[94] Calls from American customers are most likely answered from an Indian call-centre, with an Indian operator trained to mimic an American or British accent.[95] Although there are those who remain sceptical towards the concept of globalisation,[96] it is beyond doubt that this process has generated changes over political, economic, and cultural dimensions, resulting in "the expansion and intensification of social relations across world-space and world-time".[97]

Apart from companies, even individuals are now "capable of managing their affairs effectively on a global scale,"[98] new technology "allows for an increasing dissociation between spatial proximity and the performance of everyday life's functions: work, shopping, entertainment, healthcare, education, public services, governance, and the like."[99] Faced with this new technology, futurists foretold the end of cities, due to telecommuting there was no apparent need to live near your employer.[100] Companies

[90] Ibid. p. 16.

[91] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 216.

[92] Webster, Theories of the Information Society. p. 19.

[93] Saskia Sassen, *The Global City: New York, London, Tokyo* (Princeton, N.J: Princeton University Press, 1991). p. 3.

[94] Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-First Century*, 3rd ed. (New York: Picador, 2007). pp. 12-29.

[95] Ibid. p. 22.

[96] Manfred B. Steger, *Globalization: A very Short Introduction*, 3rd ed. (Oxford: Oxford University Press, 2013). pp. 71-76.

[97] Ibid. p. 128; See also: Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-First Century* (New York: Farrar, Straus and Giroux, 2007). pp. 11-76.

[98] Webster, Theories of the Information Society. p. 18.

[99] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 425.

[100] Adam Toffler refers to the Americal Council of Life Insurance, Fortune magazine and Huxiness Week assertions with regard to deconcentration of population. See: Toffler, *The Third Wave: The Classic Study of Tomorrow*. pp. 298-299.

were also deemed to disperse geographically since they were no longer restricted to economical hubs in big cities. The contrast with the actual effects of the rise of information technologies could not be sharper, we are not "witnessing the annihilation of distance [...] instead we are in the midst of the largest wave of urbanisation in human history." [101] Although some futurists were plainly wrong, many still deem the lessened impact of spatiality to "mark a revolutionary change".[102]

3.2.5 Cultural

Webster's last perspective on information society is 'cultural', which is "perhaps most easily acknowledged, yet the least measured" since "each of us is aware, from the patterns of our everyday lives, that there has been an extraordinary increase in the information in social circulation".[103] Some older generations tend to look with contempt at the screen-addiction of younger generations and fellow commuters, and reflect on days long gone without smartphones, tablets and wireless Internet. [104] But those days are indeed long gone; we live in a media-rich or even saturated environment, television has expanded from "single channel to five broadcast channels"[105] to an average of 189 channels, mobile and on-demand from 2014 onwards.[106] Radio similarly underwent major changes, from occupying a central role in "the front room" to being increasingly mobile and omnipresent, "in the car, the office, and with the Walkman and iPod, everywhere."[107] Printed books, magazines, and newspapers, often dubbed 'old media' by new media enthusiasts, are "the one kind of media that youths consume less of."[108]

The term 'cell phone' in turn has become misleading since "many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."[109] Chief Justice Roberts remarked: "they could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[110] Modern cell phones have become "such a pervasive and insistent part of

[101] Manuel Castells, "Globalisation, Networking, Urbanisation: Reflections on the Spatial Dynamics of the Information Age," *Urban Studies* 47, no. 13 (2010b), 2737.p. 2738.

[102] Webster, Theories of the Information Society

[103] Ibid. p. 21.

[104] Michael Harris, The End of Absence: Reclaiming what we'Ve Lost in a World of Constant Connection (New York: Current, 2014). pp. 44-50.

[105] Webster, Theories of the Information Society. p. 19.

[106] Megan Geuss, "On Average, American Get 189 Cable TV Channels and Only Watch 17," arstechnica.com/business/2014/05/on-average-americans-get-189-cable-tv-channels-and-only-watch-17/ (accessed October 16, 2014).

[107] Webster, Theories of the Information Society. p. 19.

[108] Harris, The End of Absence: Reclaiming what we'Ve Lost in a World of Constant Connection. p. 48.

[109] Supreme Court of the United States, *David Leon Riley, Petitioner V. California; United States, Petitioner V. Birma Wurie*, ed. Chief Justice Roberts, Vol. Nos. 18-132 and 13-212 (Washington, D.C.: Supreme Court of the United States, 2014). p. 17.

[110] Ibid. p 17.

daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[111] The integrality of mobile devices to everyday lives in the 21st century is not limited to developed regions, global penetration of mobile-cellular subscription "approaches 100% and market saturation is reached".[112] In line with cell phones, Internet access is becoming commonplace in the developed world with nearly 85% of the population being online.[113] Internet access in developing regions is also on the rise with 48% of the total population online and 70% with online access between the age of 15-24.[114]

In the late 1990s and 2000s "the social nature of media has dramatically reasserted itself."[115] After a period of decline due to centralised mass media from the mid-nineteenth century until the 1990s via the "steam-powered printing press, followed in the twentieth century by radio and television", the Internet and social media are now enabling people "to compete with broadcast media and emerge from its shadow".[116] The enormous numbers of Facebook posts (4.75 billion pieces of content shared per day), Facebook members (1.94 billion in 2017), Tweets (500 million per day), SnapChat messages (3 billion per day) and instant messages (e.g. 60 billion messages per day via Facebook Messenger and Whatsapp) would suggest that social-media is affecting the way we interact.[117] Although there are critiques as to what it exactly is that social media enables,[118] it is reasonable to assume that is unlikely that social media have "not changed [the way we interact at] all and unlikely that it has radically changed."[119] In sum, there are various developments that impact the culture, however, "it is doubtful that we are entering a genuinely new historical configuration".[120] The "postmodern condition", as cultural aspect of information society, could also be "explicable in terms of on-going, if accelerating, trends".[121]

3.2.6 Revolutionary change?

Webster's five perspectives on information society illustrate how different fields look at changing society. Employing these categories to describe change in societies does not

[111] Ibid. p. 9.

[112] International Telecommunication Union (ITU), *The World in 2013: ICT Facts and Figures* (Geneva: ICT Data and Statistics Division Telecommunication Development Bureau, 2013). p. 1.

[113] International Telecommunication Union (ITU), *The World in 2017: ICT Facts and Figures* (Geneva: ICT Data and Statistics Division Telecommunication Development Bureau, 2017). p. 1.

[114] Ibid. pp. 1-2.

[115] Tom Standage, *Writing on the Wall: Social Media-the First 2,000 Years* (New York: Bloomsbury Publishing, 2013). p. 13.

[116] Ibid. p. 13.

[117] "What Happens in an Internet Minute in 2017?" Visual Capitalist, accessed June 30, 2018, visualcapitalist.com/happens-internet-minute-2017/.

[118] Christian Fuchs, *Social Media: A Critical Introduction* (Los Angeles: SAGE, 2014). pp. 33-34.

[119] Ibid. p. 49.

[120] Webster, Theories of the Information Society. p. 262.

[121] Ibid. p. 262.

clarify what exactly constitutes and "how to distinguish, an information society."[122] Beyond doubt is the criticality of information "in the present age", what is doubtful, however, is whether "information has become the major distinguishing feature of our times".[123] Most definitions of information society "offer a quantitative measure [...] and assume that, at some unspecified point, we enter an information society".[124] Merely having more information alone does not suffice, however, to claim that something radically new is emerging before us. The fact, for instance, "that there are more automobiles today than in 1970 does not qualify us to speak of a 'car society'."[125] Although information is integral to the functioning of contemporary society, its indispensability must not be confused "with a capacity for it to define social order".[126] Crucial to ascertaining the arrival of an information age is the way "quantitative increases transform [...] into qualitative changes in the social system".[127]

There are few contemporary authors who contest the ever-increasing role of information in societies, often called 'informatisation'. What is contested, however, is the revolutionary nature of this development. On the one hand there are "those who emphasise historical continuities", who reject "any suggestion that the 'information revolution' has overturned everything that went before", they insist to explain informatisation as "an outcome and expression of established and continuing relations".[128] Drucker's *Age of Discontinuity* epitomises the alternative approach: the discontinuous nature of informatisation. [129] The most elaborate account of a new, discontinuous societal form is Castell's, who describes the naissance of the "network society", which is "the new social morphology of our societies".[130] He deems it to be revolutionary since the "diffusion of networking logical substantially modifies the operation and outcomes in processes of production, experience, power, and culture".[131] Daniel Bell before him described the changing workforce to present discontinuous change, in a relatively limited time-span the workforce changed from industrial to information workers in the tertiary, white-collar, services sector of the economy.[132] Thus, there are two approaches towards the existence of information society, the first approach is to consider our current society to be a product of ever-continuing informatisation resulting in 'informationised society' and the second is seeing the revolutionary emergence of a new 'information society'.

[122] Webster, Theories of the Information Society. p. 21.

[123] Ibid.

[124] Ibid.

[125] Ibid. p. 22.

[126] Ibid. p. 23.

[127] Ibid.

[128] Frank Webster refers to Herbert Schiller, Jürgen Habermas and Anthony Giddens as proponents of non-revolutionary, continuity of informatisation. Ibid. p. 266.

[129] Drucker, The Age of Discontinuity: Guidelines to our Changing Society. p. xiii.

[130] Castells, The Rise of the Network Society, the Information Age: Economy, Society, and Culture. p. 501.

[131] Ibid. p. 501.

[132] Bell, The Coming of Post-Industrial Society: A Venture in Social Forecasting. p. 23.

Although there are differences between informatisation and information society approaches, mainly with regard to empirics and the interpretation of what is "actually going on in the world",[133] both sides corroborate a changing society with a dominant role for information. Both sides also note the prominent (informationised society) or dominant (information society) role of information technology in boosting the process of informatisation. The informationised society approach provides the most nuanced and comprehensive description of our contemporary society as various perspectives are incorporated that overcome the techno-deterministic pitfall. At the same time the informationised society approach does note the impact of technology, hence it incorporates parts of the information society approach. Therefore, this thesis will adopt the more nuanced and comprehensive approach to 'informationised society' marking the changes in contemporary society as evolutionary and not revolutionary.

3.2.7 Sub-conclusion

This section has aimed to answer the following sub-question: *What is information society and how can it be characterised?* Sub-section 3.2.1 has discussed the technological perspective on informationised society as being brought forth from a series of technological breakthroughs from the 1950s until now spawning computing, networking, mobile computing and the Internet. The mere existence of new technology, however, does not suffice to constitute a new age. Sub-section 3.2.2 consequently described the economical perspective on information society. The defining feature of the economical perspective on information society is the new form of economy, focussing on information as product and resulting in weightless economies (i.e. no tangible products). Sub-section 3.2.3 has discussed occupational changes due to informatisation, this sub-section showed that knowledge or information work has exponentially grown and one might step to conclude that we live in an information age as our workforce is engaged in information work. As fourth, in sub-section 3.2.4 it was argued that spatiality has altered, the lessened impact of spatiality is indicative of changing society. Sub-section 3.2.5 has discussed the change in culture due to myriads of new means and methods of interaction and expression through technological means. Lastly, sub-section 3.2.6 has reflected on the revolutionary character of the changes captured within the various perspectives. It revealed that there is no clear-cut answer as to the question whether there is a revolutionary new information society or merely an evolution in society due to informatisation.

In other words, there is no clear-cut answer as to what informationised society is apart from a contested construct. The characteristics of informationised society on the contrary are much clearer. The perspectives described by Webster are indicative of changes in society captured under the ambit of the construct 'informationised society' in technological, economical, occupational, spatial and cultural sense. As a general description and characterisation of informationised society as context for power Webster's perspectives

[133] Webster, Theories of the Information Society. p. 265.

suffice, however, for specific description of changes in the power framework further research is required. There is no doubt, however, that the changes captured in Webster's perspectives on informationised society constitute the basis for new ways of influencing or projecting power in informationised society, for instance by using 'cyber' to influence.

3.3 Rise of cyber

"All I knew about the word cyberspace when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page."[134]

As the somewhat cynical quote above illustrates, the term 'cyber' is essentially meaningless, yet it is being used to refer to nearly everything related to the digital domain. We have given meaning to it, since it indeed turned out to be an effective buzzword. Within the general drive towards an informationised society 'cyber' has been a related development that impacts society in various ways. Some grassroots information technology professionals are emphasising the emptiness the current 'cyber' vocabulary.[135] Apart from annoying certain parts of the information technology community, the current haziness of 'cyber' discourse clouds the original meaning of 'cyber' and its development within informationised society. In order to comprehend the relation between informationised society and cyber this section will analyse the phenomenon by answering the following sub-question: *What is 'cyber' and how has it developed over time?*

In order to answer the sub-question this section will trace the development of 'cyber' in the second part of the 20th century. This section will first discuss the etymological origins of 'cyber' from approximately 350 BC to the 1950s (sub-section 3.3.1), as understanding its original meaning is the starting point for observing changes in its meaning and its development. Secondly, this section will discuss the 20th century etymological reinterpretation of cyber and the pivotal notion of 'cyberspace' in the timeframe of the 1960s to the 1980s (sub-section 3.3.2). After that, this section will describe the subsequent development of information and cyber warfare and associated phenomena in the 1990s (sub-section 3.3.3). Shortly after the term 'cyber' entered governmental policy and the military in the 2000s, which will be described as sixth (sub-section 3.3.4). This section will conclude with answering the sub-question in sub-section 3.3.5.

[134] *William Gibson: No Maps for these Territories,* directed by Mark Neale (New York: Docurama Films, 2000)

[135] André Koot, "Ditch Cyber Campaign," id-use.blogspot.nl (accessed October 30, 2013); Jarno Limnél, "What is Real in Cyberhype?" infosecisland.com/blogview/23393-What-is-Real-in-Cyberhype.html (accessed October 30, 2013).

3.3.1 Cyber in the 350s BC to the 1950s: Cybernetics

The terms cyber and cyberspace actually predate the dawn of the Internet.[136] Cyber is derived from the Greek *κυβερ*, which means "to steer, to discipline or to govern".[137] One of the most prominent uses of 'cyber' in Greek literature is in Plato's *First Alcibiades*.[138] Where the metaphor of *κυβερνήτης* (steersman/pilot) is essentially used to summarise "the entirety of Greek philosophy, integrating *Mythos*, *Logos* and *Nomos*" and relates to "thought-aided, purpose-directed, history-illuminated, feedback-dependent, and future-affirming or feedforward-sensitive governance".[139]

Cyber as a prefix gained wide attention due to Norbert Wiener's book *Cybernetics*.[140] He uses cybernetics to describe "the entire field of control and communication theory, whether in the machine or in the animal".[141] Wiener is said to derive the term from Greek language (*κυβερνήτης*), though it could also be the Anglicisation of the French term '*cybernétique*'. The latter is coined by André-Marie Ampère in 1843 in his book *Essai sur La Philosophie des Sciences*.[142] Ampère suggest that the term *"dans une acception restreinte*" relates to *"l'art de gouverner un vaisseau".* [143] He states, however, that even the Greek interpreted it more broadly, *"reçut de l'usage, chez les Grecs même, la signification, tout autrement étendue, de l'art de gouverner en général*".[144] In other words, Ampère understands the term to relate to the art of governing in general whereas Wiener utilises it to describe the field of control and communication theory. In all interpretations, the ancient, the 19th century or early-20th century interpretation, some form of control or governance stems from the term cyber.

Thus cyber is derived from antiquity and its meaning has changed at least twice in etymological sense up until the mid-20th century. Plato first used cyber in the sense of cybernetics to, restrictively interpreted, refer to the craftsmanship of piloting a vessel. Alternatively, as suggested by Ampère, when interpreted in a broader sense, Plato referred to the art of controlling or governing a subject. Ampère used the latter as basis for the French term *cybernétique*, as Wiener similarly did with the English cybernetics. In other words, in the early-20th century cyber was associated with cybernetics, which entails the

[136] Ananda Mitra, *Digital Security: Cyber Terror and Cyber Security* (New York: Infobase Publishing, 2010). p. 17.

[137] Jerry Everard, Virtual States: The Internet and the Boundaries of the Nation-State (New York: Routledge, 2000). p. 15.

[138] Plato, "Ἀλκιβιάδης," in *Plato with an English Translation VII*, ed. W. Lamb (London: William Heinemann Ltd., 390-342 B.C.). pp. 79, 178, 180, 259, 329, 435.

[139] Barnabas Johnson, "The Cybernetics of Society: The Governance of Self and Civilization," jurlandia.org/cybsocsum.htm (accessed October 30, 2013).

[140] Norbert Wiener, The Cybernetics of Society: The Governance of Self and CivilizatioN (Cambridge: M.I.T. Press, 1948).

[141] Ibid. p. 11.

[142] Antoine Ampère, Essai Sur La Philosophie Des Sciences Ou Exposition Analytique d'Une Classification Naturelle De Toutes Les Connaissances Humaines (Paris: Bachelier, 1843).

[143] Ibid. p. 141.

[144] Ibid. p. 141.

"science of regulation and control in animals (including humans), organisations, and machines".[145]

3.3.2 Cyber in the 1960s – 1980s: Cyberspace, hackers, and information security

The 1960s earmarked the start of modest though etymologically similar cyber prefix-use, i.e. to modern understanding, as both cyberculture and cybernauts were spawned. [146] It was, however, in the decade of the rise of the personal computer, the seventies and eighties, that a sci-fi novel spearheaded cyber as we interpret it today. William Gibson coined the term cyberspace in his sci-fi story 'Burning Chrome'.[147] He further defined cyberspace in his 1984 book Neuromancer.[148] He described cyberspace, in the context of his novel, as a "consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding".[149] Gibson's cyberspace consequently served "as the mold from which a legion of neologisms are cast: cyberpunk,[150] cyberculture,[151] cyberlife, cybernauts, cyberselves, cybersex, cybersociety, cybertime – cybereverything".[152] 'Cyberspace' was used before Gibson by the Danish artist duo Susanne Ussing and Carsten Hoff in 1968-1970. For them cyberspace "was simply about managing spaces. There was nothing esoteric about it. Nothing digital, either. It was just a tool. The space was concrete, physical."[153]

Since *Neuromancer* was written in a decade of relative Internetlessness, one might say that Gibson was a visionary foreseeing the future of the Internet. As the quote at the beginning of this section suggests, however, it was merely an effective buzzword he utilised to

[145] Merriam-Webster Dictionary, "Diplomatic,"

[146] Cyberculture: An "umbrella term for the various subcultures to which the use of computer networks has given rise and whose interaction which each other is computer-mediated (or primarily so)." Source: Daniel Chandler and Rod Munday, *A Dictionary of Media and Communication* (Oxford: Oxford University Press, 2011). p. 89.

[147] William Gibson, "Burning Chrome," *Omni,* July, 1982, 72. p. 72.

[148] William Gibson, *Neuromancer* (New York: Berkley Publishing Group, 1984).

[149] Ibid. Part two.

[150] Cyber-punk: "The very word cyberpunk is itself a portmanteau of cybernetics, the science and technology of the system, and punk, the philosophy of rebellion against the system". Source: "Seph", "What is Cyberpunk? ," cyberpunkforums.com/viewtopic.php?f=1&t=361 (accessed October 30, 2013).

[151] Cyber-culture: "[...] the study of various social phenomena associated with Internet and other new forms of network communication. Examples of what falls under cyberculture studies are online communities, online multi-player gaming, the issue of online identity, the sociology and the ethnography of email usage, cell phone usage in various communities; the issues of gender and ethnicity in Internet usage; and so on". Source: Lev Manovich, "New Media from Borges to HTML," *The New Media Reader* (2002), 13-28. p. 16.

[152] Ibid. p. 16. Lance Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation," *Western Journal of Communication (Includes Communication Reports)* 63, no. 3 (1999), 382-412. p. 382.

[153] Jacob Lillemose and Mathias Kryger, "The (Re)Invention of Cyberspace," Kunstkritikk, kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/ (accessed October 18, 2017).

great effect. Gibson's use of cyberspace is accredited to have "initiated the Cyber-prefix flood".[154] The term was effective then as it is now since it "seems to resonate with the public imagination, fitting comfortably with our contemporary encounters with electronic technologies. It also has proven to be quite flexible and open, easily translated across different sectors of society".[155]

Despite having coined the term, others have given cyberspace different meanings in the late-20th century. Gibson started with using the term to describe a fantasy world involving the graphic representation of data.[156] Some have suggested that cyberspace is in fact real and present; it is the world where cyberpunks reside, that is outlaws and hackers according to the author.[157] Others suggest that cyberspace is still under development and is a part of our desire to dwell in fiction.[158] Another approach is cyberspace as a part of virtual reality or alternatively as an overarching concept of virtual reality.[159] The notions that correlate most with our contemporary notion, however, are cyberspace as electronic storage and transmission of information,[160] or computer mediated communication.[161]

Developments within the field of information security, then only loosely connected to cyber, resulted in 'hacker' entering mainstream media and adoption of specific information security policy. A mistake at the North American Air Defense Command (NORAD) resulted in a chain of events resulting in hackers being featured on the frontpage of Newsweek.[162] A person "had mistakenly put military exercise tapes into the computer system" of the NORAD system,[163] which initiated an inadvertent injection of test scenario data in missile warning computers which resulted in false alerts"[164] That test scenario simulated an all-out nuclear strike on United States mainland.[165] The United States National Security Council assumed that the Soviet Union had launched 220 missiles; a number that was later adjusted to 2.200 missiles.[166] Nearing the moment of requesting the President to decide on ordering

[154] Robert Trappl, "Preface: The Cybernetics and Systems Revival," osgk.ac.at/emcsr/00/preface98.html (accessed November 11, 2013).

[155] Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation," , 382-412. p. 382.

[156] Gibson, *Neuromancer* Part two.

[157] Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier* (New York: Touchstone, 1992). pp. 161 and 164.

[158] Strate, "The Varieties of Cyberspace: Problems in Definition and Delimitation," , 382-412. p. 383.

[159] Michael Heim, *The Metaphysics of Virtual Reality* (Oxford: Oxford University Press, 1993). pp. 131-132

[160] Bruce Sterling, The Hacker Crackdown: Law and Disorder on the Electronic Frontier (New York: Bantam Books, 1994). pp. 9-11.

[161] Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Reading: Addison-Wesley Publishing Company, 1993). pp. 6-7.

[162] William D. Marbach, "Beware: Hackers at Play," *Newsweek, September* 6 (1983), 42-48.

[163] Robert M. Gates, The Ultimate Insiders Story of Five Presidents and how they Won the Cold War (New York: Touchstone, 1996). p. 114.

[164] United States General Accounting Office, *NORAD's Missile Warning System: What Went Wrong?* (Washington: United States General Accounting Office, 1981). p. 13.

[165] Gates, The Ultimate Insiders Story of Five Presidents and how they Won the Cold War. p. 114.

[166] Ibid. p. 114.

a retaliatory strike, when the Strategic Air Command was already launching its planes, a phone call informed the National Security Council of NORAD's error.[167]

The erroneous NORAD notification served as basis for the movie WarGames in 1983. The movie consequently triggered high school students from Milwaukee, "inspired by WarGames and calling themselves the 414s", to prove that they could gain access to military networks.[168] They succeeded and the 414s got nation-wide media attention, [169] which resulted in the use of 'hacker' in mainstream media and a year later in specific legislation in order to secure federal information systems.[170] The (then) top secret National Security Decision Directive Number 145 noted, "this trend [i.e. the application of new technologies] promises greatly improved efficiency and effectiveness, it also poses significant security challenges".[171] The directive bestowed the NSA with the responsibility "for setting standards and guidance, conducting research, and doing some monitoring of all government telecommunications systems and automated information systems".[172]

Flags were raised with regard to the prominent role of the NSA in 1985 when it turned out that NSA probed a computer program used in federal and national elections and in the process "obtained a detailed knowledge of that computer program".[173] In reaction thereto,[174] various bills were proposed to protect computer systems.[175] The different hearings and political pressure finally resulted in National Security Directive-42 which marked a "dramatic shift" in information security from military to civilian authority.[176] In sum, the 1960s to the 1980s are pivotal in the development of the cyber construct as its foundations were developed in fiction; the (general) public became aware of 'hackers'; and in politics information security received increasing attention.

3.3.3 Cyber in the 1990s: Information war, cyberwar and netwar

In the etymological origin of cyber the 1990s are most prominently marked by the development of the concepts of information war, cyberwar and netwar. The groundwork of the military use of information was laid during the Vietnam Conflict (1955-1975),

[167] Ibid. p. 114; Warner, "Cybersecurity: A Pre-History." p. 787.

[168] Gates, The Ultimate Insiders Story of Five Presidents and how they Won the Cold War. p. 114.

[169] William D. Marbach, "Beware: Hackers at Play," *Newsweek, September* 6 (1983), 42-48.

[170] United States Presidential National Security Decision Directive 145, National Policy on Telecommunications and Automated Information Systems Security, 1984).

[171] Ibid.

[172] Warner, "Cybersecurity: A Pre-History." p. 788

[173] Donald Goldberg, "The National Guards," *Omni Magazine* 9, no. 8 (May, 1987).

[174] See also: Linda Greenhouse, "Computer Security Shift is Approved by Senate," *The New York Times* (December 24, 1987). nytimes.com/1987/12/24/us/computer-security-shift-is-approved-by-senate.html?src=pm.

[175] *Computer Security Act 1987, 100th Congress (1987 - 1988) H.R.145* (1987): 1; Roe A. Robert, *Report to Accompany H.R. 145* (Washington: Committee on Science, Space, and Technology,[1987]).

[176] Ibid.

which “prompted [...] discussions with its turn toward precision-guided munitions, remote sensors on the battlefield, and computer-aided processing of all manner of logistical, administrative, and operational data”.[177] The complexity and wide usage of various intrinsically linked information systems was perceived to add to the fragility of information flows on the battlefield.[178] The understanding that the vulnerability could be turned into an opportunity within enemy ranks arrived in the 1990s.

After the rapid victory brought about in operation Desert Storm (dubbed the first ‘information war’ by some),[179] the concept of information warfare gained broad attention.[180] Illustrative for this changing focus, from defensive to offensive, is the title change of the memorandum of policy by the Chairman of the Joint Chiefs of Staff’s, the “Command, Control and Communications Countermeasures” policy from 1990 was renamed to “Command and Control Warfare” in 1993.[181] The objective of this type of warfare is the decapitation of “the enemy’s command structure from its body of combat forces”.[182]

Information warfare was further institutionalised with the creation of the Air Force Information Warfare Center (1993),[183] the Fleet Information Warfare Center (1995)[184] and the Army Land Information Warfare Activity (1995).[185] By that time other States noticed these efforts made by the United States, consequently Boris Yeltsin deemed it “necessary to devote more attention to the development of the entire complex of the means of information warfare”.[186] Similarly the Chinese noted in 1995: “In the near future, information warfare will control the form and future of war. We recognise this developmental trend of information warfare and see it as a driving force in the modernisation of China’s military and combat readiness. This trend will be highly critical to achieving victory in future wars”.[187] In 1996, spearheaded by the United States Army,

[177] Warner, “Cybersecurity: A Pre-History.” p. 789.

[178] Thomas P. Rona, “Weapon Systems and Information War,” *Boeing Aerospace Co., Seattle, WA* (1976).

[179] See for instance: Alan D. Campen, The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War (Fairfax: AFCEA International Press, 1992).

[180] Warner, “Cybersecurity: A Pre-History.” p. 790.

[181] Chairman of the Joint Chiefs of the Staff, Memorandum of Policy no. 30: Command and Control Warfare, 1993).

[182] Ibid.

[183] Air Intelligence Agency, “Air Force Information Warfare Center,” *Air Force Intelligence Agency Almanac*, no. 97 (August, 1997a). p. 20; Dan Kuehl, “Joint Information Warfare: An Information-Age Paradigm for Jointness,” *Strategic Forum Institute for National Strategic Studies*, no. 105 (March, 1997). p. 2.

[184] Office of the Chief of Naval Operations, OPNAV Instruction 3430.26: Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W), 1995a). p. 8.

[185] Richard A. Sizer, “Land Information Warfare Activity,” *Military Intelligence Professional Bulletin* (January-March, 1997).

[186] James Adams, The Next World War: Computers are the Weapons and the Front Line is Everywhere (New York: Simon and Schuster, 2001). pp. 238, 239, 244.

[187] Wang Pufeng, “The Challenge of Information Warfare,” in *Chinese Views of Future Warfare*, ed. Michael Pillsbury (Washington: National Defense University Press, 1998), 317-326. p. 318.

the United States adopted a less 'belligerent' notion, namely: 'information operations'.[188] Information security, yet to be dubbed with a cyber-prefix, played a role in the doctrinal approach to information operations formerly known as information warfare. Under the umbrella of information operations the Air Force Computer Emergency Response Team (AFCERT),[189] Army Computer Emergency Team (ACERT)[190] and Naval Computer Incidence Response Team (NAVCIRT)[191] were spawned in 1996 and 1997. These teams were responsible for safeguarding and monitoring military networks.[192] Thus for the military the 1990s marked the military integration of computers, networks and associated systems within its organisation under the ambit of information operations.[193]

While the military was institutionalizing the concept of information operations, the concept of cyberwar[194] and netwar emerged in a 1993 report of the Research and Development Corporation (RAND).[195] Arquilla and Ronfeldt suggested two different species of 'information mediated warfare': cyberwar and netwar.[196] The difference between the two lies in their nature, netwar is understood to be "refer to information-related conflict at a grand level between nations or societies [...] it means trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it"[197] and cyberwar "refers to conducting, and preparing to conduct, military operations according to information-related principles".[198]

The authors of the RAND report prefer to use the cyber-prefix as a result of the contamination of the term 'information warfare', "which has been used in some circles to refer to warfare that focuses on C3I [command, control, communication and information] capabilities".[199] Cyber, in their opinion, "is not simply a set of measures based on technology [...] and should not be confused with past meaning of computerised, automated, robotic, or electronic warfare".[200] Cyberwar is understood to be 'war' about

[188] United States Army, *Field Manual no. 100-6: Information Operations* (Washington, DC: U.S. Government Printing Office, 1996).

[189] Air Intelligence Agency, "Air Force Information Warfare Center: Air Force Computer Emergency Response Team," *Air Force Intelligence Agency Almanac*, no. 97 (August, 1997b). p. 22.

[190] Joan Fischer, "Protecting Electronic Borders," *U.S. Army Intelligence and Security Command Journal* 20, no. 2 (1997).

[191] Department of the Navy, *Forward from the Sea: Anytime, Anywhere* (Washington, DC: Department of the Navy, 1998). Chapter VIII.

[192] Fischer, "Protecting Electronic Borders," ; Air Intelligence Agency, "Air Force Information Warfare Center: Air Force Computer Emergency Response Team," ; Air Intelligence Agency, "Air Force Information Warfare Center," ; Department of the Navy, *Forward from the Sea: Anytime, Anywhere*.

[193] See also: Chris Hables Gray, *Post-Modern War: The New Politics of Conflict* (New York: The Guilford Press, 1997). pp. 23-40.

[194] There are instances of 'cyberwar' usage before the report, see for instance: Eric H. Arnett, "Welcome to Hyperwar," *The Bulletin of Atomic Scientists* 48 (1992), 14. p. 15.

[195] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12, no. 2 (1993), 141-165.

[196] Arquilla and Ronfeldt, "Cyberwar is Coming!" , 141-165. p. 145.

[197] Ibid. p. 146.

[198] Ibid. p. 148.

[199] Ibid. Note 7.

[200] Ibid. p. 148.

knowledge, about who knows what, when, where and why, and about how secure a society or military is regarding its knowledge of itself and its adversaries".[201] This notion gained acceptance amongst the military, where it was, as intended by Arquilla and Ronfeldt, conceived to be an overarching concept of information operations.[202]

3.3.4 Cyber in the 2000s: Cyber-everything

The United States government spearheaded a change in direction – some would argue in the wrong direction – by issuing Executive Order 13010.[203] 'Cyber threats' were identified in the realm of critical infrastructure protection and understood to comprise "electronic, radio-frequency, or computer-based attacks on the information or communications components that control critical infrastructures".[204] Subsequently, in a similar vein of the protection of critical infrastructure, Presidential Decision Directive 63 earmarked "cyber-based information systems" besides critical infrastructure.[205] The Decision Directive 63 also outfitted other terms with a cyber prefix, being: "cyber attacks", "cyber supported infrastructures", "cyber systems", "cyber-based systems" and "cyber information warfare threat".[206] Despite coining these various neologies, the document does not define these terms.

The next document by the United States government aimed at safeguarding information systems – in this case without a cyber-prefix – is the document "Defending America's Cyberspace, National Plan for Information Systems Protection".[207] This document spawned 33 new cyber-prefixed notions and placed them in a context of national security.[208] The only two cyber-terms defined, however, are cyberattack ("Exploitation of the software vulnerabilities of information technology-based control components") and cyberspace ("describes the world of connected computers and the society that surrounds them [...] commonly known as the INTERNET").[209] The meagre definition section leaves much issues

[201] Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Delft: Eburon Academic Publishers, 2005). p. 306.

[202] Richard Szafranski, "A Theory of Information Warfare: Preparing for 2020," *Airpower Journal* (Spring, 1995).

[203] William J. Clinton, "Executive Order 13010: Critical Infrastructure Protection," *Federal Register* 61, no. 138 (1996), 37347-37350.

[204] William J. Clinton, "Presidential Decision Directive 63," *The White House, Washington, DC* (1998).

[205] Ibid.

[206] Ibid.

[207] The White House, Securing America's Cyberspace, National Plan for Information Systems Protection: An Invitation to a Dialogue (Washington, DC: The White House, 2000).

[208] The new notions: "cyber vulnerabilities", "cyber disruptions", "cyber defense", "cyber networks", "cyber-intrusions", "cyber-security", "cyber incidents", "non-cyber systems", "cyber technology", "cyber-ethics", "Cyber Citizens Program", "cyber-driven systems", "cyber criminals", "cyber events", "cyber-burglar tool kits", "cyber intruders", "cyber warfare", "cyber status", "cyber resource guides", "cyber-reconstitution", "cyber assurance", "cyber literacy", "cyber dimensions", "cyber sensors and intrusion detection systems", "cyber situation understanding", "cyber systems command and control tools", "cyber defense strategies", "cyber crisis", "cyber disruptions" and "cyber nation".

[209] Ibid. p. 146.

unresolved, but from the tone, context and the two definitions one could argue that cyber in the document has shifted from a broad concept as intended by Arquilla and Ronfeldt to a narrow concept related to computer and network mediated issues. The focus of these documents was national security in general and not warfare in specific, however, the military soon adopted the narrow concept of cyberwar.

As a consequence of the policy with regard to the protection of critical information systems, the Department of Defense created the Joint Taskforce for Computer Network Defense (CND) in 1998.[210] Computer Network Attack (CNA) was soon added to the ambit of the Taskforce in 2001. When the United States were starting to focus on attack, the North Atlantic Treaty Organisation (NATO) first addressed the issue of cyber defence in 2002; participants of the NATO Prague Summit decided to "strengthen our capabilities to defend against cyber attacks".[211] Whilst NATO was pondering on cyber defence, the United States renamed the Computer Network Defense Taskforce to "Joint Taskforce Computer Network Operations" in order to incorporate both the offensive and defensive capabilities.[212]
In the same year the Joint Taskforce Global Network Operations was established, the mission of which was "to direct the operation and defense of the global information grid throughout the full spectrum of war fighting, intelligence and business missions within the department".[213]

The 2004 National Military Strategy of the United States mentioned cyberspace in the context of conventional war fighting domains, it stated, "the Armed Forces must have the ability to operate across the air, land, sea, space and cyberspace domains of the battlespace".[214] Cyberspace was, however, only explicitly earmarked as fifth warfighting domain in 2006 and defined as "a man-made domain" that is "characterised by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures".[215] Thus, 2006 marked the militarisation of cyberspace in the United States and other States have followed since.

[210] U.S. Department of Defense, "Joint Task Force on Computer Network Defense Now Operational," *Office of the Assistant Secretary of Defense (Public Affairs)*, no. 658-98 (December 30, 1998).

[211] North Atlantic Council, *The Prague Summit and NATO´s Transformation: A Reader's Guide* (Brussels: NATO Public Diplomacy Division, 2003). p. 74.

[212] Harry D. Raduege, "Future Defense Department Cybersecurity Builds on the Pas," *Signal* (February, 2008). p. 120; United States Strategic Command, "Fact File: Joint Task Force - Computer Network Operations," iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm (accessed November 14, 2013).

[213] Michael J. Carden, "Cyber Task Force Passes Mission to Cyber Command," defense.gov/News/NewsArticle.aspx?ID=60755 (accessed November 14, 2013).

[214] The Joint Chiefs of Staff, The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow (Washington, DC: Office of the Chairman, 2004). p. 18.

[215] The Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, DC: Office of the Chairman, 2006b). p. 3.

3.3.5 Sub-conclusion

This section has aimed to answer the sub-question: *What is cyber and how has it developed over time?* In order to answer this question this section has traced the development of 'cyber' from its etymological origins to its use in governmental publications in the 2000s. This section has first described the origin of cyber in antiquity where it was used to refer to the government element in 'cybernetics (sub-section 3.3.1). From the 1960s to the 1980s the meaning of cyber started to change as it was used in fiction and was used to describing the ethereal world of data known as cyberspace (sub-section 3.3.2). In that same timeframe the security of computers and networking became an issue in politics due to series of pivotal events resulting in the term 'hacker' entering mainstream media and specific information security policy. In the 1990s the concept of information warfare and its overarching concepts of cyberwar and netwar were developed (sub-section 3.3.3). The 2000s marked the shift to the use of the 'cyber' prefix for virtually everything related to information or computer security (see sub-section 3.3.4). This narrow approach was also adopted by the military where cyberspace was dubbed the fifth warfighting domain.

Analysis of the development of 'cyber' demonstrates that it has been used in a variety of contexts and the meaning of 'cyber' is understood differently in those contexts. 'Cyber' within the context of informationised society can be characterised as a construct epitomising the developments within a broad range of issue areas (e.g. academia, fiction, politics, military) in the time frame from 350 BC to the 2000s resulting in its contemporary usage being related to a broad range of security aspects associated with networking in informationised society. Due to the implicit adoption of the narrow perspective on 'cyber' in the late 1990s and 2000s, affixing 'cyber' to a word or using it as a noun implies a relation to cyberspace, capabilities making use of cyberspace, or other novel phenomena associated with computing, networking and/or virtualisation. Due to the prominent use of 'cyber' in publications of a security, political or military character, 'cyber' is often associated with information security and/or national and international security.

This thesis will use 'cyber' (as noun with single quotation marks) to relate to the broad development of the construct in various fields (academia, fiction, politics, military). Whereas affixing cyber to a noun, i.e. using it as a prefix, implies a relation to cyberspace for the purpose of this research. For instance, cyber-attacks are attacks in or through cyberspace and cyber capabilities are capabilities related to cyberspace. In order to understand cyber as a prefix a precise definition of cyberspace is needed, this thesis will cover this subject in depth in chapter four. This chapter will only use the 'cyber' form.

3.4 Influence of informatisation and ‘cyber’ on power

As mentioned in sub-section 3.1.1, the power framework discussed in chapter one is technology agnostic. This sub-section will confront the power framework with informationised society and ‘cyber’ as these developments provide the context for and impact the notion of power in contemporary society. This section will do so by answering the following sub-question: *What is the impact of society’s informatisation and rise of ‘cyber’ on the power concepts and dimensions?*

This section will not discuss the approaches to power (i.e. the relational power and power as resource), as little has changed in the realm of theories on and approaches to power. Instead sub-section 3.4.1 will start with discussing the influence of informatisation and ‘cyber’ on Barnett and Duvall’s power concepts (compulsory, institutional, structural and productive). Then sub-section 3.4.2 will touch upon the effects of informatisation and ‘cyber’ on the scope of power (anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation). After that, sub-section 3.4.3 will reflect on the domain dimension of power, in other words, describe changes in potentially relevant actors in informationised society. As fourth, sub-section 3.4.4 will expand on the influence of informatisation and ‘cyber’ on the means dimension of power (political, informational, economical, military instruments and civil capacities). Lastly, these insights will be adjoined in sub-section 3.4.5 where the sub-question will be answered.

3.4.1 Power concepts

The power framework as described in chapter two has used the power concepts of Barnett and Duvall to describe the various ways through which power can be conveyed (i.e. compulsory, institutional, structural and productive). This sub-section will aim to describe the effect of informatisation and ‘cyber’ on these power concepts. In doing so, this sub-section will use insights from Betz and Stevens who “have applied Barnett and Duvall’s taxonomy of power concept to analyse cyber power”.[216] These insights will be adjoined with Joseph Nye’s approach “who drew on the faces of power discussion and infused it with his hard and soft power theory to analyse power in cyberspace.”[217]

3.4.1.1 Compulsory power

Compulsory cyber power (i.e. power in or through cyberspace) according to Betz and Stevens includes the following activities: (1) control machines and networks to “change behaviours of an individual or collective human actor”; and (2) “deployment of non-material resources in order to directly affect the actions of others [...] such as the threat of military action or economic coercion”.[218] Joseph Nye similarly distinguishes two types of

[216] Jelle van Haaster, “Assessing Cyber Power” (Tallinn, NATO CCD COE, 2016). p. 14.

[217] Ibid. p. 14.

[218] Betz and Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power. p. 46.

activities under the first face of power (i.e. compulsory power), namely: (1) hard power such as "denial of service attacks, insertion of malware, SCADA disruptions, arrests of bloggers"; and (2) soft power such as an "information campaign to change initial preferences of hackers, recruitment of members of terrorist organisations".[219]

3.4.1.2 Institutional power

Betz and Stevens divide institutional cyber power into two categories: (1) "set norms and standards of a variety of institutions impacting upon users' behaviours" and (2) to "influence the opinions of foreign audiences through media institutions".[220] Examples of institutional power include the United States' control over the Internet Corporation for Assigned Names and Numbers (ICANN) and China and Russia's exercise of institutional power through the International Telecommunication Union (ITU) and Shanghai Cooperation Organisation (SCO).[221] Institutional power relates to the third face of power in cyberspace domain as described by Nye, he lists hard and soft power aspects of the third face of power as follows: (1) hard power includes "activities such as firewalls, filters, and pressure on companies to exclude some ideas" and (2) soft power though "ISPs and search engines self [monitoring], ICANN rules on domain names [and] widely accepted software standards".[222]

3.4.1.3 Structural power

Structural cyber power revolves around the way "cyberspace determines [...] structural positions" of actors in cyberspace.[223] As Nye does not refer to structural power this subsection will focus on Betz and Stevens approach to structural power. Betz and Stevens state, "it is probably not possible to conclude that cyberspace does any one thing with respect to international order", hence they "ask whether cyberspace perpetuates existing structural forms or facilitates the creation of new ones".[224] They conclude that "the competitive logic of capitalism is reproduced through transformed structures of cognitive, cooperative and communicative labour mediated to a large degree by cyberspace",[225] thus whilst the logic remain the same, particular elements are transformed. Betz and Stevens argue that there is a novel mode of "civic networks, structured around the tools, opportunities and forums of cyberspace, [which] can outflank and on occasions replace the hierarchical structures of the industrial period."[226] Thus, considering that the competitive logic remains the same but that there are also new ways of organisation: "structural cyber power therefore works both to maintain the status quo and to disrupt it".[227] For instance, the use of social-media on the one hand can facilitate disruption of the status-quo by fuelling and organising protests

[219] Nye, *Cyber Power.* p. 7.

[220] Betz and Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power. p. 47.

[221] Ibid. p. 47.

[222] Nye, *Cyber Power.* p. 7.

[223] Betz and Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power. p. 48.

[224] Betz and Stevens, Cyberspace and the State: Toward a Strategy for Cyber-Power. p. 49.

[225] Ibid.

[226] Ibid.

[227] Ibid.

against a State, as was the case in the Arab Spring.[228] On the other hand it can also be used to control or repress other actors and making them accept their position in the structure, for instance using social-media to control citizens.[229]

3.4.1.4 Productive power

Betz and Stevens argue that cyberspace "is ideally suited to the performance and transmission of a productive cyber-power."[230] Productive power is manifested "through the discursive construction of cyberspace threat actors" and "the promotion and dissemination of existing and emerging narratives and world-views".[231] Nye also notes two forms of power within the third face of power in the cyber domain, namely: hard power, including "threats to punish bloggers who disseminate censored material"; and soft power involving "information to create preferences (e.g. stimulate nationalism and 'patriotic hackers'), develop norms of revulsion (e.g. child pornography)".[232]

Joseph Nye's forms of cyber power	Betz and Stevens' forms of cyber power
First face (A induces B to do what B would otherwise not do) ***Hard power*** (Distributed) Denial of service attacks Insertion of malware SCADA/ICS disruptions Arrests of bloggers Soft power Information campaigns *Second face (agenda control)* ***Hard power*** Firewalls, filters, and pressure to exclude some ideas Soft power Self-monitoring of ISPs and search engines ICANN rules on domains Software standards *Third face (preference shaping)* ***Hard power*** Threats to punish bloggers Soft power Information to create preference Develop norms of revulsion	Compulsory (direct coercion) Control of machines or networks Deploying non-material resources (e.g. threats) **Institutional (via institutions)** Set norms and standards Influence foreign audiences via media institutions **Structural (influencing structures)** Changing structures (e.g. hierarchical to networked) **Productive (constitution of the subject)** Reproduce and reinforce existing discourses Construct and disseminate new discourses

Table 2 Forms of cyber power

[228] See: Paolo Gerbaudo, *Tweets and the Streets: Social Media and Contemporary Activism* (London: Pluto Press, 2012). pp. 2-5.

[229] See for example: Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011).pp. 143-178.

[230] Ibid. p. 50.

[231] Ibid. p. 52.

[232] Nye, *Cyber Power*. p. 7.

3.4.1.5 *Sub-conclusion*

This sub-section has set out to describe what the effect is of informatisation and the rise of 'cyber' on the power concepts described in chapter two. Betz & Stevens and Nye do not contest the notion of 'power concepts' nor their theoretical foundations in the 'faces of power' discussion. The theoretical construct remains the same; the authors only add cyberspace domain specific remarks. This is a logical consequence of affixing 'power' with cyber, as this results in 'cyber power', which is a very specific form of power in a specific context allowing the authors to make specific suggestions as to what would constitute power in cyberspace. Thus, informatisation and the rise of 'cyber' do not impact the theoretical construct of power concepts, they do affect the scope and content of the power concepts when applied to cyberspace. The scope and content changes as there are new ways of projecting power in informationised society. These novel means and methods in the specific context of cyberspace as suggested by Betz & Stevens and Nye are listed in Table 3.

3.4.2 Scope dimension

The scope dimension of power entails the objectives or ends sought after. As examples of objectives or ends the following strategic functions were used in chapter two: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation. The analysis in chapter two has shown that these strategic functions are not universally applicable, however, they do resonate within policy documents of other States. This sub-section will successively discuss the seven strategic functions and describe the effect of informatisation and rise of 'cyber' on the scope and content of these functions. The sub-sections will briefly reiterate the definition of the strategic function and their status in academia as discussed in chapter two and secondly reflect on literature marking changes in the functions due to informatisation and 'cyber'.

3.4.2.1 *Anticipation*

Anticipation was defined as function to prepare for foreseen and unforeseen developments.[233] Anticipation proved to be firmly rooted in academia: in scholarly writings the limits of human forecasting are stressed and the benefits of computed forecasting highlighted.[234] Anticipation, involving some sense of foresight, has been developing over time due to informatisation.[235] Developments in accuracy of technical forecasting of political violence in the 1990s and 2000s result in the subject being "quite well developed" in the 2010s.[236]

[233] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[234] Schrodt, Yonamine and Bagozzi, "Data-Based Computational Approaches to Forecasting Political Violence," in , 129-162. p. 131.

[235] Ibid. p. 132.

[236] Ibid. p. 132.

As a consequence of "the vast increase in the availability of data, computational power, and the resulting refinement of methodological techniques", algorithms are used in contemporary society "for all but a small fraction of the activity on financial exchanges", "weather forecasts", "public polling" in the political realm and "the assessment of athletes".[237] Similar progress in the field of anticipation or forecasting political violence, however, is expected to be much slower as "political violence is a rare event, and acts of terrorism in otherwise peaceful situations [...] are amongst the rarest."[238] There are various successes in this field, for instance by the Central Intelligence Agency's (CIA) Political Instability Task Force (PITF) which claimed to have 'substantially achieved the objective' of developing "a model capable of forecasting its occurrence accurately and with a two-year lead time."[239] Similarly DARPA's Word-Wide Integrated Crisis Early Waring System (ICEWS) uses "a mixed-model, multi-hypothesis approach [...] to enable users to more fully exploit the available information and accurately forecast [...] stability measures".[240] There are also various initiatives by non-governmental organisations that are increasingly interested in "technical political forecasting" of which two examples are "the SwissPeace FAST project and the Armed Conflict Location and Event Data (ACLED) project".[241]

These developments show a broad movement towards technological, computational or data-driven political forecasting. Due to an increasing amount of "information sources available for strategic analysis on the Internet"[242] and increasing understanding of the challenges of data-driven forecasting,[243] it is likely that forecasting and thus the feasibility of anticipation will reach new levels of maturity in the coming years due to advances in informatisation.

3.4.2.2 Prevention

Prevention was characterised as taking active steps to prevent a threat occurring to State interests. Prevention relates to the academic debate of the feasibility and viability of conflict prevention.[244] Informatisation and 'cyber' led the United Nations Development Office (UNDP) to conclude: "opportunities for applying digital tools such as mobile technology and social media for conflict prevention are increasing rapidly, paralleling the speed in

[237] Ibid. p. 155.

[238] Ibid. p. 155.

[239] Jack A. Goldstone et al., "A Global Model for Forecasting Political Instability," *American Journal of Political Science* 54, no. 1 (2010), 190-208. p. 204.

[240] Janet E. Wedgwoord, Alicia Ruvinsky and Timothy Siedlecki, "What Lies Beneath: Forecast Transparency to Foster Understanding and Trus in Forecast Models," in *Advances in Human Factors and Ergonomics Series*, eds. Gavriel Salvendy and Waldemar Karwowski (New York: CRC Press, 2010), 64-73. p. 65.

[241] Patrick T. Brandt, John R. Freeman and Philip A. Schrodt, "Real Time, Time Series Forecasting of Inter- and Intra-State Political Conflict," *Conflict Management and Peace Science* 28, no. 1 (2011), 41-64. p. 59.

[242] Ibid. p. 59.

[243] Schrodt, Yonamine and Bagozzi, "Data-Based Computational Approaches to Forecasting Political Violence," in , 129-162. p. 156.

[244] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

which access to technology is expanding."[245] The main technologies considered in this regard are: "cell phones, social media, crowdsourcing, crisis mapping, blogging and big data analytics".[246] In a 2013 report their usefulness was assessed in five case studies.[247] The following paragraph will list the seven lessons learned from the case studies in Africa, Asia, Latin America in settings of criminal violence, election related violence, armed conflict, short-term crisis as listed in the report, as these are indicative of the effect of informatisation on conflict prevention.

The first lesson learned is that "new technologies have the potential to make huge contributions to violence- and conflict-prevention efforts, but they are no panacea for holistic solutions."[248] Therefore, actors "should examine all the tools at their disposal [e.g. preventive diplomacy, governance reforms, and economic initiatives] when designing prevention initiatives, not just technological tools."[249]A second lesson learned is that context matters, "[technology penetration and use, literacy levels,] demographics, rural versus urban contexts, gender considerations, and generational factors" all impact the potential receptiveness and usefulness of a technological initiative for conflict prevention in a specific context.[250] The third lesson learned is that actors wishing to use technology should be aware of the "possible negative and knock-on effects emerging from their use of specific technologies."[251] Fourthly, "the application of new technological tools to prevention efforts at the local level works best when integrated into existing civil society initiatives."[252] As fifth, when looking to bridge the warning-response gap, technology works best to share information horizontally (to connect "warners and responders") than vertical (government-citizen) due to the slow decision-making process within governments.[253] As sixth, there should be consensus "around questions of privacy, access, and use of digital data in any given initiative" in order to make the "prevention efforts more legitimate in the eyes of affected communities".[254] Lastly, partnering between

[245] United Nations Development Programme, *Issue Brief: Using Technologies for Conflict Prevention* (New York: United Nations Development Programme,[2012]). p. 1.

[246] Francesco Mancini and Marie O'Reilly, "New Technology and the Prevention of Violence and Conflict," *Stability : International Journal of Security and Development* 2, no. 3 (2013), Art. 55. p. 2.

[247] Francesco Mancini, ed., *New Technology and the Prevention of Violence and Conflict* (New York: International Peace Institute, 2013).

[248] Mancini and Marie O'Reilly, "New Technology and the Prevention of Violence and Conflict." Art. 55. pp 4-5. See also: Anne Kahl and Puig Larrauri, "Technology for Peacebuilding," *Stability: International Journal of Security & Development* 2, no. 3 (2013). pp. 1-3. Tim Kelly and David Souter, *The Role of Information and Communication Technologies in Postconflict Reconstruction* (Washington, D.C.: World Bank, 2014). pp. 9-13. Mark Nelson Quihuis and Karen Guttieri, "Peace Technology: Scope, Scale, and Cautions," *Building Peace*, no. 5 (2015), 14-16. pp. 15-16.

[249] Ibid. p. 5.

[250] Mancini and Marie O'Reilly, "New Technology and the Prevention of Violence and Conflict." p. 5.

[251] Ibid. p. 5.

[252] Ibid. p. 6.

[253] Ibid. p. 6.

[254] Ibid. p. 7.

"international donors, governments, the private sector, and civil society proved more effective".[255]

As the editor of the report on new technology and the prevention of conflict notes: "At this early stage in the consideration of new technology's role in preventing violence and conflict, it is only possible to sketch out very tentative conclusions."[256] The lessons learned from the uses of new technology indicate that it is not a silver bullet; many similar issues arise as with traditional conflict prevention. Thus, informatisation and the rise of 'cyber' do impact conflict prevention, however, technology has its limits.

3.4.2.3 Deterrence

Deterrence was defined in chapter two as discouraging activities that conflict with the interests of the State or the international rule of law by holding out the prospect of retaliatory measures.[257] The debate surrounding deterrence was characterised as experiencing a reconsideration of the value of deterrence in the 21st century due to informatisation and the rise of 'cyber'. In other words, from the outset it is evident that deterrence is impacted by developments in the 21st century. This sub-section will discuss the effects of informatisation on specific concepts of deterrence and dissuasion, namely: deterrence by punishment, deterrence by denial, dissuasion through entanglement, and dissuasion through norms and taboos. By discussing these concepts generally associated with deterrence many of the developments with deterrence in informationised society are unveiled.

3.4.2.3.1 Deterrence by punishment

Deterrence is "usually said to have two components: deterrence by denial (the ability to frustrate the attacks) and deterrence by punishment (the threat of retaliation)".[258] Libicki places cyber deterrence by punishment responses by States along a ladder of belligerence as follows, from less belligerent to more belligerent: diplomatic and economic, cyber, physical force, and nuclear force.[259] In discussing deterrence by punishment Libicki points to three issues: (1) attribution, (2) feasibility of the response; and (3) feasibility of repeatability.

Certain difficulties arise with attribution in the realm of cyber deterrence. Before being able to retaliate (punish), "one should know who attacked", as "hitting the wrong person back not only weakens the logic of deterrence [...] but makes a new enemy."[260] An retaliatory attacker wishing to deter the opponent via punishment has to "to be convinced that the attribution is correct" as due to myriads of obfuscation techniques and general characteristics of cyberspace discerning and attributing an attack is notoriously difficult

[255] Ibid. p. 7.

[256] Ibid. p. 8.

[257] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[258] Libicki, Cyberdeterrence and Cyberwar. p. 7.

[259] Ibid. p. 29.

[260] Ibid. p. 41.

and could easily be misattributed.[261] Besides convincing nationally, the retaliator has to convince "third parties that the attribution is correct", as these "may not even be convinced that the retaliator was really attacked or had struck back for unrelated reasons".[262] Some have provided an alternative view to the binary approach – an event is either attributable or not – to the 'attribution problem' and have argued that attribution is "not binary, but measured in uneven degrees, it is not black-and-white, yes-or-no, but appears in shades."[263] This notion combined with developments in the field of technologically attributing events (e.g. via artificial intelligence) results in the 'attribution problem' losing some of its importance.[264]

As to the second issue, feasibility of the response, Libicky points to the limits of assessing the effect of a retaliatory measure in cyberspace due to interconnection of systems, networks and processes. Deterrence by punishment "requires the ability to hold something at risk" as in cyberspace it is sometimes unknown what targets are vulnerable and what the recovery time is, "it is difficult to know, much less promise, what damage retaliation can wreak."[265] Also, the retaliatory attack may go unnoticed and therefore fail its purpose (deterrence) or come to late and hence create other ambiguities.[266] Thus, difficulties in feasibility of threatening with or conducting a retaliatory response result in deterrence by punishment being complicated in the cyber realm.

The third issue Libicki raises is the feasibility of repeatability. Repeatability may be necessary in the context of cyber deterrence in the face of an attacker not being deterred, in other words the retaliator has to retaliate once more. Libicki argues that in response to the initial retaliatory strike defences may be hardened (e.g. patches applied, personnel trained, vulnerabilities mitigated), as a consequence, it may gradually become harder to strike the attacker. According to Libicki, together these three issues result in "deterrence based on threats of punishment will not play as large a role in strategies for cyberweapons as it does for nuclear weapons."[267]

[261] Libicki, Cyberdeterrence and Cyberwar. p. 42; See also: P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014). p. 73; David Betz and Tim Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-Power.* p. 32; W. Earl Boebert, "Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy" (Washington, D.C., National Academies Press, June 10 2011). pp. 43-50; Nicholas Tsagourias, "Cyber Attacks, Self- Defence and the Problem of Attribution," *Journal of Conflict and Security Law* 17, no. 2 (2012), 229-244. pp. 233-236. Hal Berghel, "On the Problem of (Cyber) Attribution," *Computer* 50, no. 3 (2017), 84-89. pp. 84-87; Eric Nunes et al., "Argumentation Models for Cyber Attribution," (2016). p. 1.

[262] Libicki, Cyberdeterrence and Cyberwar. p. 42.

[263] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* (2014), 1-34. p. 7.

[264] See for instance: Eric Nunes et al., *Artificial Intelligence Tools for Cyber Attribution* (New York: Springer, 2018).; Eric Nunes et al., "Argumentation Models for Cyber Attribution," (2016).; Li Qiang et al., "A Reasoning Method of Cyber-Attack Attributions Based on Threat Intelligence," *International Journal of Computer and Systems Engineering* 10, no. 5 (2016).

[265] Libicki, Cyberdeterrence and Cyberwar. p. 52.

[266] Ibid. p. 52.

[267] Joseph S. Nye, "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (2016), 44-71. p. 55.

3.4.2.3.2 Deterrence by denial

Deterrence by denial seeks “to lower the benefit of an action rather than raise the cost” as is the aim of deterrence by punishment.[268] The purpose is “making a target so difficult to attack that it is not worth the adversary trying to do so”.[269] According to Nye, “deterrence by denial (which is indifferent to attribution) has regained some of its importance” in the context of cyberspace.[270] Or as others have argued, with attribution as primary limiting factor in cyberspace, deterrence by denial “may be more viable than deterrence by retaliation [i.e. punishment]”.[271]

Deterrence by denial in the cyber realm involves “continuing investment in technology along with policies and procedures designed to minimise the vulnerabilities and reduce the potential attack surface.”[272] More concretely these measures could include: “hardening targets; controlling access to facilities; screening exits; deflecting offenders; controlling tools; strengthening surveillance; using place managers; reducing peer pressures; and so forth.”[273] As noted by Denning, considering these measures, “deterrence by denial is practiced every day in cyberspace via cyber security mechanisms and practices”.[274] Besides these technical measures, “deterrence depends on perceptions, and different parts of complex organisations [...] often perceive the same actions [...] from different perspectives”,[275] hence “understanding the cognitive framework of an adversary” is required to successfully deter various attackers.[276] In other words, an actor wishing to deter by denial should also “ensure an effective approach to messaging and signalling”, making actors aware of the costs involved in attacking the defender.[277]

3.4.2.3.3 Entanglement

Deterrence by punishment and deterrence by denial epitomize the traditional approaches to deterrence. Entanglement and norms could be considered to fall within the scope of broad deterrence, or alternatively: other means of dissuasion. The concept of entanglement “refers to the existence of various interdependencies that make successful attack simultaneously impose serious costs on the attacker as well as the victim.”[278] Entanglement

[268] Liam Nevill and Zoe Hawkins, *Deterrence in Cyberspace: Different Domain, Different Rules* (Barton: The Australian Strategic Policy Institute,[2016]). p .15.

[269] Ewan Lawson, “Deterrence in Cyberspace: A Silver Bullet Or a Sacred Cow?” *Philosophy & Technology* (2017). p. 2.

[270] Nye, “Deterrence and Dissuasion in Cyberspace,” , 44-71. p. 56.

[271] “Cyber Conflict and Deterrence.” *Strategic Comments* 22, no. 7 (2016), iii-v. p. iv; See also: Kenneth Geers, “The Challenge of Cyber Attack Deterrence,” *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 3 (2010), 298-303. pp. 299-301.

[272] Lawson, “Deterrence in Cyberspace: A Silver Bullet Or a Sacred Cow?” . p. 5.

[273] Nye, “Deterrence and Dissuasion in Cyberspace.” 44-71. p. 56; Referring to: Bruce Schneier, *Liars and Outliers: Enabling the Trust that Society Needs to Thrive* (Indianapolis: John Wiley, 2012). p. 130.

[274] Dorothy E. Denning, “Rethinking the Cyber Domain and Deterrence,” *Joint Force Quarterly* 77, no. 2nd Quarter (2015), 8-15. p. 14.

[275] Nye, “Deterrence and Dissuasion in Cyberspace.” 44-71. pp. 57-58.

[276] Lawson, “Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?” p. 2.

[277] Ibid. p. 4.

[278] Nye, “Deterrence and Dissuasion in Cyberspace.” 44-71. p. 58.

dissuades potential attackers by the following logic: “if there are benefits to the status quo and its continuation, a potential adversary may not attack – even if its attack is not defended against and there is no fear of retaliation – because it has something highly valuable to lose, and this contributes to deterrence.”[279] The criticality of the Internet and information technologies for societies “may increase general incentives for self-restraint” and result in States desiring systemic stability of the Internet resulting in a re-evaluation of the costs and risks of cyber operations to the extent of ‘self-deterrence’.[280]

3.4.2.3.4 Norms

Norms and taboos are a second form of dissuasion, based upon the notion that “normative considerations can deter actions by imposing reputational costs that can damage an actor’s soft power beyond the value gained from a given attack.”[281] Nye points the use of nuclear weapons, poisons, chemical weapons and biological warfare as examples of development of normative taboos.[282] Should evidence leak regarding the development or use of these means, the actor would “face widespread international condemnation”.[283] Nye argues that “normative taboos may become relevant to deterrence of some aspects of cyberattacks”, he then states that cyber arms control is not viable due to the nature of virtual nature of ‘cyber weapons’. He deems developing taboos “against certain types of targets” to be more feasible, for instance not using “cyber instruments against civilian facilities in peacetime”.[284] Potential multilateralisation of such norms may increase “the reputational costs of bad behavior” in cyberspace, for the first steps in norm development in cyberspace Nye refers to the United Nations Group of Governmental Experts (GGE) report regarding the use of cyber capabilities.[285]

3.4.2.3.5 Deterrence: in sum

In conclusion, this sub-section has aimed to describe the effects of informatisation and the rise of ‘cyber’ on deterrence. In order to do so the following aspects related to deterrence were discussed: (a) deterrence by punishment; (b) deterrence by denial; (c) dissuasion through entanglement; and (d) dissuasion through norms and taboos. The first two are traditionally, i.e. during the Cold War, included under the narrow concept of deterrence. Deterrence by punishment is deemed infeasible in the context of cyber operations due to the difficulty of attribution, complexity of retaliation, and doubtful repeatability (see 3.4.2.3.1). More contemporary scholarly writings suggest, however, that attribution is more feasible than suggested by, for instance, Libicki. Deterrence by denial is regaining attention as way of deterring potential adversaries (see 3.4.2.3.2), however, in a realm were “offense dominates defense” relying entirely on denial strategies is costly

[279] Nye, “Deterrence and Dissuasion in Cyberspace.” 44-71. p. 60.

[280] Ibid. p. 58.

[281] Ibid. p. 60.

[282] Ibid. p. 61.

[283] Ibid. p. 61.

[284] Nye, “Deterrence and Dissuasion in Cyberspace.”. p. 61.

[285] Ibid. p. 62.

in itself.[286] As the traditional concept of deterrence is clearly undergoing revaluation, elements from the broad concept of deterrence may prove most useful in the context of cyberspace. Two examples of these means of dissuasion were discussed: entanglement and norms. Entanglement results in self-deterrence (see 3.4.2.3.3), as an attack in cyberspace, a collection of interdependent systems, will likely impose costs on both the attacker and the victim. Norms and consequently taboo development similarly dissuades attackers due to the risk of reputational damage (see 3.4.2.3.4). Although there is progress, norm development in cyberspace is a slow process and State practices in cyberspace currently evidence all but a taboo on the use of cyber operations in inter-State affairs. Thus, informatisation and the rise of 'cyber' result in deterrence as strategic function undergoing a critical re-evaluation and consequently there are no clear-cut answers as to the relevance of deterrence in this context.

3.4.2.4 Protection

In chapter two protection was defined as protecting and defending the territory and inhabitants of a State.[287] Governmental publications generally acknowledge a variety of intentional/unintentional and internal/external threats. Protection in academia was found to belong to the general debate of national security, this discussion was deemed to give a theoretical basis for the scope of protection and the dimensions that could be considered (e.g. values protected, degree of security, threats, etc.). This sub-section will evaluate the impact of informatisation and 'cyber' on the strategic function protection.

The informatisation of society and rise of 'cyber' have resulted a new distinct field of security, namely information security and many sub-fields such as cyber security. This new field of security and importance of 'connectivity' as value to be protected resulted in "a heated debate [...] about the appropriate role of nation-states in Internet governance and enhancing cybersecurity".[288] Providing security or protection is a classical governmental function, "some observers believe that growing insecurity will lead to an increased role for governments in cyberspace".[289] Various issues in the context of cyberspace affect states, such as: standard setting, crime, war, sabotage, espionage, privacy issues, content control and human rights.[290] States "want to protect the Internet so their societies can continue to benefit from it, but at the same time, they also want to protect their societies from what might come through the Internet."[291] Thus States have a somewhat paradoxical relation to cyberspace.

[286] Ibid. p. 70.

[287] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[288] Scott Shackelford and Amanda Craig, "Beyond the New'Digital Divide': Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity (Forthcoming)," *Stanford Journal of International Law* 50, no. 119 (2014). p. 2.

[289] Joseph S. Nye, "The Regime Complex for Managing Global Cyber Activities," *Global Commission on Internet Governance Paper Series* 1 (2014), 5-16. p. 6.

[290] Ibid. p. 9.

[291] Ibid. p. 7.

The role States play in information and cyber security is different from the traditional role of a State in security affairs.[292] As in the fields of "sustainability, environment [and] climate", Internet governance – spanning information and cyber security – has a multistakeholder model to decision making.[293] The reason is that "unified Internet, that's unfragmented, interconnected, interoperable, open, inclusive, secure, stable, resilient, and trustworthy" would be unachievable if only States were involved.[294] In order to achieve these goals representatives "from different groups interested in or affected by the issue" are involved such as: "civil society, government, private sector, and technical and academic communities."[295] In other words, States are not the sole actor involved in protecting cyberspace.

Although decision-making in the area of cyber security differs from traditional decision-making, for instance when protection a State's borders, actors can still take steps unilaterally to protect their interests from threats in cyberspace inside and outside their territory. States could take various protective measures, for example: adopt an active posture to "to disrupt or halt malicious cyber activity at its source";[296] invest in cyber or information security to protect information and communication systems;[297] or strengten the capabilities of other actors in so-called "cyber capacity building" measures, for instance by giving workshops, training, exchanging personnel, etc.[298]

Thus, the strategic function 'protection' has been impacted by informationised society and the rise of cyber; the scope of the protection has broadened to include the Internet or more generally connectivity. The role States play in protecting connectivity is different from traditional protection, for instance of territorial integrity, as protection of connectivity can only be reached effectively through a multistakeholder model.

[292] Robert Latham, ed., Bombs and Bandwith: The Emerging Relationship between Information Technology and Security (New York: The New Press, 2003). pp. 79-82; Paul Rosenzweig, Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World (Santa Barbara: Praeger, 2013). pp. 171-175.

[293] Virgilio Almeida, Demi Getschko and Carlos Afonso, "The Origin and Evolution of Multistakeholder Models," *IEEE Internet Computing* 19, no. 1 (2015), 74-79. p. 74.

[294] Ibid. p. 75.

[295] Ibid. p. 75.

[296] U S Department of Defense, Cyber Strategy: Summary (Washington, D.C.: U.S. Department of Defense, 2018). p. 1.; "The Pentagon's New Cyber Strategy: Defend Forward" , accessed October 27, 2018, lawfareblog.com/pentagons-new-cyber-strategy-defend-forward.

[297] See for instance: "NATO to Spend 2.6 Billion on Satellites, Cyber Security and Drones," Independent, accessed October 31, 2018, independent.co.uk/news/world/politics/nato-to-spend-three-billion-euros-on-satellites-cyber-security-and-drones-a7651966.html.; "DHS is Reshaping Federal Cybersecurity with a $1 Billion Contract," Defense One, accessed October 31, 2018, defenseone.com/business/2018/08/dhs-reshaping-federal-cybersecurity-1-billion-contract/150775/.; "Why the UK is Investing £1.9bn in Cyber Security," NewStatesman, accessed October 31, 2018, newstatesman.com/spotlight/cyber/2018/05/why-uk-investing-19bn-cyber-security.

[298] See for instance: "Global Cyber Capacity Building at a Glance," University of Oxford, accessed October 27, 2018, sbs.ox.ac.uk/cybersecurity-capacity/explore/gfce. This inventory lists approximately 160 initiatives worldwide aimed at building cyber capacities. See also: U S Department of Defense, Cyber Strategy: Summary (Washington, D.C.: U.S. Department of Defense, 2018). p. 5.

3.4.2.5 Intervention

In chapter two intervention as strategic function was defined as a function to induce a change in behaviour, most likely outside a State's territory, involving the armed forces and/or other capacities. Contrary to States' conception of intervention as 'obviously effective', the academic debate on intervention expresses that it is not obvious that intervention is effective. In academia the effectiveness of intervention is highly contested and deemed dependent of normative constraints such as the feasibility, legality and perceived legitimacy. This sub-section will reflect on the effects of informatisation and 'cyber' on the strategic function intervention.

Informatisation and the rise of 'cyber' have resulted in States using informational and/or cyber means to intervene to induce behavioural change in target actors. There are many examples of States using these means, for instance China (retaliation for embassy bombing, 1999; self-defence cyber war versus U.S. aggression, 2001), Israel (Operation Orchard, 2007; Operation Cast Lead, 2008), Russia (Second Russian-Chechen War, 1997-2001; Estonian cyber attacks, 2007; Russia-Georgia War, 2008), Iran (election fraud protests, 2009), and North Korea (DDoS versus U.S. and South Korean websites, 2009).[299] In other words, States have used and will most likely continue to use cyber means and methods for intervention into the sovereign affairs of other States. As with traditional means, assuming that these interventions are 'obviously' effective would be narrow sighted, as indicated in chapter two, there are many factors involved in the perceived effectiveness of intervention.

The academic debate on intervention stressed feasibility, legality and perceived legitimacy by States and domestic publics to be the key element defining the success of intervention. The remainder of this sub-section will briefly reflect on these three factors in relation to intervention via cyber means and methods. As mentioned in chapter two, he feasibility of intervention is "always about judging the required means to achieve a particular end" and how, how long and by whom intervention "will be implemented".[300] As evidenced by the many uses of cyber means and methods by States and the creation of cyber warfare capabilities by nation-States intervention through cyber means and methods is feasible.[301]

Chapter two defined legality as being typically understood to be specified by article 2 and 51 of the UN Charter "which firmly defend the sovereign equality for all member states, while sanctioning war only in the case [of] self-defense and threats to international peace and security".[302] The applicability of these and other legal instruments to cyber means and methods has been much debated in 2000s. This has settled to some extent by various efforts in this field such as the establishment of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of

[299] Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld*, 2nd ed. (Farnham: O'Reilly, 2012). pp. 2-4.

[300] Held and McNally, eds., Lessons from Intervention in the 21st Century: Legality, Feasibility and Legitimacy. p. 6.

[301] Carr, Inside Cyber Warfare: Mapping the Cyber Underworld. pp. 243-262.

[302] Held and McNally, eds., Lessons from Intervention in the 21st Century: Legality, Feasibility and Legitimacy. p. 6.

International Security (the 'GGE'),[303] the first Tallinn Manual[304] and the second Tallinn Manual.[305] These affirm that many international law instruments apply to cyber means and methods, and specify further how international law should be applied to particular means and methods during conflict and peacetime. The legality or illegality of cyber means and methods is based on, amongst other, the principles of "sovereignty, State responsibility, human rights, and the [laws of armed conflict], air, space and the sea".[306] Issues regarding legality such as applicability and application of legal instrument to cyber means and methods during conflict will be discussed extensively in chapter six.

Chapter two deemed legitimacy to connote "whether an intervention is regarded as acceptable and/or 'right' – be it morally, or otherwise justified".[307] In the context of cyber means and methods there is very little empirical data regarding the perceived empirical legitimacy as often cyber means and methods are supporting a broader intervention involving traditional means as well. For instance, the Russian involvement in Crimea (2014) used traditional and informational means, whilst being illegal; it could be argued that it had empirical legitimacy and effectiveness.[308] From this, however, one cannot deduce that the use of informational means impacts the legitimacy of the intervention, or the opposite, that they do not impact legitimacy. As to normative legitimacy, interventions involving cyber means and methods are subject to much concern, this is exemplified by the establishment of the GGE for instance to address this concern. Paradoxically, States are also conducting interventions using cyber means and methods to forward their interests as evidenced by the list of States conducting intervention through cyber means and methods above.[309]

In sum, the strategic function of intervention is impacted by informatisation and 'cyber'. There are novel informational and cyber means and methods for intervening abroad. The effectiveness of interventions through these new means and methods is unclear. Effectiveness is deemed to be dependent of, amongst other, feasibility, legality and legitimacy. Whilst the novel ways of intervention are feasible and the framework governing their legality is crystallising, their legitimacy or contribution to legitimacy of interventions is not settled.

[303] United Nations General Assembly, A/RES/68/243: Developments in the Field of Information and Telecommunications in the Context of International Security (New York: United Nations,[2014]).

[304] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

[305] Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

[306] Ibid. p. 1.

[307] Held and McNally, eds., Lessons from Intervention in the 21st Century: Legality, Feasibility and Legitimacy. p. 82.

[308] Ibid. p. 76.

[309] See also: "Significant Cyber Incidents since 2006," CSIS, accessed May 24, 2018, csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

3.4.2.6 Stabilisation and normalisation

Stabilisation was defined in chapter two as "establishing security in a current or former conflict zone to achieve political stability and economic and social development."[310] Normalisation was defined as "restoring normal living conditions after a conflict or disaster".[311] This sub-section will discuss the impact of informatisation and cyber on both stabilisation and normalisation. These will be discussed together as the effects are almost identical and the technologies impacting the functions are similar.

The three pivotal technologies impacting stabilisation and normalisation are the Internet, mobile telephony and social networking, which in turn result in developments to be used in stabilisation and normalisation such as: communicate and engage via text messaging, instant messaging, web and social media; data mapping; and big data analytics.[312] The uses of these technologies will not be described in detail here, as this will be the subject of Chapter Four, neither will it touch upon lessons learned in using these technologies as these are similar as those described in the sub-section on prevention (see 3.4.2.2). Instead, this sub-section will make a general remark regarding the contribution of technologies to stabilisation and normalisation (or post-conflict reconstruction).

The formal adoption of using information technologies for stabilisation and normalisation is marked by the launch of the 2005 UN-report "Communication Technology for Peace".[313] In that report specific information technologies are highlighted that could serve a role during conflict stabilisation and post-conflict reconstruction. The key-authors of the 2005 report have launched an update on the progress in the field of information technologies in 2013 that cynically notes: "The assault of visualisation tools, of real-time, of data-mining, of crowdsourcing, of government 2.0; all these obscure the fact that our ability to respond to crises does not appear to improve much, year after year."[314] Where the 2005 report is marked by a sense of techno-utopianism, the 2013 reports communicates a more realistic view that "political problems cannot be solved by technological solutions, and at root most problems in [in conflict] are political in one way or another."[315]

Thus, in other words, technological advancements brought forth by informatisation have resulted in new means and methods of stabilising and normalising conflicts as the 2005

[310] Ministry of Defence (Netherlands), *Future Policy Survey: Summary and Conclusions*. p. 15.

[311] Ibid. p. 15.

[312] Zyck and M., "Preparing Stabilisation for 21st Century Security Challenges." pp. 6-7; Sanjana Hattotuwa, "Big Data and Peacebuilding," *Stability : International Journal of Security and Development* 2, no. 3 (2013). pp. 1-2; Anne Kahl and Puig Larrauri, "Technology for Peacebuilding," *Stability: International Journal of Security & Development* 2, no. 3 (2013). p. 3; Tim Kelly and David Souter, *The Role of Information and Communication Technologies in Postconflict Reconstruction* (Washington, D.C.: World Bank, 2014). pp. 42-43; Daniel Stauffacher et al., ed., *Peacebuilding in the Information Age: Sifting Hype from Reaility* (Geneva: ICT4Peace Foundation, 2011). p. 6; Daniel Stauffacher et al., *Communication Technology for Peace: The Role of ICT in Preventing, Responding to and Recovering from Conflict* (New York: The United Nations Information and Communication Technologies Task Force, 2005). pp. 23-36.

[313] Ibid.

[314] Stauffacher et al., ed., Peacebuilding in the Information Age: Sifting Hype from Reaility. p. 41.

[315] Ibid. p. 41.

report notes. These new means and methods, however, are not the ultimate solution to achieving a stabile and normal situation – as nearly ten years of using information technologies in these contexts has evidenced according the 2013 report. Technology is only one aspect of a complex whole comprising many political, informational, military, economical and civil factors.

3.4.2.7 Sub-conclusion

This sub-section has reflected on the impact of informatisation and rise of cyber on the seven strategic functions by subsequently discussing these in sub-sections 3.4.2.1 to 3.4.2.6. The common denominator is that the developments described in section 3.2 (informatisation) and section 3.3 (rise of cyber) impact the strategic functions. The scope of the strategic functions, however, is still very similar. There are no indications in literature giving rise to a new distinct form of function not included in the ambit of the strategic functions or the decline of a specific strategic function. The content and dynamics of the functions does change. The impact of informatisation and rise of cyber can best be characterised as resulting in a re-evaluation of the content of strategic functions and how new technological means and methods can assist in achieving the desired outcome. As demonstrated by the theoretical literature review on informatisation's ramifications on strategic functions, there is an on-going debate on this subject in most areas, hence the re-evaluation is well underway. There are, however, no clear-cut answers yet as to what exactly the contribution of new technologies and dynamics is to the scope of power in international relations.

3.4.3 Domain dimension

Domain is one of the accepted power dimensions and refers to the actors subject to the influence attempt.[316] Informatisation and the rise of 'cyber' has affected the way types of actors are able of influencing each other. As to the notion of actors in informationised society Nye notes: "What is distinctive about power in the cyberdomain is not that governments are out of the picture, as the early cyberlibertarians predicted, but that different actors possess different power resources and that the gap between state and nonstate actors is narrowing in many instances."[317] This sub-section will briefly reflect on the effect of informatisation and rise of 'cyber' on State and non-State actors.

3.4.3.1 State actors

State actors enjoy sovereign rights over their territory, as the physical infrastructure constituting the basis of cyberspace is often located on a State actor's territory, hence a State actor has considerable influence over cyberspace. This sovereign control over cyberspace's physical infrastructure and the access to vast resources is what still distinguishes a State from a non-State actor. This allows a State actor to, for example,

[316] Baldwin, "Power and International Relations." p. 180; Guzzini, "Structural Power: The Limits of Neorealist Power Analysis." p. 453.

[317] Nye, The Future of Power. p. 132.

"subsidize infrastructure, computer education, and protection of intellectual property that will encourage (or discourage) the development of capabilities within their borders"; "exercise legal coercion and control"; "exert its power extraterritorially" for instance through enforcing privacy standards; and "carry out offensive cyber attacks".[318] Some techno-deterministically foretold the decline of the State actor due to informatisation, however, it turned out that "some aspects of the information Revolution help the small; but some help the already large and powerful. Size still matters."[319]

3.4.3.2 Non-State actors

Nye divides non-State actors in (a) actors with highly structured networks and (b) individuals with lightly structured networks.[320] Examples of the first category are transnational corporations, criminal organisations, and terrorist organisations. Large corporations often "have huge budgets, skilled human resources, and control of proprietary code that give them power resources larger than those of many governments" (e.g. Microsoft, Apple, Amazon, or Google).[321] These corporations "have strong incentives to stay compliant with local legal structures" such as "preserving their legal status as well as their brand equity".[322] Criminal organisations, a second type of highly structured network non-State actor, whether through quick operations or prolonged transnational campaigns, are also potent players within cyberspace. The gains of cybercrime are estimated to be $375-$575 billion per year,[323] dwarfing the size of the nominal GDPs in many States.[324] As third, terrorist organisations continue to be influential actors, however, "from a terrorist perspective, cyber attacks appear much less useful than physical attacks: they do not fill potential victims with terror, they are not photogenic, and they are not perceived by most people as highly emotional events."[325] Whilst not using it for offensive cyber activities, information technologies such as the Internet, (social-)networking and mobile telephony have "become a crucial tool that allows [terrorist organisations] to operate as networks of decentralised franchises, create a brand image, recruit adherents, raise funds, provide training manuals, and manage operations."[326] Thus there are various actors with

[318] Nye, *The Future of Power*. pp. 133-135.

[319] Ibid. p. 117.

[320] Nye, "The Regime Complex for Managing Global Cyber Activities," , 5-16. pp. 136-138.

[321] Nye, The Future of Power. p. 136.

[322] Ibid. p. 137.

[323] Center for Strategic and International Studies (CSIS), *Net Losses: Estimating the Global Cost of Cybercrime* (Washington, D.C.: Center for Strategic and International Studies (CSIS),[2014]). p. 2.

[324] The World Bank, "GDP (Current US$)," data.worldbank.org/indicator/NY.GDP.MKTP.CD?year_high_desc=true (accessed July 25, 2017).

[325] Irving Lachow, "Cyber Terrorism: Menace Or Myth?" in *Cyber Power and National Security*, eds. Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz, 1st ed. (Dulles: National Defense University Press, 2009), 437. p. 447. See also: Ben Saul and Kathleen Heath, "Cyber Terorism," in *Research Handbook on International Law and Cyberspace*, eds. Nicholas Tsagourias and Russell Buchan (Cheltenham: Edward Elgar Publishing, 2015), 147-167; Counter-Terrorism Implementation Task Force, *Report of the Working Group on Countering the use of the Internet for Terrorist Purposes* (New York: United Nations,[2009]). §92.

[326] Nye, The Future of Power. p. 138. See also: United Nations Office on Drugs and Crime, *The use of the Internet for Terrorist Purposes* (New York: United Nations,[2012]). pp. 3-11; Howard Rheingold, *Smart Mobs: The Next Revolution* (New York: Basic Books, 2002). pp. 157-182; Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in*

highly structured networks who can rival or at least contest States more easily due to informatisation and cyber.

The second category of non-State actors are individuals with lightly structured networks; "individuals can easily play in the cyberdomain because of the low cost of investment for entry, virtual anonymity, and ease of exit."[327] This category in informationised society has come to include for example hacktivists; black-, grey- or whitehat hackers; hacker groups; script kiddies and insider threats (e.g. disgruntled employees, financially motivated thieves, and employees causing unintentional damage.[328] Whilst this category of non-state actors access to resources is very limited compared to State or large corporations, the individual actor does enjoy asymmetric advantages. The individual actors can be subjected to legal coercion; however, they are not easily caught due to obfuscation techniques and the complexity of attribution in cyberspace in general. These individual actors can wreak havoc at little cost in "easily disrupted complex systems, political stability, and reputational soft power" of larger actors. [329] Examples of system disruption by individual actors with lightly structured networks include campaigns conducted by Lulz Security (LulzSec),[330] Anti Security (AntiSec),[331] and the many large and small Anonymous campaigns against governments and large corporations.[332] Examples of disruption of political stability and reputational damage include the WikiLeaks,[333] Snowden,[334] and Manning revelations[335] and the resulting debates.[336]

the Inforamtion Age (London: Praeger Security International, 2009). pp. 207-211; Marc Sageman, *Leaderless Jihad: Terror Networks in the Twenty-Frist Century* (Philadelphia: University of Pennsylvania Press, 2008). pp. 109-123; James P. Farwell, "The Media Strategy of ISIS," *Survival* 56, no. 6 (2014), 49-55.

[327] Nye, The Future of Power. pp. 138-139;

[328] Jason Andress and Steve Winterfeld, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, 2nd ed. (New York: Syngress, 2014). pp. 29-30. See also: National Coordinator for Security and Counterterrorism, *Cyber Security Assessment Netherlands 2017* (The Hague: National Coordinator for Security and Justice,[2017]). p. 8.

[329] Nye, The Future of Power. p. 139.

[330] Gabriella E. Coleman, Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous (New York: Verso, 2014). pp. 237-275.

[331] Ibid. pp. 277-315.

[332] Brian Feldman, "An Incomplete List of Every Person, Place and Institution upon which Anonymous has 'Declared War'," New York Magazine, nymag.com/selectall/2016/03/everything-upon-which-anonymous-has-declared-war.html (accessed July 27, 2017).

[333] WikiLeaks, "What is WikiLeaks," WikiLeaks, wikileaks.org/What-is-Wikileaks.html (accessed July 27, 2017).

[334] The Intercept, "Snowden Archive," The Intercept, theintercept.com/snowden-sidtoday/ (accessed July 27, 2017).

[335] Charlie Savage and Emmarie Huetteman, "Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files," The New York Times, nytimes.com/2013/08/22/us/manning-sentenced-for-leaking-government-secrets.html (accessed July 27, 2017).

[336] See for example: Benedetta Brevini, Arne Hintz and Patrick McCurdy, *Beyo*Nicholas J. Cull, "WikiLeaks, Public Diplomacy 2.0 and the State of Digital Public Diplomacy," *Place Branding and Public Diplomacy* 7, no. 1 (2011), 1-8.; Mark Page and J. E. Spence, "Open Secrets Questionably Arrived at: The Impact of Wikileaks on Diplomacy," *Defence Studies* 11, no. 2 (2011), 234-243; *WikiLeaks: Implication for the Future of Communications, Journalism and Society* (New York: Palgrave MacMillan, 2013). pp. 123-145; Richard Dalton, "WikiLeaks: Diplomacy as Usual," *The World Today* 67, no. 1 (2011), 12-13.

3.4.3.3 *Sub-conclusion*

This sub-section has set out to reflect on the effect of informatisation and 'cyber' on the domain dimension of power. As to the range of actors active in international relations there are no indications of new types of actors, however, there is a form of power diffusion. The State actor still is an important factor in international relations by virtue of their sovereign status and their accompanying powers and access to resources (see 3.4.3.1). The non-State actor is increasingly empowered by virtue of informatisation and the rise of 'cyber'. They have new new means and methods at their disposal to organise and influence. These actors consist of (a) non-State actors with highly structured networks such as large corporations, criminal organisations, and terrorist organisations (see 3.4.3.1); and (b) individual actors with lightly structured networks such as hacktivists, black-, grey- or whitehat hackers in hacker groups; script kiddies, insider threats (see 3.4.3.2). In other words, the domain dimension of power as a concept is unaffected by informatisation and the rise of 'cyber', however, in the context of influence attempts using informational means there are new dynamics in the to be reckoned with such as a new power configuration.

3.4.4 Means dimension

In Chapter Two the means dimension of power was defined to comprise the political, economical, informational and military instruments and civil capacities. These are broad categories incorporating the means at a State's disposal for influencing other actors. This sub-section will reflect on the influence of informatisation and cyber on the means dimension of power. As mentioned regularly in the previous sub-sections on on power concepts (3.4.1), the scope dimension (3.4.2), and domain dimension (3.4.3): there are new means and methods in informationised society. These new means, methods and dynamics influence the contents of instruments of State power and civil capacities. This sub-section will map the various means and methods discussed earlier in this chapter and categorise these within the means dimension of power (3.4.4.1). Secondly, this sub-section will reflect on the contemporary approaches to wielding instruments, means, and their informational and cyber aspects (3.4.4.2).

3.4.4.1 *Categorising means and methods*

This sub-section will use the means categorisation as presented in chapter two and adjoin it with the informational and cyber means and methods as discussed throughout this chapter.

Betz & Stevens, and Nye have advanced various cyber means and methods to be included under the ambit of cyber power (see Table 3). Mapping these means and methods to the means dimension of the power framework is fairly straightforward as demonstrated in Table 4, however, the place of certain means and methods is context specific. For instance every instrument could utilise distributed denial of service (DDoS) attacks in order to achieve a goal, in Table 4 it is categorised as an informational aspect of the military instrument as this would be the most likely place of such offensive cyber capabilities in the Dutch context.[337] In some States this is similar, however, some outsource offensive cyber capabilities to private firms, in that case mapping DDoS to civil capacities would be more logical.[338]

The means and methods discussed in sub-sections 3.4.2 and 3.4.3 also fit easily within the instrument framework. Again, some are contextual and could be categorised differently, for instance multi-stakeholder Internet governance, which could fall within the political instrument or the use of civil capacities when using civil intermediaries in the process. Although some categorisations are contextual, mapping informational and cyber aspects to the means dimension of power clearly shows that all instruments and civil capacities have information aspects to them in contemporary society.

Instrument	Means	Informational and 'cyber' aspects
Political	Wield other instruments (Carr) Internal politics (Mann) Geopolitical diplomacy (Mann) Achieving foreign policy objectives (DIME)	Sub-section 3.4.1 Set norms and standards (Betz and Stevens) Deploy non-material resources such as threats (Betz and Stevens) Sub-section 3.4.2 Internet governance in a multi-stakeholder model (protection)

[337] Melissa Hathaway and Francesca Spidalieri, *The Netherlands Cyber Readiness at a Glance* (Arlington: Potomac Institute for Policy Studies, 2017). pp. 36-38.

[338] Jennifer Valentino-DeVries, Lam Thuy Vo and Danny Yadron, "Cataloging the World's Cyberforces," The Wall Street Journal, graphics.wsj.com/world-catalogue-cyberwar-tools/ (accessed July 28, 2017).

Informational	Gain power over opinion (Carr) Unify meaning, norms and aesthetic and ritual practices (Mann) Controlled release of information (DIME) Protecting own information (DIME) Collecting information (DIMEFIL)	Sub-section 3.4.1 Reproduce and reinforce existing discourses (Betz and Stevens) Construct and disseminate new discourses (Betz and Stevens) Influence foreign audiences via media institutions (Betz and Stevens) Information campaigns (Nye) Firewalls, filters, and pressure to exclude some ideas (Nye) Self-monitoring of Internet Service Providers (ISPs) and search engines (Nye) Disseminate information to create preference (Nye) Develop norms of revulsion (Nye) Sub-section 3.4.2 Computational or data driven political forecasting (anticipation) Using mobile technology and social media for conflict prevention (prevention) Attribution of cyber operations to an actor (deterrence) Minimising vulnerabilities and reduce the attack surface (deterrence) Multilateralisation of normative constraint on the use of cyber capabilities (deterrence)
Economical	Gain autarky or influence abroad (Carr) Monopolise control over classes (Mann) Support or combat other actors (DIME) Disrupt finance of other actors (DIMEFIL)	Sub-section 3.4.3 Subsidize infrastructure Subsidize computer education
Military	Extending foreign policy (Carr) Intensive power over limited space (Mann) Extensive power over larger space (Mann) Hard coercive power (DIME) Soft attractive power (DIME)	Sub-section 3.4.1 Control of machines or networks (Betz and Stevens) (Distributed) Denial of Service attacks (Nye) Sub-section 3.4.2 Use offensive cyber capabilities to influence actors (intervention) Using information technologies to support military endeavours during stabilisation and normalisation (stabilisation and normalisation) Sub-section 3.4.3 Carry out offensive cyber attacks
Civil capacities	Legal power (DIME) Law enforcement (DIMEFIL) Administrative organisations (DIME) Education (DIME) Healthcare (DIME) Utility companies (DIME)	Sub-section 3.4.1 Influence institutions ICANN, ISPs, etc. (Nye) Software standards (Nye) Threats to punish bloggers (Nye) Sub-section 3.4.2 Using information technologies to support civil endeavours during stabilisation and normalisation (stabilisation and normalisation) Sub-section 3.4.3 Exercise legal coercion and control Enforcing privacy standards

Table 4 Mapping informational means and methods to the means dimension of power

3.4.4.2 Wielding instruments, means and their cyber or informational aspects

As mentioned in 3.4.4.1, the means and their informational and cyber aspects can be used for a variety of purposes. Depicting specific means as belonging to a specific instrument does not reflect the contemporary approach to wielding these instruments and means, however, it does serve to illustrate the consequences of informatisation and 'cyber' on the means dimension of power – the purpose of sub-section 3.4.4.1. This sub-section will reflect on the modern approaches to wielding instruments of state power by reflecting on smart power, the whole of government approach, comprehensive approach, and the JIMP-approach.

The broad, integrative approach to using State instruments has been dubbed 'smart power' in academia, epitomising "an actor's ability to combine elements of hard and soft power mutually reinforcing them, making the actor's purposes more effective and efficient".[339] Nye's hard power concept consists of the "familiar" conception that "military and economic might often get others to change their position", this type "rest on inducements ('carrots') or threats ('sticks')."[340] Soft power "rests heavily on three basic resources of an actor: its culture (in places where it is attractive to others), its political values (when it lives up to them at home and abroad), and its foreign policies (when others see them as legitimate and having moral authority)."[341] Some of these elements reside in governmental hands (e.g. the military and foreign policy), others are primarily civilian (brands, culture, etc.).

Hard and soft power are often interrelated, the smart power approach stresses that "hard power behaviour [e.g. force, coercion and threats] can produce soft power behaviour depending on the context and how they are used" and vice versa.[342] Although it has garnered criticism,[343] the concept of smart power is influential, perhaps even "greater outside academia than inside of it."[344] The criticism focuses mainly on details within the smart power concept, in doing so they fail to acknowledge the main point of smart power: integrative use of capabilities is more effective and efficient than using capabilities stand-alone. Notwithstanding that smart power has been criticised, the concept could be considered to best reflect the contemporary notion of integrative application of the instruments and means described in Table 4 in academia and governments.

[339] Juan Emilio Cheyre, "Defence Diplomacy," in *The Oxford Handbook of Modern Diplomacy*, eds. Andrew F. Cooper, Jorge Heine and Ramesh Thakur (Oxford: Oxford University Press, 2013). p. 373.

[340] Joseph S. Nye, *Soft Power: The Means to Success in World Politics* (New York: PublicAffairs, 2004). p. 5.

[341] Joseph S. Nye, "Hard, Soft, and Smart Power," in *The Oxford Handbook of Modern Diplomacy*, eds. Andrew F. Cooper, Jorge Heine and Ramesh Thakur (Oxford: Oxford University Press, 2013). p. 565.

[342] Joseph S. Nye, "Hard, Soft, and Smart Power". p. 564.

[343] Niall Ferguson, "Power," *Foreign Policy*, no. 134 (2003), 18. p. 21; Todd Hall, "An Unclear Attraction: A Critical Examination of Soft Power as an Analytical Category," *Chinese Journal of International Politics* 3, no. 2 (2010), 189-211. pp. 206-207; Gray, *War, Peace and International Relations: An Introduction to Strategic History*. pp. v-vi and 29-30.

[344] Christopher M. Schnaubelt, "The Illusions and Delusions of Smart Power," in *Towards a Comprehensive Approach: Integrating Civilian and Military Concepts of Strategy*, ed. Christopher M. Schnaubelt (Rome: NATO Defense College, 2011). p. 27.

Whilst smart power is an accepted concept in academia and governments, other fields have named similar approaches differently. In the realm of complex policy issues, such as economic cooperation, fragile states or security, the concept of "working in a coherent way across diplomatic, security, development and financial agencies"[345] or "political, security, economic and administrative domain" to combat departmentalism is characterised as a "joined-up government"[346] or the more modern "whole of government approach".[347] This approach is required in order to be "successful" when facing complex issues that transcend the capability of a single department, agency or organisation.[348]

In military policy papers and military academia this broad approach has been dubbed the comprehensive approach, which "is not about hierarchy but about recognising that security has military, political, economic and social dimensions",[349] all these elements are necessary "for effective crisis management."[350] To express which elements are to be included in the comprehensive approach the DIME or DIMEFIL instrument construct is often used.[351] The comprehensive approach expresses that an integrative application of these instruments will enable effective crisis management.[352]

Another (inter-)related concept is the JIMP concept, stemming from Canadian military academia, it stresses "the various categories of players (i.e. organisations, interest, groups, institutions) that inhabit the broad environment within which military operations take place", namely: Joint ("involving other national military elements and support organisations"), Interagency ("involving other government departments [and agencies]"), Multinational ("involving one or more allies") and Public ("involving [...] domestic and international societies").[353] Actively engaging these actors "in a cooperative, collaborative relationship" results in an increased likelihood of the required "skills and resources needed to address the problems and challenges" being used most effectively in a complex security environment.[354]

[345] Organisation for Economic Co-operation and Development, *Policy Coherence and Whole Government Approaches in Fragile States* (Paris: OECD, 2005). p. 2.

[346] D. Kavanagh and D. Richards, "Departmentalism and Joined-Up Government," *Parliamentary Affairs* 54, no. 1 (2001), 1-18.

[347] Organisation for Economic Co-operation and Development, *Whole of Government Approaches to Fragile States* (Paris: OECD, 2006). p. 13.

[348] Ibid. p. 13.

[349] Group of Experts on a New Strategic Concept for NATO, *NATO 2020: Assured Security; Dynamic Engagement* (Brussels: NATO,[2010]). p. 22.

[350] North Atlantic Treaty Organisation, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation (Brussels: NATO, 2010b). §21.

[351] Schnaubelt, "The Illusions and Delusions of Smart Power," in . p. 51.

[352] North Atlantic Treaty Organisation, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation (Brussels: NATO, 2010). §21.

[353] Andrew Leslie, Peter Gizewski and Michael Rostek, "Developing a Comprehensive Approach to Canadian Forces Operations," *Canadian Military Journal* 9, no. 1 (2007). p. 14.

[354] Ibid. p. 17.

The four aforementioned approaches differ in name and focal area, for instance smart power focuses on the general realm of international relations; the whole of government approach on complex issues irrespective of conflict that exceed the capability of a single department, organisation or agency; and the comprehensive and JIMP-approach primarily on conflict (before, during and after). The whole of government approach expresses a potential way of organising instruments to be able to orchestrate the use of hard and soft power capabilities in a mutually reinforcing, most effective and efficient way, in other words, of operationalising smart power. The comprehensive and JIMP-approach are focused on the military instrument and conflict, however, both rely on the integrative approach to using capabilities captured in the concept of smart power and whole-of-government approach. Irrespective of the names of the approaches, all affirm the current push towards integrative strategies and organisational forms enabling mutually reinforcing relations between capabilities (smart power); departments, agencies and organisations (whole-of-government) and security partners (comprehensive and JIMP-approach). Thus understood, the contemporary approach towards wielding instruments, means, and the informational and cyber aspects is that this should be done in an integrative way in one form or another.

3.4.4.3 In sum: wielding instruments

This sub-section has set out to determine the influence of informatisation and the rise of 'cyber' on the means dimension of power. In order to do so this sub-section has first categorised the various informational and cyber means described throughout this chapter (see 3.4.4.1). This showed that due to informatisation and the rise of 'cyber' all the instruments of power and civil capacities have now informational aspects to them. In other words, the content of the means dimension is influenced by informatisation and the rise of cyber. Not only the content of the instruments has changed, there are also novel ways of using instruments and capacities (see 3.4.4.2). Contemporary research and policy stresses that the integrative application of instruments works mutually reinforcing and hence is most efficient and most effective in achieving goals. Whilst the integrative use of State instruments is still coupled with problems and there are still many cases of a single instrument approach, in contemporary society there is a drive towards more integrative approaches to wielding means. Thus, the means dimension of power has been affected by informatisation and by advancements in approaches to orchestrating the means.

3.4.5 Sub-conclusion

Section 3.4 has aimed to answer the sub-question: *What is the impact of society's informatisation and rise of 'cyber' on the power concepts and dimensions?* In order to answer this question, the power framework as described in chapter two was confronted with two developments: informatisation and the rise of 'cyber'.

Sub-section 3.4.1 has focused on describing the effects of these developments on the power concepts (compulsory, institutional, structural and productive). It concluded that informatisation and cyber do not impact the theoretical constructs underlying the power concepts, however, the developments do result in changes in to the scope and content of concepts as there are novel and more efficient ways to influence in informationised society.

Sub-sections 3.4.2 to 3.4.4 focused on the impact of informatisation and rise of 'cyber' on the most accepted power dimensions as described in chapter two: scope, domain, and means. Sub-section 3.4.2 found that there are no indications as to new strategic functions, however, the content and dynamics of the functions change necessitating a re-evaluation of how to best achieve the required outcome in informationised society. For instance, whereas a traditional intervention often involved military formations crossing a border, in contemporary society an intervention may involve cyber capabilities. Sub-section 3.4.3 concluded that there are no new categories of actors. Power diffusion has taken place, however, amongst the various actors resulting in the empowerment of non-State actors to a degree that they can potentially rival State actors. Lastly, sub-section 3.4.4 concluded that these developments have resulted in all contemporary means used by States having an informational or 'cyber' component to them. Also, the sub-section found that the notion of integrative application of means is increasingly influential, spawning terms such as smart power strategy and whole-of-government approach.

In sum, every aspect of the power framework is impacted by informatisation and 'cyber'. The impact is limited, however, to the content and/or scope of the various parts of the power framework. The common denominator in discussions regarding the power concepts and power dimensions in informationised society is that they rarely evaluate or contest the relevance of 20th century concepts or theories in the realm of power. Instead, the relevance is quickly assumed and the discussions then focus on the impact of new means and methods on the existing concept or theory. On the one hand this can be seen as evidencing the continuing value of these concepts or theories in the 21st century, on the other this could be considered a lacuna in contemporary research regarding informatisation, 'cyber' and power. This thesis will assume that it evidences the continuing value of nearly a century's worth of debate regarding power and its constitutive elements and that the concepts embodied in the power framework are able of incorporating developments in informationised society.

3.5 Conclusion

As mentioned in the introduction (see 3.1.1), informationised society is a key driver for the existence, use and utility of cyber capabilities. Apart from constituting the foundation of these capabilities, informationised society is the context of all influence attempts and hence is crucial in understanding power and powerfulness in contemporary society.

Therefore, this chapter has sought to answer the following in sub-question: *What is the impact of informationised society and 'cyber' on power?*

Section 3.2 started with specifying the concept of informationised society by answering the sub-question: *What is information society and how can it be characterised?* The concept of information society proved to be a contested construct with no clear-cut answer as to what is constitutes. The discussion did yield insights as to its characteristics. Whilst their revolutionary character is contested, there have been changes in technological, economical, occupational, spatial and cultural sense due to informatisation. These developments have gradually changed or continue to change dynamics within society. This thesis has adopted the more nuanced and comprehensive approach, namely: 'informationised society', marking the changes in contemporary society as evolutionary and not revolutionary (e.g. in the realm of technology, economy, occupation, spatiality and culture).

Section 3.3 has discussed a development parallel to informatisation, namely the rise of cyber. In order to grasp what 'cyber' is and how it could affect power this section has answered the sub-question: *What is 'cyber' and how has it developed over time?* By tracing 'cyber' from its etymological origins to contemporary usage, analysis showed that 'cyber' has been used in varying context and that its meaning differs per context. This thesis will use 'cyber' (as noun with single quotation marks) to relate to the broad development of the construct in various fields (academia, fiction, politics, military). Whereas affixing cyber to a noun, i.e. using it as a prefix, implies a relation to cyberspace (e.g. cyber attack).

Section 3.4 has aimed to delineate the influence of the developments in sections 3.2 and 3.3 on the power framework (see chapter two) by answering the following sub-question: *What is the impact of society's informatisation and rise of 'cyber' on the power concepts and dimensions?* In discussing the influence on the power concepts (compulsory, institutional, structural and productive) and the dimensions (scope, domain and means), section 3.4 concluded that the content and/or scope of these elements has been impacted by informatisation and the rise of 'cyber' due to new means, methods and approaches.

In sum, the answer to this chapter's sub-question is that informatisation and the rise of 'cyber' affect power in various ways. Although the power framework as presented in chapter two remains theoretically and conceptually valid, the content of all the elements presented therein are affected: the context, the dimensions, the power concepts and the target actors. The power concepts, for example, now embody new means to coerce opponents via cyber capabilities such as a DDoS or establishing control over machines (compulsory); new institutions such as ICANN which can be used for a State's interest (institutional); the rise of knowledge industries (e.g. Apple, Facebook, Amazon, Microsoft, Tencent, etc.) resulting in changing power structures (structural); and new means to influence discourse such as social-media (productive). The scope of power is affected as there are new means and methods to attain goals. Developments in information and communication technologies have increased the potential of forecasting (anticipation); offer new ways to pursue conflict-prevention by using new technologies such as cell phones, social media, crowdsourcing or big data analytics (prevention); result in a revaluation of the value of deterrence of cyber activities and using cyber activities to deter (deterrence); create new interests such as connectivity to protect (protection); offer new ways of intervening by using cyber capabilities (intervention); and could assist in post-conflict reconstruction (normalisation and stabilisation). The domain dimension is affected as both non-State and State actors are empowered by virtue of informatisation and the rise of 'cyber'. Informatisation also turns actors receptive to influence activities making use of cyber means and methods. The means dimension is affected as actors have new means and methods at their disposal. The 'instruments of power' all have a 'cyber' or informational component to them in contemporary society, as such actors have new ways of seeking to pursue their interests.

3.5.1 Relevance

The insights from this chapter serves to highlight how informatisation impacts the way actors can influence each other. Informatisation is instrumental to military cyber operations as the informatisation of society is the reason that cyber capabilities came into being, acquired relevance, and it forms the context for the utility of military cyber operations. Without informatisation our society could not harness cyber capabilities to influence other actors. Also, without informatisation societies would be less susceptible to influence attempts using cyber capabilities. Similar to States' desire to forward their interests in their international relations (chapter two), informationised society forms the '*condicio sine qua non*' of the utility of cyber capabilities in general and military cyber operations in specific (see Figure 8).

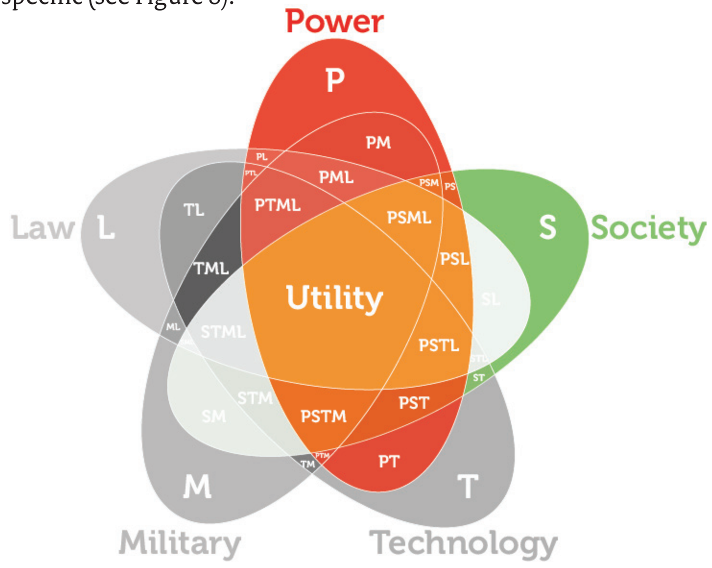

Figure 8 The 'power' and 'society' perspective to the utility of military cyber operations.

Due to informatisation, most, if not all, actors have the ability to influence others and vulnerability to military cyber operations. Military cyber operations have no utility when used directly at an adversary who does not rely on information and communication technologies. It is very unlikely, however, that actors have no reliance on these technologies in today's interconnected and globalised world. For instance, most international logistic (e.g. shipping), trade (e.g. stock markets), electricity, and finance (e.g. SWIFT) systems rely on information technology. Thus, although a target actor might not be susceptible to influence attempts using military cyber operations, the network surrounding the target actor most likely is vulnerable and can be used against the target. Eritrea for example, is considered the least developed State in information and communication technologies by the International Telecommunication Union (ITU).[355] Its regime, however, is engaged in an online information campaign with its opponents.[356] In other words, informatisation enables every actor to affect and be affected by military cyber operations. Thus, society's informationised condition results in military cyber operations having *potential* utility.

[355] "ICT Development Index 2017," ITU, accessed June 25, 2018, itu.int/net4/ITU-D/idi/2017/index.html.

[356] "From Online Trolling to Death Threats - the War to Defend Eritrea's Reputation," The Guardian, accessed June 25, 2018, theguardian.com/world/2015/aug/18/eritrea-death-threats-tolls-united-nations-social-media.

4

On Technology

4 On Technology

4.1 Introduction

“Clear communication begins with clear thinking. You have to be precise in your language and have the big ideas right if you are going to accomplish anything. I am reminded of that lesson as I witness and participate in discussions about the future of things ‘cyber.’ Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon.”[1]

Hayden, former director of the NSA and CIA, points to one of the largest issues plaguing the debate on ‘cyber’: misunderstanding. ‘Cyber’ and all its offshoots are contested issues. As there is no clarity regarding the meaning of the ‘cyber’ prefix – as evidenced by its changing meaning over time (see chapter three) – the meaning of the neologies created by affixing a word with ‘cyber’ logically is diffuse. Besides that, the many disciplines, fields and professions utilising the prefix and its offshoots result in many different perspectives on its meaning (e.g. academic, fictional, political, military or sociological). Defining the context is crucial for any statement on ‘cyber’ related issues.

4.1.1 Goal of this chapter

Cyber capabilities are instrumental to military cyber operations as these offer ways of influencing in or through cyberspace. This chapter will describe the cyber capabilities which can potentially be used in these operations. As the meaning of ‘cyber’ is contested the question rises what cyber capabilities are. As described in chapter three, this thesis uses two forms of ‘cyber’: ‘cyber’ as noun to relate to the broad development of the construct in academia, fiction, politics, and the military; and cyber as a prefix, implying a relation to cyberspace. Cyber capabilities would consequently relate to capabilities in cyberspace. This results in the question what cyberspace is. This chapter will provide cyber capabilities with the required context by discussing the ‘realm’ where actors try to influence each other (i.e. cyberspace) and list the capabilities with which they seek to do so (i.e. cyber capabilities). This chapter will do so by answering the following sub-question: *How are cyber capabilities conceptualised and utilised?*

4.1.2 Structure

Cyber capabilities make use of cyberspace, which in some way or another makes use of the Internet and associated technologies (see chapter three). The relation of ‘cyberspace’

[1] Michael V. Hayden, “The Future of Things “Cyber”,” *Strategic Studies Quarterly*, no. Spring (2011). p. 3.

with 'the Internet' is diffuse, often it is unclear whether they are synonymous or not.[2] The two terms also relate to a different perspective on the 'realm' where cyber capabilities are used. 'Cyberspace' is often used in governmental publications and as such captures the State conceptualisation of this 'realm'. 'The Internet' is often used in technical or engineering publications regarding networking and captures the technical perspective. Whilst 'the Internet' is considered one of the pivotal technologies for 'cyberspace' and is used copiously throughout publications regarding 'cyberspace',[3] the interrelation of these two concepts is rarely discussed.

This chapter will first discuss the State conceptualisation of 'cyberspace' (section 4.2). This perspective will be adjoined with the technological perspective on 'the Internet' (section 4.3) in order to facilitate a comparison between the 2000s cyberspace concept and the pre-2000s Internet (section 4.4). After that, this chapter will provide an overview of State and non-State cyber capabilities (section 4.5). As last, this chapter will provide an answer to the research question (section 4.6).

4.2 Cyberspace

Chapter three has briefly touched upon cyberspace's origins from its pristine inception in Gibson's *Neuromancer*, White Papers and doctrines clouding its meaning in the late 1990s, to adoption as warfighting domain in 2006. The military spawned various conceptualisations of cyberspace in order to foster understanding of cyberspace's military potential. These models best reflect how State actors conceptualise cyberspace, partly because there are no other public conceptualisations by State organs. This section will answer the following sub-question: *How do State actors conceptualise cyberspace?*

Before turning to the military conceptualisations of cyberspace this section will first describe the origin of cyberspace as it was conceptually understood by its 'creator' Gibson (sub-section 4.2.1). Although not a State perspective, this detour into the conceptual origin of cyberspace creates understanding of derivative models and points to certain issues within those models. After that, this sub-section will discuss the military conceptualisations of cyberspace (sub-section 4.2.2). This section will conclude with answering the sub-question (sub-section 4.2.3).

[2] See for example: "Difference between Cyberspace and Internet," accessed May 24, 2018, differencebetween.info/difference-between-cyberspace-and-internet.; "Cyberspace - what is it?" , accessed May 24, 2018, blogs.cisco.com/security/cyberspace-what-is-it.; Mark Nunes, "Jean Baudrillard in Cyberspace: Internet, Virtuality, and Postmodernity," *Style* 29, no. 2 (1995), 314-327.

[3] See for example: Department of the Army, *Field Manual 3-12: Cyberspace and Electronic Warfare Operations* (Washington, D.C.: Department of the Army, 2017).; The Joint Chiefs of Staff, *Joint Publication 3-12 (R): Cyberspace Operations* (Washington, D.C.: The Joint Chiefs of Staff, 2013).

4.2.1 Cyberspace in Neuromancer

William Gibson etymologically created cyberspace, “not merely the word; the place”.[4] He later often “said that he intended cyberspace to be nothing more than a metaphor”, but “once a creation goes out in the world its creator, like any parent, loses control once so easily exertable over the offspring; another variety of emergent behaviour”.[5] We now live in conditions sketched in *Neuromancer*, “a cybercondition if you must”, “rather than the theoretical Matrix, we now [...] have the actual Web – same difference, for all intents and purposes, or it will be soon enough”.[6] Thus although not intended, Gibson foretold the coming of the Internet.[7] Cyberspace as described by Gibson is, however, somewhat different than the Internet today. In order to comprehend the original model and its differences with contemporary conceptualisations this sub-section will briefly describe Gibson’s cyberspace. First, the entities occupying Gibson’s cyberspace will be described (sub-section 4.2.1.1). Secondly, as *Neuromancer* is fiction, this sub-section will reflect on the differences between Gibson’s cyberspace and the current ‘state’ of the Internet (sub-section 4.2.1.2).

4.2.1.1 Entities

Gibson depicted cyberspace or the Matrix as “bright lattices of logic unfolding across that colorless void”;[8] ‘cyberspace cowboys’ could manifest themselves in that space. In order to manifest in cyberspace, the operators require a connected cyberspace deck or console and attach electrodes (“dermatrodes”) to their head.[9] By doing so, the operator enters a state of bodilessness in a virtual reality and is able to perceive other entities in cyberspace. Whilst immersed in cyberspace, the operator is vaguely aware of real-life physical and auditory stimulae. The deck generates a graphic representation of logical information understandable by trained operators and projects/injects this image inside the operator’s vision. The virtual reality called cyberspace houses a variety of entities, amongst other: (1) data, (2) other operators, (3) human constructs, (4) self-aware artificial intelligences (AI), (5) intrusion countermeasures electronics (ICE) and (6) malware (viruses and worms).

These entities take different geometrical shapes and depending on their complexity, have different densities. Complexity of cyberspace entities influences the graphical representation; the cyberspace deck sometimes struggles to translate very complex code to an understandable image. An operator can manipulate real-life objects via cyberspace by altering code. *Neuromancer* is set in a world of bio-enhancement via technological implants, persons “go silicon” to enhance their motoric or neural skills.[10] Via cyberspace a person’s bio-enhancement implants can be accessed and manipulated, an operator can, for instance,

[4] Jack Womack in Gibson, *Neuromancer*. p. 537.

[5] Jack Womack in Gibson, *Neuromancer*. p. 540..

[6] Ibid.

[7] Ibid. pp. 540-541.

[8] Ibid. p. 14.

[9] Ibid.

[10] Ibid. p. 149.

access the feed from another person's special contact lenses. All real-life connected automata can be manipulated, such as displays, phones, speakers, household machines, drones, consoles and doors. Although many consider Gibson's cyberspace prophecy to be fulfilled by the coming of Internet, there are some differences.

4.2.1.2 *Neuromancer and reality*

The first inconsistency is the 'immersiveness' of the manifestation in cyberspace. Entering cyberspace results in an out-of-body experience, leaving the operators unable to respond to most of physically induced, real-life stimulae. The operators perceive space and time differently, they see a different virtual reality and hours in cyberspace may only take a couple of real-life minutes. Although some would argue that there is a sense of fading space and time when using the Internet and its applications, it is neither as drastic nor immersive.

The second inconsistency is the lethality of venturing inside cyberspace. In *Neuromancer* operators can encounter black intrusion countermeasures electronics (ICE), which trap the virtual operator inside a void. When trapped the operator's physical body endures a cardiac arrest and consequently has to be resuscitated. Using the Internet or its applications (currently) does not pose an imminent risk to one's health. Contrary to *Neuromancer* where operators 'jack-in' via electrodes, there is no direct link – yet – between the user's nerve or other bodily systems and the interface used to access the Internet. Of course Internet applications can indirectly kill after manipulation, opening a connected floodgate via its control software or tampering with a pacemaker's software would for instance lead to bodily harm. But it differs from Gibson's cyberspace where jacked-in operators can be killed directly as a consequence of actions in cyberspace without involving other physical elements causing lethal damage.

Thus, there are differences between the Internet as used in contemporary society and Gibson's cyberspace, nonetheless *Neuromancer* hosted the most adequate description of the future of networked technology of its time. Although many features it foretold have become reality, Gibson's cyberspace is still ahead of today's Internet. There are, however, technological developments that may overcome the apparent inconsistencies between Gibson's conceptualisation of cyberspace and contemporary society.

Technology companies, the gaming industry, and a variety of government and semi-government institutions are aiming to fulfil the prophetical technologies envisioned in *Neuromancer*. Mouse, keyboard, touchpad and screens currently hamper integrative interaction with hard- and software. Hands, currently administering input, are slow to translate thoughts into input. Therefore many organisations are seeking to provide an integral link between man and machine, also called a 'brain-machine interface'.[11] These

[11] See for instance: Sebastian Anthony, "The First Human Brain-to-Brain Interface has been Created. in the Future, Will we all be Linked Telepathically?" extremetech.com/extreme/188883-the-first-human-brain-to-brain-interface-has-been-created-in-the-future-will-we-all-be-linked-telepathically (accessed January 14, 2015); Andy Greenberg, "Darpa Turn Oculus into a Weapon for Cyberwar," Wired, wired.com/2014/05/darpa-is-using-oculus-rift-to-prep-for-cyberwar/ (accessed January 14, 2015); John Hewitt, "New Brain Implant Tech from Blackrock

technologies coupled with advancements in virtual reality technologies could possibly lead to an equally immersive experience of the Internet as cyberspace in *Neuromancer*.

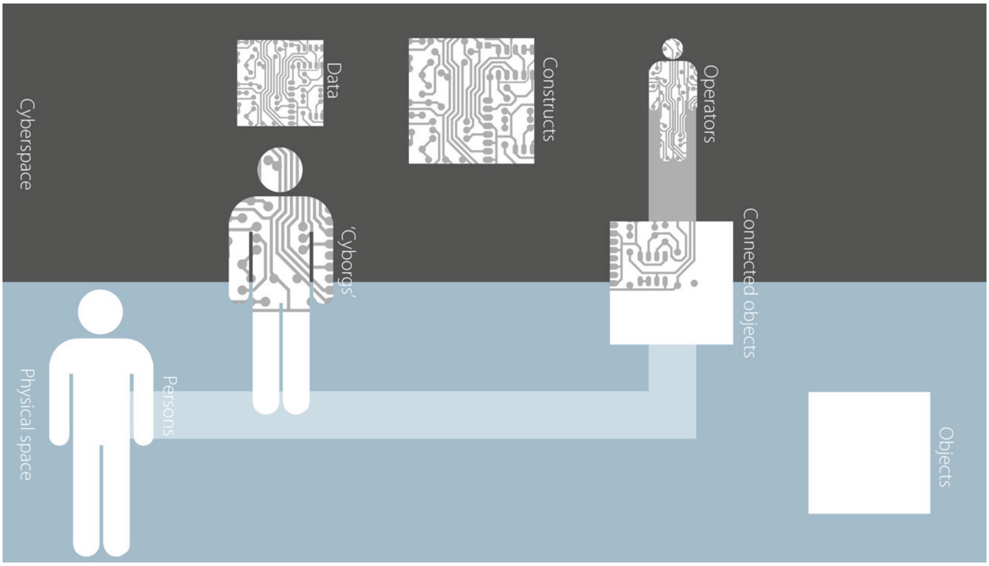

Figure 9 Gibson's physical- and cyberspace

4.2.1.3 Gibson's conceptualisation of cyberspace

Gibson did not intend cyberspace to become the all-encompassing term used in military and political affairs today, hence *Neuromancer* has no clear conceptualisation or model of how cyberspace permeates the physical domain. By liberally interpreting *Neuromancer* and ignoring Gibson's remarks that he had not intended cyberspace to be used for this purpose, however, one can deduce a conceptualisation of Gibson's notion of cyberspace.

Gibson's conceptualisation of cyberspace could be interpreted as follows: People ('persons'), bio-enhanced people (popularly called 'cyborgs'), non-connected objects ('objects') and connected objects (cyberspace decks, robots, screens etc.) inhabit physical space (figure 1 blue part). Bio-enhanced people (if connected) and connected objects transcend physical space and manifest themselves in cyberspace as well as in physical space. Data, constructs (artificial intelligence, malware, self-aware human constructs, intrusion

is Making 'Mind Over Matter' a Reality," extremetech.com/extreme/194935-new-brain-implant-tech-from-blackrock-is-making-mind-over-matter-a-reality (accessed January 14, 2015); John Hewitt, "We can Now Remotely Control Paralyzed Rats, Letting them Walk again: Humans are Next," extremetech.com/extreme/190882-we-can-now-remotely-control-paralyzed-rats-letting-them-walk-again-humans-are-next (accessed January 14, 2015); Greg Miller, "Is this Mind-Controlled Exoskeleton Science of Spectacle?" Wired, wired.com/2014/05/world-cup-exoskeleton-demo/ (accessed January 14, 2015); David Orenstein, "Brown Unveils Novel Wireless Brain Sensor," news.brown.edu/articles/2013/02/wireless (accessed January 14, 2015); Antonio Ragalado, "Military Funds Brain-Computer Interfaces to Control Feelings," MIT Technology Review, technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/ (accessed January 14, 2015).

countermeasures electronics) and jacked-in operators reside virtually in cyberspace (figure 1 grey part). Physical persons can manifest themselves in cyberspace through connected objects, most prominently by using cyberspace consoles or decks (figure 1 arrow from 'person' through 'connected objects' to 'operators'). The operator in cyberspace has a direct link with the real-life person and if the operators' non-physical manifestation dies, the real-life person flat-lines.

4.2.2 Conceptualisations of cyberspace in governmental perspective

For most people talking about 'cyberspace', primarily non-technical ones, cyberspace is synonymous with 'the Internet'. This confusion is only logical considering that 2000s White Papers simply replaced the Internet and associated information systems with cyberspace (see chapter three). The cyberspace construct is, however, more comprehensive in scope than the Internet, primarily because cyberspace also encompasses the social aspects of human interrelation with the Internet instead of focusing on the technological aspects of computing and networking. The most influential model conceptualising 'cyberspace' is the United States Army's three-layer model,[12] which found its way to United States joint doctrine,[13] and is globally used throughout doctrines and other publications.[14] This sub-section will first describe the 'original' three-layer U.S. military conceptualisation in sub-section 4.2.2.1. Secondly the most influential offshoot will be discussed in sub-section 4.2.2.2, namely, the three-layer and later six-layer U.K. cyberspace models. As third, sub-section 4.2.2.3 will reflect on the gaps and overlaps between the U.S. and U.K. cyberspace conceptualisations.

4.2.2.1 U.S. conceptualisations

The models start with the basis for cyberspace, that is: the physical (U.S. Army, 2010) or physical network layer (U.S. Joint Doctrine, 2013). This layer contains a geographic component and physical network components (see Figure 10). The geographic component is "the location in land, air, sea, or space where elements of the network reside".[15] Although border can easily be crossed in cyberspace, the geographic component emphasises that "there is still a physical aspect tied to the other domains".[16] The physical network component includes "hardware, systems software, and infrastructure (wired, wireless, cabled links, satellite, and optical)".[17]

[12] United States Army, *Cyberspace Operations Concept Capability Plan 2016 2028* (Fort Eustis: The United States Training and Doctrine Command, 2010). p. 8.

[13] The Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (Washington, DC.: Joint Chiefs of Staff, 2013c). p. I-3.

[14] Development, Concepts and Doctrine Centre, *Joint Doctrine Publication 04: Understanding* (Shrivenham: Ministry of Defence, 2010). p. 2-10; Ministry of Defence (United Kingdom), *Cyber Primer*, 1st ed. (Shrivenham: The Development, Concepts and Doctrine Centre, 2013); Ministry of Defence (United Kingdom), *Cyber Primer*, 2nd ed. (Shrivenham: The Development, Concept and Doctrine Centre, 2016).

[15] The Joint Chiefs of Staff, Joint Publication 3-12: Cyberspace Operations. pp. I-2, I-3.

[16] United States Army, Cyberspace Operations Concept Capability Plan 2016 2028. p. 9.

[17] The Joint Chiefs of Staff, Joint Publication 3-12: Cyberspace Operations. p. I-3.

The logical layer (U.S. Army, 2010) or logical network layer (U.S. Joint Doctrine, 2013) enables communication over the physical network components. 'Logic' as term should be understood to refer to 'computational logic' and not 'logic' as traditionally understood as "determining whether a given conclusion (or theorem) C is logically implied".[18] Computational logic has no generally agreed meaning, in this context it seems to relate to the use of logic for all aspects of computing, for "representing programs, program specifications, databases, and knowledge bases" and "for processing, developing and maintaining them".[19] Computational logic is more generically and commonly known as 'software': a "general term for the various kinds of programs used to operate computers and related devices."[20] The logical layer comprises the logical network component. This component consists of "the logical connections that exist between network nodes."[21] Nodes are devices such as "computers, personal digital assistants, cell phones".[22]

The social layer comprises the cyber persona component in both models and in the 2010 U.S. Army model also the persona component. The cyber persona component comprises "a person's identification or persona on the network"[23] and "may relate fairly directly to an actual person or entity, incorporating some biographical or corporate data, e-mail and IP [addresses], Web pages, phone numbers, etc." and social networking profiles.[24] The U.S. Army model initially designated a distinct persona component consisting of the "people actually on the network", but since 2013 this component has been removed from the model and subsumed in the cyber persona component.[25]

[18] J. W. Lloyd, ed., *Computational Logic Symposium Proceedings* (London: Springer-Verlag, 1990). p. 2.

[19] Ibid. p. 1.

[20] Margaret Rouse, "Software," TechTarget, searchmicroservices.techtarget.com/definition/software (accessed August 13, 2017).

[21] United States Army, Cyberspace Operations Concept Capability Plan 2016 2028. p. 9.

[22] Ibid. p. 9.

[23] United States Army, Cyberspace Operations Concept Capability Plan 2016 2028. p. 9.

[24] The Joint Chiefs of Staff, Joint Publication 3-12: Cyberspace Operations. p. I-4.

[25] Department of the Army Headquarters, *Field Manual 3-38: Cyber Electromagnetic Activities* (Washington, DC.: Department of the Army, 2014). pp. 3-8, 3-9.

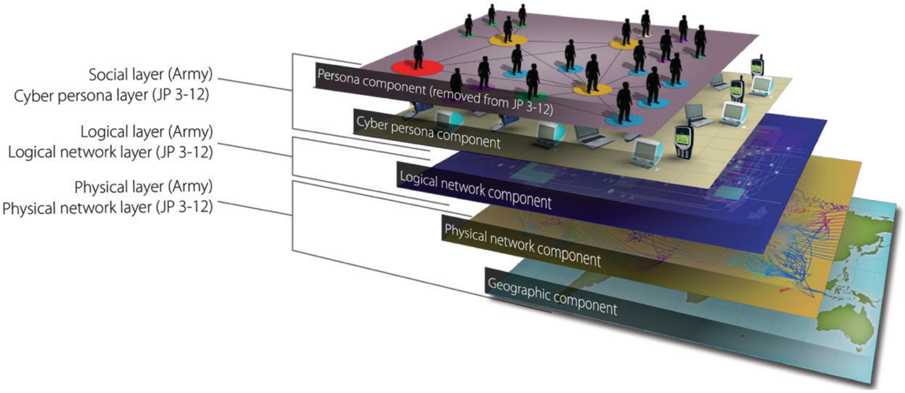
Social layer (Army)
Cyber persona layer (JP 3-12)
Logical layer (Army)
Logical network layer (JP 3-12)
Physical layer (Army)
Physical network layer (JP 3-12)
Persona component (removed from JP 3-12)
Cyber persona component
Logical network component
Physical network component
Geographic component

Figure 10 United States department of defence cyberspace conceptualisation

4.2.2.2 U.K. conceptualisations

The U.K.'s first public 'cyberspace' conceptualisation followed ten months after the U.S. Army model and is published in a doctrine on understanding.[26] The sources facilitating understanding are derived from "the cognitive, the physical and the virtual information domains [(*plural*)]".[27] In order to visualise the information domain (*singular*), the doctrine visualises the layers of the information domain, namely the cognitive, virtual and physical domains (see Figure 11).[28] The right side of the figure lists the "key elements of understanding" and their interrelation.[29] Neither the model nor its accompanying text explain what elements (social, people, persona, information, network and real) belong to which domain (cognitive, virtual and physical).

[26] Development, Concepts and Doctrine Centre, *Joint Doctrine Publication 04: Understanding*. p. iii.

[27] Ibid. p. 2-5.

[28] Ibid. pp. 2-7 to 2-8.

[29] Ibid. p. 2-9.

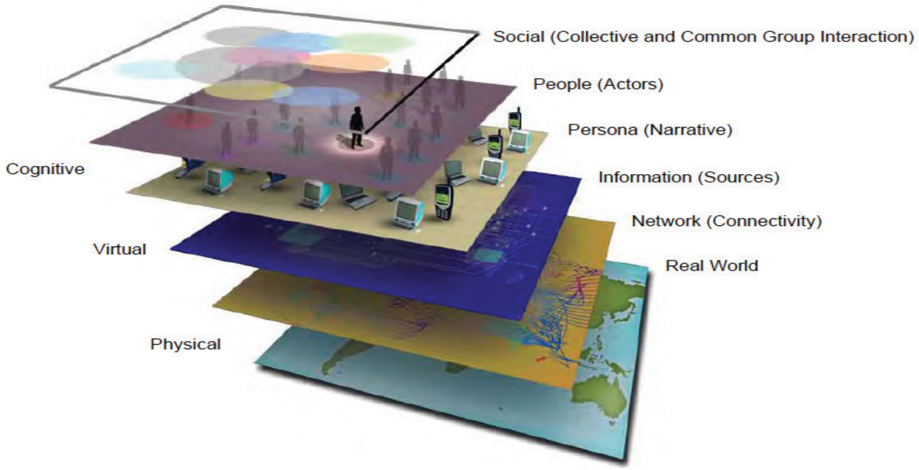

Figure 11 U.K. "visualising the information domain"[30]

The model of the information domain is used three years later in the document "Cyber Primer", which aims to "provide baseline awareness of cyber for the entire audience" and as "a good precursor to reading doctrine on the subject."[31] In a section on 'intelligence support to cyber operations', the primer uses the 2010 information domain model to describe cyberspace.[32] Although using the visualisation of the information domain, the figure is dubbed "the layers of cyberspace".[33] Cyberspace is considered to have "three interdependent layers which align with, and span, the physical, virtual and cognitive domains".[34] The layers are described and listed as follows (see Figure 12): "[a] Physical layer. The physical layer (*real*) consists of the physical network components and their associated geography. [b] Virtual layer. The virtual layer (*network, information*) consists of the software/application and connections between network nodes. [c] Cognitive layer. The cognitive layer (*persona, people, social*) consists of the information that connects people to cyberspace and the people and groups who interact by using and operating the networks."[35] As the colours of elements (social, people, persona in a green shade; information in blue; and real and network in red) relate to the particular layer it belongs to there is a discrepancy in the text describing the model and the actual model. From the text describing the physical layer and the visualisation it follows that the network element should be included under the physical layer.

[30] Ministry of Defence (United Kingdom), Cyber Primer. p. 2-9.

[31] Ibid. p. v.

[32] Ibid. p. 1-25.

[33] Ibid

[34] Ibid. p. 1-26.

[35] Ministry of Defence (United Kingdom), *Cyber Primer*. p. 1-26.

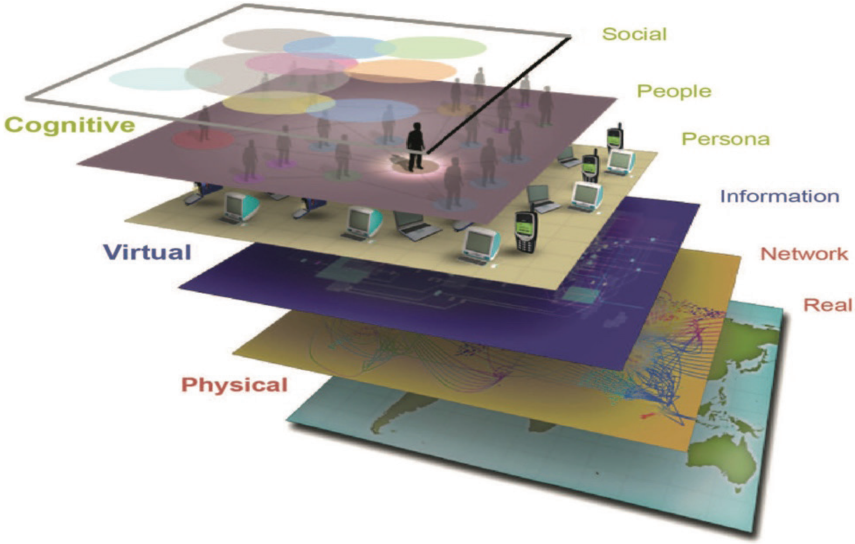

Figure 12 "The layers of cyberspace"[36]

The cognitive, virtual and physical 'domains' in 2010 or 'layers' in 2013 are removed altogether in the model used in the second edition of the Cyber Primer in 2016.[37] Instead, it dubs the social, people, persona, information, network and real elements 'layers' (see Figure 13). The social, people and persona layers "consist of the details that connect people to cyberspace and the people and group who interact with and operate the networks."[38] The information layer "consists of the connections that exist between network nodes" where a "node is a physical device connected to a network, such as a computer, smartphone or other mobile device."[39] The network layer "uses logical constructs as the primary method of security (for example, information assurance) and integrity".[40] The real layer "consists of a geographic aspect and a physical aspect. The geographic aspect relates to the location of elements of a network, such as the sea or ground, or in a building. The physical aspect concerns what components are present – such as hardware, systems software and infrastructure."[41] Again there is a mistake in the description of the network 'layer', the real layer should only comprise the geographic aspect and the 'physical aspect' now included under the real 'layer' should replace the nonsensical text describing the network 'layer'.

[36] Ibid. p. 1-26.

[37] Ministry of Defence (United Kingdom), *Cyber Primer,* 2nd ed. pp. 5-6.

[38] Ibid.

[39] Ibid. p. 6.

[40] Ibid. p. 7.

[41] Ibid. p. 7.

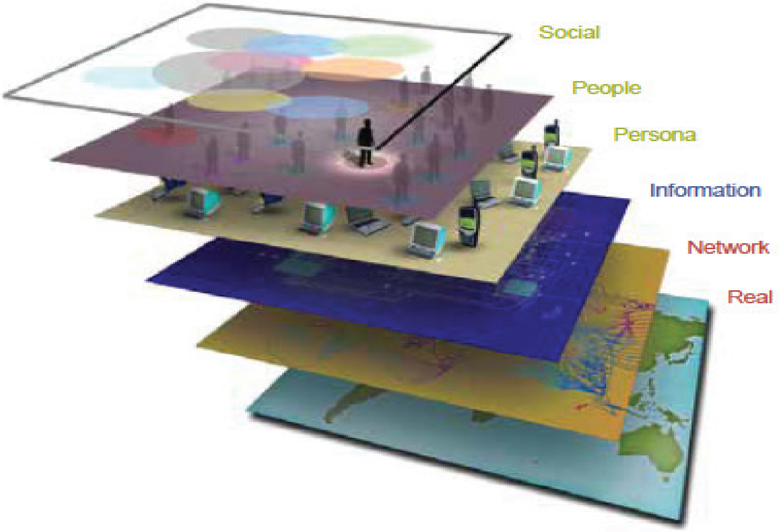

Figure 13 "The six layers of cyberspace"[42]

4.2.2.3 Gaps and overlaps U.K. and U.S. conceptualisations

This sub-section will analyse the gaps and overlaps between the U.S. and U.K. cyberspace conceptualisations. As first, the visuals used in the U.K. models are all based on the 2010 U.S. Army model of cyberspace. The only visual addition made is the social element in 2010. Besides sharing the visual basis, the conceptual basis is also nearly identical. The latest U.S. model of cyberspace (2013) comprises three layers: cyber-persona, logical network and physical network. The U.K. models have utilised three layers but these have been omitted in the latest publication (2016), in the previous versions (2010 and 2013) the layers were as follows: cognitive, virtual and physical. The layers are very similar, the cyber-persona layer shares aspects of the cognitive layer, the logical network layer is identical to the virtual layer, and the physical network layer is identical to the physical layer. As to the U.S. components or U.K. elements (2010) or layers (2016), these are also very similar: The geographic component is identical in scope to the real element or layer; the physical network component to the network element or layer; the logical component to the information element or layer; the cyber persona component to the persona element or layer; and the persona component (2010) to the people element or layer. In other words, the conceptualisations are nearly identical; the difference lies in the addition of the people and social element or addition in the U.K. conceptualisation.

[42] Ministry of Defence (United Kingdom), Cyber Primer. p. 5.

The U.S. persona component, which used to refer to the people actually on the network (see 4.2.2.1), was removed in the 2013 iteration of the model. This is logical as the persona component overlaps entirely with the cyber-persona component, comprising 'a person's identification or persona on the network'. There are no actual physical people on networks, all human interaction via cyberspace happens via cyber-personas, such as mail addresses, social media profiles and phone numbers. This conceptualisation of cyberspace is different from the U.K. models; however, this is likely based on a misinterpretation of the 2010 model.

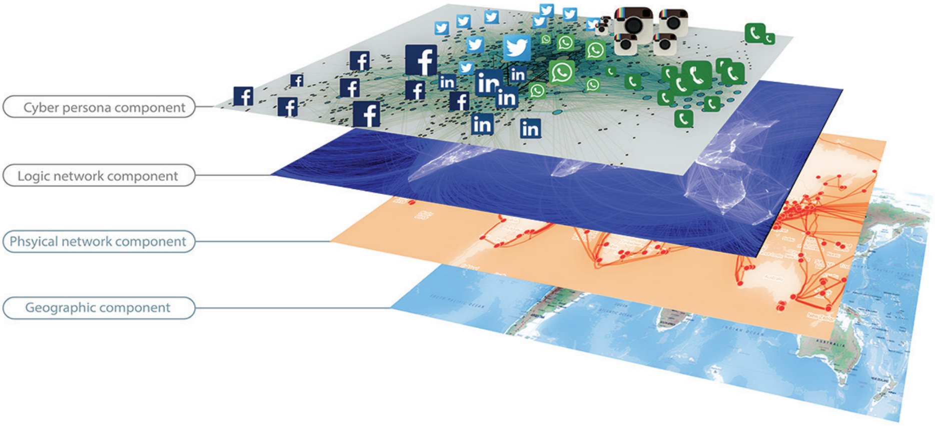

Figure 14 Military conceptualisation of cyberspace by integrating insights from U.S. and U.K. publications resulting in the 2013 U.S. conceptualisation of cyberspace.

The U.K. 2013 and 2016 conceptualisations of cyberspace use the 2010 model of the 'information domain'. This results in the information domain being used to conceptualise cyberspace. The information domain, in military doctrine referred to as the information environment, however, is broader in scope than cyberspace and includes people and groups as it is defined as "the aggregate of individuals, organisations, and systems that collect, process, disseminate or act on information".[43] Thus, whereas for the purpose of describing the information environment the 2010 model could be deemed suited, it is not suited for visualising cyberspace as these are two different concepts. Cyberspace does not include physical people or groups as the U.K. publications affirm themselves: there is no single mention of people or groups in the 2013 or 2016 U.K. documents when defining cyberspace.[44] As such, the conceptualisation with the social and people layer does not

[43] The Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations* (Washington, D.C.: The Joint Chiefs of Staff, 20 November 2014). p. vii.

[44] Ministry of Defence (United Kingdom), *Cyber Primer*. pp. 1-1 to 1-2; Ministry of Defence (United Kingdom), *Cyber Primer*. pp. 4-5.

reflect the accompanying definition of cyberspace. In other words, the 2013 and 2016 models reflect the information environment and not cyberspace.

In conclusion, from interpretation of the U.S. and U.K. models of cyberspace it follows that cyberspace comprises the following components (U.S.) or layers (U.K.): geographic component/real layer, physical network component/network layer, logical network component/information layer, and cyber persona component/persona layer (see Figure 14).

4.2.3 Sub-conclusion

This section has aimed to answer the sub-question: *How do State actors conceptualise cyberspace?* As starting point this section has described cyberspace as understood by Gibson (see 4.2.1). This detour was necessary as Gibson coined 'cyberspace' and his term has considerably influenced the debate regarding 'cyber'. By liberal interpretation of *Neuromancer* this section has derived the entities Gibson understands to reside in cyberspace, namely: data, constructs, jacked-in operators and the hybrid (physical/cyber) entities of 'cyborgs' and 'connected objects'. This section then turned to governmental conceptualisations (see 4.2.2). After having analysed the U.S. and U.K. models the sub-section concluded that correct interpretation of the models results in cyberspace being conceptualised as having four components (or layers): geographic, physical network, logical network, and cyber persona component/persona layer. This model can be considered to be the most influential and representative public depiction of how State actors conceptualise cyberspace.

It is interesting to note the overlaps within Gibson's and the military conceptualisations of cyberspace. As the military conceptualisation, Gibson implicitly distinguishes connected objects that facilitate the virtual representation of people in cyberspace. The connected objects are examples of the physical network components, and their virtual representation would be considered to belong to the 'cyber persona component'. Gibson's model of cyberspace, however, also points to some shortcomings or unclear issues with the military conceptualisations, namely, (1) the place of data, (2) constructs and (3) hybrid persons ('cyborgs').

Data is a non-human entity residing in cyberspace in *Neuromancer.* Data in the military conceptualisation has no clear place, data could have a physical form, for instance, a USB flash drive holding a document; logical form, such as a document being transmitted from one point to another; or constitute a cyber-persona, for example, the profile data stored on a server belonging to a social-media platform. One explanation could be that three of the four components constitute data in the military conceptualisations: a cyber-persona component is data regarding a person, the logical component is data resulting in logical networking for instance networking software or protocols and the geographical component is data regarding the physical location of physical network infrastructure, the latter logically is the only component not considered data as it is hardware. Thus, data could be considered too fundamental to be included in one of the components as it is the basis of three of the four components.

Cyberspace constructs in *Neuromancer* include entities such as artificial intelligences (AI) and self-aware human constructs. As in contemporary society these technologies are still nascent compared to the world of *Neuromancer*, AI and self-aware constructs are logically not yet covered by cyberspace conceptualisations. These entities would most likely fall under the ambit of the logical network component, however, progress in these fields could result in disappearance of a distinction between the cyber persona component and logical component.

Similarly, hybrid persons ('cyborgs'), people with an integral connection to cyberspace and who consequently do not need computers to interact with cyberspace have yet not been addressed by the military conceptualisations. These hybrid persons would fall somewhere between the physical network component (the actual physical implant creating the connection), logical component (the software and data allowing the person to 'enter' cyberspace), and cyber-persona component (the visual representation of the person in cyberspace). The integrality of the connection could foster the notion that there are actually people in cyberspace.

Whilst Gibson's model of cyberspace points to some issues in the military conceptualisations, these models should be understood in their proper context: operationalising the cyberspace construct in the contemporary context. These models aim to describe the elements that can be attacked, defended or exploited in the context of cyberspace in contemporary society. In doing so these models never have pretended to be an all-encompassing nor future proof model of cyberspace.

4.3 Technical perspective on the Internet

Before 'cyberspace' materialised in military doctrine in the 2000s, networking and the international interconnected network (the Internet) already existed. The factors involved in engineering the Internet and networking in general are captured in the TCP/IP and ISO/OSI models. [45] This section will answer the sub-question: *How is the Internet conceptualised?*

The pre-cyberspace models of the Internet, TCP/IP and ISO/OSI, consist of layers. The TCP/IP has four layers (application, transport, Internet, and link) and ISO/OIS seven layers (application, presentation, session, transport, network, link, and physical) – see Figure

[45] See: Charles M. Kozierok, "TCP/IP Overview and History," tcpipguide.com/free/t_TCPIPOverviewandHistory.htm (accessed January 28, 2015); Jon Postel, *Internet Engineering Note #2: Comments on Internet Protocol and TCP*, 1977). p. 1; C. Meinel and H. Sack, "The Foundation of the Interenet: TCP/IP Reference Model," in *Internetworking* (Berlin: Springer-Verlag, 2013), 29-61. p. 46; Andrew L. Russel, "OSI: The Internet that was Not," spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt (accessed February 2, 2015);

15.[46] These layers interact with each other in order to facilitate networking. Although both models yield general insights regarding the conceptualisation of the Internet from a technical perspective, they lack concrete footholds that enable an in-depth comparison of gaps and overlaps between 'cyberspace' and 'Internet' conceptualisations. In order to create better understanding of the technical Internet conceptualisation this section will briefly describe the Internet from a technical perspective. This section will describe the Internet's physical and logical foundations by providing a very basic introduction to networking in the most prevalent networking model: client-server.[47] It will describe the client hard- and software at the side of the user (4.3.1), the intermediaries mediating the connection to a server (4.3.2), and the servers (4.3.3).

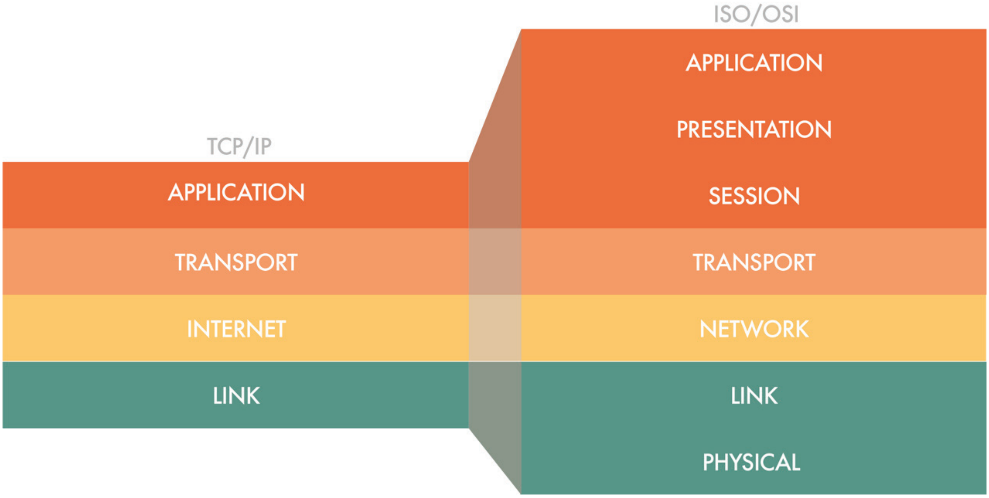

Figure 15 The TCP/IP and ISO/OSI model. The ISO/OSI model further divides TCP/IP's application layer into three separate layers and the link layer in two layers, however, the models are very similar.

4.3.1 User side

The device used for computing and networking differs per person and per situation, since the 2000s mobile Internet access has become common and from the 2010s

[46] Meinel and Sack, "The Foundation of the Interenet: TCP/IP Reference Model." p. 46; Andrew L. Russel, "OSI: The Internet that was Not," spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt (accessed February 2, 2015).

[47] See for example: "Introduction to Client Server Networks", accessed May 28, 2018, lifewire.com/introduction-to-client-server-networks-817420.; "Client/Server Technology," accessed May 28, 2018, encyclopedia.com/computing/news-wires-white-papers-and-books/clientserver-technology.

connecting everything to the Internet has become increasingly commonplace.[48] All these devices are, however, very similar from a component point of view (see Figure 16). They resemble the basic architecture of computers, albeit in a miniaturised form. All these devices are generally made up of hardware such as display, battery (in the case of mobile or laptops), central processing unit (CPU), graphical processing unit (GPU), static and/or dynamic random-access memory (SRAM and/or DRAM), read-only memory (ROM) with system files, application storage and caches (L1, L2, L3 and/or L4) and network interfaces (e.g. Wi-Fi, NFC and/or cellular).[49] Software runs on this hardware such as firmware, the operating system (OS) and applications.

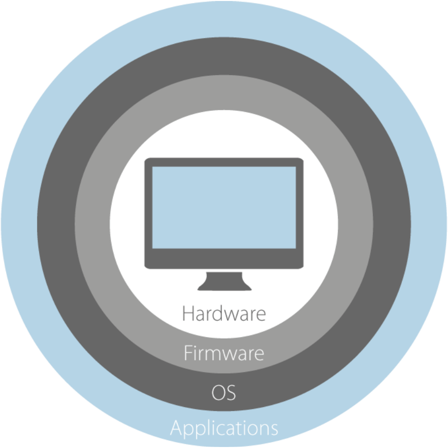

Figure 16 Client logical foundations

Firmware is the read-only software installed on a hardware component enabling the functioning and interoperability of that specific piece of hardware.[50] Examples include the control system of a washing machine or of a digital watch. Normally users never alter this software except for an update initiated by the manufacturer. The operating system of a device is software that administers hardware, software and common services for applications. An OS consists of a kernel that processes the input and output of applications and translates it into instructions for the central processing unit (CPU), memory and

[48] Dieter Uckelmann, Mark Harrison and Florian Michahelles, *Architecting the Internet of Things* (New York: Springer, 2011). pp. V-VIII; Skaržauskienė and Kalinauskas, "The Future Potential of Internet of Things." 102-113

[49] Microsoft, "Parts of a Computer," windows.microsoft.com/en-us/windows/computer-parts#1TC=windows-7 (accessed July 9, 2015); Kailash Jayaswal, *Administring Data Centers: Servers, Storage, and Voice Over IP* (Indianapolis: Wiley Publishing, Inc., 2006). pp. 132-133; Joel Hruska, "How L1 and L2 CPU Caches Work, and Why they're an Essential Part of Modern Chips," extremetech.com/extreme/188776-how-l1-and-l2-cpu-caches-work-and-why-theyre-an-essential-part-of-modern-chips (accessed July 9, 2015).

[50] Tim Fisher, "Firmware," pcsupport.about.com/od/termsf/g/firmware.htm (accessed July 9, 2015); TechTerms, "Firmware," techterms.com/definition/firmware (accessed July 9, 2015).

devices.[51] Popular operating systems include Windows, Mac OS, Linux (e.g. Ubuntu) and their mobile counterparts Windows Mobile OS, iOS and Android. [52]

Applications are the installed software with which users interact when using their device. It differs per platform – mobile or desktop – what applications are used. On desktop users employ a variety of applications for productivity (e.g. word processor, presentation tools, spread sheet editor, mail, video, website, code and photo editing tools), video games, browsing (e.g. Chrome, Firefox, Safari, Opera and Internet Explorer), music (e.g. iTunes, Spotify) and a variety of utilities (e.g. virtual private network services, time out tools, network assistance, antivirus), assistance (Help), user management tools (Finder, command line tools), etc. Some of these applications come with the OS others users have to install themselves. In other words, users personalise their machine by installing applications.

Users install 'apps' on a mobile system (short for applications) specifically tailored to the platform on which the app is installed (e.g. Android, iOS, Windows mobile). Apps are generally more specialised than the applications on a desktop, there are, for instance, specific apps for social networking (e.g. Facebook, Twitter, Instagram, Linkedin, etc.) and getting directions (e.g. Google Maps, Maps) whereas desktop users mostly utilise the website variant of these social networking sites. In sum, the user's device (client) to access the Internet and use in day-to-day activities consists of hardware, firmware, operating system (OS) and various applications tailored to the user's needs.

4.3.2 Intermediaries

Connecting the aforementioned devices to the Internet is commonplace. In order to facilitate Internet services intermediary devices are involved such as switches, hubs, bridges, modems, and routers. The following paragraph will first briefly summarise what these devices are and after that this sub-section will focus more in-depth on the key intermediary device: routers.

A switch connects devices in a local area network (LAN) and filters data packets, for instance, it determines whether a data packet is local – i.e. within the network – or remote, i.e. outside the network. If the packet is local it is routed through the switch to the appropriate device, when it is remote it will be sent upstream to the router.

A hub is somewhat similar to a switch, but it differs intelligence wise. Hubs route or broadcast data addressed to a specific machine to all machines connected to the hub, a switch on the contrary learns the media access control (MAC) addresses of machines and

[51] Andrew S. Tanenbaum, *Modern Operating Systems*, 2nd ed. (Upper Saddle River: Prentice Hall, 2001). pp. 1-6.

[52] NetMarketShare, "Desktop Top Operating System Share Trend," netmarketshare.com (accessed July 9, 2015); NetMarketShare, "Mobile/Tablet Operating System Market Share," netmarketshare.com (accessed July 9, 2015).

routes traffic to the machine addressed. Bridges are the predecessors of switches; switches could be called multiport bridges since they offer the same functionality.[53]

A modem (modulator-demodulator) is generally used to refer to the device enabling sending digital packets over an analogue medium such as copper wire. Less well known is a wireless modem, which is a functionality every modern smartphone offers. These devices serve as a modem between mobile data networks (GPRS, E, 2G, 3G, 4G, etc.) and devices such as laptops that can normally not utilise mobile data networks.

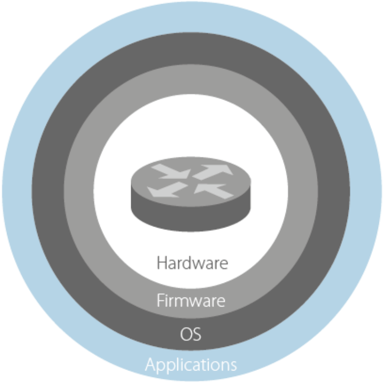

Figure 17 Router

A router is a device consisting of hardware, firmware, OS and applications used to route the user's data onto and from the wide-area network (see Figure 17).[54] A metaphor often used is to characterise a router as a post-office, by using postal codes the office decides where packets need to go.[55] Routers do the same with data packets by using Internet Protocol (IP).[56]

Perhaps the most familiar intermediary device for typical users is their router at home, called the subscriber, customer or residential edge, or gateway router.[57] A modern day customer router combines the functionalities of all intermediary devices mentioned

[53] "Cisco Learning Network: Switch Vs. Bridge," Cisco, accessed June 29, 2018, learningnetwork.cisco.com/thread/41392.

[54] Michael Seese, *Scrappy Information Security* (Silicon Valley: Scrappy About, 2009). pp. 58-59; Behrouz A. Forouzan, *Data Communications and Networking*, 4th ed. (New York: McGraw-Hill, 2007). p. 455.

[55] See for instance: Larry Press, "Analogy between the Postal Network and TCP/IP," California State University, bpastudio.csudh.edu/fac/lpress/471/hout/netech/postofficelayers.htm (accessed July 9, 2015).

[56] Seese, Scrappy Information Security. pp. 58-59; Forouzan, Data Communications and Networking. p. 455.

[57] Tim Fisher, "Router: Everyting You Need to Know about Routers," About Tech, pcsupport.about.com/od/componentprofiles/p/router.htm (accessed July 9, 2015); Heather M. Kosur, "The Definition of a Network Router for the Non-Technical Person," Bright Hub, brighthub.com/computing/hardware/articles/51073.aspx (accessed July 9, 2015); Cisco, "Designing MPLS Extensions for Customer Edge Routers, no. 1575," Cisco, cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html#wp30266 (accessed July 9, 2015).

above. Often the device has multiple inputs for network cables (UTP, FTP, etc.), which is the function of a switch. Many (digital subscriber line) routers also can fulfil a modem function. The key function, however, is routing traffic from the local area network (LAN) to the Internet (WAN). Whilst doing so it also does network address translation (NAT), checks data traffic via a firewall, manages incoming and outgoing (IP) phone calls, and performs a variety of other functions. Whether a user accesses the Internet, uses digital television (also called IPTV) or makes a call using his IP telephone: the home router is his gateway to the wide area network. As such, the router has an IP address provided by the Internet service provider that identifies the router on the Internet. The router passes all the packets (the envelopes in the post office analogy) coming from the local area network through with a header signalling, amongst other: the source, destination and protocol used. These packets are then passed on to the ISPs network; the ISPs first router is called an (Internet) provider edge, boundary, aggregation or access gateway router.[58] In order to send data to the ISP's edge router cabling is used (e.g. coaxial cable, copper cable, fibre-optic) and depending on the physical media a variant from the Ethernet protocol family is used.[59]

The aggregation or access router provides access to the Internet service provider's network, which often is an autonomous system (AS). An aggregation router aggregates the data traffic coming from the users and passes this through. When the destination lies within the network of the ISP it will route the traffic to the next router closer to the destination using an internal routing protocol such as routing information protocol (RIP), interior gateway routing protocol (IGRP), open shortest path first (OSPF) or intermediate system to intermediate system (IS-IS).[60] Within the network users can access services hosted by the Internet service provider, for instance IPTV, HTTP servers, HTTP (cache) servers, database servers and mail servers (see 4.3.3). If the traffic's destinations lies outside the provider's network it will pass through the network – often via 'core' routers – and go to a border router, which is a router that connects the Internet service provider's network with other autonomous systems such as other Internet service providers and Internet exchange points.

The border router uses an external routing protocol in order to communicate with other border routers in other autonomous systems and uses internal routing protocol for routers inside its autonomous system.[61] The protocol it uses for this purpose is border gateway protocol (BGP),

[58] Robert D. Doverspike, K. K. Ramakrishnan and Chris Chase, "Structural Overview of ISP Networks," in *Guide to Reliable Internet Services and Applications*, eds. Charles R. Kalmanek, Sudip Misra and Yang Richard Yang (London: Springer, 2010). p. 36; Juniper Networks, "OSPF Areas and Router Functionality Overview," juniper.net/documentation/en_US/junos12.1/topics/concept/ospf-routing-understanding-ospf-areas-overview.html#id-11620170 (accessed July 9, 2015); RCRWireless, "MPLS PE the Provider Edge," rcrwireless.com/20140513/wireless/mpls-pe (accessed July 9, 2015); Charles M. Kozierok, "OSPF Hierarchical Topology, Areas and Router Roles," tcpipguide.com/free/t_OSPFHierarchicalTopologyAreasandRouterRoles-2.htm (accessed July 9, 2015).

[59] Savvius, "Ethernet Protocols and Packets," wildpackets.com/resources/compendium/ethernet/ethernet_packets (accessed July 9, 2015).

[60] InetDaemon, "Interior Vs. Exterior Routing Protocols," inetdaemon.com/tutorials/internet/ip/routing/interior_vs_exterior.shtml (accessed July 9, 2015).

[61] Ibid.

the successor of external gateway protocol (EGP).[62] This protocol allows a border router to make routing decisions on basis of availability of neighbouring routers, paths and predefined rule sets.[63] The border router communicates the IP-addresses that it can reach to other border routers; or in other words, it tells other border routers "send those packets to me, I know how to deliver them".[64] The autonomous systems create the global coverage of the Internet, through their networks clients can access all sorts of Internet services.

Although the function of various routers is different, their basis is the same, they consist of hardware and firmware enabling basic functionality, atop of the hard and firmware a specialised 'OS' runs specialised applications for routing traffic.

4.3.3 Server side

Clients (users) access almost all Internet services on servers. As such, for every action that involves using the Internet there is a server to facilitate that action – peer-to-peer and other non-client-server models exempt which create 'horizontal' networks between clients. There are many types of servers, such as application, cache, catalogue, communications, database, file, game, mail, message, name, proxy and web servers.[65] Whilst these servers provide different services, their physical design is very similar and resembles that of a 'basic' computer, be it in a more specialised form. Servers can be run from virtually every machine as long it runs software capable of accepting client requests and provide appropriate responses. Although server software can be run from a regular computer, almost all services are placed on servers specifically designed for server tasks.

[62] Y. Rekhter, T. Li and S. Hares, *Request for Comments 4271: A Border Gateway Protocol 4 (BGP-4)* (Fremont: Internet Engineering Task Force,[2006]). pp. 7-8.

[63] Iljitch Van Beijnum, *Bgp* (Sebastopol, CA: O'Reilly, 2002). pp. 19-26.

[64] Iljitch Van Beijnum, "What is BGP, Anyway?" bgpexpert.com/what.php (accessed July 9, 2015).

[65] Kanika Khara, "Different Types of Servers," Buzzle, buzzle.com/articles/different-types-of-servers.html (accessed July 9, 2015); Breylan Communications, "What are some of the Different Kinds of Servers?" breylancommunications.com/productsupport/5/what_are_some_of_the_different_kinds_of_servers.php (accessed July 9, 2015); Scottish Qualifications Authority, "Types of Network Server," sqa.org.uk/e-learning/HardOSEss04CD/page_33.htm (accessed July 9, 2015); Jayaswal, *Administring Data Centers: Servers, Storage, and Voice Over IP*. p. 4.

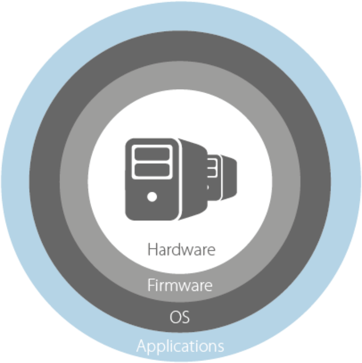

Figure 18 Servers

The architecture of these servers is very similar to that of a computer, at the basis there is hardware (see Figure 18). This hardware can be alike to a desktop computer (without a monitor) or rack-mountable (to be used in server rack). In order to enable the operating systems (OS) to make use of this hardware, firmware is installed on read-only memory (ROM). A server operating system, called a server platform, runs on top of the hardware and firmware, these differ from 'regular' operating systems and are much more specialised. Examples include Microsoft's Windows Server, Apple's OS X Server and a variety of Linux distributions such as Ubuntu Server, Red Hat Enterprise Linux or CentOS.[66] Thus, the basis for a server is (specialised) hardware, firmware and a server platform.

This is, however, only the basis for providing services over the Internet, additional software needs to be installed to make a server provide specific services. A server is simply a basis on top of which software is installed turning it into a more specialised type, such as application, cache, catalogue, communications, database, file, game, mail, message, name, proxy and web servers (see Appendix A). Depending on the software installed, a server can fulfil one or more of these tasks.

4.3.4 Sub-conclusion

The insights from previous sub-sections evidence that the Internet is technical in character. The visual conceptualisation of the Internet is found in the TCP/IP and ISO/OSI models that represent the Internet as a layered construct with distinct technological functionalities. The layers describe functionalities that are present in logical components of the Internet on client devices (e.g. smartphones, tablets, desktops and laptops), intermediary devices (e.g. routers, switches, hubs, bridges and modems) and servers (e.g. application, cache, catalogue, communications, database, file, game, mail, message, name, proxy and web

[66] Kenneth Hess, "Top 10 Linux Distributions of 2015," ServerWatch, serverwatch.com/columns/article.php/3900711/The-Top-10-Linux-Server-Distributions.htm (accessed July 9, 2015); Entrepreneur, "5 Server Operating Systems for Your Business," entrepreneur.com/article/200856 (accessed July 9, 2015).4

servers). The TCP/IP and ISO/OSI models are only concerned with the logical aspects of the Internet, for example, the link (TCP/IP) or link and physical (ISO/OSI) layers only comprise the interface with the hardware and not the actual hardware itself. Although not represented in the visual conceptualisations, the technical perspective on the Internet cannot be seen in isolation from the notion that the foundation of the Internet rests on physical hardware and logical components on clients, intermediaries and servers.

4.4 Cyberspace and the Internet

This section will analyse the gaps and overlaps between the cyberspace (see 4.2) and Internet conceptualisations (see 4.3). In doing so it addresses the second part of the sub-question: how State ('cyberspace') and non-State ('the Internet') conceptualisations relate.

Section 4.2 concluded that the State conceptualisation depicts cyberspace as having four components (or layers): geographic, physical network component, logical network, and cyber persona component. The publications expressing this layered model of cyberspace acknowledge that cyberspace is broader than the Internet. Cyberspace is defined as "the interdependent network of information [or digital] technology infrastructures, (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers) […]".[67] Considering the technical perspective (see 4.3), the relation between the Internet and cyberspace is best characterised as follows: The Internet conceptualisation and technical perspective are an exemplification of the logical and physical network components in the cyberspace model. The Internet conceptualisation specifies software that enables functionality and networking in client devices, intermediaries, and servers.

The cyber persona component and geographical component are not included in the Internet conceptualisations or in the technical perspective. The technical perspective is characterised by a technological focus, considering the Internet to be a technological construct and not necessarily a social-technological construct such as cyberspace, hence it does not include elements such as a cyber-persona component. The non-State perspective does neither involve the geographical component, as the geographical position of devices does not impact networking.

Thus, the Internet conceptualisation is narrower in scope than cyberspace. Cyberspace comprises technological and social aspects of networking whereas the Internet conceptualisation captures only the technological aspects. The relation between the concepts is visually depicted in Figure 19, where the technical perspective on the 'realm' wherein cyber capabilities are used (the Internet) is placed in context with the State perspective (cyberspace).

[67] Ministry of Defence (United Kingdom), *Cyber Primer*. p. 1; Ministry of Defence (United Kingdom), *Cyber Primer*. p. 1-1; United States Army, *Cyberspace Operations Concept Capability Plan 2016 2028*. p. 6.

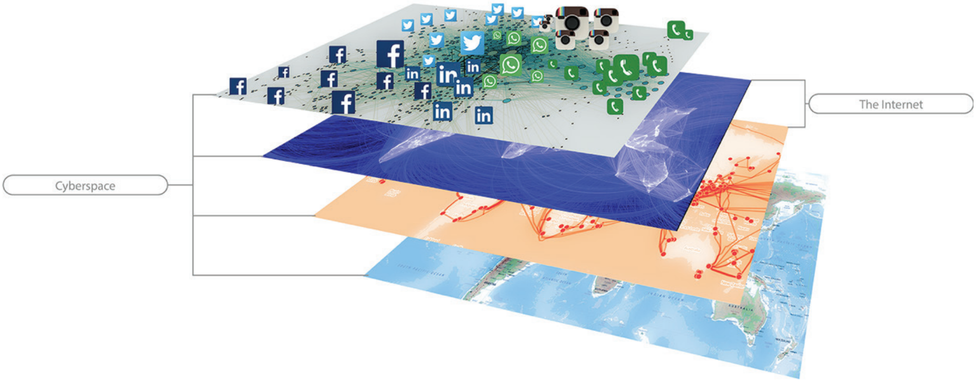

Figure 19 Cyberspace and the Internet

4.5 Cyber capabilities

This section will provide an overview of State and non-State capabilities used in cyberspace by answering the following sub-question: *What cyber capabilities do State and non-State actors use?*

As 'cyber' as prefix has various meanings, the scope and content of the neology created by affixing 'cyber' to a word requires precise definition, in this case: 'cyber capabilities'. As this term is essential for this section, sub-section 4.5.1 will start with defining 'cyber capabilities'. After having defined the term, sub-section 4.5.2 will provide an overview of cyber capabilities being used by State and non-State actors. As last, this section will provide an answer to the sub-question in sub-section 4.5.3

4.5.1 Defining cyber capabilities

This short sub-section will touch upon the two words included in the neology 'cyber capabilities'. The cyber prefix has been discussed in chapter three, there it was concluded that 'affixing the word 'cyber' to a term implies that it relates to cyberspace. Thus understood, affixing capabilities with cyber results in a neology referring to capabilities related to cyberspace.'Capabilities' are defined as "the quality or state of being capable";[68] 'capable' is defined as "having attributes [...] required for performance or accomplishment".[69] A military capability, for instance, is about "the willingness and

[68] Merriam-Webster Dictionary, "Definition of Capability," Merriam-Webster, merriam-webster.com/dictionary/capability (accessed August 8, 2017).

[69] Merriam-Webster Dictionary, "Definition of Capable," Merriam-Webster, merriam-webster.com/dictionary/capable (accessed August 8, 2017).

ability to deploy [means]".[70] A business capability, for example, "is the expression or the articulation of the capacity, materials and expertise an organisation needs in order to perform core functions."[71] In other words, a capability is generally about the attributes required to engage in an activity, examples of attributes are capacity, willingness and ability.

Accordingly, a 'cyber capability' is understood as having the attributes for activity in cyberspace, it involves capacity (means) and subsidiary attributes such as willingness, ability or expertise to engage in activities in cyberspace. Applied to the context of this section, State and non-State cyber capabilities refer to activities being conducted by State and non-State actors in cyberspace.

4.5.2 Overview of cyber capabilities

Cyberspace was defined as comprising four components: the geographical, physical network, logical network, and cyber persona (see section 4.2). This sub-section will use the components to categorise cyber capabilities, however, it will not use the geographical component; as this is 'merely' about the notion that physical network infrastructure is located in other domains (land, sea, air, space) and does not relate to cyber capabilities.

As there are vast amounts of cyber capabilities being used in contemporary society and some uses of cyber capabilities go unnoticed, this sub-section cannot describe all capabilities being used by State and non-State actors. Instead this sub-section will aim to provide an overview of relevant cyber capabilities used by State and non-State actors to influence each other. The selected cyber capabilities are those that are covered in publications within various disciplines. These will be described in general terms as providing an in-depth explanation would go beyond the purpose of this section.

This sub-section will describe cyber capabilities making use of the physical network component (4.5.2.1), the logical network component (4.5.2.2), and the cyber persona component (4.5.2.3). This sub-section will conclude with an overview of cyber capabilities per component (4.5.2.4).

4.5.2.1 *Physical network component*

The physical network component was defined to comprise elements such as hardware, systems software, and infrastructure (see sub-section 4.2.2.1). The elements 'hardware' and 'infrastructure' are logically included under the physical network component. Including 'systems software' in the physical network component on the contrary results in confusion. Systems software includes elements such as the operating system (OS), BIOS/UEFI/EFI (firm-

[70] Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p. 66.

[71] Margaret Rouse, "Business Capability," TechTarget, searchmicroservices.techtarget.com/definition/business-capability (accessed August 8, 2017).

ware) or boot loader (firmware).[72] Although these elements enable functioning of physical hardware, they are software or 'logic'; hence, this sub-section will describe these types of software in the sub-section on the logical network component (see 4.5.2.2). This creates a sharper conceptual distinction between the physical network and logic network components. Thus, this sub-section will discuss illustrative cyber capabilities aimed at the physical network component, namely: hardware Trojans and emanation exploitation.

4.5.2.1.1 Hardware Trojans

The prime concern with hardware used to revolve around "the question how intellectual property can be protected by preventing integrated circuits from being replicated by a competitor".[73] In recent years this has shifted to the issue of "external attacks that use vulnerabilities in transmission protocols or test mechanisms" in hardware.[74] The most prominent issue for hardware being a "Trojan horse",[75] "which adds additional, non-specified functionality to the hardware."[76] This action is about tampering with the "trusted design in an untrusted fabrication facility with the insertion of malicious circuitry that triggers a malfunction conditionally. This malicious circuitry, referred to as a 'hardware Trojan', can trigger and affect normal circuit operation, potentially with catastrophic outcome."[77]

The trigger activating the Trojan can be (1) external via "receiver/antennae [or] access data" or (2) internal via an "always on" or "condition based" configuration such as sensor conditions, for instance temperature and voltage or logic conditions such as "internal state, input or [clock count]".[78] After being triggered, the hardware Trojan can (1) modify the "original functionality of the logic", for instance removing logic, disabling functionality or "addition of extraneous logic to realize something additional to what is intended"; (2) modify the "properties of the chip such as delay to realize their intended objective"; and (3) transmit info, whilst not interfering with the operation of a device, this class of Trojans "emit signals containing such key information [i.e. important internal information embedded within the device]".[79]

[72] Margaret Rouse, "System Software," Tech Target, whatis.techtarget.com/definition/system-software (accessed August 9, 2017).

[73] Christian Krieg et al., "Hardware Malware," in *Synthesis Lectures on Information Security, Privacy, & Trust*, eds. Elisa Bertino and Ravi SandhuMorgan&Claypool Publishers, 2013). p. 7.

[74] Ibid. p. 7.

[75] Department of Defense, *Defense Science Board Task Force on High Performance Microchip Supply* (Washington, D.C.: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, 2005). p. 4.

[76] Krieg et al., "Hardware Malware," in . p. 7.

[77] Francis Wolff et al., "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme" (Munich, ACM, March 10-14, 2008). p. 1.

[78] Mainak Banga, "Partition Based Approaches for the Isolation and Detection of Embedded Trojans in ICs" (Master, Virginia Polytechnic Institute). pp. 10-11.

[79] Mainak Banga, "Partition Based Approaches for the Isolation and Detection of Embedded Trojans in ICs" (Master, Virginia Polytechnic Institute). pp. 12-13.

Hardware manipulation in integrated circuits and other components can serve as a (covert) channel into systems. Physical access is required in order to install covert circuits, which entails having access to the hardware before it reaches the user. Access depends on the location of the hardware (geographical component) and the ability of an actor to reach the hardware. If successfully implemented, this covert channel can serve to manipulate hardware and software on the target system. The effects to which this channel can contribute are diverse, it could be used to monitor the device, get information from and into the system, get information from and to the system's user(s), or manipulate the functioning of a system.

4.5.2.1.2 *Compromising emanations*

There are passive and active attacks that "compromise optical, thermal and acoustic emanations from various kinds of equipment."[80] Passive attacks are those "attacks in which the opponent makes use of whatever electromagnetic signals are presented to him without any effort on his part to create them."[81] Passive attacks come in three forms: 'Hijack', "involving the signal [being] conducted over some kind of circuit (such as a power line or phone line); 'Tempest', involving signals being "radiated as radio frequency energy"; and side-channel attacks.[82]

The first ('Hijack') induces information by analysing timing intervals or power analysis, as different processes consume different lengths of time or levels of power, the attacker can gain insight in the information being processed. [83] The second ('Tempest') induces information from the radio frequency energy of hardware such as displays, laptops, fax machines or Ethernet cables. This enables the attacker to reconstruct information processed on hardware, for instance the contents of a laptop screen "several rooms away, through three plasterboard walls".[84] Other types of passive attacks include optical, acoustic and thermal side-channels through which information can be inferred from hardware. These attacks can induce information from the glow from a monitor reflected on the user;[85] the LED-light status indicators on systems, routers and other equipment;[86] the sound typing makes on a keyboard;[87] or the frequency of capacitors on motherboards.[88]

[80] Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. (Indianapolis: Wiley Publishing, Inc., 2008). p. 523.

[81] Ibid. p. 530.

[82] Ibid. p. 530.

[83] Ibid. pp. 531-532.

[84] Ibid. p. 535.

[85] Markus G. Kuhn, "Optical Time- Domain Eavesdropping Risks of CRT Displays" (Berkeley, IEEE, 12-15 May, 2002).

[86] Joe Loughry and David Umphress, "Information Leakage from Optical Emanations," *ACM Transactions on Information and System Security (TISSEC)* 5, no. 3 (2002), 262-289.

[87] D. Asonov and R. Agrawal, "Keyboard Acoustic Emanations" (Berkeley, IEEE, 12 May, 2004).

[88] Daniel Genkin, Adi Shamir and Eran Tromer, *RSA Key Extraction Via Low-Bandwidth Acoustic Cryptanalysis* (Tel Aviv: Tel Aviv University, 2013).

Active compromisation of emanations involves hostile induced or provoked emanations "from telecommunications and automated information systems equipment".[89] This can be done via Tempest viruses that "infect a target computer and transmit the secret data it steals to a radio receiver hidden nearby [which] can happen even if the machine is not connected to the net"; 'Nonstop' methods that exploit cases where "equipment processing sensitive data is used near a mobile phone, then the phone's transmitter may induce current in the equipment that get modulated with sensitive data by the nonlinear junction effect and reradiated"; or 'selective code execution attack' where an attacker "inserts transients into the power or clock supply [...] in the hope of inducing a useful error".[90] Via active or passive use of emanations an attacker can induce information being processed by the hardware.

4.5.2.2 *Logical network component*

The logical network component was defined as consisting of the logical connections between nodes such as computers, personal digital assistants and cell phones (see section 4.2.2.1). Besides that, the logical network component also includes firmware and software located on systems that enables functioning and use of the system. This sub-section will discuss cyber capabilities aimed at the logical network component, more specifically: firmware (4.5.2.2.1) and software (4.5.2.2.2).

4.5.2.2.1 *Firmware*

Firmware malware is rarely seen outside lab-environments, it has been called an "urban legend" and "the advanced persistent threat equivalent of a Bigfoot sighting".[91] Although there are early 'sightings', firmware malware came of age in 2015,[92] most prominently by the discovery of the advanced-persistent threat "Equation" and series of presentations on information security conferences.[93]

[89] Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. p. 539.

[90] Ibid. pp. 538-541.

[91] Dan Goodin, "Meet "badBIOS," the Mysterious Mac and PC Malware that Jumps Airgaps," Ars Technica, arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/ (accessed August 31, 2015).

[92] Ernesto Corral, "#badBIOS," Security Artwork, securityartwork.es/2013/10/30/badbios-2/?lang=en (accessed August 31, 2015); Goodin, "Meet "badBIOS," the Mysterious Mac and PC Malware that Jumps Airgaps,"

[93] GReAT, "Equation: The Death Star of Malware Galaxy," Securelist, securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/ (accessed August 31, 2015); Serge Malenkovich, "Indestructible Malware by Equation Cyberspies is Out there - but Don'T Panic (Yet)," blog.kaspersky.com/equation-hdd-malware/7623/ (accessed Augst 31, 2015); Corey Kallenberg and Xeno Kovah, *How Many Million BIOSes would You Like to Infect?*Legbacore, 2015); Trammel Hudson, Xeno Kovah and Corey Kallenberg, *Thunderstrike 2 Sith Strike: A MacBook Firmware Worm*, 2015); Darlene Storm, "Macs can be Remotely Infected with Firmware Malware that Remains After Reformatting," Computerworld, computerworld.com/article/2955641/cybercrime-hacking/macs-can-be-remotely-infected-with-firmware-malware-that-remains-after-reformatting.html (accessed August 31, 2015); Lucian Constatin, "Design Flaw in Intel Processors Opens Door to Rootkits Researcher Says," PCWorld, pcworld.com/article/2965872/components-processors/design-flaw-in-intel-processors-opens-door-to-rootkits-researcher-says.html#tk.rss_security (accessed August 31, 2015).

Firmware runs when booting a machine, "it launches the operating system", which is a point where antivirus and other security controls are not yet loaded.[94] When the BIOS/UEFI/EFI of a system is infected, firmware malware can "be used to render a computer unusable, [...] steal passwords and intercept encrypted data."[95] Infecting the firmware of a system can be done "via a phishing mail and a malicious site", via peripheral devices (e.g. adapters and USB devices), and via the network.[96] Some firmware infections can be removed by re-installing the operating system. There is firmware malware, however, that is considered "an ultimate persistence mechanism, and it has the ultimate resilience to removal [...]", it is called "nls_933w.dll" and was used by the Equation APT.[97] This firmware gives an attacker "eternal persistence that allows them to survive disk formatting and operating system reinstalls [and act as] undetectable persistent storage inside the hard drive."[98] Thus, firmware malware as cyber capability opens up new channels into a system, once settled it can be used at the attackers discretion.

4.5.2.2.2 Software

Hardware and firmware infection occur rarely and only target a "very select list of victims".[99] The common user or administrator will often not be target of these types of cyber capacities. They are far more likely to be targeted by cyber capabilities aimed at the software, such as the operating system or applications, located on client, intermediary or server systems. The software of a system is an attractive target as users and administrators secure these components; it is the user or administrator's duty to secure the system via updates, patches and general responsible use. As many users are blissfully unaware of this responsibility and lack the knowledge to adequately perform these actions and administrators sometimes lack the resources and knowledge as to specific types of attacks, there are many weaknesses to be exploited in the software on these systems. This sub-section will first discuss cyber capabilities aimed at systems in general (4.5.2.2.2.1) and then focus on specific capabilities aimed at the network (4.5.2.2.2.2) and servers (4.5.2.2.2.3)

4.5.2.2.2.1 Systems in general

There are many tools "focused on gaining access to systems and escalating [the] level of privilege".[100] Targeted systems could comprise client-devices such as mobile phones, tablets, laptops or desktops; intermediary devices such as routers and switches; and servers. These are all protected by very similar access controls; hence, the cyber capabilities that can

[94] Storm, "Macs can be Remotely Infected with Firmware Malware that Remains After Reformatting,"

[95] Mark Wilson, "LightEater Malware Attack Places Millions of Unpatched BIOSes at Risk," Beta News, betanews.com/2015/03/21/lighteater-malware-attack-places-millions-of-unpatched-bioses-at-risk/ (accessed August 31, 2015).

[96] Kallenberg and Kovah, *How Many Million BIOSes would You Like to Infect?*; Hudson, Kovah and Kallenberg, *Thunderstrike 2 Sith Strike: A MacBook Firmware Worm*; Storm, "Macs can be Remotely Infected with Firmware Malware that Remains After Reformatting,"

[97] Michael Mimoso, "Inside NLS_933W.DLL, the Equation APT Persistence Module," Threat Post, threatpost.com/inside-nls_933w-dll-the-equation-apt-persistence-module/111128 (accessed August 31, 2015).

[98] Ibid.

[99] Ibid.

[100] Andress and Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. p. 118.

be used against them are similar. This sub-section will discuss ways of obtaining access by (1) using flaws in authentication and (2) exploiting vulnerabilities.

Flaws in authentication

Access to most systems is restricted via username and password, which can be considered a relatively safe access control, however, most users do not update their passwords regularly, use the same passwords across different systems and generally use poorly constructed passwords. Their username often is simple to guess (e.g. their full name or initials) and the administrative accounts are the default ones (admin, administrator, root, test, guest, etc.). Apart from that, users increasingly post personal information on social-media, which proves to be a treasure trove for those wishing to break a user's password. Passwords are often based on names of loved ones, sports clubs, pets, children, etc.; most people list these parameters on their social-media profiles.

If the user's password is not based on any of these parameters, but it is too simple, an attacker can still guess the password. Password tools can break simple passwords with ease; these tools, for instance, parse a list of frequently used passwords and/or usernames, parameters derived from social-media and other websites and try these credentials against the authentication mechanism of a system. Popular password cracking tools are THC-Hydra, Inguma, John the Ripper or Cain and Able, but there are many more, all tailored to a specific system or password (e.g. clear-text, dictionary, rainbow tables, etc.).[101]

Exploiting vulnerabilities

Systems are often protected by a security perimeter consisting of elements such as firewalls, passwords, operating systems design, application design, and malware detection. Of course, there are gaps in the perimeter, these weaknesses and vulnerabilities offer attackers ways of entering and/or manipulating a system. These weaknesses and vulnerabilities are often discovered by an attacker through tools that fingerprint the system (e.g. revealing OS, version, ports used, etc.); using specialised online vulnerability databases (e.g. Shodan); or simply by using Google to search for specific information regarding a target. Although manual matching of vulnerabilities is possible and sometimes necessary, increasingly attackers use automated tools for entering systems. The most prominent and illustrative of these (semi-)automated tools is the "Metasploit framework" (MSF),[102] however, there are many other frameworks such as Kali Linux, Immunity's Canvas, and Core Impact.[103]

[101] Kali Linux, "Kali Linux Tools: Passwords," tools.kali.org/tag/passwords (accessed September 1, 2015).

[102] Rapid 7, "The Attacker's Playbook: Test Your Network to Uncover Exploitable Security Gaps with Metasploit." rapid7.com/products/metasploit/ (accessed March 14, 2014).

[103] Kali Linux, "What is Kali Linux," docs.kali.org/introduction/what-is-kali-linux (accessed August 31, 2015); Immunity, "Canvas," Immunity, immunityinc.com/products/canvas/ (accessed August 10, 2017); Core Security, "Core Impact," Core Security, coresecurity.com/core-impact (accessed August 10, 2017).

The Metasploit framework is “a free, open source penetration testing framework” with the “world’s largest database of tested exploits”.[104] Metasploit enables an attacker to (1) “collect information [...] using scanning and vulnerability assessment tools, such as nmap”; (2) “select an exploit that matches the system based on the collected information”; (3) “select a payload to accompany the exploit, often a remote shell”; and (4) “execute the exploit and payload”.[105] The exploit is “a code which allows an attacker/pentester to take advantage of the vulnerable system and compromise its security”.[106] The exploits could be aimed at the operating system (OS) or the applications on a systems, for instance the browser, compressing utilities (e.g. zip), software-managing utilities, coding frameworks, certain protocols, antivirus, file readers, file formats, VPN software, etc. The payload is “the actual code which does the work [...] it runs on the system after exploitation”, it is the mechanism that enables action after entry is gained via the exploit.[107] Payloads have different functions and manipulate different components of a system, very similar to exploits.

Once an attacker is inside, either via guessing credentials, social engineering or exploiting vulnerabilities, the attacker can use the system at his discretion. The system could be used to get information about the user or system, the network of the user or system, turned into a zombie, get information to the user or system, install additional software, make configuration changes, render the system inoperable, etc.

4.5.2.2.2.2 Network

Instead of targeting the client, intermediary or server systems, some cyber capabilities are aimed at the network they create, which is often called “network hacking” or network attack.[108] This sub-section will describe two types of cyber capacities aimed at the network, namely: (1) wiretapping and (2) (distributed) denial-of-service.

Wiretapping

Packet analysis, that is, “capturing [...] data passed over the local area network”, used to be performed by system administrators “to troubleshoot network problems [...]”.[109] The use of packet analysis tools, however, moved away from their original intent: “packet sniffers are considered security tools instead of network tools now.”[110] Packet analysis in the context of security tools comes in two forms: passive and active wiretapping. Wiretapping in general is “an attack that intercepts and accesses information contained in a data flow in

[104] Monika Agarwal and Abhinav Singh, *Metasploit Penetration Testing Cookbook*, 2nd ed. (Birmingham: Packt Publishing, 2013). p. 9.

[105] Andress and Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. p. 120.

[106] Agarwal and Singh, Metasploit Penetration Testing Cookbook. p. 8.

[107] Ibid. p. 8.

[108] Bastian Ballman, *Understanding Network Hacks: Attack and Defense with Python* (Berlin: Springer-Verlag, 2015). p. 35.

[109] Andrian Hannah, “Packet Sniffing Basics,” Linux Journal, linuxjournal.com/content/packet-sniffing-basics (accessed September 5, 2015).

[110] Ibid.

a communication system" in attempting "to observe the data flow and gain knowledge of information contained in it".[111]

Passive wiretapping aims "only to observe a communication flow and gain knowledge of the data it contains, but does not alter or otherwise affects that flow."[112] The most basic form of passive wiretapping is simply installing a sniffing tool, for instance Wireshark or TCPdump and monitoring network flows.

The active variant of wiretapping does "alter data being communicated or otherwise [affects] data flow".[113] The alteration could comprise "substituting valid data" or "introducing false data [...] that serves to deceive" other entities (e.g. users, administrators, authorised processes).[114] These alterations could serve, for instance, to conduct a hijack attack by seizing "control of a previously established communication association";[115] to conduct a man-in-the-middle attack through which the attacker functions "as a clandestine proxy server between [users] to capture or modify sensitive information that [the users] think they are sending only to each other;"[116] or to engage in replay/playback attacks that "maliciously or fraudulently" intercept data and retransmit it.[117] Examples of tools for carrying out these types of active wiretapping attacks are Ettercap, sslstrip, evilgrade or Ncat.[118] By gathering information on the network flows an attacker gains insight in, for example, the network architecture, active systems, and data such as user information, credentials etc.

(Distributed) Denial of Service

A denial of service (DoS) attack prevents "authorised access to a system resource or [delays] systems operations and functions".[119] This is a relatively simple attack as the only requirement is that the attacker knows the address of his target and the susceptibility of the target to the DoS attack. There are two forms of DoS attack: denial of service (DoS) attack and distributed denial of service (DDoS) attack.

DoS attacks are generally aimed at "flooding services or crashing services. Flood [or buffer overflow] attacks occur when the system receives too much traffic for the server to buffer,

[111] R. Shirey, *Request for Comments 4949: Internet Security Glossary Version 2* (Fremont: Internet Engineering Task Force,[2007a]). pp. 336.337.

[112] Ibid. p. 213.

[113] Ibid. p. 15.

[114] Ibid. p. 126.

[115] Ibid. p. 141.

[116] Ibid. p. 248.

[117] Ibid. p. 248.

[118] Alberto Ornaghih et al., "Welcome to the Ettercap Project," ettercap.github.io/ettercap/index.html (accessed August 10, 2017); Offensive Security, "Sslstrip," Offensive Security, tools.kali.org/information-gathering/sslstrip (accessed August 10, 2017); Infobyte, "Evilgrade," infobyte, github.com/infobyte/evilgrade (accessed August 10, 2017); Nmap, "Ncat Users' Guide," Nmap, nmap.org/ncat/guide/ (accessed August 10, 2017).

[119] Shirey, Request for Comments 4949: Internet Security Glossary Version 2. p. 100.

causing them to slow down and eventually stop." [120] There are many methods for flooding targets, such ping floods, smurf attack, fraggle attack and syn floods. Methods for crashing services are tools such as ping of death or teardrop attack. All these attacks use flaws in particular networking protocols in order to deny a system to users or slow down the system.

DDoS attacks are very similar to DoS attacks as they use similar flaws in network protocols. These DoS attacks, however, are then 'distributed' to other systems, resulting in the target machine being attacked from "multiple computers".[121] At the centre of DDoS attacks and many other cyber capabilities "is a large pool of compromised computers located in homes, schools, businesses, and governments around the world."[122] These so-called 'zombies' are used "as anonymous proxies to hide their real identities and amplify their attacks. Bot software enables an [attacker] to remotely control each system and group them together to form what is commonly referred to as a zombie army or botnet."[123] In creating DDoS capability an attacker faces two issues, first he has to propagate malware ('bot software') that compromises target systems and secondly he has to be able to communicate with the compromised systems.[124]

Propagation has moved from a "manual installation process [to] multiple automated propagation vectors", resulting in automated compromise of vulnerable systems.[125] Communication or command and control, the second issue, could be addressed by using different command and control topologies: centralised, peer-to-peer and unstructured.[126] The method for command and control of Botnets has steadily become "more sophisticated – moving from simple readily detectable IRC communication to complex anonymity providing [peer-to-peer] communication."[127] Once the attacker has overcome the issues he can use the network for DDoS attacks, however, also for myriads of other 'attacks' such as distributing other malware, spam, phishing campaigns, click fraud, search engine optimisation, storing and serving illegal material or mining cryptocurrency.

4.5.2.2.2.3 Server

As mentioned in sub-section 4.3.3, the foundations of servers are similar; they are distinctive through the applications or web applications installed on the server. These web applications are different from each other and each "may contain unique vulnerabilities."[128] Often

[120] Palo Alto Networks, "What is a Denial of Service Attack (DoS)?" Palo Alto Networks, paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos (accessed August 10, 2017).

[121] United States Computer Emergency Response Team, "Security Tip (ST04-015): Understanding Denial-of-Service Attacks," US-CERT, us-cert.gov/ncas/tips/ST04-015 (accessed August 10, 2017).

[122] Michael Bailey et al., "A Survey of Botnet Technology and Defenses" (Washington, D.C., March 3-4, 2009). p. 299.

[123] Ibid. p. 299.

[124] Ibid. pp. 299-300.

[125] Ibid..

[126] Michael Bailey et al., "A Survey of Botnet Technology and Defenses". pp. 299-300.

[127] Ibid. p. 300.

[128] Dafydd Stuttard and Marcus Pinto, *The Web Application Hacker's Handbook: Finding an Exploiting Security Flaws*, 2nd ed. (Indianapolis: John Wiley & Sons, Inc., 2011). p. 3.

these web applications “require connectivity to internal computer systems that contain highly sensitive data and that can perform powerful business functions.”[129] Consequently, web applications are an attractive target.

The majority of web applications are insecure and affected by vulnerabilities such as: broken authentication (enabling guessing of weak passwords, bypassing login or brute-forcing); broken access controls (enabling viewing of “other users’ sensitive data held on the server or carry out privileged actions”); SQL injection (enabling “an attacker to submit crafted input to interfere with the application’s back-end databases” which allow the attacker to “retrieve arbitrary data from the application, interfere with its logic, or execute commands on the database server”); cross-site scripting (enabling “an attacker to target other users of the applications, potentially gaining access to their data, performing unauthorised actions on their behalf, or carrying out other attacks against them”); information leakage (the “application divulges sensitive information that is of use to an attacker in developing an assault against the application”); or cross-site request forgery (enabling an attacker interact on an authorised user’s behalf “to perform actions that the user did not intend”).[130] Tools for attacking web applications include tool suites such as Burp Suite, WebScarab, paros and Zed Attack Proxy.[131] Cyber capabilities aimed at servers allow an attack to gather information about the users or systems, the network of the users or systems, install additional software, make configuration changes, render the system inoperable, etc.

4.5.2.3 Cyber persona component

The cyber persona component is the digital representation of people in cyberspace.[132] Although impossible to verify or contradict, almost every person has attributes in cyberspace, a cyber persona of sorts. Even if individuals resist to creating a cyber persona, the surrounding network constructs a persona for them, either ‘implicitly’ or ‘explicitly’. Implicitly as a consequence of his surroundings having a cyber persona with a common denominator, being, the person not being online. This implicit persona is called a “shadow profile”.[133]

[129] Ibid. p. 3.

[130] Ibid. pp. 7-8.

[131] PortSwigger, “Burp Suite,” PortSwigger, portswigger.net/burp (accessed August 11, 2017); Open Web Application Security Project, “OWASP WebScarab Project,” OWASP, owasp.org/index.php/Category:OWASP_WebScarab_Project (accessed August 11, 2017); Kuen and Mike, “Paros,” sourceforge.net/p/paros/wiki/Home/ (accessed August 11, 2017); Open Web Application Security Project, “OWASP Zed Attack Proxy Project,” OWASP, owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project (accessed August 11, 2017).

[132] The Joint Chiefs of Staff, Joint Publication 3-12 (R): Cyberspace Operations. p. I-3.

[133] Emre Sarigol, David Garcia and Frank Schweitzer, “Online Privacy as a Collective Phenomenon” (Dublin, Conference on Online Social Networks, October 1-2, 2014); Chloe Albanesius, “Facebook Ireland Facing Audit Over Privacy, ‘Shadow Profiles’,” PC Magazine, pcmag.com/article2/0,2817,2395109,00.asp (accessed July 14, 2015); Kate Knibbs, “What’s a Facebook Shadow Profile, and Why should You Care?” Digital Trends, digitaltrends.com/social-media/what-exactly-is-a-facebook-shadow-profile/ (accessed July 14, 2015); David Veldt, “Is LinkedIn the Creepiest Social Network?” Gizmodo, gizmodo.com/is-linkedin-the-creepiest-social-network-498946693 (accessed July 14, 2015); The Archive Team, “Friendster Snapchot Collection,” Internet Archive, archive.org/details/archive-team-friendster (accessed July 14, 2015); Jamie Condliffe, “Even if You Don’T use Social Networks, they Still Know Stuff about You,” Gizmodo, gizmodo.com/even-if-you-dont-use-social-networks-they-still-know-s-1643246882 (accessed July 14, 2015).

Explicit cyber persona creation occurs as a consequence of societies being increasingly informationised. As societies increase to be informationised, citizens acquire a cyber persona as records are digitised, for instance social security numbers, birth certificates, bank accounts, postal addresses, student and staff numbers, employment history and other personally identifiable information. These records are stored digitally on a database server in a local area network (intranet) or wide area network (Internet). In other words, even if a person resists to having a cyber persona, the efforts are thwarted by contemporary society. Thus, it is safe to assume that almost every human being can potentially be influenced via his or her cyber persona.

This sub-section will discuss cyber capabilities aimed at influencing the cyber personas. In order to be able to be capable of influencing humans via their cyber persona the attacker needs information, for instance, whom to target. Therefore, this sub-section will start with describing cyber capabilities aimed at gathering information about cyber personas (4.5.2.3.1). After having information regarding the target, an attacker can use cyber capabilities to engage the cyber persona. This sub-section will describe the cyber capabilities aimed at engagement as second (4.5.2.3.2).

4.5.2.3.1 Gathering information

The practice of gathering information about cyber personas is known as target group analysis (traditional marketing),[134] target audience analysis (military),[135] or the more modern 'customer intelligence'.[136] The goal of each of these concepts is to segment "large, heterogeneous markets into smaller segments that can be reached more efficiently and effectively with products and services that match their unique needs."[137] Segmenting factors that could be taken into account are: geographic ("nations, states, regions, counties, cities, or even neighbourhoods"); demographic (age, life-cycle stage, gender, income, occupation, educations, religion, ethnicity, and generation"); psychographic ("social class, lifestyle, or personality characteristics"); and behavioural ("user status, usage rate, loyalty status").[138] This sub-section will first discuss why these insights are required for engagement (4.5.2.3.1.1) and secondly describe cyber capabilities for creating insight (4.5.2.3.1.2).

4.5.2.3.1.1 Relevance

The segmenting factors serve to select the most effective message, transmitter and channel for a specific receiver and destination. Different target groups are receptive to different forms of engagement. Those without smartphones (receiver) cannot receive Whatsapp messages (channel), those without a Twitter profile cannot receive Tweets directed at them,

[134] Gary Armstrong and Philip Kotler, *Marketing: An Introduction*, 12th ed. (London: Pearson Education, 2015). pp. 199-206.

[135] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p I-4.

[136] Margaret Rouse, "Customer Intelligence (CI)," Techtarget, searchbusinessanalytics.techtarget.com/definition/customer-intelligence-CI (accessed July 16, 2015).

[137] Armstrong and Kotler, *Marketing: An Introduction*. p. 199.

[138] Armstrong and Kotler, *Marketing: An Introduction*. pp. 199-206.

those without a phone number cannot be phoned. Engaging a target group has become a great deal more complicated than before, there are considerably more transmitters/encoders, receivers/decoders and channels (see Figure 20).

As a consequence of the complexity, understanding the target group is more important than ever. Before being able to engage and influence cyber personas via cyber capabilities, one must now identify what devices people are using to send and receive messages ('encoder'/'decoder' in Figure 20) and what channels they are using (see Figure 20, e.g. Tumblr, Facebook, Instagram, Linkedin, Mail, Pinterest, YouTube, Google+, RenRen, Xing, Short Message Service, Whatsapp, regular telephone or VoIP telephone). These types of channels have different means of messaging, for instance via video (e.g. YouTube), image (e.g. Pinterest and Instagram), written text (e.g.pWhatsapp, SMS) audio (e.g. telephone) or a combination thereof (Facebook, Twitter, Linkedin, RenRen, Xing, etc.). Besides that, communication or engagement does not take place in splendid isolation; there are complicating factors such as personal context, situational context and different types of noise (see Figure 20). Context and noise as complicating factors will be briefly described in the following paragraphs.

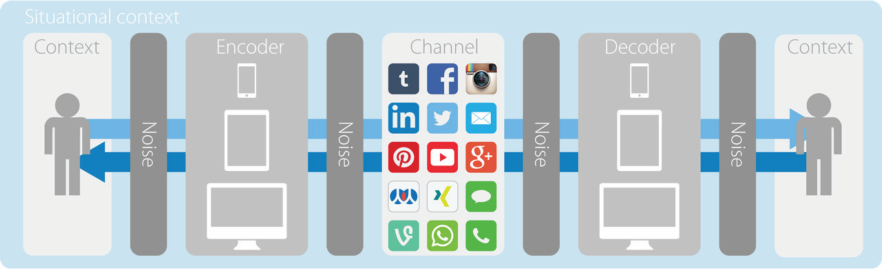

Figure 20 Online engagement.[139]

Context "is multidimensional and can be physical, cultural, psychological, or historical".[140] Physical context is about the location or "environmental conditions", cultural context "refers to the rules, roles, norms, and patterns of communication that are unique to particular cultures", social-emotional context refers to the "relational and emotional environment in which communication occurs [e.g.] friendly or unfriendly, supportive or unsupportive" and historical context expresses the mechanism that "messages are understood in relationship to previously sent messages".[141] When for instance, somebody tries to communicate with a person in a crowded room or in extreme heat the physical context can impair the effectiveness of the message. Communicating without taking note of certain norms (cultural context) the person may take offense and ignore the message. Trying to intimidate someone via a message – an unfriendly message – may or may not

[139] Loosely based on: C. E. Shannon, "A Mathematical Theory of Communication," Bell System Technical Journal 27, no.3 (1948), 379-423.

[140] Richard West and Lynn H. Turner, *Understanding Interpersonal Communication: Making Choices in Changing TImes*, 2nd ed. (Boston: Wadsworth Cengage Learning, 2009). pp. 14-15.

[141] Ibid. pp. 14-15.

impede effectiveness of the message (social-emotional context), safe to say is that such a message will have an impact on the receptiveness to future messages (historical context).

Apart from context as complicating factor there is noise, which is "anything that interferes with accurate transmission or reception of a message."[142] There are four types of noise that can occur at any time when communicating, namely: physical, physiological, psychological and semantic noise.[143] Physical noise is external noise and "involves any stimuli outside of the receiver that makes the message difficult to hear", physiological noise "refers to biological influences on message reception [such as] hearing or visual impairments, and the physical well-being of a speaker", psychological noise is internal noise and "refers to a communicator's biases, prejudices, and feelings towards a person or a message" and semantic noise "occurs when senders and receivers apply different meaning to the same message [e.g.] jargon, technical language, and other phrases that are familiar to the sender but that are not understood".[144] Whereas physiological, psychological and semantic noise are identical in the context of cyber capabilities, physical noise – or rather external noise in order to comprise both physical and logical sources – could include elements such as severed physical connections (e.g. unplugged Ethernet cable or transatlantic fibre-optic cable damage); server downtime (e.g. scheduled maintenance or DDoS attack); power outage; connection downtime (e.g. no connection to ISP or faulty settings); or device downtime (e.g. empty battery or loss of access).

Understanding a target group's preferred encoders/transmitters, decoder/receivers, channels, situational context, personal context and potential noise sources is imperative for effective target group engagement. These aspects could be taken into account before engaging a target group, however, most of the time this is a process of trial and error based on partial understanding of the target group. The following sub-section will describe cyber capabilities aimed at creating understanding of the target group.

4.5.2.3.1.2 Data mining

As Internet usage surges and the use of social-media rises, many companies have specialised in analysing target audiences. Whilst it is possible to analyse virtual target groups manually,[145] this is a very labour-intensive activity. Since almost every activity online is monitored and logged, from visiting websites,[146] to using social-media,[147] to online banking

[142] Ibid. p. 13.

[143] Ibid; Frank R. Oomkes, *Communicatieleer*, 8th ed. (Amsterdam: Boom, 2003). pp. 33-34.

[144] West and Turner, Understanding Interpersonal Communication: Making Choices in Changing TImes. pp. 13-14.

[145] Emmanuel Trenche, "5 Ways to Get Customer Intelligence for Free," Business 2 Community, business2community.com/customer-experience/5-ways-get-customer-intelligence-free-0686435 (accessed July 17, 2015).

[146] Google, "Measure Learn and Grow," google.com/analytics/standard/ (accessed July 17, 2015); Matt McGee, "Google Analytics is Installed on More than 10 Million Websites," Marketing Land, marketingland.com/google-analytics-is-installed-on-more-than-10-million-websites-9935 (accessed July 17, 2015).

[147] YouTube, "YouTube Analytics Basics," support.google.com/youtube/answer/1714323?hl=en (accessed July 17, 2015); Harry Readhead, "Your Facebook, Twitter and Blog are about to be Monitored for References to the Government," Metro, metro.co.uk/2015/06/05/your-facebook-twitter-and-blog-are-about-to-be-monitored-for-references-to-the-government-5232639/ (accessed July 17, 2015); Facebook, "Platform Insights: Measure and

and all other actions,[148] it increasingly becomes feasible to automatically generate target group (or market) insights. These insights can capture almost any aspect of an individual's life: sentiment at a given time, location, relationship status, financial status, social network(s), employment history, education, political preferences, sexual preferences, shopping habits, devices used to browse the Internet, IP address, MAC address and many more. The large quantities of data are analysed via a method called 'data mining'.[149]

Data mining is part of a process called knowledge discovery in databases (KDD); it is about the "nontrivial process of identifying valid, novel, potentially useful, and ultimately understandable patters in data."[150] Nontrivial implies inference; data mining "is not a straightforward computation of predefined quantities like computing the average value of a set of numbers."[151] Process implies "that KDD comprises many steps, which involve data preparation, search for patterns, knowledge evaluation and refinement, all repeated in multiple iterations."[152] The data analysed can comprise virtually any form of digitised information. Before being able to mine the data, it has to be selected, pre-processed and transformed. After the data mining is done, the outcome has to be interpreted and evaluated.

Data mining tools come in different forms, all of them have the ability to aggregate and correlate data. These tools have been employed from the late 1990s until now within different sectors, for instance science (image analysis), marketing (customer intelligence and behaviour forecasting), investment (managing portfolios), fraud detection (identifying financial transactions), manufacturing (fault detection) and telecommunication (rule detection).[153] These tools can map intricate (social) networks, map who is most influential, and all of the insights in online behaviour mentioned earlier (sentiment, location, relationship status, etc.).[154] The insights generated with these tools are presented in a human understandable such as graphs, heat maps, map clusters, word clouds and a variety

Optimize Your Facebook Page Or Domain," developers.facebook.com/docs/platforminsights (accessed July 17, 2015); Alex Fitzpatrick, "Facebook Monitors Your Chats for Criminal Activity [REPORT]," Mashable, (accessed July 17, 2015).

[148] Catherine New, "Beyond Card Fees: Banks Look to Sell Your Data," Daily Finance, dailyfinance.com/2011/10/25/beyond-card-fees-banks-look-to-sell-your-data/ (accessed July 17, 2015); Blake Ellis, "The Banks' Billion-Dollar Idea," CNN, money.cnn.com/2011/07/06/pf/banks_sell_shopping_data/ (accessed July 17, 2015); Consumer Reports, "Big Brother is Watching," consumerreports.org/cro/money/consumer-protection/big-brother-is-watching/overview/index.htm (accessed July 17, 2015).

[149] Seán Kelly, *Customer Intelligence: From Data to Dialogue* (Chichester: John Wiley & Sons Ltd, 2006). p. 60.

[150] Usama Fayyad, Gregory Piatetsky-Shapiro and Padhraic Smyth, "From Data Mining to Knowledge Discovery in Databases," *AI Magazine* 17, no. 3 (1996), 37. p. 40.

[151] Usama Fayyad, Gregory Piatetsky-Shapiro and Padhraic Smyth, "From Data Mining to Knowledge Discovery in Databases. p. 41.

[152] Ibid.

[153] Ibid. p. 39.

[154] Salesforce Radian6, "Marketing Cloud: Radian6 Introduction," esources.docs.salesforce.com/rel1/radian6/en-us/static/pdf/MarketingCloudRadian6Introduction.pdf (accessed August 20, 2015); See for instance: Klout, "The Klout Score," klout.com/corp/score (accessed August 20, 2015).

of other formats. Irrespective of its form, all tools are aimed at creating understanding of the (online) surroundings of a brand, company, or other organisation.

KDD and data mining can serve to analyse target audiences, they deliver insights rapidly and can be used to differentiate a large audience into smaller target groups sharing common characteristics. As these smaller audiences are more homogeneous, messages can be tailored more specifically and effectively to their needs. Apart from increasing understanding of the target audience it can serve to illuminate influential persons (so called key-influencers in industries or key-leaders/stakeholders in the military) and many other facets. Notwithstanding the complexity and broad use of these capabilities, "they are not a substitute for the creativity of the human actor".[155] Nevertheless, as the rate of data creation has and will continue to increase exponentially, data mining tools have become vital in analysing target groups with more than a few persons. The data mining tools serve to create understanding of target groups and to consequently decide which capabilities to use to engage with them most effectively and efficiently. The cyber capabilities aimed at engagement will be discussed in the following sub-section.

4.5.2.3.2 *Engagement*

Via the channels and devices depicted in Figure 20, organisations and individuals can create effects in target groups. These effects can range from being constructive ("helping to develop or improve something") to destructive ("causing destruction or harm") and from very intrusive to not intrusive. [156] Apart from using the channel to spread messages, an organisation could also deny, disrupt or destroy the channel to prevent communication from taking place. The capabilities described below are neutral, they are not necessarily constructive or destructive, intrusive or not intrusive: they are 'simply' channels of communication in contemporary society. This sub-section will describe the following cyber capabilities aimed at engaging cyber personas: websites, social media, mail, instant messaging, text messages, forums, blogs and other capabilities.

4.5.2.3.2.1 *Websites*

Online presence of an organisation, groups or individuals often starts with building a website that functions as a hub, "a centralised place where people can go to learn more about what an organisation has to offer, [find contact information, engage with content and the ability to interact with the organisation]".[157] The benefits of having a website is the "power to change [an organisation's] messaging and imaging within seconds."[158] Apart from that,

[155] Kelly, *Customer Intelligence: From Data to Dialogue*p. 61; Tyler Vigen, "Spurious Correlations," tylervigen.com/spurious-correlations (accessed August 20, 2015). See also:

[156] Merriam-Webster Dictionary, "Constructive," merriam-webster.com/dictionary/constructive (accessed August 21, 2015); Merriam-Webster Dictionary, "Destructive," merriam-webster.com/dictionary/destructive (accessed August 21, 2015).

[157] Kate Erickson, "7 Ways to Build Your Online Presence Now," eofire.com/7-ways-to-build-your-online-presence/ (accessed August 24, 2015).

[158] Chuck Cohn, "A Beginner's Guide to Establishing an Online Presence on a Budget," Forbes, forbes.com/sites/chuckcohn/2015/03/13/a-beginners-guide-to-establishing-an-online-presence-on-a-budget/ (accessed August 24, 2015).

websites serve as a tool for one-to-many asynchronous communication (organisation to group). Having a website does not, however, necessarily result in the target group automatically visiting the website, for that, other capabilities are needed such as search engine optimisation ("what you can do to improve your search results"), search engine marketing ("what search engines can do for you" to be found online) and increasingly important: social media.[159]

4.5.2.3.2.2 Social media

Some consider social media to be a revolutionary new reality, but social media only is "a new set of tools, new technology that allows us to more efficiently connect and build relationships [...]. It's doing what the telephone, direct mail, print advertising, radio, television and billboards did for us up until now [...]".[160] Before being able to engage with a target group using social media, an organisation or individual requires a social-media profile, as social media sites are often isolated from non-users to some extent.[161] The activities an individual or organisation could engage in on social media are listening (or consuming), reacting (or curating), producing (or creating) or interacting (or collaborating).[162]

Listening is very similar to target group analysis (see 4.5.2.3.1); it is about understanding the online sentiment (also called 'buzz') regarding a particular issue and the persons or parties engaged in an issue. Understanding buzz is made easy by social media analysis tools, which resemble data mining tools. After generally understanding the environment, an organisation or individual could take steps to react to content created by others, for instance correct erroneous facts, rectify a situation or concur with a post.[163] An organisation could also produce own messages or content; the format (text, photo, audio, or video) of the content depends on the platform used. Every social networking site has specific dynamics regarding content, Facebook, Linkedin and Twitter can facilitate most formats whilst Instagram centres on photo and video, and YouTube focuses on videos. By listening, reacting, creating content, and interacting an organisation or individual can build a virtual community and gains a foothold in the 'buzz' surrounding relevant issues.

In sum, social media can serve to listen, react to, create content for, and interact with online communities consisting of cyber personas. Social media can facilitate asynchronous one-to-many communication (organisation posts content) and many-to-one communication (community gives feedback). They also often facilitate synchronous communication, for instance one-to-one (e.g. Facebook's instant messaging service) or

[159] Leland Harden and Bob Heyman, *Digital Engagement* (New York: Amacom, 2009). p. 76.

[160] Lon Safko, The Social Media Bible: Tactics, Tools and Strategies for Business Success, 3rd ed. (New Jersey: John Wiley & Sons, 2012). p. 5.

[161] Ibid. p. 43.

[162] Dave Evans and Jake McKee, *Social Media Marketing: The Next Generation of Business Engagement* (Indianapolis: Wiley Publishing, Inc., 2010). pp. 15-19; The Rackspace, "Five Function of Effective Social Marketing Strategy," rackspace.com/blog/social-marketing-strategy/ (accessed August 25, 2015).

[163] Jeremiah Owyang, "Diagram: How the Air Force Responds to Blogs," web-strategist.com/blog/2008/12/31/diagram-how-the-air-force-response-to-blogs/ (accessed August 25, 2015).

one-to-many communication (instant messaging groups). The range of possible activities is limited only by an organisation or individual's creativity; there are many creative ways of engaging online communities both constructively, destructively and anything in between.

4.5.2.3.2.3 Mails

Cyber persona engagement is also possible via electronic mail, referred to as 'mail' in this sub-section. Before being able to use mail, an organisation or individual needs the mail addresses of the target group. Many people litter mail addresses across the web, for example on company websites or social media profiles. Besides that, there are established practices of getting a target group to disclose mail addresses, for instance "put an email sign-up box prominently" on websites, make "promotions and special offers" to provide an incentive for signing up, buy "lists of consumer names" or "put ads and links in specialised email newsletters".[164] There are also data mining tools for gathering mail addresses automatically.

Mail is "one of the oldest forms of digital [...] media, and it is by far one of the most effective ways to stay in touch with your customers, transact with them, resolve their issues, recruit new customers, and develop [a] trusted network", whilst being "practically free."[165] Many mail users receive large quantities of mail and deem a large portion of those to be spam, that is, "unsolicited commercial [or] bulk email".[166] If a user decides the mail is not relevant (psychological noise) or is considered spam by the spam filters ('logical' noise) the message will most likely not be read. The timeframe in which a user decides whether the mail is relevant is "roughly 1.5 seconds"; hence understanding of the target group is essential to best tailor the mail to the recipient.[167]

Mails aimed at a target group can be used for constructive and destructive effects both as asynchronous one-to-one (organisation to individual) and one-to-many communication (organisation to group). Informing a target group on a particular issue or asking feedback on an issue is an example of constructive usage. Phishing, spear-phishing and whaling mails are examples of disruptive uses of the mail channel to get sensitive information from a target group.[168]

4.5.2.3.2.4 Instant messaging

Organisations and individuals increasingly use instant messaging platforms such as Whatsapp, Facebook Messager, WeChat, Line and Viber.[169] Instant messaging services offer new channels for engaging cyber personas. Instant messaging platforms enable the

[164] Microsoft, "Seven Ways to Get Customer Email Addresses," microsoft.com/en-us/business/articles/seven-ways-to-get-customer-email-addresses (accessed August 26, 2015).

[165] Safko, The Social Media Bible: Tactics, Tools and Strategies for Business Success. p. 63.

[166] Indiana University, "What is Spam?" kb.iu.edu/d/afne (accessed August 26, 2015).

[167] Safko, The Social Media Bible: Tactics, Tools and Strategies for Business Success. p. 73.

[168] Andress and Winterfeld, Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners.

[169] Casengo, "How to WhatsApp Your Way into Extraordinary Customer Service," casengo.com/blog/how-to-whatsapp-your-way-into-extraordinary-customer-service/ (accessed August 26, 2015); Catherine Clifford, "Top 10 Apps for Instant Messaging," Entrepreneur, entrepreneur.com/article/230335 (accessed August 26, 2015).

creation of chat rooms or conversations with single or multiple individuals on basis of a mobile phone number or social media account. Before being able to create a chat room, an organisation or individual needs the phone numbers or social media account names of the target group.

Some people are listed in white and yellow page phonebooks with their mobile number, others have their mobile number listed in their social media profile and there are some who have no public record of their mobile number. An organisation could take the same type of actions as with getting mail addresses to learn the numbers of the target audience (i.e. provide incentives for subscription, buy mobile phone lists, etc.). After having obtained the phone numbers of a target group, an organisation could use the instant messaging channel for synchronous one-to-many (organisation to group), many-to-one (group to organisation) and one-to-one communication (organisation to individual). The effects, again, depend on the message, not on the channel. Contrary to mail, instant messaging is closer to real-time communication, after having received a message the receiver is prompted to open and read the message.

4.5.2.3.2.5 Text messages

Although being very similar to instant messaging, short messaging service (SMS) uses “the fundamental voice network, [...] making it a universal service.”[170] Every mobile phone with a cellular signal can send and receive text messages whilst instant messaging can only be done on smartphones connected to the Internet. Text messaging via SMS offers no possibilities to add media (audio, images, videos). A protocol offering this functionality is Multimedia Messaging Service (MMS), which is often integrated in proprietary mobile operating systems (e.g. Apple’s Message app). MMS, logically, requires more bandwidth and thereby negates the universality of SMS. Contrary to instant messaging, group chats are not integral to SMS applications, hence, it primarily serves synchronous one-to-one communication (organisation to individual). There are, however, solutions for sending SMS messages to groups of contacts.[171] Before being able to do so an organisation needs to find out the phone numbers within the target group, ways of finding these out have been described above (see 4.5.2.3.2.4).

4.5.2.3.2.6 Forums

Another type of channel for engaging with cyber personas is a discussion site such as forums or community bulletin boards. A forum “is a web site application that manages and provides a medium for on-going online discussion on a particular subject,[172] these sites ”contain several categories, consisting of [sub-forums], topics and individual posts.”[173] When con-

[170] Robert Triggs, “What is SMS and how does it Work?” Android Authority, androidauthority.com/what-is-sms-280988/ (accessed August 14, 2017).

[171] See for instance: FrontlineSMS, “The FrontlineSMS Platform,” FrontlineSMS, frontlinesms.com/product (accessed August 11, 2017).

[172] Safko, The Social Media Bible: Tactics, Tools and Strategies for Business Success. p. 120.

[173] vBulletin, “Forums, Topics and Posts,” vbulletin.com/forum/help?faq=vb3_board_usage#faq_vb3_forums_threads_posts (accessed August 26, 2015).

ducting target group analyses, it may become apparent that the target group is using a particular forum. Apart from being a rich source of information regarding topics of interest of a particular target group, the forum can also serve as channel. Organisations can react and interact with individuals regarding specific issues of interest. Dedicated forums, not being facilitated by social media, often require separate credentials; hence organisations need to create a profile before being able to engage cyber personas via forums. Forums facilitate asynchronous many-to-many (group to group) communications; anyone can talk to those engaged on the same forum. Forums can be used constructively for sending out informational messages or for disruptive effects via trolls, flame wars and forum spamming.[174]

4.5.2.3.2.7 Blogs

Web logs or 'blogs' are online journals "maintained by an individual with regular entries or posts that include commentary, thoughts, and ideas, and may contain photos, graphics, audio, or video."[175] Blogs can be "personal- or business-related", the latter can be used "for internal communication to employees, or designed to be viewed by the public".[176] These business-related, public or corporate blogs can be used for "sales, marketing, branding, PR, and communicating with customers and prospects."[177] Starting a blog is "as simple as going to Wordpress [a blogging website], creating an account, selecting the New Post button, typing your thoughts, and hitting Publish."[178] Apart from a blog hosted by a third-party (e.g. Wordpress), corporate blogs can also be maintained on an organisation's website. Blogs differ from 'regular' content on a website as it is more detailed and often less formal in tone and expresses the writers view on an issue. Potential readers (the virtual community) sometimes are made aware of new blog via Rich Site Summary (RSS, "a format for delivering [updates on] regularly changing web content"), social media, mailings or other channels.[179] As with other channels blogs can be used for a variety of purposes, such as highlighting successes, informing the target group, or slandering an opponent.

4.5.2.3.2.8 Other capabilities

The previous sub-sections have described how websites, social media, mailing, instant messaging, text messaging, forums and blogs can serve as (relatively) new channels for engaging with cyber personas. There are, of course, many other capabilities not covered here that could affect cyber personas. This section, for instance, has not covered Wiki's, Podcasts, Vlogs, livecasting and photo sharing. These capabilities, however, resemble the capabilities described above which are the most illustrative for a range of capabilities. Apart from that, this section has also not covered traditional means of influencing humans such as talks, telephone, direct mail, print advertising, radio, television and billboards. These traditional means may affect cyber personas as well, a telephone call to somebody

[174] Safko, The Social Media Bible: Tactics, Tools and Strategies for Business Success. pp. 125-126.

[175] Ibid. p. 145.

[176] Ibid. p. 145.

[177] Ibid. p. 145.

[178] Safko, The Social Media Bible: Tactics, Tools and Strategies for Business Success. p. 155.

[179] What Is RSS, "RSS Explained," whatisrss.com (accessed August 28, 2015).

in a target group may result in him posting a message on Twitter recounting the call for instance. The capabilities described above are relatively novel ways making use of cyberspace to influence groups and individuals via their cyber persona in contemporary society, they should be seen as an addition and not a substitute to the more traditional ways of influencing target groups.

These capabilities can be used for various goals, the most prominent in the realm of information security is their use for social engineering. Social engineering "is a method of gaining access to systems, data, or buildings through the exploitation of the human psychology. Instead of using technical techniques or breaking in, social engineering involves non-technical schemes that attackers employ."[180] These methods include, for instance, use of (spear-) phishing mail, phone calls or the media described above to get a user or administrator to disclose sensitive information such as credentials.[181]

4.5.2.4 Overview

This sub-section has described the cyber capabilities being used by State and non-State actors. These capabilities were categorised by using the physical network, logical network, and cyber persona components of the cyberspace conceptualisation. Sub-section 4.5.2.1 has discussed cyber capabilities aimed at the physical network component, that is, hardware Trojans and emanation compromise. Sub-section 4.5.2.2 has reflected on the following cyber capabilities aimed at the logical network component: firmware malware, authentication flaw exploitation, social engineering, vulnerability exploitation, wiretapping, denial of service, distributed denial of service, SQL injection, cross-site scripting and cross-site request forgery. Sub-section 4.5.2.3 has examined cyber capabilities aimed at the cyber persona component, resulting in the following cyber capabilities: data mining, websites, social media, mail, instant messaging, text messages, forums and blogs. These cyber capabilities have been mapped to their respective cyberspace component in Table 5.

[180] Vince Reynolds, Social Engineering: The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception (North Charleston: CreateSpace, 2016). p. 13.

[181] There are also specialised technological frameworks tailored to social engineering such as the Social Engineering Toolkit (SET) and Maltego inc Social Engineer: "Maltego," Social Engineer, inc., social-engineer.org/framework/se-tools/computer-based/maltego/ (accessed August 10, 2017); inc Social Engineer, "The Social Engineering Framework," Social Engineer, inc., social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/ (accessed August 10, 2017).

Cyberspace component	**Cyber capability**
Cyber persona	• Data mining • Websites • Social media • Mail • Instant messaging • Text messages • Forums • Blogs • Social engineering
Logical network	*Firmware* • Firmware malware injection Systems in general • Authentication flaw exploitation • Vulnerability exploitation *Network* • Wiretapping • Denial of service attack • Distributed denial of service attack *Server* • SQL injection • Cross-site scripting exploitation • Cross-site request forgery
Physical network	• Hardware Trojan injection • Emanation compromise
Geographic	

Table 5 Overview illustrative cyber capabilities

4.5.3 Sub-conclusion

This section has aimed to create an illustrative overview of State and non-State cyber capabilities by answering the following sub-question: *What cyber capabilities do State and non-State actors use?* In order to answer the sub-question, sub-section 4.5.1 has started by defining 'cyber capabilities'. It concluded that in the context of this section a 'cyber capability' refers to activities being conducted in cyberspace. After having defined the term, sub-section 4.5.2 has discussed cyber capabilities being used by State and non-State actors. The sub-section combined the definition of cyber capabilities with the cyberspace conceptualisation by using the cyberspace components to categorise cyber capabilities.

The answer to the sub-question is provided by the overview in Table 5. There are, however, many more cyber capabilities used by State and non-State actors. The general categories depicted in Table 5 could be further divided in many sub-categories with specific cyber capabilities aimed at specific systems or applications. As such the overview is by no means exhaustive, the overview is merely a representative reflection of cyber capabilities used by State and non-State actors in contemporary society.

The cyber capabilities are not categorised by using their intent, that is, offensive, defensive or exploitation (i.e. gathering information). Considering the cyber capabilities included in the overview, some may conclude that the focus of the included cyber capabilities is offensive and/or exploitation and not defensive. Many of the cyber capabilities in the overview, however, can also be used for defence. For example, data mining could be used to process data for attributing cyber activities, engagement of cyber personas could be aimed at internal communication creating security awareness in personnel, wiretapping could be done to monitor suspicious behaviour on networks, web application security tools can be used to scan potentially vulnerable applications, modules could be introduced in hardware in order to enable secure backdoor access, etc. Thus the cyber capabilities are intent-agnostic, they could serve offensive, defensive or exploitation activities.

4.6 Conclusion

This chapter has sought to create understanding of cyberspace and cyber capabilities by addressing the following sub-question: *How are cyber capabilities conceptualised and utilised?*

The first part of the research question – how cyber capabilities are conceptualised– was answered in sections 4.2 and 4.3. The State conceptualisation in the form of the 'cyberspace' construct was found to be broad enough to encompass the technical perspective of the Internet. Cyberspace was defined as comprising four layers or components: cyber persona, logical network, physical network, and geographical. The second part of the research question – how cyber capabilities are utilised by State and non-State actors – was answered in section 4.5 by providing an illustrative overview of cyber capabilities being used in contemporary society. The cyber capabilities being used today were categorised per component.

4.6.1 Relevance

The insights from this chapter serve to highlight the cyber capabilities involved in military cyber operations and the environment wherein these capabilities are used. These capabilities constitute an integral part of military cyber operations and the utility of military cyber operations is determined, in part, by the technical proficiency of an actor in harnessing cyber capabilities. Although there are exemptions in which an actor can influence in or through cyberspace without technical proficiency, for instance in the case of the institutional power, the ability of an actor to integrate cyber capabilities determines the possible uses of military cyber operations.

This research, so far, has discussed three of five perspectives impacting the utility of military cyber operations. The 'power' perspective has highlighted for what purposes actors seek to influence each other and the factors that determine whether they succeed at doing so. The 'societal' perspective has provided the contemporary informationised context wherein actors seek to influence each other with new means such as 'cyber'. This chapter, the 'technological' perspective, adds the insight with which novel cyber capabilities actors can influence each other. Although general in character and not yet tailored to military cyber operations, the cyber capabilities described above illustrate the potential of military cyber operations.

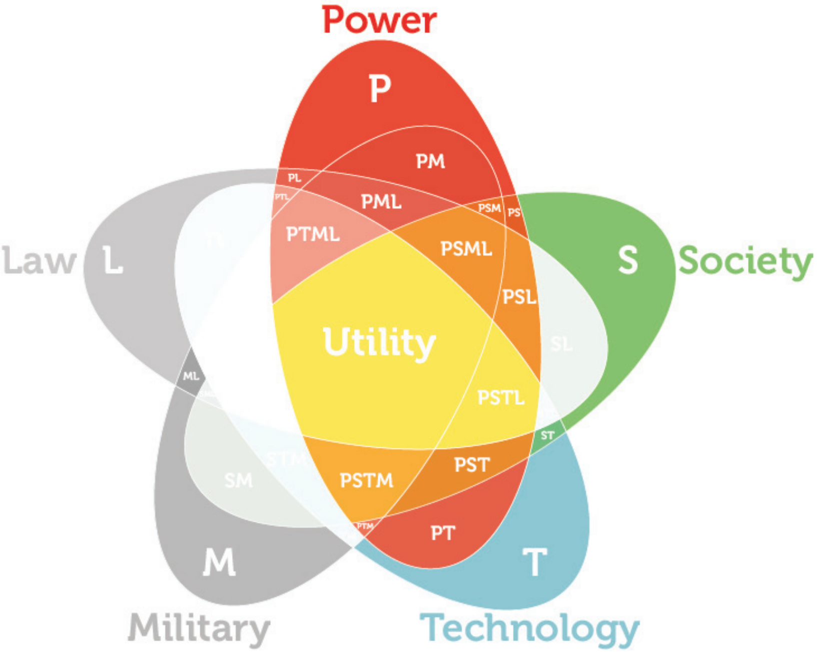

Figure 21 'Power', 'society' and 'technological' perspective on the utility of military cyber operations.

5

On Fighting

5 On Fighting

5.1 Introduction

The military's operating context in contemporary society is "characterised by the existence of multi-dimensional problems (e.g. security, failed public systems, economic misery), paradox (simultaneous existence of inconsistent states), and stakeholders within and outside a theater having diverse and contradictory logics".[1] Military organisations, however, still "define themselves in terms of capabilities required for successfully handling violent conflicts by creating military advantage".[2] Consequently, in the contemporary context "military organisations need to rethink their capabilities [...] current and future capabilities should enable organisations to handle activities across the full spectrum of violence with a variety of organisations, anywhere on the globe."[3] This complex context requires the military to develop, strengthen, or diversify organisational capabilities.[4]

Due to informatisation every State instrument has informational or 'cyber' aspects, including the military instrument (see chapter three). Apart from the military's aforementioned general challenges due to complexity of the operating context, there is a specific challenge of integrating new cyber capabilities (see chapter four). Many militaries from the 2000s until now have taken up this challenge integrated cyber capabilities within their organisation.[5] The military has organised these capabilities in 'military cyber operations', one of the pivotal notions in this research.

5.1.1 Goal of this chapter

This chapter will focus on creating understanding of military cyber operations and its relation with other military operations. Understanding of the concept and use of military cyber operations is essential for assessing the utility of military cyber operations. Therefore, this chapter will focus on military organisation in general and the place of military cyber operations in specific by answering the following sub-question: What is the conceptual place of cyber capabilities within the military organisation and how are cyber capabilities integrated in the armed forces?

[1] Joseph Soeters, Paul C. van Fenema and Robert Beeres, eds., *Managing Military Organisations: Theory and Practice* (Abingdon: Routledge, 2010). p. 256.

[2] Ibid. p. 257.

[3] Ibid. pp. 257-258.

[4] Ibid. p. 258.

[5] See: James R. Clapper, Marcel Lettre and Micahel S. Rogers, Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States (Washington, D.C.: U.S. Senate Armed Services Committee, 2017).

5.1.2 Structure

In order to answer the sub-question this chapter will first discuss the basic concepts in military organisation. Before being able to conduct any activity at all in furtherance of strategic goals, the military requires the conceptual, moral and physical attributes for doing so. These aspects are embodied in the concept of fighting power which will be discussed in section 5.2. By organising fighting power, the military can manifest fighting power by using it´s capabilities in the form of military operations. The conceptual foundations and types of military operations will be discussed in section 5.3. After having discussed fighting power and military operations as the basic concepts in military organisation, this chapter will focus on the place of cyber capabilities within military organisation in section 5.4. This chapter will conclude with answering the sub-question in section 5.5.

5.2 Fighting power

This section will highlight the concept of fighting power by answering the sub-question: What is fighting power? In order to answer the sub-question this section will first reflect on the concept of fighting power itself (5.2.1) and then on its constituent components (5.2.2).

5.2.1 Fighting power in general

Fighting power, consisting of a conceptual, moral and physical component "has been used in doctrine since the 1990s".[6] The components have, however, "played a major role in the deployment of the armed forces" throughout history.[7] For instance Fuller in 1929 deemed that "human force is threefold: it is mental, moral and physical, and no one of these forms of force can be expended without influencing the remaining two."[8] The expression of these components in the unifying concept of fighting power "became common in Martin van Creveld's much debated work on the American and German soldiers in the Second World War".[9] Creveld defines fighting power as "the sum total of mental qualities that makes armies fight and it rests on mental, intellectual, and organisational foundations".[10] There are also other definitions of fighting power, French deems fighting power to be "composed of three elements, the conceptual, the material, and the moral."[11] Carrier defines fighting

[6] Dutch Ministry of Defence, *Netherlands Defence Doctrine* (Den Haag: Ministerie van Defensie, 2013). p. 63.

[7] Ibid. p. 63.

[8] J. F. C. Fuller, *The Generalship of Ulysses S. Grant* (New York: Dodd, Mead and Company, 1929). p. 10.

[9] Richard Carrier, "Some Reflections on the Fighting Power of the Italian Army in North Africa, 1940– 1943," *War in History* 22, no. 4 (2015), 503-528. p. 508.

[10] Richard Carrier, "Some Reflections on the Fighting Power of the Italian Army in North Africa, 1940– 1943." p. 508.

[11] David French, Raising Churchill's Army: The British Army and the War Against Germany, 1919-1945 (Oxford: Oxford University Press, 2000). p. 11.

power “as the capacity (‘the ability to understand or to do something’) to engage the enemy and to sustain combat.”[12]

As this chapter is discussing the foundations of military organisation, it will use the military description of fighting power. The military defines fighting power as “the ability to conduct military operations in a cohesive totality”.[13] The components of fighting power are depicted in Figure 22 and described as follows: “it consists of a conceptual component (the ideas behind how to operate and fight), a moral component (the ability to get people to operate and fight) and a physical component (the means to operate and fight).”[14] By harmonising these components the military is able to effectively conduct military operations and contribute to achieving strategic goals.[15]

Although being a military and Western approach to military organisation, the concept of fighting power is sufficiently general to comprise contemporary approaches to force projection. For instance, the three components are not explicitly mentioned in Russian doctrine and whitepapers, but the publications incorporate very similar themes such as training,[16] education,[17] equipment,[18] morale,[19] and military planning.[20] Also when looking at Chinese doctrine, the components of fighting power are reflected in their publications, the following concepts are earmarked: “deployment (bushu)”, “coordination (xietong)” and “command (zhihui)”.[21] Although not using the same wording as Western doctrine, the Chinese and Russian views affirm that fighting power or military power in general comprise certain components required for conducting military activities. The names of the components are different; however, they essentially are concepts/ideas/education, means/methods/training, and morale/mindset/psyche. Thus, at a conceptual level the concept of fighting power, or military organisation in general, is fairly universal. The following sub-section will describe the components involved in the concept of fighting power.

[12] Carrier, “Some Reflections on the Fighting Power of the Italian Army in North Africa, 1940– 1943.” p. 509.

[13] Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p. 66.

[14] British Army, *Army Doctrine Publication: Operations* (Shrivenham: Development, Concepts and Doctrine Centre, 2010). p. 2-2.

[15] Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p. 63.

[16] Ministry of Defence of the Russian Federation, *Aktual’nyye Zadachi Razvitiya Vooruzhënnykh Sil Rossiyskoy Federatsii* [The priority tasks of the development of the Armed Forces of the Russian Federation] (Moscow: Ministry of Defence of the Russian Federation, 2003). pp. 69-82; Security Council of the Russian Federation, *Military Doctrine Russian Federation* [ОЕННАЯ ДОКТРИНА РОССИЙСКОЙ ФЕДЕРАЦИИ] (Moscow: Security Council of the Russian Federation, 2010). ss. 40-44.

[17] Ministry of Defence of the Russian Federation, Aktual’nyye Zadachi Razvitiya Vooruzhënnykh Sil Rossiyskoy Federatsii . pp. 86-93.

[18] Ibid. pp. 82-84.

[19] Ibid. pp. 96-103.

[20] Security Council of the Russian Federation, *Military Doctrine Russian Federation*. ss. 35-37.

[21] Nan Li, “The PLA’s Evolving Campaign Doctrine and Strategies,” in *The People’s Liberation Army in the Information Age*, eds. James C. Mulvenon and Richard H. Yang (Santa Monica: RAND, 1999), 146-174. pp. 151-161.

5.2.2 Components of fighting power

The components of fighting power are conceptual, moral and physical, these will be described in this sub-section. The conceptual component "provides a framework of thinking within which military personnel can develop understanding about both their profession and the activities that they may have to undertake."[22] The aim of the conceptual component is "to provide the intellectual basis for [Armed Forces]; theoretically justify providing and employing [Armed Forces]; and preserve and take forward corporate memory, experience and knowledge."[23] Besides understanding, this component comprises 'education, innovation and lessons'; and doctrine (see Figure 22). Education, innovation and lessons are aimed to continually improve the conceptual component through conceptual innovation, "whereby consideration is given to what changes could occur because of a changing environment, new technologies and challenges".[24] Doctrine "is the formal expression of military thinking, valid for a particular period of time".[25] As such it lies at the core of the conceptual component, however, to properly understand doctrine, "the arguments, the underlying motives, the alternatives and the context that have led to this doctrine" have to be understood as well.[26]

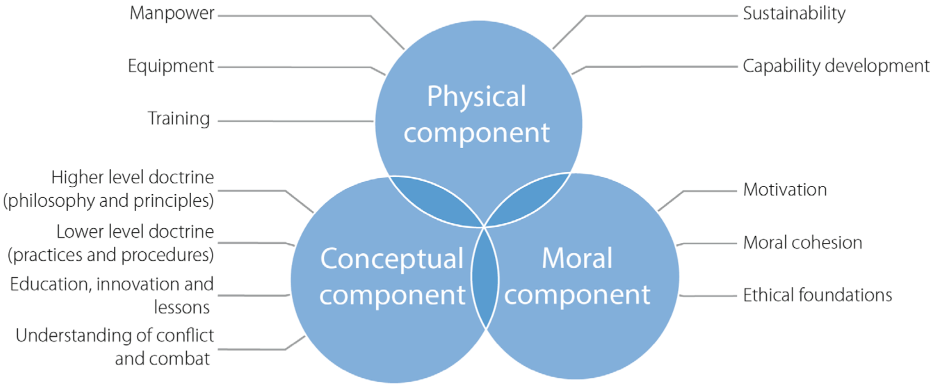
Manpower
Equipment
Training
Higher level doctrine (philosophy and principles)
Lower level doctrine (practices and procedures)
Education, innovation and lessons
Understanding of conflict and combat
Physical component
Conceptual component
Moral component
Sustainability
Capability development
Motivation
Moral cohesion
Ethical foundations

Figure 22 Components of fighting power[27]

[22] Ministry of Defence (United Kingdom), *Joint Doctrine Publication 0-01: UK Defence Doctrine*, 5th ed. (Shrivenham: Ministry of Defence, 2014). p. 27.

[23] Ibid. p. 27.

[24] Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p. 71.

[25] Ibid. p. 71.

[26] Ibid. p. 71.

[27] Based on figure 2.1 in British Army, *Army Doctrine Publication: Operations*. p. 2-2; Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p. 66. See also: Colin S. Gray, "RMAs and the Dimensions of Strategy," *Joint Force Quarterly*, no. Autumn/Winter (1998). p. 50.

The moral component "exerts a decisive psychological influence, both individually and collectively. Whilst morals (principles of right and wrong) are one aspect which enhances cohesion and morale (a sense of confidence and well-being) is another which promotes courage and commitment, the moral component is considerable broader."[28] The moral component involves moral cohesion ("prepared to fight"), motivation ("enthused to fight") and leadership ("inspired to fight") as depicted in Figure 22.[29]

The physical component is "underpinned by the conceptual and moral components; alone, it does not adequately compensate for their absence. On the other hand, without physical delivery the moral and conceptual component remain [...] in a theoretical domain."[30] In other words, the physical component provides the means to engage in military operations: "manpower, equipment, collective performance through integrated education, training and the coherent development of capabilities; the ability to deploy, globally if necessary; and sustainment, all at the required state of readiness."[31]

5.2.3 Sub-conclusion

This brief section has highlighted the concept of fighting power by reflecting on the concept of fighting power (see 5.2.1) and its components (see 5.2.2). The answer to the sub-question – what is fighting power - is that fighting power is a military concept of organising the military by taking into account different components required for the military organisation to function, namely: the conceptual, moral and physical. These components are described separately to categorise elements that are required for military organisation, however, only together the elements constitute fighting power. The pivotal notion is that fighting power is "more than the availability of operational means [(physical component)]; there must also be the willingness and ability to deploy these means [(moral component)]; [...] and a well-considered, doctrine-based deployment method [(conceptual component)]."[32] In other words, the military instrument requires the elements included in all three components of fighting power to engage in military activities more commonly known as military operations. The latter will be the subject of the following section.

5.3 Military operations

The military can manifest fighting power in the form of military operations. A military operation is "a military action or the carrying out of strategic, tactical, service, training, or administrative military mission; the process of carrying on combat, including movement,

[28] Ministry of Defence (United Kingdom), Joint Doctrine Publication 0-01: UK Defence Doctrine. p. 32.

[29] Ibid. p. 33.

[30] British Army, Army Doctrine Publication: Operations. p. 2-31.

[31] Ibid. p. 2-31.

[32] Dutch Ministry of Defence, *Netherlands Defence Doctrine*. p. 66.

supply, attack, defence and manoeuvres needed to gain the objectives of any battle or campaign."[33] NATO's 1973 definition of a military operation was updated in 2014 to a more general description: "A sequence of coordinated action with a defined purpose", noting that "NATO operations are military" and "NATO operations contribute to a wider approach including non-military actions".[34] The latter reflects the contemporary approach to wielding State instruments, namely, in an integrated way as embodied in smart power, whole-of-government, comprehensive and JIMP approaches (see Chapter Three). This section will aim to describe the conceptual foundations and types of military operations conducted by the military instrument, it will do so by answering the sub-question: How are military operations conceptualised and utilised by the military instrument?

This section will start with describing the conceptualisation of the operational environment in which military operations take place (5.3.1). This understanding of the operational environment is essential for determining the relation to the cyberspace conceptualisations. After having discussed the operational environment, this section will discuss what types of military operations are utilised by the military (5.3.2). Understanding the types of military operations conducted is essential for assessing the function of military cyber operations in the military. As last, this section will conclude with answering the sub-question (5.3.3).

5.3.1 The operational environment

The operational environment is the conceptual 'place' where military operations are conducted, it consists of the "composite of the conditions, circumstances and influences that affect the employment of capabilities and bear on the decisions of the commander."[35] The operational environment "encompasses physical areas of the air, land, maritime, and space domains; the information environment (which includes cyberspace); the electromagnetic spectrum; and other factors."[36] Understanding of the operational environment gives insight in how the military conceptualises military operations. The following sections will highlight elements included in the operational environment construct by discussing environments (5.3.1.1), dimensions (5.3.1.2), domains (5.3.1.3) and layers (5.3.1.4).

[33] North Atlantic Treaty Organisation, Allied Administrative Publication 06: NATO Glossary of Terms and Definitions (English and French) (Brussels: NATO Standardization Agency, 2012). p. 2-O-2.

[34] North Atlantic Treaty Organisation, Allied Administrative Publication 06: NATO Glossary of Terms and Definitions (English and French) (Brussels: NATO Standardization Agency, 2014). p. 2-O-2.

[35] North Atlantic Treaty Organisation, Allied Administrative Publication 06: NATO Glossary of Terms and Definitions (English and French). p. 2-O-3.

[36] The Joint Chiefs of Staff, *Joint Publication 3-0: Joint Operations* (Washington, D.C.: The Joint Chiefs of Staff, 2017b). p. xiv.

5.3.1.1 *Environments*

Following the definition of the operational environment it consists of (1) physical areas; (2) the information environment; (3) the electromagnetic spectrum; and (4) other factors. The latter will not be discussed in this sub-section, 'other factors' strikes as a catchall phrase; besides that, it is not further defined. This section will describe the other three elements of the operational environment and their relations.

Physical areas include factors such as "terrain, population, weather, topography, hydrology, EMS, and other environmental [(i.e. relating to the natural world)] conditions".[37] This thesis will refer to these factors as the 'physical environment' as implicitly acknowledged in doctrine. The operational environment also comprises one explicit sub-environment, namely: the information environment. The information environment "is the aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information."[38] The electromagnetic spectrum (EMS) is defined as "the highly regulated continuum of [electromagnetic waves]", the electromagnetic spectrum "is constrained by both civil uses and adversary attempts to deny the use of the EMS – creating a congested and contested environment."[39] The notion of EMS as equal order concept as the information environment is contested as another publication states that information,[40] cyberspace, and electronic warfare operations are "conducted in the information environment".[41] Following this line of reasoning, the electromagnetic spectrum is a lower order concept than the information environment. This points to the issue that the electromagnetic spectrum is difficult to categorise as physical or informational as it utilises physical and information elements, whilst at the same time enabling physical networking and informational networking. For conceptual clarity, this thesis will not consider the electromagnetic spectrum or the electromagnetic operating environment to be an equal-order concept as the physical and information environment. Electronic warfare, the EMS and the electromagnetic operating environment will be discussed in more depth in section 5.4.1.2. In sum, the operational environment consists of two sub-environments the physical and information environment as depicted in Figure 23.

[37] Ibid. p. xiv.

[38] The Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations* (Washington, D.C.: The Joint Chiefs of Staff, 20 November 2014). p. I-1. See also: Marc Romanych and Robert Cordray III, "Objectives in the Information Environment," *IOSphere*, no. Winter 2006 (2006); Daniel Ventre, *Information Warfare*, 2nd ed. (London: Wiley, 2016). pp. 257-262; Arto Hirvelä, "Discovering how Information Warfare Distorts the Information Environment," in *Proceedings of the 5th European Conference on Information Warfare and Security*, ed. Dan Remenyi (Reading: Academic Conferences Limited, 2006). pp. 73-74.

[39] The Joint Chiefs of Staff, *Joint Publication 3-13.1: Electronic Warfare* (Washington, D.C.: The Joint Chiefs of Staff, 2012). p. I-1.

[40] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. ix.

[41] Department of the Army, *Field Manual 3-12: Cyberspace and Electronic Warfare Operations* (Washington, D.C.: Department of the Army, 2017). p. 1-12.

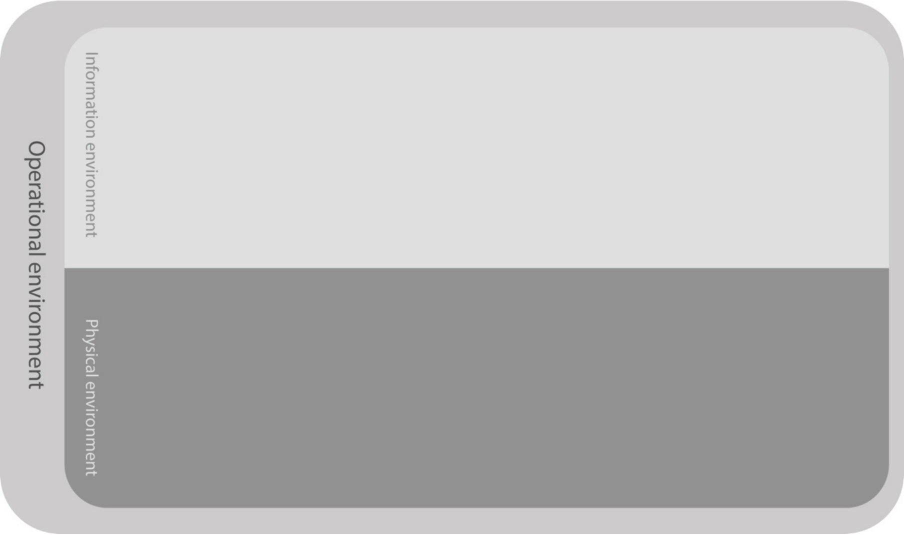

Figure 23 Operational environment and sub-environments

5.3.1.2 Dimensions

Dimensions are used within the concept of the information environment to refer to different informational aspects of the operating environment. Within the information environment, there are three dimensions: physical, virtual and cognitive.[42] The physical dimension "includes, but is not limited to, human beings, C2 facilities, newspapers, books, microwave towers, computer processing units, laptops, smart phones, tablet computers, or any other objects that are subject to empirical measurement."[43] As such, the physical dimension of the information environments encompasses "the tangible elements of cyberspace and access to the EMS".[44] The virtual dimension "encompasses where and how information is collected, processed, stored, disseminated, and protected".[45] The cognitive dimension "encompasses the minds of those who transmit, receive, and respond to or act on information. It refers to individuals' or groups' information processing, perception, judgment, and decision making."[46] These elements are impacted by factors such as "individual and cultural beliefs, norms, vulnerabilities, motivations, emotions, experiences, morals, education, mental health, identities, and ideologies."[47] There are

[42] The Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*. pp. I-2 and I-3; See also: Blaise Cronin and Holly Crawford, "Information Warfare: Its Application in Military and Civilian Contexts," *The Information Society* 15, no. 4 (1999). pp. 257-258; Ventre, *Information Warfare*. pp. 262-264; See also: Cordray III and Romanych, "Mapping the Information Environment." pp. 7-8.

[43] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. I-2.

[44] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations. p. 1-13.

[45] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. I-3.

[46] Ibid. p. I-3.

[47] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. I-3.

different names for the dimensions in different military doctrines, the cognitive dimension in U.S. and U.K. doctrine is known as the psychological dimension within NATO.[48] The informational dimension in U.S. doctrine is known as the virtual dimension in NATO and U.K. doctrine.[49]

The only elements not included in the descriptions of the dimensions are physical factors such as: terrain, weather, topography, hydrology, and other environmental conditions (see 5.3.1.1). These elements clearly belong to the physical environment; however, they do not constitute the physical dimension of the information environment (as this was defined to include objects and persons holding or acting on information – see above). This thesis will hold that these entities reside in the physical environment. These factors are instrumental to military operations and may impact decisions, however, they do not hold or act on information.

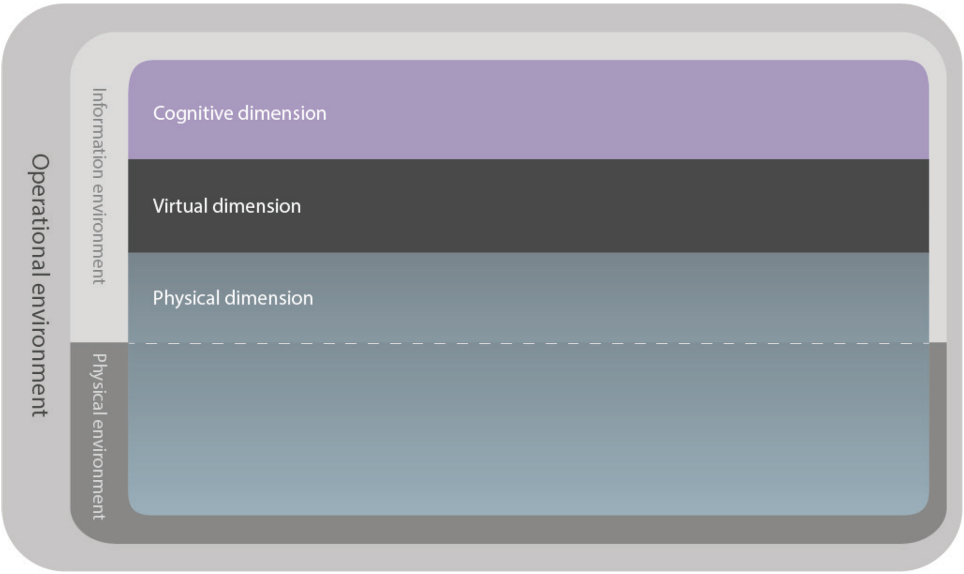

Figure 24 Integrating dimensions with environments

5.3.1.3 Domains

21st century military doctrines generally acknowledge five domains: land, sea, air, space, and cyberspace. Before the concept of domains became accepted, "military operations

[48] North Atlantic Treaty Organisation, *Allied Joint Doctrine for Information Operations*, Edition A Version 1 ed. (Brussels: NATO, 2015). p. 1-2.

[49] Ibid. p. 1-2.

were typically described in only three physical dimensions".[50] These are not the dimensions as discussed in the previous section, they are the predecessors of domains. The military was organised in departments using these 'dimensions', namely: the army for the land 'dimension', navy for the maritime 'dimension' and air force for the air or aerospace 'dimension'.[51] As a consequence of developments in spaceflight from 1942 – the year the first man-made object reached space – to the 1980s, space was added as a 'dimension' and various 'space commands' were created within the departments in the 1980s.[52] Developments in the realm of informatisation in the 1990s and consequent military possibilities of protecting, supplying or denying information on the battlefield resulted in information operations and the addition of the 'dimension' 'information' in the late-1990s and early 2000s.[53] The five 'dimensions' of land, sea, air, space, and information were retitled as domains in the 2000 document 'Joint Vision 2020', the document states: "U.S. forces are able to [...] operate in all domains – land, sea, air, space and information."[54] The information domain "was recast as cyberspace, a decidedly more accessible term" in the 2000s.[55] In sum, the acknowledged domains of military operations are land, sea, air, space, and cyberspace.

The land domain is defined as "the area of the Earth's surface ending at the high water mark and overlapping with the maritime domain in the landward segment of the littorals."[56] The air domain as "the atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible."[57] The maritime or sea domain is defined as "the oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals."[58] The space domain as "the earth's ionosphere and magnetosphere, interplanetary space, and the solar atmosphere."[59] Cyberspace as

[50] Erik Heftye, "Multi-Domain Confusion: All Domains are Not Created Equal," RealClear Defense, realcleardefense.com/articles/2017/05/26/multi-domain_confusion_all_domains_are_not_created_equal_111463.html (accessed August 28, 2017).

[51] 80th Congress of the United States of America, *National Security Act of 1947* (Washington, D.C.: Department of State, 1947).

[52] Jan V. Harvey, *Space: The Fourth Military Dimension* (Carlisle Barracks: U.S. Army War College Strategic Studies Institute, 1988). pp. 15-24.

[53] Office of the Chief of Naval Operations, OPNAV Instruction 3430.26: Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W), 1995a); United States Army Training and Doctrine Command, TRADOC Pamphlet 525-69: Military Operations Concept for Information Operations (Fort Monroe: Department of the Army, 1995); The Joint Chiefs of Staff, Joint Publication 3-13: Joint Doctrine for Information Operations (Washington, D.C.: The Joint Chiefs of Staff, 1998).

[54] The Joint Chiefs of Staff, "Joint Vision 2020: America's Military - Preparing for Tomorrow," *Joint Force Quarterly* (2000b), 57-76. p. 61.

[55] Heftye, "Multi-Domain Confusion: All Domains are Not Created Equal," ; See also: The Chairman of the Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations* (Washington, DC: Office of the Chairman, 2006). p. 3.

[56] The Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Washington, D.C.: Joint Chiefs of Staff, 2017a). p. 137.

[57] The Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Washington, D.C.: Joint Chiefs of Staff, 2017a). p. 10.

[58] Ibid. p. 146.

[59] Ibid. p .213.

"a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[60] The domain constructs serve to "create a frame of reference that defines the preparation and conduct of war. Each military institution and Service crafts doctrine and platforms that are designed to operate or manoeuvre in their dominant domain."[61]

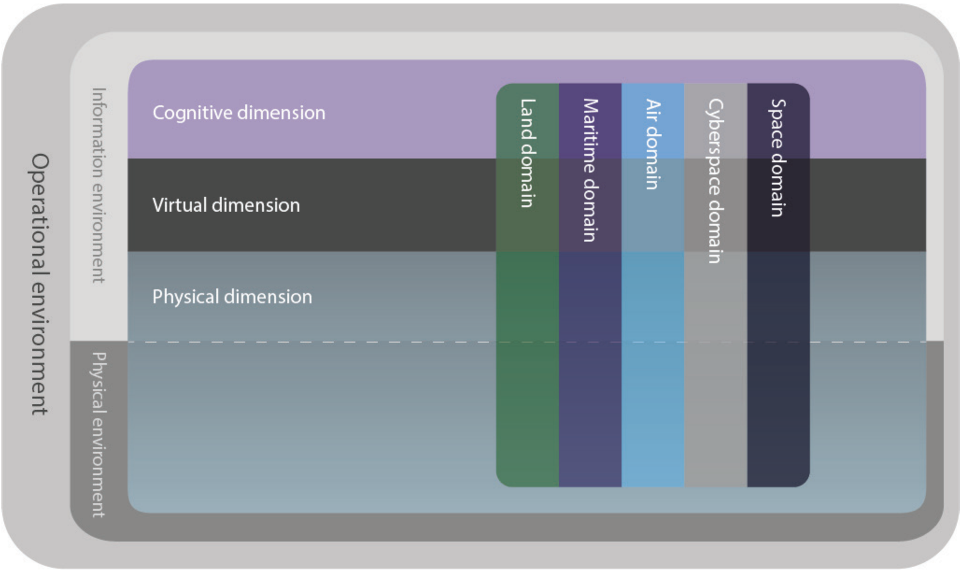

Figure 25 Domains integrated with dimensions and the environments

In the context of the operational environment and the dimensions, the domains can be mapped as constituent elements of the operational environment and dimensions as depicted in Figure 25. The land, sea, air, space and cyberspace domains run vertically over the cognitive, informational, and physical dimensions. The five domains overlap with the three dimensions since they all have a cognitive dimension (e.g. perception, judgement, decision-making, people interacting using cyberspace); informational dimension (e.g. command and control hardware, command and control, data and software regarding objects and persons software, sensor data, data, etc.); and a physical dimension (e.g. armour, ships, planes, personnel, and network hardware located on land, sea or in the air or space).

[60] The Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms* (Washington, D.C.: Joint Chiefs of Staff, 2017a). p. 58.

[61] Frank Hoffman and Michael C. Davies, 2013, "Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework," Small Wars Journal, smallwarsjournal.com/jrnl/art/joint-force-2020-and-the-human-domain-time-for-a-new-conceptual-framework (accessed August 28, 2017).

5.3.1.4 *Layers or components*

Whilst giving the conceptual context of military operations, the overview depicted in Figure 25 does not describe entities being subjected to fighting power. This subsection will highlight the entities targeted by military operations by describing the layers and components construct. The layers of the information environment as described in chapter four (i.e. social, people, persona, information, network and real world) can be mapped to the three dimensions as depicted in Figure 26, these layers in turn host certain targetable entities as illustrated in Figure 27.

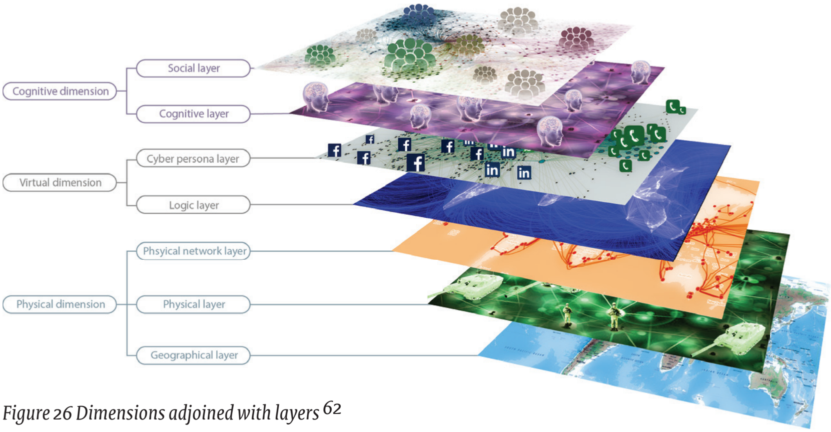

Figure 26 Dimensions adjoined with layers [62]

The cognitive dimension encompasses the social and cognitive layer; the virtual dimension envelops the cyber persona and logical layer and the physical dimension includes the physical network, physical and geographical layer. The layers host the following targetable entities: the social layer hosts the cognitive aspects of groups and audiences (e.g. group psychology); the cognitive layer individual psyche (will, perception, behaviour); the cyber persona layer ‘cyber personas’ (e.g. social media profiles, mail accounts, phone numbers); the logic layer ‘cyber objects’ (e.g. data and software); the physical network layer physical network infrastructure (e.g. routers, cables, systems hardware); the physical layer physical objects and persons (e.g. physical instance of people, materiel, buildings, terrain, etc.); and the geographical layer geographical locations. Although seemingly independent, the entities are interconnected and interrelated; affecting one will affect others too. For instance, a text message to a person’s cyber persona warning him of an impending air strike on his location will affect his psyche in the cognitive layer (e.g. distress) and his physical movements in the physical layer (e.g. leaving

[62] Based on: United States Army, Cyberspace Operations Concept Capability Plan 2016 2028. p. 2-9; The Joint Chiefs ofStaff, Joint Publication 3-12 (R): Cyberspace Operations (Washington, D.C.: The Joint Chiefs of Staff, 2013b). p. I-3; PaulDucheine and Jelle van Haaster, “Fighting Power, Targeting and Cyber Operations” (Tallinn, NATA CCD COE, 3-6 June,2014); Patrick Dekkers A.P, Chris Benten and Han Dijkstra, Advisory Report: Information as Weapon, Vector andTarget, 2016; Paul A. L. Ducheine, Jelle van Haaster and Richard van Harskamp, “Manoeuvring and Generating Effectsin the Information Environment,” in Netherlands Annual Review of Military Studies 2017: Winning without Killing, theStrategic and Operational Utility of Non-Kinetic Capabilities in Crises, eds. Paul A. L. Ducheine and Frans P. B. Osinga(The Hague: Asser Press, 2017), 155-179.

the area). Similarly, for example, conducting an airstrike on a data centre (accommodating physical network infrastructure) will result in the unavailability of software (cyber object) and may result in an annoyed user (psyche) or groups of users (groups and audience).

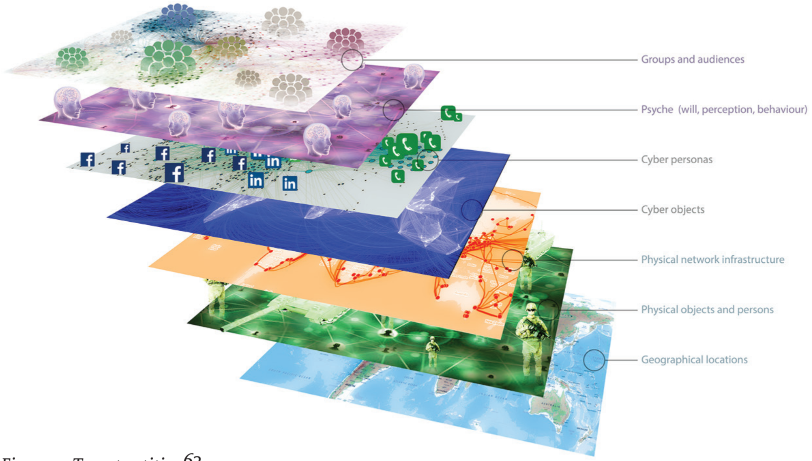
Groups and audiences
Psyche (will, perception, behaviour)
Cyber personas
Cyber objects
Physical network infrastructure
Physical objects and persons
Geographical locations

Figure 27 Target entities [63]

5.3.1.5 *Sub-conclusion*

This sub-section has aimed to create conceptual understanding of military operations. First, the environments were discussed (see 5.3.1.1). Within the operational environment, the highest conceptual construct, there is one explicit sub-environment, i.e. the information environment, and one implicit sub-environment designated the physical environment in this chapter. There are three dimensions to these environments (see 5.3.1.2): the cognitive, informational and physical. The military organises for conducting operations in the environments and dimensions by using domains, that is: land, sea, air, space and cyberspace (see 5.3.1.3). These operations are aimed at concrete entities included within the layers construct: groups and audiences; psyche; cyber personas; cyber 'objects'; physical network infrastructure; physical objects; physical persons; and geographical locations (see 5.3.1.4).The summary of the conceptual context of military operations is depicted in Figure 28. The distinction between the physical and information sub-environments is omitted as they both share the same dimensions. Also, the domains are omitted, as they are an organisational construct and not necessarily a conceptualisation of the context of military operations. The layers are not included either, as they serve to distinguish concrete entities that affect

[63] Based on: United States Army, Cyberspace Operations Concept Capability Plan 2016 2028. p. 2-9; The Joint Chiefs ofStaff, Joint Publication 3-12 (R): Cyberspace Operations. p. I-3; Ducheine and Van Haaster, "Fighting Power, Targetingand Cyber Operations" ; Dekkers, Benten and Dijkstra, Advisory Report: Information as Weapon, Vector and Target, ;Ducheine, van Haaster and van Harskamp, "Manoeuvring and Generating Effects in the Information Environment". pp.155-179.

and can be affected by military operations – the latter are included in Figure 28. The following sub-section will discuss how these entities are affected by military operations.

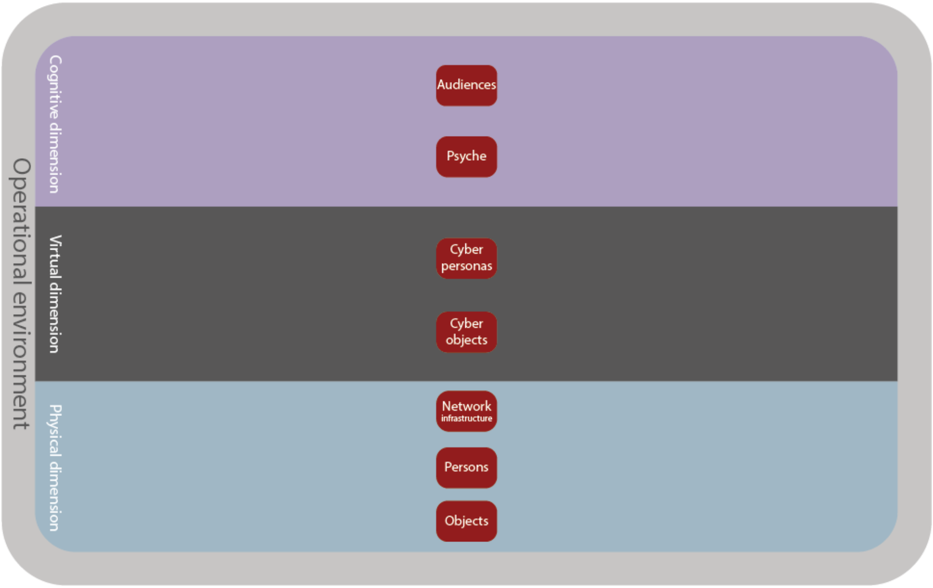

Figure 28 Conceptualisation of the context of military operations

5.3.2 Types of military operations

This section will discuss what types of military operations are utilised by the military and what effects they seek to achieve. This sub-section will first briefly discuss traditional operations (5.3.2.1) and secondly information operations and activities (5.3.2.2). This understanding of traditional and information operations is necessary to analyse the place of cyber operation amongst them in section 5.4.

5.3.2.1 *'Traditional' operations*

Traditional military operations are undertaken in the physical dimension. The organisations typically conducting these operations are the army, navy and air force. Often the aim of these traditional operations is wrongly deemed to be destroying adversaries' forces and materiel, or destruction of infrastructure. Although using the physical dimension as medium, the ultimate goal of these operations is to influence via the cognitive dimension. Cognitive effects such as subduing the enemy or compelling an adversary to do one's will are long established as the supreme goal of military ventures.[64] Also in contemporary doctrine, the cognitive dimension is earmarked as "most important".[65]

Traditional military operations primarily involve physical action to affect the physical instance of people, objects, or physical network infrastructure (e.g. command, control and communication facilities) – ultimately resulting in the aforementioned cognitive effect. The goal of a military operation depends entirely on the context of the operation; however, there are generalised taxonomies of physical effects sought after by projecting physical force. Effect taxonomies by Davis, Smith and Romanych are listed in Table 6, they describe typical physical effects sought after in traditional military operations.

Davis[1]	**Smith**[2]	**Romanych**[3]
Damage equipment and systems	Destruction	Limit/deny
Disrupt processes	Physical attrition	Disrupt
Kill people	Chaos/entropy	Delay
		Divert
		Destroy

Table 1 Physical effect taxonomies

5.3.2.2 Information operations

Early doctrines regarding what we have come to know as information operations emphasise the need for protection of own information systems and denying, degrading or destroying adversarial capacities in the realm of command and control, for instance via "computer viruses". [66] Information operations doctrine denominated its capabilities

[64] See for instance: Sun Tzu, "The Art of War," The Internet Classics Archive, classics.mit.edu/Tzu/artwar.html (accessed August 30, 2017); Carl von Clausewitz, *On War, Translated and Edited by Michael Howard and Peter Paret* (Princeton: Princeton University Press, 1976). p. 13; G. J. David and T. R. McKeldin III, eds., *Ideas as Weapons: Influence and Perception in Modern Warfare* (Washington, D.C.: Potomac Books, 2009). pp. 404-406; John Arquilla and Douglas A. Borer, eds., *Information Strategy and Warfare: A Guide to Theory and Practice* (New York: Routledge, 2007). pp. 4-9; Scot Macdonald, *Propaganda and Information Warfare in the Twenty-First Century* (Oxford: Routledge, 2007). pp. 1-4.

[65] North Atlantic Treaty Organisation, Allied Joint Doctrine for Information Operations. p. 1-2.

[66] See for instance: Office of the Chief of Naval Operations, *OPNAV Instruction 3430.26: Implementing Instrution for Information Warfare/Command and Control Warfare (IW/C2W)* (Washington, D.C.: Department of the Navy, 1995b); United States Army Training and Doctrine Command, *TRADOC Pamphlet 525-69: Military Operations Concept for Information Operations.* See also: David and McKeldin III, eds., *Ideas as Weapons: Influence and Perception in Modern Warfare*. pp. 7-12 and pp. 27-34; Arquilla and Borer, eds., *Information Strategy and Warfare: A Guide to Theory and Practice*. pp. 56-230; Macdonald, *Propaganda and Information Warfare in the Twenty-First Century*. pp. 6-117; Ventre, *Information Warfare*.; Hirvelä, "Discovering how Information Warfare Distorts the Information Environment.".; Cordray III and Romanych, "Mapping the Information Environment."

as follows: "major capabilities to conduct [information operations] include, but are not limited to, OPSEC, PSYOP, military deception, EW, and physical attack/destruction, and could include CNA."[67] Later documents removed the 'could' syntax and firmly indicated that information operations have a subset of activities known 'computer network operations'.[68]

This resulted in a confusing situation where 'information operations' were designated as a new concept with "five core capabilities", being EW, PSYOP, OPSEC, military deception and CNA.[69] In the late 1990s and early 2000s various older commands were merged/renamed into information operations commands, primarily older information warfare staffs tasked with encryption, EW, OPSEC and PSYOPS were merged into these 'new' commands.[70] As most of the organisations did not have capabilities, they primarily served as an advisory organisation to combatant commands and an overarching organisational unit for different types of niche capabilities.

In the 2010s these rather arbitrary doctrinal views were adjusted, information operations doctrine shied away from the ownership over capabilities. The relationship and integration of information operations with other capabilities was formulated as follows: "IO is not about ownership of individual capabilities but rather the use of those capabilities as force multipliers to create a desired effect. [...] there are many military capabilities that contribute to IO and should be taken into consideration during the planning process."[71] There are, however, different perspectives on information operations and the capabilities or activities it encompasses. From NATO perspective information operations (InfoOps or IO) are "a staff function to analyse, plan, assess and integrate information activities"; information activities being "actions designed to affect information or information systems".[72] The U.S. perspective to information operations is that they entail the "integrated employment, during military operations, of information-related capabilities in concert with other lines of operation".[73] The UK has a similar terminological approach to information operations, namely as a "coordinated military activity undertaken to affect decision-makers".[74] As NATO's information activities are labelled information operations in UK and US doctrine,

[67] The Joint Chiefs of Staff, Joint Publication 3-13: Joint Doctrine for Information Operations. pp I-9 and I-10.

[68] See for instance: United States Department of Defense, *Information Operations Roadmap* (Washington, D.C.: Department of Defense, 2003); United States Marine Corps Combat Development Command, *A Concept for Information Operations* (Quantico: United States Marine Corps, 2002); The Joint Chiefs of Staff, *Joint Publication 3-51: Joint Doctrine for Electronic Warfare* (Washington, D.C.: The Joint Chiefs of Staff, 2000a).

[69] United States Department of Defense, *Information Operations Roadmap*. p. 9.

[70] Navy Information Operations Command, "NIOC Norfolk's History," United States Navy, public.navy.mil/fcc-c10f/niocnorfolk/Pages/NIOCNorfolkHistory.aspx (accessed February 8, 2016); United States Army Intelligence and Security Command, "The INSCOM Story," INSCOM History Office, inscom.army.mil/organisation/History.aspx (accessed February 8, 2016); 688th Cyberspace Wing, *A Brief History of the 688th Cyberspace Wing* (Joint Base San Antonio-Lackland: 688th Cyberspace Wing History Office, 2016).

[71] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. 3-14.

[72] North Atlantic Treaty Organisation, Allied Joint Doctrine for Information Operations. p. 1-5.

[73] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. GL-3.

[74] The Joint Doctrine & Concepts Centre, *Joint Warfare Publication 3-80: Information Operations* (Shrivenham: Ministry of Defence, 2002). p. 1-2; The Development, Concepts and Doctrine Centre, *Joint Doctrine Publication 3-45.1: Media Operations* (Shrivenham: The Development, Concepts and Doctrine Centre, 2007). p. 1-2.

it depends per State what the scope of information operations and/or activities is. It is evident, however, that information operations involve certain activities that are related to information, which are called information-related capabilities (U.S.) or information activities (NATO).

The following information-related capabilities are earmarked to be included in information operations: psychological operations; presence, posture, profile; information and operations security; military deception; electronic warfare; physical destruction; key leader engagement; cyber operations; civil-military cooperation; military information support operations; strategic communication; and other supporting and coordinating mechanisms. These capabilities are discussed in more depth in Appendix B.

The capabilities target different entities, for example, psychological operations seek to influence audiences or psyche via the physical dimension (e.g. talking to persons) or informational dimension (e.g. sending messages to a cyber persona). Electronic warfare capabilities are aimed at physical network infrastructure (e.g. transmission stations) or cyber objects (e.g. radio transmissions), whilst the aim is to degrade an adversary's command, control and understanding (cognitive dimension). In other words, using different target entities, these capabilities aim to influence the cognitive dimension. The effects sought after in the cognitive dimensions are diverse. There are taxonomies for these behavioural (Davis), cognitive (Romanych) or psychological (Smith) effects as depicted in Table 7.

Davis[4]	**Smith**[5]	**Romanych**[6]
Demoralise	Chaos/entropy	Mislead
Paralyse/slow	Foreclosure (passive/active)	Confuse
Divert/confuse	Shock	Degrade
Influence	Psychological attrition	Promote
		Inform
		Destroy
		Degrade
		Protect
		Isolate

Table 2 Effect taxonomies of information activities

5.3.2.3 Sub-conclusion

This sub-section has discussed the military operations utilised by the military and the type of effects operations seek to achieve. First the traditional operations via the land, maritime and air domains were briefly discussed (see 5.3.2.1). Although aimed at entities in the physical dimension, the goal of these traditional operations was found to lie in the cognitive dimension. Secondly information operations and activities were discussed (see 5.3.2.2). The information operations and activities concept encompass many military capabilities related to the information environment. The information activities or information-related capabilities utilise different entities to create effects in the cognitive dimension.

In sum, military operations, involving traditional and information activities, are directed at cyber personas, cyber objects, network infrastructure, persons and objects (see Figure 29). Although the prime effect or aim of all activities is creating an effect in the cognitive dimension, currently audiences and psyche cannot be affected directly with military activities, however, audiences and psyche can be affected indirectly as a consequence of military activities. This cognitive effect always involves another medium such as cyber personas, cyber objects, physical network infrastructure, persons or objects. Examples of physical and cognitive effects are listed in Table 6 and Table 7.

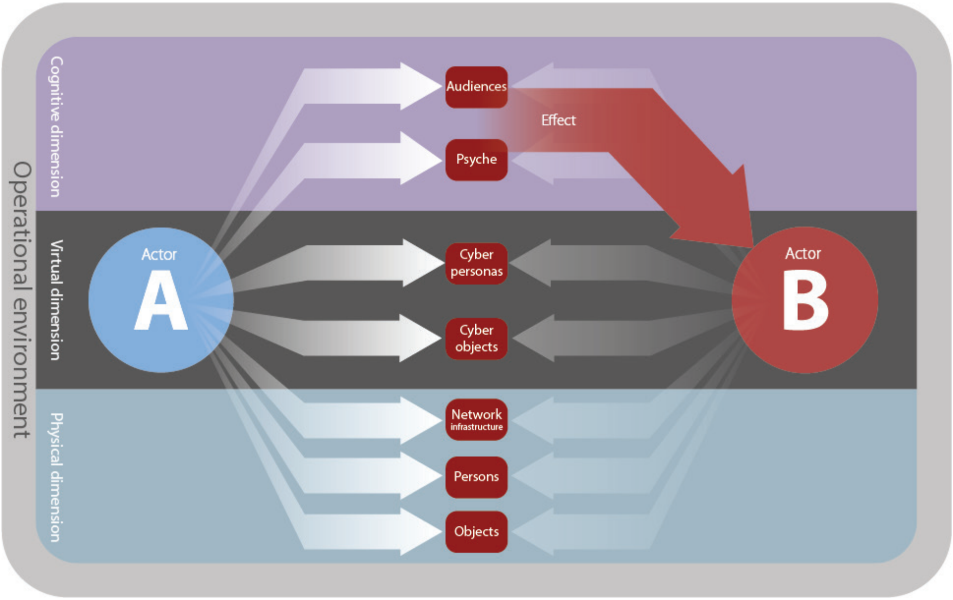

Figure 29 Military operations, target entities and effects

5.3.3 Sub-conclusion

This section has sought to describe the conceptual foundations and types of military operations utilised by the military instrument by answering the sub-question: How are military operations conceptualised and utilised by the military instrument?

This section has started with describing the conceptualisation of the operational environment in which military operations take place (see 5.3.1). The operational environment provides the context for military operations and it is conceptualised using various conceptual constructs such as sub-environments, dimensions, domains, layers and entities/elements. After having analysed the operational environment concept, this section has turned to the military operations conducted in that environment (see 0). The military utilises military operations and activities to ultimately create an effect in the cognitive dimension, creating such an effect, however, always involves another medium such as cyber personas, cyber objects, physical network infrastructure, persons or objects.

5.4 Military cyber operations

This chapter has discussed fighting power (see 5.2) and its manifestation in military operations (see 5.3). The purpose of this chapter is creating understanding of military operations and its relation with the relatively novel military cyber operations. Military cyber operations have yet to be defined, its definition can be deduced from this and previous chapters. Chapter three has discussed the 'cyber' prefix; it concluded that affixing the word 'cyber' to a term implies that it relates to cyberspace or other novel phenomena associated with computing, networking and/or virtualisation. Chapter four defined cyber capabilities as 'having the attributes for activity in cyberspace'. Section 5.3 of this chapter has used NATO's definition of military operations: "a sequence of coordinated action with a defined purpose".[75] Consequently, military cyber operations involve a sequence of coordinated actions with a defined purpose (see section 5.3) in cyberspace (see chapter three); requiring cyber capabilities as they enable activity in cyberspace (see chapter four). This section will focus on these military cyber operations by answering the sub-question: What is the conceptual place of military cyber operations and how are they utilised by the military?

This section will start with describing the place of military cyber operations within the operational environment concept (5.4.1). After that, types of military cyber operations utilised by the military will be discussed and the effects they seek to achieve (5.4.2). As last, this section will conclude with answering the sub-question (5.4.3).

[75] North Atlantic Treaty Organisation, Allied Administrative Publication 06: NATO Glossary of Terms and Definitions (English and French). p. 2-O-2.

5.4.1 Conceptual place military cyber operations

This sub-section will discuss the conceptual place of military cyber operations within the operational environment. First, the somewhat confusing relations of military cyber operations with information operations (5.4.1.1) and electronic warfare (5.4.1.2) will be discussed. After that, the targeted entities of military cyber operations will be discussed (5.4.1.3).

5.4.1.1 Relation to information operations

For a period of time, military cyber operations used to fall under the ambit of information operations. As mentioned in 5.3.2.2, information operations doctrine has shied away from ownership over capabilities in 2010. From 1998 to 2010 military cyber operations were a part of information operations, in 2010 information operations doctrine dubbed military cyber operations an information-related capability. When used in that role, military cyber operations support information operations objectives by denying or manipulating "adversary or potential adversary decision making through targeting an information medium [...], the message itself [...], or a cyber persona".[76] 2013 military cyber operations doctrine affirmed this position. As an information-related capability military cyber operations may contribute to effects in the cognitive dimension; however, they do not exclusively contribute to those effects. Military cyber operations may also "be conducted in support of target objectives, or to support operations in the physical domains [(i.e. land, sea, air and space)] to achieve objectives". [77] In other words, military cyber operations may support information operations objectives, however, they are a separate capability that may also be used for other purposes.

5.4.1.2 Relation to electronic warfare

Another issue with military cyber operations is their somewhat confusing relation to electronic warfare. Early doctrine (2000) regarding electronic warfare is fairly clear on the overlaps and differences: military cyber operations target networks but as "many computer networks are linked electronically, incorporating the results of EW planning is crucial to both offensive and defensive computer network warfare operations".[78] Networks can be targeted via military cyber operations and/or electronic warfare capabilities, for instance, "sending a code or instruction to a central processing unit that causes the computer to short out the power supply is [a military cyber operation]. Using an electromagnetic pulse device to destroy a computer's electronics and causing the same result is [electronic warfare]".[79] The difference between cyber operations and electronic warfare was defined as follows: [computer network attack] relies on the data stream to execute the attack while [electronic attack] relies on the electromagnetic spectrum.

[76] The Joint Chiefs of Staff, Joint Publication 3-13: Information Operations. p. II-9.

[77] The Joint Chiefs of Staff, Joint Publication 3-12 (R): Cyberspace Operations. pp. I-5 and I-6.

[78] The Joint Chiefs of Staff, Joint Publication 3-51: Joint Doctrine for Electronic Warfare. p. iv-7.

[79] Ibid. p. gl-5.

This doctrine, however, was written well before wireless networks became commonplace that rely fully on the electromagnetic spectrum. This "increasing prevalence of wireless [Internet] and telephone networks in the operational environment has created a wide range of opportunities and vulnerabilities when [electronic warfare] and [computer network operations] tactics, techniques and procedures are used synergistically."[80] These potential synergistic advantages and interdependencies have resulted in the creation of a set of activities called 'cyber electromagnetic activities (CEMA)'.[81] Although mutually enforcing and interdependent, electronic warfare and cyber operations are not the same; they use different means and methods but may target the same entities, as will be discussed next.

5.4.1.3 *Targeted entities*

The purpose of military cyber operations is "to achieve objectives in or through cyberspace."[82] Military cyber operations do so by targeting entities in cyberspace (as part of the information environment), these entities are cyber personas, cyber objects and/or physical network infrastructure. Military cyber operations involve the use of cyber capabilities for doing so; as demonstrated in chapter four these capabilities can be grouped using the layers of cyberspace, that is, the cyber persona layer, logic layer and physical network layer.

Cyber capabilities can be used for various purposes. Mails can be sent to a cyber persona in a target audience to convince the target of the legitimacy of military activity, that same channel could be used to trick the target to disclose his credentials to a target system. Similarly, a website could be defaced using web-application vulnerabilities resulting in reputation damage or a website could be launched to inform a target audience. Alternatively, military cyber operations can also be aimed at disrupting the air defence system of an opponent in support of an air raid,[83] or stand-alone to disrupt the critical infrastructure of a State actor.[84] In other words, the use of cyber capabilities depends on the goal of the military cyber operation; it could be used as information-related capability in information operations (e.g. informing target audience or launching a website), in support of physical activities (e.g. disrupting air defense systems) or stand-alone (e.g. disrupting critical infrastructure).

Military cyber operations are not unique in using cyber capabilities to target cyber personas, cyber objects or physical network infrastructure. Most information-related

[80] The Joint Chiefs of Staff, *Joint Publication 3-13.1: Electronic Warfare* (Washington, D.C.: The Joint Chiefs of Staff, 2007). pp. x-xi.

[81] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations

[82] The Joint Chiefs of Staff, Joint Publication 3-12 (R): Cyberspace Operations. p. v.

[83] See for instance: "Mossad Hacked Syrian Official's Computer before Bombing Mysterious Facility," Wired, accessed June 5, 2018, wired.com/2009/11/mossad-hack/. For more context on the operation, see: Caren Kaplan, "Air Power's Visual Legacy: Operation Orchard and Aerial Reconnaissance Imagery as Ruses De Guerre," *Critical Military Studies* 1, no. 1 (2015), 61-78.

[84] See for example: "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," Wired, accessed February 10, 2017, wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

capabilities in contemporary society rely on cyberspace and cyber capabilities and could target entities in the information dimension. For instance, 'military influence support operations' could use and target cyber personas with modern media to influence foreign target audiences (i.e. websites, blogs, social media), 'psychological operations' could use text messages aimed at cyber personas, and key-leader engagement could be conducted via Skype, etc. Therefore, it is only logical that military doctrine affirms that these capabilities cannot be seen in isolation from each other, this notion is encompassed in the purpose of information operations, namely: a staff function to analyse, plan, assess and integrate information-related capabilities or information activities (see 5.3.2.3).

5.4.1.4 *Sub-conclusion*

This sub-section has discussed the conceptual place of military cyber operations within the operational environment. First, the confusing relation with information operations and electronic warfare was discussed (see 5.4.1.1). Information operations used to include military cyber operations as information activity from 1998 to 2010, from 2010-on this has changed and military cyber operations have a separate place in military doctrine. Electronic warfare is closely related to military cyber operations (see 5.4.1.2). Whereas in the early 2000s the distinction between electronic warfare and military cyber operations was relatively clear, with the ubiquity of wireless networking this distinction has faded resulting in many synergistic advantages and interdependencies as embodied in the new activity cyber electromagnetic activities (CEMA). After delineating the relations of military cyber operations with information operations and electronic warfare, this section has highlighted the entities targeted with military cyber operations, namely, cyber objects, cyber personas and physical network infrastructure (see 5.4.1.3). Military cyber operations utilise the information dimension of the operational environment for doing so.

5.4.2 Types of military cyber operations

As any operation, the goal of military cyber operations is context dependent, however, there are specific types of military cyber operations tailored to achieving a specific goal. The following sub-sections will discuss illustrative types of military cyber operations: enabling (5.4.2.1); defensive (5.4.2.2); offensive (5.4.2.3); and intelligence, surveillance and reconnaissance (5.4.2.4).

5.4.2.1 *Enabling*

Before being able to engage in any activity at all in cyberspace, an actor needs the infrastructure for doing so. Enabling military cyber operations involve actions "taken to design, build, configure, secure, operate, maintain, and sustain [armed forces] communications systems and networks in a way that creates and preserves data availability, integrity, confidentiality, as well as user/entity authentication and non-repudiation."[85]
In doing so these operations support the conduct of military cyber operations but enable

[85] The Joint Chiefs of Staff, Joint Publication 3-12 (R): Cyberspace Operations. p. II-3.

other military operations as well, for instance through operating and securing networks needed for communication in land, air, maritime or space operations.

5.4.2.2 Defensive

Defensive military cyber operations “are passive and active cyberspace operations intended to preserve the ability to utilise friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems”. Defensive military cyber operations respond “to unauthorised activity, alerts, and threat information against [military networks], and leverages intelligence, counterintelligence, law enforcement, and other military capabilities as required.”[86] There are two types of defensive military cyber operations: “internal defensive measures” conducted inside armed forces networks and “response action” aimed at targets outside these networks.[87] Internal measures include reconnaissance within networks “to locate internal threats and may respond to unauthorised activity, alerts, and threat information”.[88] Response actions are defined as “deliberate, authorised defensive measures or activities taken outside of the defended network to protect and defend [cyberspace] capabilities or other designated systems”.[89] As such they resemble offensive cyber operations, however, they are conducted with a defensive purpose in mind.

5.4.2.3 Offensive

Offensive cyberspace operations “are cyberspace operations intended to project power by the application of force in or through cyberspace.”[90] These operations are conducted outside armed forces networks and are aimed at “targeting objectives in or through cyberspace and related portions of the [electromagnetic spectrum]”.[91] The common effects of offensive cyber operations (and defensive cyber operations response activities) are deny, degrade, disrupt, destroy or manipulate. Denial “prevents enemy or adversary use of resources”, degrade denies “access to, or operation of, a target to a level represented as a percentage of capacity”, disruption involves complete but temporary denial of “access to, or operation of, a target for a period of time”, destroy involves permanent, complete, and irreparable denial of “access to, or operation of, a target”, manipulation involves control or change of “enemy or adversary’s information, information systems, and/or networks in a manner that supports the commander’s objectives.”[92] There are other effects taxonomies for cyber operations; the effects mentioned above are, however, the most commonly used.[93]

[86] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations. p. 1-7.

[87] The Joint Chiefs of Staff, *Joint Publication 3-12: Cyberspace Operations* (Washington, DC.: Joint Chiefs of Staff, 2013c). p. 1-8.

[88] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations. p. 1-8.

[89] Ibid. p. 1-8.

[90] The Joint Chiefs of Staff, Joint Publication 3-12 (R): Cyberspace Operations. p. II-2.

[91] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations. p .1-8.

[92] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations. pp. 1-10 to 1-11.

[93] See for instance: Deborah Bodeau, Richard Graubart and William Heinbockel, “Characterizing Effects on the Cyber Adversary,” *MTR130432, MITRE Corporation, November* (2013).

5.4.2.4 ISR

Cyberspace intelligence, surveillance and reconnaissance (ISR) "includes activities in cyberspace conducted to gather intelligence required to support future [offensive cyber operations] or [defensive cyber operations]."[94] Cyberspace ISR "focuses on tactical and operational intelligence and on mapping enemy and adversary cyberspace to support military planning."[95] All levels of war– strategic, operational and tactical –have "corresponding levels of intelligence operations".[96] Strategic intelligence supports preparations of "strategic estimates, strategies, and plans to accomplish missions assigned by higher authorities."[97] Operational intelligence "focuses on answering the commander's [intelligence requirements], assessing the effectiveness of operations, maintaining situational awareness of adversary military disposition, capabilities, and intentions, and other relevant aspects of the [operating environment]."[98] Tactical intelligence "addresses the threat across the range of military operations. [They] identify and assess the adversary's capabilities, intentions, and vulnerabilities, as well as describe the physical environment."[99]

Cyber operations aimed at gathering intelligence can contribute to all levels. The organisation involved in gathering intelligence is dependent of the information sought after, intelligence for the strategic level often involves the use of intelligence agencies as they are sometimes better equipped or have a broader legal basis for gathering specific types of information. Cyber operations aimed at gathering information by intelligence agencies are often not considered cyberspace ISR, they often are a part of a broader all-sources intelligence process.[100] Cyberspace ISR as indicated in the U.S. Army Field Manual, aims to provide operational and tactical intelligence and may come from Army personnel "trained and certified to a common standard with the intelligence community".[101] As such they are distinct from operations by intelligence agencies.

A somewhat related activity to cyberspace ISR is cyberspace operational preparation of the environment, which consists "of the non-intelligence enabling activities for the purpose of planning and preparing for ensuing military operations."[102]Although seemingly non-intelligence enabling activities, operational preparation of the environment is often used in order to "distinguish particular operations as traditional military activities and

[94] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations. p. 1-9.

[95] Ibid. p. 1-9.

[96] The Joint Chiefs of Staff, *Joint Publication 2-0: Joint Intelligence* (Washington, D.C.: The Joint Chiefs of Staff, 2013a). p. I-23.

[97] Ibid. p. I-23.

[98] The Joint Chiefs of Staff, *Joint Publication 2-0: Joint Intelligence* (Washington, D.C.: The Joint Chiefs of Staff, 2013a). p. I-24.

[99] Ibid. p. I-25.

[100] Ibid. p. GL-5.

[101] Department of the Army, Field Manual 3-12: Cyberspace and Electronic Warfare Operations. p. 1-9.

[102] Ibid. p. 1-10.

not as intelligence functions",[103] whilst the purpose of these operations "is to gather intelligence".[104] In other words, these operations are very similar to cyberspace ISR.

5.4.2.5 *In sum: Types of military cyber operations*

This sub-section has described four types of military cyber operations: enabling operations creating, maintaining and securing military networks to be used in traditional, information and cyber operations (see 5.4.2.1); defensive cyber operations aimed at protecting the networks by actively mitigating threats inside and outside military networks (see 5.4.2.2); offensive cyber operations focused on projecting power in or through cyberspace (see 5.4.2.3); and cyberspace ISR operations directed at obtaining intelligence to be used on the operational and tactical levels of warfighting (see 5.4.2.4).

5.4.3 Sub-conclusion

This section has focused on the military cyber operations within armed forces by answering the sub-question: *What is the conceptual place of military cyber operations and how are they utilised by the military?*

In sum, the conceptual place of military cyber operations is not different from other military operations, they fit within the operational environment construct and they utilise the information dimension to target entities in the information environment, more specifically, target entities in cyberspace as part of the information environment. Military cyber operations are closely related to other information-related capabilities or information activities and electronic warfare. Military cyber operations, as all other operations, can be utilised for various purposes, for instance enabling communication (enabling cyber operations), gathering information or intelligence (ISR cyber operations), safeguarding freedom of movement in the information environment (defensive cyber operations) or influencing adversaries (offensive cyber operations).

5.5 Conclusion

This chapter has aimed to create understanding of military cyber operations and their relation with other military operations This chapter has done so by focusing on the place of military cyber operations within military organisation using the following sub-question: *What is the conceptual place of cyber capabilities within the military organisation and how are cyber capabilities integrated in the armed forces?*

[103] 111th Congress House of Representatives, "Report 111-186: Intelligence Authorization Act for Fiscal Year 2010," House of Representatives, fas.org/irp/congress/2009_rpt/hrpt111-186.html (accessed September 3, 2017).

[104] Ibid.

In order to answer the sub-question this chapter has first discussed two basic concepts in military organisation: fighting power and military operations. Section 5.2 has discussed the organisational principles of the military as embodied in the concept of fighting power. This concept expresses the different components required for the military organisation to function, namely: the conceptual, moral and physical. These components are described separately to categorise elements that are required for military organisation, however, only together the elements constitute fighting power. Fighting power consequently can be manifested in the form of military operations.

Section 5.3 has described how military operations are conceptualised and utilised by the military. The conceptualisation of military operations is epitomised in the operational environment construct, which conceptually divides the environment where military operations are conducted in sub-environments (physical and informational), dimensions (cognitive, virtual and physical), domains (land, sea, air, space, cyberspace), and layers (geographical, physical, physical network, logic, cyber persona, cognitive and social). These layers host certain targetable entities, namely: persons, objects, physical network infrastructure, cyber objects, cyber personas, psyche and audiences. The military operations targeting these entities are generally divided into traditional operations conducted in the traditional domains (land, sea, air and space) and information operations conducted in or seeking to affect the information environment. The military utilises these military operations and activities to ultimately create an effect in the cognitive dimension (psyche or audiences), creating such an effect, however, always involves another medium such as cyber personas, cyber objects, physical network infrastructure, persons or objects.

After having described the pivotal concepts of fighting power and military operations, this chapter has turned to delineating the place of military cyber operations within those concepts. Section 5.4 has started with defining military cyber operations as involving a sequence of coordinated actions with a defined purpose in cyberspace; requiring cyber capabilities as they enable activity in cyberspace. After that, the place of military cyber operations within the operational environment concept from section 5.3 and their use by the military were discussed. The conceptual place of military cyber operations is not different from other military operations. Military cyber operations fit within the operational environment construct. They utilise the information dimension of the operational environment to target entities in the information and physical dimension to ultimately create an effect in the cognitive dimension. The specific types of military cyber operations could be generalised as (1) enabling, (2) defensive, (3) offensive, and (4) ISR.

By integrating the insights from the sections this chapter's sub-question can be answered. Before being able to engage in military cyber operations, the military requires the conceptual, moral, and physical components for doing so, or in other words it needs to organise fighting power (see Figure 29). By integrating cyber capabilities using the components of fighting power, the military is able of engaging in military cyber operations.

The conceptual place of military cyber operations is as a specific sub-type of military operations with close ties to information operations and electronic warfare. Military cyber operations are aimed at cyber personas, cyber objects and physical network infrastructure; their ultimate goal is affecting psyche or audiences – as all other military operations. They are not unique by virtue of their target entities, many operations, amongst other information-related capabilities and electronic warfare, share target entities with military cyber operations.

5.5.1 Relevance

The insights from this chapter serve to highlight how the military instrument, as one of the instruments of power, has integrated cyber capabilities by creating a new form of military operations, being: military cyber operations. These operations can create effects in or through cyberspace (e.g. deny, disrupt, degrade, destroy, promote, inform, protect, etc.) in various roles (e.g. enabling, defensive, offensive, or ISR). This 'military' perspective adds that the military has operationalised cyber capabilities and that the military instrument could potentially contribute to achieving an actor's goals using military cyber operations. This results in military cyber operations having potential utility to an actor in its international relations, for example anticipating a threat by gathering intelligence in cyberspace, preventing a threat from emerging by engaging actors via social-media, deterring actors by signalling offensive military cyber capabilities, or intervening in a State using offensive capabilities.

The addition of the 'military' perspective to this research results in the following insights: The 'power' perspective clarifies what goals actors seek to achieve and what impacts their success; the 'society' perspective illustrates how informationised society results in new ways for achieving goals; the 'technology' perspective highlights new cyber capabilities that can be used to influence actors; and the 'military' perspective illustrates that the military instrument can operationalise cyber capabilities in military cyber operations and use these operations for various purposes (see Figure 30).

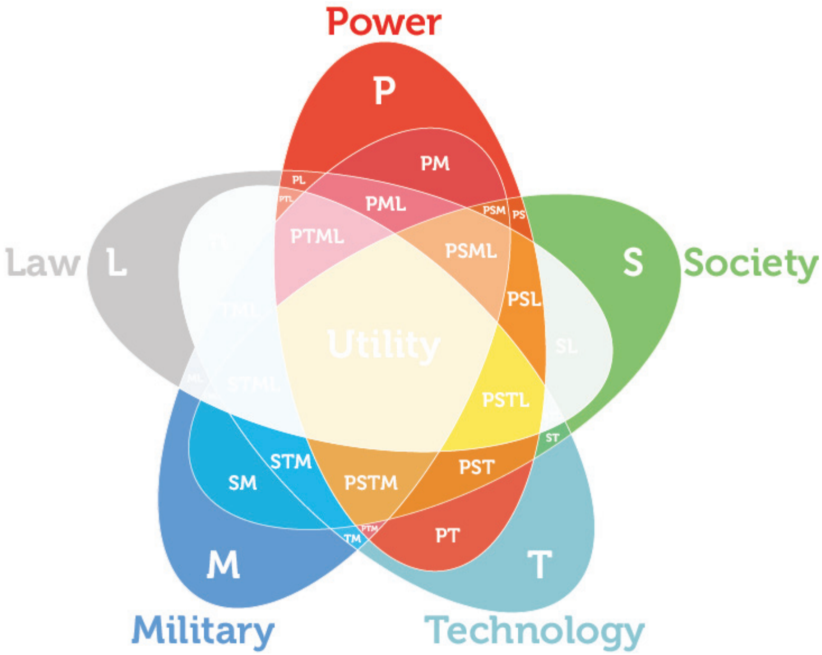

Figure 30 Integrating the ‘power’, ‘society’, ‘technology’, and ‘military’ perspective.

6

On Law

6 On Law

6.1 Introduction

The legal framework applicable to the activities of armed forces differs per situation, e.g. before, during or after a conflict. Whether a State may use force is embodied in the *jus ad bellum*.[1] The use of force in international relations is prohibited,[2] unless used in self-defence,[3] after United Nations authorisation,[4] or "after invitation or with the consent of the target State".[5] During conflict 'international humanitarian law' (IHL) or 'law of armed conflict' (LOAC) largely supersedes "the international law of peace" between the involved parties.[6] Some instruments, however, still apply, such as International human rights law (IHRL) as it applies "at all times".[7] Although *jus ad bellum* and IHRL could impact the way in which military cyber operations are used in specific contexts, IHL best illustrates how international law impacts the way military cyber operations can be used during conflict. Therefore, this chapter will focus exclusively on IHL.[8]

IHL embodies that a State's and its armed forces' right to "choose methods or means of warfare is not unlimited",[9] "whether the armed conflict concerned is considered by the protagonists to be lawful or unlawful, general or local, a war of liberation or a war of conquest, a war of aggression or of self-defence, limited or "total" war, using conventional weapons or not, the Parties to the conflict are not free to use any methods or any means of warfare whatsoever."[10] Although for some time it was contested whether cyber capabilities were governed by these legal frameworks, now "it seems to be widely accepted that international law not only applies, but is capable of being applied, albeit with some adaptations and the liberal use of analogous interpretation, to cyber activities across a

[1] International Committee of the Red Cross, *International Humanitarian Law* (Geneva: ICRC, 2015). p. 8; Terry D. Gill and Dieter Fleck, eds., *The Handbook of the International Law of Military Operations* (Oxford: Oxford University Press, 2011). p. 3.

[2] Art. 2 (4) UN Charter.

[3] Art. 51 UN Charter

[4] Art. 42 UN Charter

[5] Vaughan Lowe and Antonios Tzanakopoulos, "Humanitarian Intervention," Oxford Public International Law, accessed June 6, 2018, opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e306.

[6] Dieter Fleck, ed., *The Handbook of International Humanitarian Law*, 3rd ed. (Oxford: Oxford University Press, 2013). p. 45

[7] Jann K. Kleffner, "Human Rights and International Humanitarian Law: General Issues," in *The Handbook of the International Law of Military Operations*, eds. Terry D. Gill and Dieter Fleck (Oxford: Oxford University Press, 2011). p. 68.

[8] For an overview on *jus ad bellum* considerations in the context of cyber operations, see for instance: Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017). Chapter 13-15; Nicholas Tsagourias and Russell Buchan, eds., *Research Handbook on International Law in Cyberspace* (Cheltenham: Edward Elgar Publishing, 2015). pp. 233-304;

[9] Article 35 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (Geneva: International Committee of the Red Cross, 1977a).

[10] Claude Pilloud et al., Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Geneva: Martinus Nijhoff Publishers, 1987). p. 390.

wide spectrum, including cyber warfare."[11] Thus, contemporary legal frameworks govern the use of military cyber capabilities and hence impact the potential uses of military cyber operations during conflict.

6.1.1 Goal of this chapter

On basis of the assumption that an armed conflict exists, this chapter will discuss the IHL framework applicable to military cyber operations conducted in the context of an armed conflict. This chapter will do so by answering the sub-question: *What is the international humanitarian law framework for employing military cyber operations above the threshold of attack during armed conflict?*

This chapter will assume that an armed conflict exists as this is understood under IHL with an international or non-international character.[12] This chapter will refer to differences in the law relating to non-international and international armed conflict. Current practice suggests, however, that many rules and regulations applicable in international armed conflict apply in non-international armed conflict, since "what is inhumane, and consequently proscribed, in international wars, cannot but be inhumane and inadmissible in civil strife."[13] Besides that, "common sense would suggest that such rules [i.e. regarding distinction and proportionality], and the limits they impose on the way war is waged, should be equally applicable in international and non-international armed conflicts."[14] Although not codified in treaties, many rules applicable in international armed conflicts are applicable in non-international armed conflict by their customary nature. For instance, "the 2005 ICRC Study on Customary International Humanitarian Law identified 148 rules (out of 161) that apply to both international and non-international armed conflicts, as, according to the Study, state practice does not distinguish between the two types of conflict in the application of such rules".[15] Differences, however, continue to exist in specific cases

[11] Terry D. Gill, Jelle van Haaster and Mark P. Roorda, "Some Legal and Operational Considerations regarding Remote Warfare: Drones and Cyber Warfare Revisited," in Research Handbook on Remote Warfare, ed. Jens David Ohlin (Northampton: Edward Elgar Press, 2017).

[12] As described in: common article 2 Geneva Conventions.

[13] Appeals Chamber, "Prosecutor V. Dusko Tadic Aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)," International Criminal Tribunal for the former Yugoslavia, icty.org/x/cases/tadic/acdec/en/51002.htm (accessed May 12, 2016). §119.

[14] Jean-Marie Henckaerts et al., Customary International Humanitarian Law, Vol. 1: Rules (Cambridge: Cambridge University Press, 2005). p. xxxv.

[15] Marco Roscini, Cyber Operations and the use of Force in International Law (Oxford: Oxford University Press, 2014). p. 165.

such as combatant status,[16] detention[17] and belligerent occupation.[18] These exceptions will not be discussed in detail as they are not as relevant in the context of this chapter.

6.1.2 Structure

In order to answer the sub-question this chapter will start with describing the applicability of IHL in general and to military cyber operations in specific (section 6.2). After having specified if and when IHL applies to military cyber operations, this chapter will discuss how IHL could be applied to military cyber operations (section 6.3). Then this chapter will discuss the actual contents of the IHL legal framework applicable to military cyber operations above the threshold of attack (section 6.4). As last, the findings of the sections will be integrated and the sub-question answered (section 6.5).

6.2 Applicability of IHL

This section will touch upon the applicability of IHL in general and specifically to military cyber operations by answering the sub-question: *When does IHL apply in general and does it apply to the military cyber operations?* Sub-section 6.2.1 will discuss the general applicability, section 6.2.2 will focus on the applicability to military cyber operations, and lastly sub-section 6.2.3 will provide an answer to the sub-question.

6.2.1 Applicability in general

There are two main types of armed conflicts in IHL, this sub-section will first discuss the applicability of IHL to international armed conflicts (6.2.1.1) and secondly to non-international armed conflicts (6.2.1.2).

6.2.1.1 International armed conflict

IHL "[regulates] and as a rule applies in times of armed conflict",[19] it applies to "all cases of declared war or any other armed conflict which may arise" between States or cases "of partial of total occupation" of territory.[20] In other words, "the law of international armed conflict applies from the first moment that force is used by one state against another state",

[16] See for example: Knut Dörmann, "The Legal Situation of "Unlawful/Unprivileged Combatants"," *International Review of the Red Cross* 85, no. 849 (2003). pp. 47-48.

[17] Ibid. pp. 68-70.

[18] Antonio Cassese, ed., *Realizing Utopia: The Future of International Law* (Oxford: Oxford University Press, 2012). pp. 528-529.

[19] Fleck, ed., The Handbook of International Humanitarian Law. p. 43.

[20] Article 2 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention) (Geneva: International Committee of the Red Cross, 1949).

this is the so-called 'first-shot theory'.[21] There is, however, a different perspective that promotes the view that for IHL to apply, the fighting between parties to the conflict should be of some intensity. The following paragraphs will highlight the 'first-shot theory' and the 'intensity approach'.

Pictet's frequently cited 1952 ICRC commentary to the 1949 Geneva Conventions states: "any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2, even if one of the parties denies the existence of a state of war. It makes no difference how long the conflict lasts, or how much slaughter takes place".[22] The ICRC's approach nullifies the influence of intensity to triggering IHL. Instead, the activity involved is most important, namely: a State's armed forces and/or deployment of military means.[23]

The ICRC's 2016 commentary to the Geneva convention reiterates this approach, stating that there are "compelling protection reasons for not linking the existence of an international armed conflict to a specific level of violence".[24] Noting the International Law Association's extensive study into the characteristics of armed conflict,[25] the ICRC's 2016 commentary acknowledges: "that some consider that hostilities must reach a certain level of intensity to qualify as an armed conflict".[26] Although acknowledging this perspective, it firmly holds that it is "logical and in conformity with the humanitarian purpose of the Conventions that there be no requirement of a specific level of intensity of violence to trigger an international armed conflict".[27]

Apart from the International Law Association's statement there are many other views that do support the notion of a certain level of intensity.[28] Many States do not take a broad view as forwarded by the ICRC, consequently "many isolated incidents, such as border clashes

[21] Fleck, ed., The Handbook of International Humanitarian Law. p. 44.s

[22] Jean S. Pictet, The Geneva Conventions of 12 August 1949: Commentary. (Geneva: International Committee of the Red Cross, 1952). p. 32.

[23] Cordula Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," International Review of the Red Cross 94, no. 886 (2012), 533-578. p. 546.

[24] International Committee of the Red Cross, Commentary on the First Geneva Convention, 2nd ed. (Cambridge: Cambridge University Press, 2016). §236.

[25] International Law Association, Final Report on the Meaning of Armed Conflict in International Law (The Hague: International Law Association, 2010). pp. 1-2.

[26] International Committee of the Red Cross, Commentary on the First Geneva Convention. §242.

[27] Ibid. §244.

[28] See for instance: Christopher Greenwood, "Scope of Application of Humanitarian Law," in The Handbook of International Humanitarian Law, ed. Dieter Fleck, 2nd ed. (Oxford: Oxford University Press, 2011), 45-78; Advisory Council on International Affairs and Advisory Committee on Issues of Public International Law, Cyber Warfare (The Hague: AIV/CAVV, 2011); Roscini, Cyber Operations and the use of Force in International Law; International Law Association, Final Report on the Meaning of Armed Conflict in International Law; Michael N. Schmitt, "The State of Humanitarian Law in Cyber Conflict," justsecurity.org/18891/state-humanitarian-law-cyber-conflict/ (accessed July 27, 2016).

and naval incidents, are not treated as conflicts".[29] Hence there is a certain threshold being applied by States, should the incident or act "reach a sufficient level of intensity [...] the humanitarian law of war applies".[30] The approach advocated by the International Law Association and States, however, "bears the risk of creating an international legal vacuum or of depriving certain categories of persons the protections that international humanitarian law provides".[31] As such, the approach advocated by the ICRC – the 'first-shot theory' – seems to best reflect and suit the purpose of IHL. The existence of international armed conflict triggers the application of the four Geneva conventions, Additional Protocol I, and customary international humanitarian law for international armed conflict.[32]

6.2.1.2 *Non-international armed conflict*

There are two generally accepted requirements for the existence of a non-international armed conflict: "the armed violence must be of sufficient intensity and the parties must be sufficiently organised."[33] Factors to be taken into account when assessing intensity are "the number, duration, and intensity of individual confrontations; the type of weapons and other military equipment used; the number and calibre of munitions fired; the number of persons and type of forces partaking in the fighting; the number of casualties; the extent of material destruction; and the number of civilians fleeing combat zones."[34] Indicators for organisation are "the existence of a command structure and disciplinary rules and mechanisms within the group; the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits, and military training; its ability to plan, coordinate and carry out military operations, including troop movements and logistics; [etc.]".[35] Should the two requirements be met, there is a non-international armed conflict.

The rules applicable to non-international armed conflict are different than those of international armed conflict, the former are "subject to a different and more limited legal regime than that which applies in an international armed conflict".[36] The legal instruments applicable during non-international armed conflict are Common Article 3 of the Geneva Conventions, in some specific cases Additional Protocol Two, customary international humanitarian law regarding non-international armed conflict and conventions such as

[29] Greenwood, "Scope of Application of Humanitarian Law," in , 45-78. p. 48.

[30] Advisory Council on International Affairs and Advisory Committee on Issues of Public International Law, Cyber Warfare. p. 23.

[31] Fleck, ed., The Handbook of International Humanitarian Law. p. 45.

[32] International Committee of the Red Cross, International Humanitarian Law (Geneva: International Committee of the Red Cross, 2015). p. 21.

[33] Fleck, ed., The Handbook of International Humanitarian Law. p. 50.

[34] "Prosecutor V. Ramush Haradinaj, Idriz Balaj, Lahi Bahimaj (Judgement)," International Criminal Tribunal for the former Yugoslavia, 2008, icty.org/x/cases/haradinaj/tjug/en/080403.pdf. §49.

[35] Fleck, ed., The Handbook of International Humanitarian Law. p. 50.

[36] Ibid. p. 51.

the Hague Convention for the Protection of Cultural Property and Protocol II to the 1980 Convention on Certain Conventional Weapons.[37]

Common Article 3 "provides minimum protection in non-international armed conflicts" and is regarded "as a treaty in miniature, representing a minimum standard from which belligerents should never depart."[38] Additional Protocol II is narrower in scope than Common Article 3 as its applicability depends on "a requirement of territorial control" and it "expressly applies only to armed conflicts between State armed forces and dissident armed forces or other organised armed groups. Unlike common Article 3, Additional Protocol II does not apply to armed conflicts between organised non-State armed groups."[39] As noted above (see 3.1.1), "the evolution of conventional and customary international humanitarian law has brought about a tangible approximation between the law of international and non-international armed conflicts."[40] There are, however, some differences, namely: "the absence of combatant status in non-international armed conflicts, which entails the right to participate directly in hostilities";[41] absence of "the law of occupation, which exclusively applies to international armed conflicts";[42] and doubt regarding specific rules on the "improper use of the flags or military emblems, insignia or uniforms of the adversary" or neutral parties.[43]

6.2.1.3 Sub-conclusion

In sum, IHL is applicable in the case of armed conflict between State, State and non-State, or non-State and non-State actors. The IHL instruments applicable in a specific situation depends on the type of armed conflict: in the case of intra-State armed conflict the four Geneva Conventions, Additional Protocol I, and applicable customary international humanitarian law for international armed conflict; in the case of inter-State armed conflict – whether State versus non-State or non-State versus non-State – Common Article 3, customary international humanitarian law for non-international armed conflict, and in some specific cases Additional Protocol II.

[37] Article 3 Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention); Article 1 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (Geneva: International Committee of the Red Cross, 1977b); Henckaerts et al., Customary International Humanitarian Law; Appeals Chamber, "Prosecutor V. Dusko Tadic Aka "Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction)," International Criminal Tribunal for the former Yugoslavia, icty.org/x/cases/tadic/acdec/en/51002.htm (accessed May 12, 2016). §268; Article 1(2) Amended Protocol II to the Convention on Certain Conventional Weapons.

[38] International Committee of the Red Cross, International Humanitarian Law. p. 24.

[39] International Committee of the Red Cross, International Humanitarian Law. p. 20.

[40] Fleck, ed., The Handbook of International Humanitarian Law. p. 51.

[41] Ibid. p. 51.

[42] Ibid. p. 51.

[43] Henckaerts et al., Customary International Humanitarian Law. Rules 61 and 62. pp. 213-219.

6.2.2 Applicability to military cyber operations

Debate on the applicability of IHL to cyber operations has settled, as one author argues: "no serious international law expert questions the full applicability of IHL to cyber operations".[44] Although law experts might have agreed upon IHL's applicability to cyber operations, many States are struggling with the issue of how to apply IHL to cyber operations.[45] In order to find common ground a group of governmental experts was mandated[46] by the United Nations in order to study if, when and how international law applies to, amongst other, cyber operations.[47] As to the applicability of IHL there is some form of consensus amongst States as forwarded in the 2015 report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (the 'GGE').[48] The GGE "notes the established international legal principles, including where applicable, the principles of humanity, necessity, proportionality and distinction".[49]

By noting the cardinal principles of international humanitarian law, the twenty States in the GGE have – somewhat implicitly – acknowledged that IHL applies to military cyber operations during conflict.[50] There is no explicit referral to IHL provisions as that might infer the possibility of cyberspace being used for military activities – a view strongly opposed by China and Russia.[51] The main goal of the latter two is "not to legalize and not to regulate conflicts in the information space, but to prevent using the [information and communication technologies] in the political and military purposes."[52] Hence any reference to IHL will be avoided as they expect that it may result in States using cyberspace for military purposes. Despite some minority views, most States have acknowledged IHL's applicability to cyber operations and even conflicting views are converging with the general

[44] Schmitt, "The State of Humanitarian Law in Cyber Conflict,"

[45] Li Zhang, "A Chinese Perspective on Cyber War," Internation Review of the Red Cross 94, no. 886 Summer 2012 (2012). p. 804.

[46] United Nations General Assembly, A/RES/68/243: Developments in the Field of Information and Telecommunications in the Context of International Security

[47] NATO Cooperative Cyber Defence Centre of Excellence, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law," CCD COE, ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html#footnote6_e3nqd0e (accessed July 27, 2016).

[48] United Nations General Assembly, A/70/174: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (New York: United Nations,[2015]).

[49] Ibid. p. 12, §28(c).

[50] NATO Cooperative Cyber Defence Centre of Excellence, "2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law,"

[51] Ibid.

[52] Sputnik International, "UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official," sputniknews.com/politics/20150817/1025819426/UN-cybersecurity-report-compromises-on-self-defence.html (accessed July 28, 2016).

opinion that IHL is applicable to cyber operations.[53]

6.2.3 Sub-conclusion

This section has focused on the applicability of IHL in general and to military cyber operations in specific by answering the sub-question: *When does the IHL apply and does it apply to the military cyber operations?*

Sub-section 6.2.1 has argued that IHL applies when there is an armed conflict, the IHL instruments applicable in a specific situation are dependent of the type of conflict: international armed conflict or non-international armed conflict. In either case, certain parts of IHL are applicable. Sub-section 6.2.2 has discussed the applicability of IHL to military cyber operations. Debate no longer revolves around the question whether or not IHL is applicable to cyber operations; instead, discussion focuses on how to apply IHL on military cyber operations.

6.3 Applying IHL to military cyber operations

As noted in section 6.2, it is clear that IHL applies to military cyber operations, however, how to best apply IHL to military cyber operations is subject of debate. The difficulties in applying IHL are caused by military cyber operations' often non-physical way of achieving effects when used stand-alone, that is, without any other traditional operation creating effects in the physical dimension (e.g. death, damage or injury). When used side-by-side with the traditional operation, that is, as "an integral part of an operation that constitutes an attack", then the "law of armed conflict on attacks applies fully to such cyber operations."[54] This section will discuss difficulties of applying IHL to stand-alone military cyber operations by answering the following sub-question: *How should the legal framework of IHL be applied to stand alone military cyber operations?*

The basic principles of IHL "such as distinction and prohibitions of unnecessary suffering apply to cyber operations", whether or not "a number of specific limitations and prohibition in the law of armed conflict" are applicable depends on the qualification of the military cyber operations as 'attack'.[55] 'Attack' in the context of military cyber operations is fluid: it's meaning depends per discipline involved in military cyber operations (e.g. legal, technical and military). Therefore, this section will start with clarifying the approach taken to attack in this section (6.3.1). After having clarified the different meanings of attack, this section will discuss legal approaches to attack and related elements of harm and damage in

[53] "The State of Humanitarian Law in Cyber Conflict," accessed July 27, 2016, justsecurity.org/18891/state-humanitarian-law-cyber-conflict/.

[54] Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Rule 92.

[55] Ibid. Rule 92.

the context of stand-alone military cyber operations (6.3.2). This section will conclude with answering the sub-question (see 6.3.3).

6.3.1 Seven shades of attack

Before touching upon the qualification of military cyber operations as attack, it is necessary to touch upon the many variants of 'attack' and/or 'cyber attack' used in the discourse regarding military cyber operations as there are fundamental differences in the understanding of 'attack' in (1) legal, (2) technical, (3) military and (4) media sense.

The legal discipline distinguishes 'attack' in the *Jus ad Bellum* and the IHL sense. 'Attack' in the *Jus ad Bellum* is short for an 'armed attack' which may trigger a target-State's right to self-defence.[56] Cyber attack in this case would relate to a cyber operation constituting an armed attack triggering an armed conflict. 'Attack' in IHL involves an "act of violence against the adversary, whether in offence or in defence".[57] Thus it relates to the (violent) acts carried out by the actors involved in a conflict against each other. Cyber attack consequently would pertain to a cyber operation reaching the threshold of Article 49 (1) of Additional Protocol I. Consequently, this cyber attack would be governed by the laws on the conduct of hostilities (see 6.4)

In a technical sense, for example in the field of information security or cyber security, 'attack' is understood differently. It is used to relate to an "intentional act by which an entity attempts to evade security services and violate the security policy of a system. That is, an actual assault on system security that derives from an intelligent threat."[58] It is often used interchangeably, however, with a security incident, which is defined as "a security event that involves a security violation [...] in other words, a security event in which the system's security policy is disobeyed or otherwise breached."[59] Security incidents and events are also often mistaken. A security event is "an occurrence in a system that is relevant to the security of the system".[60] Thus a 'security event' is not yet a violation of security, it may simply entail somebody logging into a system (benign usage). If the 'security event', however, involves a violation of security policy, for instance unauthorised access to a system, it is a 'security incident'. If that 'security incident' is intentional and derived from an intelligent threat it is an 'attack'. Thus, within the field of information security, 'cyber attack' would be understood as the latter.

[56] See Article 51 United Nations, Charter of the United Nations (New York: United Nations, 1945).

[57] Article 49 (1) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[58] Shirey, Request for Comments 4949: Internet Security Glossary Version 2. p. 21.

[59] Ibid. p. 270.

[60] Ibid. p. 268.

In a military sense 'attack' relates to one of the eight offensive tactical activities (i.e. attack, raid, reconnaissance in force, exploitation, pursuit, ambush, breakout of encircled forces and feint and demonstration) and is further specified as "to attack is to take offensive action against a specified objective".[61] This is reflected in contemporary cyber operations doctrine, cyber attack is often one of the activities conducted under the ambit of offensive cyber operations.[62] Thus understood, the military would simply understand 'attack' and 'cyber attack' as denoting offensive action.

The source of most of the confusion regarding 'attacks' and 'cyber attacks' are the media and governmental officials using terms interchangeably. They often report mere security events or incidents as cyber attacks.[63] For instance, officials and the media dub probe scans, which are security events reported by a firewall, 'cyber attacks'.[64] Considering the various interpretations of 'attack' and 'cyber attack' within the different disciplines, media reporting "1.8 billion" cyber attacks a month logically leads to confusion.[65] From a technical perspective large portions of the 'cyber attacks' merely involve 'security events' (an event in the defensive perimeter of an organisation). These 'security events' involve a portion that may constitute 'security incidents' (breach of security policy). These 'security incidents' may include some 'cyber attacks' (deliberate breach). None of these have constituted an armed attack in the Jus ad Bellum sense and most likely will not include or contain very few cyber attacks in the IHL sense – as the latter would, for instance, require a state of conflict in which the target-State is a party and consequently it is being attacked by another party to the conflict. From a military perspective these security events may or may not be a part of a cyber attack, this entirely depends on the purpose of the attacker. This section discusses 'attack' in the IHL sense, involving the qualification of military cyber operations as 'attack' during conflict.

6.3.2 Threshold of Attack

Instrumental to the discussion on the qualification of military cyber operations as 'attack' is article 49 of AP I, which defines attacks as "acts of violence against the adversary, whether in offence or in defence".[66] This sub-section will briefly highlight the general discussion regarding 'acts of violence' (6.3.2.1) and then focus on its interpretation in the specific context of stand-alone military cyber operations (6.3.2.2).

[61] North Atlantic Treaty Organisation, ATP 3.2.1: Allied Land Tactics (Brussels: North Atlantic Treaty Organisation, 2009b). p. 5-5.

[62] See for instance: The Joint Chiefs of Staff, Joint Publication 3-12 (R): Cyberspace Operations. p. II-5.

[63] Brian Fung, "How Many Cyberattacks Hit the United States Last Year," Nextgov, nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/ (accessed January 1, 2017).

[64] Sean Lawson, "Just how Big is the Cyber Threat to the Department of Defense?" Forbes, forbes.com/sites/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod/#7dd5408175e3 (accessed January 3, 2017).

[65] Erika Lovley, "Cyberattack Explode in Congress," Politico, politico.com/story/2010/03/cyberattacks-explode-in-congress-033987 (accessed January 3, 2017).

[66] Art. 49 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

6.3.2.1 *Acts of violence in general*

Dörmann argues that certain authors have advanced the view that the Commentary to Protocol I has denoted 'acts of violence' as "physical force" only.[67] Careful reading of the Commentaries suggests, however, that attack must be understood broadly as denoting "combat action".[68] Whilst the drafting history of the Protocol indicates that once attack was defined as 'acts of violence committed against the adversary by means of arms, in the course of hostilities",[69] this has disappeared in the final article. Still there are remnants of this earlier notion in discussions. Today, however, "it seems to be generally recognised that 'acts of violence' do not necessarily require the use of kinetic violence, but that it is sufficient if the resulting effects are equivalent to those normally associated with kinetic violence".[70] Despite general recognition, AP I leaves considerable room for interpretation when faced with new phenomena such as military cyber operations and other 'non-violent' military operations/activities.

6.3.2.2 *Acts of violence in cyberspace*

In the context of cyber operations there are four approaches to Article 49 AP I that have different consequences for the application of "a number of specific limitations and prohibition in the law of armed conflict", most prominently the permissibility of targeting civilians and civilian objects. Michael Schmitt has dubbed the two approaches the "permissive (in the sense of allowing a wider range of cyber operations against the civilian population)" and the "restrictive (restricting cyber operations as a matter of law)".[71] The permissive and restrictive approaches have been the two prevailing views from 2004 until 2014. Another approach could be called a "functional approach",[72] including a 'functionality test', which emerged during the Tallinn Manual project in 2014. In the wake of the latter, another, different discussion, arose that circumvents many of the debates in the other three approaches, namely the notion of data as object. This sub-section will highlight these four approaches: data as object (6.3.2.2.1), permissive (6.3.2.2.2), restrictive (6.3.2.2.3), and functional (6.3.2.2.4).

6.3.2.2.1 *Data as an object*

The first approach is often considered to be a different debate, revolving around the notion of 'object' in relation to Article 49 (attack) AP I. Should data qualify as an object "then cyber

[67] Knut Dörmann, "Applicability of the Additional Protocols to Computer Network Attack" (Stockholm, ICRC, November 17-19, 2004). p. 4.

[68] Pilloud et al., Commentary on the Additional Protocols: Of 8 June 1977 to the Geneva Conventions of 12 August 1949. p. 603.

[69] Committee III, Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, Vol. XIV (Bern: Federal Political Department, 1978). p. 44.

[70] Nils Melzer, "Cyberwarfare and International Law," United Nations Institute for Disarmament Research Resources (2011). p. 26.

[71] Michael N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack," International Review of the Red Cross 96, no. 893 (2014), 189-206. pp. 192-198.

[72] Joost R. H. Bunk, "The Protection of Intellectual Property in Cyber-Space Under International Humanitarian Law during Cyber Operations" (Master, Leiden Law School), . pp. 14-15.

operations that destroy or alter data are attacks, and those directed against civilian and other protected data are unlawful."[73] In other words, instead of concentrating on the act (attacking) this approach focuses on the target (object) for qualifying the act as attack. When the target is an object, it should be subjected to a "two-pronged test, which requires that the object in question makes an effective contribution to military action and that its destruction, capture or neutralisation offers a definite military advantage".[74] There are, however, two diverging opinions on this matter, namely: the traditional (or 'orthodox') view denying data's qualification as object (6.3.2.2.1.1) and a 'contemporary' view affirming data's qualification as object (6.3.2.2.1.2).

6.3.2.2.1.1 Traditional ('Orthodox')

The traditional or "orthodox"[75] view is forwarded in Rule 38 and its commentary in the Tallinn Manual where Article 52(2) API is slightly rephrased and the following sentence is added: "military objectives may include computers, computer networks, and cyber infrastructure."[76] In the Commentary to Rule 38, the Manual follows the notion of 'objective' as forwarded in the ICRC Commentary to the Additional Protocols, that is, "something that is visible and tangible".[77] Following this notion, "computers, computer networks, and other tangible components of cyber infrastructure constitute objects."[78] Data is not ipso facto interpreted as object in de Tallinn Manual hence data is not subjected to the two-pronged test and consequently data as 'non-object' may be targeted more freely, that is, below the threshold of attack – which in turn depends on the approach taken, which will be discussed later in this section (see 6.3.2.2.2 to 6.3.2.2.4).

6.3.2.2.1.2 Contemporary

The 'contemporary' view – amongst other held by a minority of the Experts involved in the Tallinn Manual,[79] Mačák,[80] and Harrison Dinniss[81] – consider data to be an object and hence it should be subjected to the two-pronged test. This position is characterised as "de lege ferenda" or in other words, law as it should be and not as it stands today in the Tallinn Manual.[82] It is, however, important to highlight their views as they offer an alternative to the traditional approach forwarded in the Tallinn Manual.

[73] Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack," , 189-206. p. 200.

[74] Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law," Israel Law Review 48, no. 1 (2015). p. 12.

[75] Ibid. p. 3.

[76] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 125.

[77] Pilloud et al., Commentary on the Additional Protocols: Of 8 June 1977 to the Geneva Conventions of 12 August 1949. p. 624. §2008.

[78] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 127.

[79] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 127.

[80] Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law,"

[81] Heather Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives," Israel Law Review 48, no. 1 (2015), 1-16; Heather Harrison Dinniss, Cyber Warfare and the Laws of War (Cambridge: Cambridge University Press, 2012). pp. 184-185.

[82] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 127.

The minority in the Tallinn Manual held that "for the purposes of targeting, data per se should be regarded as an object [...] failure to do so would mean that even the deletion of extremely valuable and important civilian datasets would potentially escape the regulatory reach of the law of armed conflict, thereby contradicting the customary premise of that law that the civilian population shall enjoy general protection from the effects of hostilities".[83]

Mačák, after extensive legal reasoning based on the rules on treaty interpretation, accuses the Tallinn Manual of a single-faceted approach.[84] He offers an alternative route to interpreting data as object by holding that the status of 'object' should be open for evolutive interpretation.[85] In this day and age, i.e. as of 2014, that evolutive interpretation entails that "data is an 'object' for the purposes of the IHL rules on targeting."[86]

Harrison Dinniss agrees on Mačák's point of departure that objects do not require to have a tangible or material form and thus "the term 'objects' must be interpreted to include intangible things such as code."[87] She argues that data is not a single entity and distinguishes content-level ('text of an article, contents of databases, library catalogues') and operational-level data ('operating systems, software applications and SCADA/ICS systems').[88] Content-level data, apart from the specifically protected categories ("medical records and material, cultural property"), can be targeted more freely and is not protected per se as it does not impede on functionality. Targeting operational-level data will result in loss of functionality of the system and hence qualify as damage, destruction or neutralisation and be subjected to the rules on attack.[89] Using different lines of reasoning, the minority of the Tallinn Manual, Mačák and Harrison Dinniss arrive at a similar conclusion: data is an object under IHL and targeting civilian objects is prohibited.

6.3.2.2.1.3 In sum: Data as object

There are two diverging opinions regarding data as object, the 'traditional' (see 6.3.2.2.1.1) and contemporary (see 6.3.2.2.1.2). The former is posited in the Tallinn Manual and is long established in IHL, the latter is based on evolutive interpretation of the notion of object under IHL. This thesis will hold that the traditional approach best captures the current state of IHL, as some have argued before, the contemporary approach should be characterised de lege ferenda. The following three approaches focus on the act (attacking) instead of the target (object).

[83] Ibid. p. 127.

[84] Article 31 Vienna Convention on the Law of Treaties (Vienna: United Nations, 1969).

[85] Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law." pp. 18-19.

[86] Ibid. p. 30.

[87] Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives". pp. 42-46.

[88] Ibid. p. 41.

[89] Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives". p. 42.

6.3.2.2.2 Permissive

The permissive approach takes the position that "only cyber operations that constitute attack are subject to the principles of distinction, proportionality, and precaution."[90] Thus understood, a military cyber operation "intended to, or would foreseeably, cause injury, death, damage or destruction" is subject to the laws on the conduct of hostilities.[91] Controversially, however, "unless otherwise prohibited by specific provisions of humanitarian law, [military cyber operations] unlikely to result in the aforementioned consequences are permissible against non-military objectives, such as the population."[92] This is an approach based on the structure and wording of AP I, which shows that "Article 48 provides a general principle of protection of the civilian population [and that] this general principle is 'operationalised' in the subsequent articles".[93] In other words, article 48 AP I (general principle) is understood as an overarching rule, for guidance as to permissible activities, however, one must look at the subsequent articles. When a cyber operation does not qualify as attack under Article 49 AP I, then it may be used against a wider audience such as the population.

6.3.2.2.3 Restrictive

In 2004 Knut Dörmann advanced what Michael Schmitt has dubbed the 'restrictive approach'.[94] Dörmann points to Article 52(2) AP I, which refers to 'neutralisation', in order to advance the view that "by referring not only to destruction or capture of the object but also to its neutralisation the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way."[95] Following this line of reasoning, Dörmann disagrees with Schmitt's notion that "the use of CNA expands the range of legitimate targets", that is, the permissive approach. In other words, military cyber operations not qualifying as attack are not permissible against the population.

In a similar way although with different reasoning Melzer interprets article 48 AP I more broadly, resulting also in a restrictive approach. Nils Melzer agrees with the permissive approach that indeed the concept of attack is narrower than military operations and/or hostilities. He argues, however, that military cyber operations that constitute "part of hostilities" are subject to the "restraints imposed by IHL".[96] Hence not only cyber operations qualifying as attack, but also operations below the threshold of attack are governed by IHL. He focuses on to the basic treaty rule (article 48 AP I) that uses military operations for specifying the ground rule on distinction. He deems that the subsequent

[90] Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians". 533-578. p. 554.

[91] Michael N. Schmitt, "Wired Warfare: Computer Network Attack and Jus in Bello," International Review of the Red Cross 84, no. 846 (2002). p. 378.

[92] Ibid. p. 378.

[93] Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians".,533-578. p. 554.

[94] Dörmann, "Applicability of the Additional Protocols to Computer Network Attack"

[95] Ibid. p. 6.

[96] Melzer, "Cyberwarfare and International Law." p. 27.

articles, amongst other article 49 AP I (attack), should be interpreted with the scope of article 48 AP I (ground rule) in mind – contrary to the permissive approach. Thus when a cyber operation qualifies as conduct of hostilities then it is governed by IHL. Hostilities are much broader than attack, they refer to "the (collective) resort by the parties to the conflict to means and methods of injuring the enemy, and could be described as the sum total of all hostile acts carried out by individuals directly participating in hostilities."[97] For determining whether an activity qualifies as conduct of hostilities Melzer uses the criteria from the notion of direct participation in hostilities, namely: threshold of harm, direct causation and belligerent nexus.[98] Melzer's reasoning results in a restrictive approach similar to Dörmann's: military cyber operations below the threshold of attack may not be directed against the civilian population.

Droege and Harrison Dinniss put forward another view advocating a restrictive approach, both interpret articles 48-57 AP I in a non-sequential way. Pointing "to the wording of article 48 of Additional Protocol I and the first sentences of Articles 51 and 57", Dinniss argues that "the civilian population must be protected not only against attacks, but also more generally against the effects of military operations".[99] Droege, similar to Dörmann, focuses on neutralisation in Article 51 by referring to an (unofficial) commentary to AP I, she states "that 'neutralisation' was meant to encompass 'an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it".[100] Although using different argumentations, Dörmann, Melzer, Droege and Dinniss arrive at a similar conclusion and advance a restrictive view implying that the laws on the conduct of hostilities govern 'military cyber operations' below the threshold of attack.[101]

6.3.2.2.4 Functional

The functional approach revolves around the 'functionality test', which was "a major breakthrough in the dialogue [...] in the [Tallinn Manual] project's final year".[102] Functional in this sense should be understood as involving the assessment of the loss of functionality of a target object in order to establish whether the military cyber operation targeting the object reaches the threshold of attack. Until 2013 the permissive and restrictive approaches were the prevailing views, the functional approach "establishes substantial common

[97] Ibid. p. 27; Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law (Geneva: International Committee of the Red Cross, 2009). pp. 47-48.

[98] Melzer, "Cyberwarfare and International Law." pp. 27-28.

[99] Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," , 533-578. p. 555.

[100] Michael Bothe, Karl Josef Partsch and Waldemar A. Solf, New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949 (Dordrecht: Martinus Nijhoff Publishers, 1982). p. 325; Droege, "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," , 533-578. p. 558; Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack". pp. 197-198.

[101] In the IHL sense a 'military operation' *ipso facto* qualifies as an attack as it is defined as operations "during which violence is used", see: Claude Pilloud et al., Commentary on the Additional Protocols: Of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Geneva: Martinus Nijhoff Publishers, 1987). §1875. p. 600. 'Military cyber operations' here should be understood in the military sense as advanced in chapter five.

[102] Ibid. p. 199.

ground between the permissive and restrictive approaches".[103] The notion lying at heart of the functional approach is that "an operation that 'damages' an object is logically an attack" and that damage should be understood as including interference "with the functionality".[104] Thus, a military cyber operation that does not reach the 'traditional' threshold of attack (encompassing physical injury or damage) may still be an attack by virtue of it interfering with the functionality of an object, hence qualify as attack, and consequently be governed by the laws on the conduct of hostilities.

Within the functional approach there are three interpretations of the type of damage required to constitute 'damage' and consequently 'attack' in the 'functionality test'. The first interpretation has the lowest threshold, "it is immaterial how an object is disabled: the object's loss of usability constitutes the requisite damage".[105] In other words, irrespective of the type of damage or its duration, loss of function constitutes an attack. A second interpretation is that when an operating system (OS) needs reinstalling the "damage requirement is met".[106] The third interpretation with the highest threshold is "that interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components."[107]

6.3.2.3 Sub-conclusion

In the matter of stand-alone military cyber operations there are many different perspectives and approaches that require anyone wishing to determine the legal framework for stand-alone military cyber operations to choose a preferred approach. This choice impacts upon whether military cyber operations below the threshold of attack need to (a) comport with the basic principles of IHL, however, targeting of the civilian population and objects is permissible; or (b) comport with IHL in full, including rules on the conduct of attack. The choices and their consequences have been visually depicted in Figure 31.

Before applying the framework, it is necessary to determine the type of operation: a military cyber operation side-by-side with a traditional military operation qualifying as force or a stand-alone military cyber operation. The former, by virtue of the traditional operation, will qualify as an attack and consequently trigger the full IHL framework on the law on the conduct of hostilities. Stand-alone military cyber operations, the subject of the overview in Figure 31, are more difficult to assess, as there are a variety of successive viewpoints to choose from.

[103] Ibid. p. 203.

[104] Ibid. p. 203.

[105] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 109.

[106] Ibid. p. 109.

[107] Ibid. p. 108.

The first step in the framework is assessing whether the stand-alone military cyber operation will likely cause death, damage, injury or otherwise violent consequences. Should the cyber operation qualify as such, it is an attack and hence covered by the full IHL framework. A military cyber operation without these consequences is a cyber operation below the threshold of Article 49 API, which is a much-debated category of cyber operations.

Consequently, a second selection has to be made regarding a majority (traditional) or minority (contemporary) view on the notion of data being an object (see 6.3.2.2.1). This is essentially choosing the majority approach taken by the Tallinn Manual and Michael Schmitt or a minority approach championed by Harisson Dinniss and Mačák. Selecting the minority view will result in all data being an object and hence the military cyber operation below the threshold of force will still qualify as an attack as it is directed against an object and consequently trigger the full framework on the law on the conduct of hostilities. Selecting the majority view, disqualifying data as object per se, consequently requires a view to be taken as to the permissibility of harm/damage caused and qualifying criteria for damage.

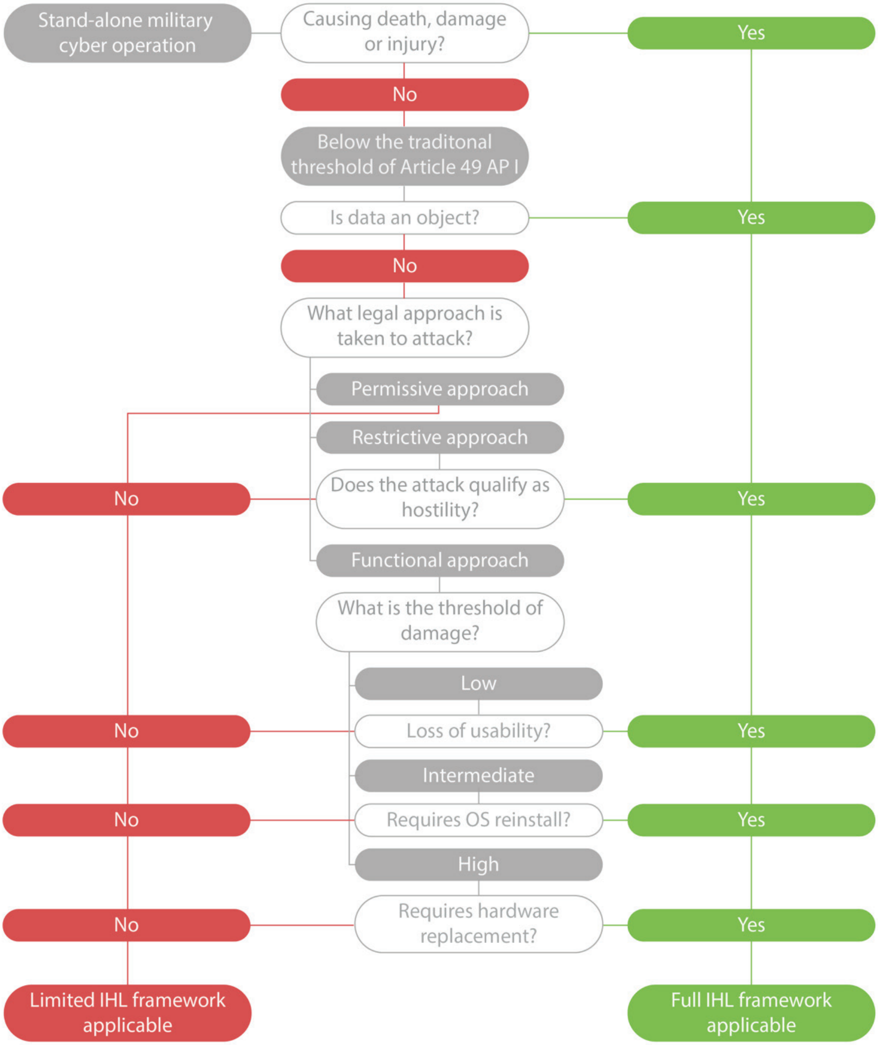
Stand-alone military cyber operation
Causing death, damage or injury?
Yes
No
Below the traditonal threshold of Article 49 AP I
Is data an object?
Yes
No
What legal approach is taken to attack?
Permissive approach
Restrictive approach
No
Does the attack qualify as hostility?
Yes
Functional approach
What is the threshold of damage?
Low
No
Loss of usability?
Yes
Intermediate
No
Requires OS reinstall?
Yes
High
No
Requires hardware replacement?
Yes
Limited IHL framework applicable
Full IHL framework applicable

Figure 31 Overview of legal approaches and consequences

There are three approaches in this matter: (1) the permissive approach forwarded by Michael Schmitt (see 6.3.2.2.2); (2) the restrictive approach promoted by – amongst other – Dörmann, Droege, Melzer and Harisson Dinniss (see 6.3.2.2.3); and (3) the functional approach promoted by the Tallinn Manual (see 6.3.2.2.4). The permissive approach is straightforward, if a military cyber operation does not reach the threshold of Article 49 AP I (attack), objects normally protected from attack, such as the civilian population, may be targeted, that is, unless they are specifically protected (medical units etc.).

The restrictive approach interprets Article 49 AP I more broadly and thereby restricting the options to a Party as a matter of law (see 6.3.2.2.3). Within this approach 'attack' is understood to envelop all military operations – including military cyber operations below the threshold of attack. Although trying to maximally protect non-military objects, even within the restrictive approach there is an implicit criterion for a cyber operation, namely: that it qualifies as conduct of hostilities or military operation. This is, however, a relatively low threshold looking at the criteria used to qualify military cyber operations as hostility. The full IHL framework on the conduct of hostilities applies to a cyber operation qualifying as hostility.

The functional approach to damage forks into three different views on the threshold of damage for a military cyber operation to qualifies as damaging: low, intermediate and high (see 6.3.2.2.4). The low threshold involves 'loss of usability', the intermediate 'requiring a OS reinstall' and the high 'replacement of hardware'. Depending on the approach taken, a military cyber operation below the threshold of damage is not an attack, whereas military cyber operations reaching the threshold of attack are governed by the laws on the conduct of hostilities.

Thus, there are two outcomes: (1) the military cyber operation below the threshold of Article 49 AP I is governed by the well-defined laws on the conduct of hostilities or (2) it is governed by a much vaguer framework for military operations below the threshold of Article 49 AP I. This chapter will focus on the former, as to the latter: this is a lacuna requiring scholarly, policy and military attention.[108]

6.3.3 Sub-conclusion

This section has attempted to answer the sub-question: *How should the legal framework of IHL be applied to stand alone military cyber operations?* 'Military cyber operations' are governed by basic principles of IHL at the least (e.g. distinction and prohibition of unnecessary suffering). Depending on the qualification of the military cyber operations as attack additional limitations and prohibitions apply as enclosed in the laws on the conduct of hostilities (see 6.3).

This section has first discussed the different meanings of 'attack' in the context of military cyber operations in technical, legal, military and other disciplines (see 6.3.1). After specifying the type of 'attack' being subject of research in this section, that is, the legal understanding in the IHL sense, this section has focused on the different perspectives on

[108] See for instance: Bart van den Bosch, "Non-Kinetic Capabilities and the Threshold of Attack in the Law of Armed Conflict," in Netherlands Annual Review of Military Studies 2017: Winning without Killing, the Strategic and Operational Utility of Non-Kinetic Capabilities in Crises, eds. Paul A. L. Ducheine and Frans P. B. Osinga (The Hague: Asser Press, 2017), 255-273; Bart van den Bosch, "War without Violence: An Analysis of Rules of International Humanitarian Law Applicable to the Military Cyber Operations Below the Threshold of Attack" (Ph.D., Netherlands Defence Academy and University of Amsterdam), .

the qualification of military cyber operations as attack (see 6.3.2). These perspectives and approaches were synthesised into a model depicting the choices to be made in determining the legal framework applicable to a specific military cyber operation. There is no single answer to the sub-question; it depends on the type of military cyber operation (side-by-side or stand-alone), the cyber capabilities involved therein, and the effects (e.g. death, injury, and damage).

Although the answer to the sub-question is context specific, the remainder of this sub-section will highlight this research's preferred approach to the threshold of attack – as this is context agnostic. The functional approach seems to strike a balance between a too restrictive and a too permissive view. The restrictive approach would favour humanitarian concerns over military requirements and hence overly restrict the options open to belligerents and prohibit activities such as psychological operations that are considered permissible in contemporary conflict. At the same time the functional approach would recognise the fact that although not being damaging, cyber operations can still wreak havoc throughout the civilian population by disrupting functionality. The permissive approach fails to address this notion, as it would allow activities disrupting functionality (albeit to a specific extent and in specific conditions) and hence promote an overly permissive approach. In sum, the functional approach offers an elegant way of balancing the permissive and restrictive approaches and follows the line of reasoning used in many issues in applying IHL to military cyber operations: a consequence-based approach ('it is irrelevant how the harm/damage manifests, it is about the effects or consequences').

As to the threshold of harm/damage this chapter holds that loss of usability is best suited for application in IHL and not the intermediate (operating system reinstall) or high threshold (hardware replacement). The reason is that the OS or hardware thresholds make little sense from a technical perspective. An OS reinstall says little about the severity of harm caused to a target, it is one of the many recovery 'strategies' open to an information security professional or user after a system has been affected by a cyber capability. An OS reinstall is considered a 'best practice' irrespective of the severity of harm to a system.

The same is the case of the hardware replacement, this also says little about the severity of harm caused to a system. In this context the 2013 Shamoon/Saudi Aramco case is often cited as a situation where physical replacement of hardware was required. Hardware replacement, however, was not the only option open to Saudi Aramco. They made a conscious choice for selecting replacement as opposed to fixing the hard drives master boot records (MBR) – which is an equally feasible recovery option. It would be odd that when Saudi Aramco would select an OS reinstall or MBR fix over hardware replacement the cyber operation would fail to qualify as an attack when the highest threshold is adopted, that is, in the case of an armed conflict. Similarly, when an OS reinstall is conducted as a 'security best practice', irrespective of the extent of harm to the system, it would qualify the military cyber operation as an attack. If a user or administrator appraises a security incident wrong for instance, and decides to reinstall the OS, or simply follows standard operating procedures including an OS reinstall, the operation would qualify as an attack by virtue of the subjective choice of the administrator. As such, this thesis holds that the 'loss of usability' would best mitigate the effect of subjectivity and offer those conducting military cyber operations a predictable and objective criterion.

6.4 Conduct of hostilities

When an armed conflict arises, certain rules come to apply to military cyber operations conducted within the context of that armed conflict (see 6.2). Whether or not the laws on the conduct of hostilities govern a military cyber operation in full or in part depends on the viewpoints chosen to the issue of data as an object and the qualification as an attack (see 6.3). This section will focus on the contents of the legal framework triggered by a military cyber operation's positive qualification as 'attack'. In other words, it will discuss the legal framework enveloping military cyber operations above the threshold of attack contained in article 49 (1) AP I by answering: Which IHL rules and regulations apply to military cyber operations above the threshold of attack?

In order to answer the sub-question this section will first briefly discuss the need for a weapons review (6.4.1). Then it will discuss the main rules governing the conduct of hostilities: distinction (6.4.2), precautions (6.4.3) and proportionality (6.4.4). After that, this section will briefly highlight other relevant rules in the context of conduct of hostilities (6.4.5). After having specified the main rules, this section will point to certain difficulties in applying the legal framework to military cyber operations (6.4.6). As last, the sub-question will be answered by integrating the insights from the various sections (6.4.7).

6.4.1 Weapons review

The obligation to conduct a weapons review is only loosely tied to the legal framework on the conduct of hostilities, it is a prerequisite derived from one of the fundamental tenets of IHL, namely "in any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited."[109] Although it is a general obligation that States should "ensure that the cyber means of warfare that they acquire or use comply with the rules of the law of armed conflict that bind the State",[110] the more specific obligation to conduct a weapons review is only binding upon the 174 States who have ratified AP I. There are numerous specific weapons that are prohibited or restricted under additional international treaty law, these treaties also bind States not party to AP I.[111] In other

[109] Article 35 (1) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I); Article 22 Second International Peace Conference, Convention (IV) Respecting the Laws and Customs of War on Land (The Hague: International Conferences (The Hague), 1907).

[110] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 153.

[111] See for a detailed list on treaty law prohibiting specific weapons: Kathleen Lawand, Robin Coupland and Peter Herby, A Guide to the Legal Review of Weapons, Means and Methods of Warfare: Measures to Implement Article 36

words, even States not party to AP I have to assess whether a weapon, mean or method is specifically prohibited or restricted by any of its international obligations. This subsection will focus on the AP I weapons review for the remainder, some considerations will, however, apply to non-parties as well – this depends on the specific context.

The weapons review to be conducted by a State wishing to study, develop, acquisition or adopt "a new weapon, means or method of warfare" in essence involves three steps. The first step is assessing the applicability of prohibitions or restrictions on the use of *specific* weapons, means and methods of warfare under (a) treaty obligations and (b) customary law. The treaty obligations may include the prohibitions or restrictions stemming from treaties on asphyxiating gases, expanding bullets, environmental modification techniques or excessively injurious or indiscriminate effects.[112] The customary law provisions for example comprise the prohibition or restriction on the use of poison, biological weapons, chemical weapons, and riot-control agents as a method of warfare.[113]

Secondly, should "no specific prohibition or restriction [be] found to apply, the weapon or means of warfare under review and the normal or expected methods by which it is to be used must be assessed in light of the general prohibitions or restrictions provided by treaties and by customary law".[114] This step similarly comprises (a) treaty obligations and (b) customary law. The general provisions under international treaty law include for instance the prohibition "to employ weapons, projectiles and material and methods of warfare of a nature to cause superfluous injury or unnecessary suffering" or "methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment".[115] Under customary law they may involve the customary law equivalent of the treaty provisions such as the prohibition of the use on weapons that may "cause superfluous injury or unnecessary suffering" or indiscriminate weapons.[116]

The third step is perhaps the vaguest and least formal, it involves assessing the weapon, means or methods vis-à-vis the Martens clause. The Martens clause emphasises that "in cases not covered by this Protocol or by other international agreements, civilians and combatant remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from dictates of

of Additional Protocol I of 1977 (Geneva: International Committee of the Red Cross, 2006). pp. 11-13.

[112] Kathleen Lawand, Robin Coupland and Peter Herby, A Guide to the Legal Review of Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977. pp. 12-13.

[113] Henckaerts et al., Customary International Humanitarian Law. p. 251, 257, 259. Rule 72, 73, 74.

[114] Lawand, Coupland and Herby, A Guide to the Legal Review of Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977. p. 15.

[115] Article 35 (2)(3) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I); See for a more detailed list: Lawand, Coupland and Herby, A Guide to the Legal Review of Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977. pp. 15-16.

[116] Henckaerts et al., Customary International Humanitarian Law. p. 237, 244. Rule 70, 71.

public conscience".[117] In other words, when a weapon, means or method of warfare is not found to be prohibited or restricted in step one or two, it "would be considered contrary to the Martens clause if it is determined per se to contravene the principles of humanity or the dictates of public conscience".[118]

Similar to conventional weapons, the review of cyber operations and/or cyber capabilities should also include the aforementioned steps. The data to be considered in such a review by a reviewing authority "will have to take into consideration a wide range of military, technical, health and environmental factors".[119] Not all cyber operations necessitate a review, only means that are by design, use, or intended use capable of reaching the threshold of attack and only methods qualifying as "cyber tactics, techniques and procedures whereby hostilities are conducted".[120] The ability of military cyber operations to reach the threshold of attack depends on the approach taken to attack and damage (see 6.3). It is clear, however, that more general 'cyber activities', such as "communications between friendly forces", do not qualify and hence do not need to be reviewed.[121] After having reviewed the weapon, means or method, and reached a "favourable" conclusion, the weapon may be used during conflict. It is, of course, still subjected to rules relating to attack, involving the principles of distinction, precaution and proportionality.

6.4.2 Distinction

One of the "cardinal principles" of IHL is distinction, which is "aimed at the protection of the civilian population and civilian objects and establishes the distinction between combatants and non-combatants; States must never make civilians the object of attack [...]".[122] This principle is considered customary law and is codified and operationalised in article 48 AP I, which adds to the above: "[...] Parties to the conflict shall [...] direct their operations only against military objectives".[123] Not all operations are subjected to the principle of distinction, for instance "psychological operations such as dropping leaflets or making propaganda broadcasts are not prohibited even if civilians are the intended audience".[124] Military cyber operations constituting these types of operations, by analogy

[117] Article 1 (2) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[118] Lawand, Coupland and Herby, A Guide to the Legal Review of Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977. p. 17.

[119] Lawand, Coupland and Herby, A Guide to the Legal Review of Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977. p. 17.

[120] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 142.

[121] Ibid. p. 142.

[122] International Court of Justice, Advisory Opinion of 8 July 1996: Legality of the Threat Or use of Nuclear Weapons (The Hague: International Court of Justice, 1996). p. 257. §78.

[123] Article 48 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[124] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 112.

"comport with the law of armed conflict".[125] Only in those cases where the operation qualifies as attack, it must discriminate between military objectives and the civilian population and civilian objects. As mentioned before, with military cyber operations it depends on the approach taken whether one considers a certain cyber operation to constitute an attack (see 6.3).

If the cyber operation qualifies as an attack, the operation may only be directed against military objectives, which comprise persons or objects. Objects constituting a military objective are defined as "those objects which by their nature, location purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage."[126]

As to persons, only "(a) members of armed forces; (b) members of organised armed groups; (c) civilians taking a direct part in hostilities; and (d) in an international armed conflict, participants in a levee en masse" may be attacked.[127] There are some exceptions to these rules, members of armed forces may be attacked unless they are hors de combat, including, amongst other, being 'in the power of an adverse party, defenceless because of unconsciousness, or expresses an intention to surrender' or are considered to be medical or religious personnel.[128] Members of organised armed groups are understood to be limited to those fulfilling "a continuous combat function for an organised armed group belonging to a party to the conflict".[129] There is also an alternative view that mere membership of an organised armed group would negate the protection from attack.[130] As to the civilians directly participating in conflict, there is an extensive interpretive guidance on the subject that formulates criteria for assessing direct participation, namely: (1) threshold of harm, (2) direct causation and (3) belligerent nexus.[131] When a person qualifies as one of categories of persons that may be attacked or when an object qualifies as military objective, it may be attacked. In attacking, "constant care must be taken to spare the civilian population, civilians and civilian objects",[132] this is known as "the principle of precautions in attack".[133]

[125] Ibid. p. 112.

[126] Article 52(2) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[127] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 115; See also: Henckaerts et al., Customary International Humanitarian Law. pp. 3, 11, 14, 19, 25. Rule 1, 3, 4, 6, 7.

[128] Ibid. p. 164. Rule 47.

[129] Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. p. 73.

[130] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 116.

[131] Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. pp. 46-64.

[132] Henckaerts et al., Customary International Humanitarian Law. p. 51. Rule 15; Article 57(1) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[133] Henckaerts et al., Customary International Humanitarian Law. p. v.

6.4.3 Precautions

Contained within article 57(2) of AP I are the precautions to be taken with respect to attack, namely: '(1) do everything feasible to verify that the objects to be attacked are neither civilians nor civilian objects; (2) take all feasible precautions in the choice of means and methods of attack; (3) refrain from an attack causing excessive collateral damage vis-à-vis the direct military advantage gained; (4) suspend an attack if it becomes apparent that the objective is not a military one or under special protection; (5) if circumstances permit, give an effective advance warning; and (6) if there is choice between military objectives for a similar advantage, select the one causing the least amount of danger to civilian lives and objects'.[134] The duty to take precautions in attack applies to military cyber operations above the threshold of attack as it applies to traditional attacks.[135]

6.4.4 Proportionality

When the target of an attack is a military objective, precautions are taken, and collateral damage or incidental injury occurs or is expected ('collateral damage') the attack should "comply with the rule of proportionality".[136] The rule of proportionality is based on the prohibition on "launching an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".[137] In other words, if an attacker has taken all feasible precautions, but still the attack could result in 'collateral damage or incidental injury' it should be assessed whether it is disproportionate to the military advantage gained. This should be done on basis of the "information reasonably available to the attacker at the time the attack was planned, approved, or executed."[138]

After specifying that the rule of proportionality is also applicable to military cyber operations, the Tallinn Manual notes that the expected collateral damage can occur "during transit [or] because of the cyber attack itself" and that both types should be considered. The type of damage to be taken into account is loss of civilian life, injury and damage to object, not mere "inconvenience, irritation, stress or fear".[139] The collateral damage can

[134] Article 57 (2)(3) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[135] As done by the Tallinn Manual, see: Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. pp. 164-179.

[136] Paul A. L. Ducheine, Michael N. Schmitt and Frans P. B. Osinga, Targeting: The Challenges of Modern Warfare (The Hague: Asser Press, 2016). p. 140.

[137] Henckaerts et al., Customary International Humanitarian Law. p. 46. Rule 14; See also: Articles 51(5)(b) and 57(2)(b) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[138] Ducheine, Schmitt and Osinga, Targeting: The Challenges of Modern Warfare. p. 141.

[139] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 160.

consist “of both direct and indirect effects” or the first-order and higher-order effects.[140] Only the effects, however, that are expected should be factored in, not the “unexpected or unforeseeable”.[141]

6.4.5 Other rules

Apart from the rules on distinction, precaution and proportionality there are other factors that are relevant to the legal framework governing cyber operations amounting to attack. The first involves the geographical scope of operations, this revolves around the notion that the “territory of third States is inviolable, barring exceptional circumstances that would necessitate conducting attacks on targeting located there.”[142] Thus, “targeting may be conducted against valid military objectives within the territory or any of the belligerent States”.[143] They may not be conducted against neutral States. These States, however, “must equally prohibit the use of its territory by any of the belligerents.”[144] In the event that a neutral State is unable or unwilling, “the opposing belligerent parties may conduct operations, including attacks, necessary to put an end to its opponent’s misuse of neutral territory”.[145] As to the geographical scope of non-international armed conflict there are different views, the most prevalent is “that LOAC applies in cross-border areas into which a NIAC’s hostilities have spilled over and thus would govern any targeting there”.[146]

A second relevant rule is the prohibition on perfidy,[147] which involves “acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with the intent to betray that confidence [...]”.[148] This prohibition contains four elements: “(1) an act inviting particular confidence of the adversary; (2) an intent to betray that confidence; (3) a specific protection provided for in international law; and (4) death or injury of the adversary.”[149] The special protections referred to here involve, for instance, simulation of being hors de combat, simulation of an intent to negotiate under a flag of truce, simulation of protected status by using the red cross, red crescent, United Nations emblems, other protective emblems (e.g. cultural property), simulation of civilian status, wearing uniforms

[140] Ibid. p. 160.

[141] Ibid. p. 161.

[142] Ducheine, Schmitt and Osinga, Targeting: The Challenges of Modern Warfare. p. 111.

[143] Ibid. p. 142.

[144] Ibid. p. 142.

[145] Ibid. p. 142.

[146] The International Committee of the Red Cross, 31st International Conference of the Red Cross and Red Crescent: International Humanitarian Law and the Challenges of Contremporary Armed Conflicts (Geneva: The International Committee of the Red Cross,[2011]). p. 22.

[147] Henckaerts et al., Customary International Humanitarian Law. p. 221. Rule 65.

[148] Article 37(1) Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I)

[149] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 181.

or emblems of neutral States or other States not party to the conflict.[150]

6.4.6 Difficulties

States and non-States should apply the legal framework on the conduct of hostilities to military cyber operations above the threshold of attack; however, there are specific difficulties in applying IHL to cyber operations. Although the Tallinn Manual has addressed many of these concerns, there are still remaining issues. This sub-section will highlight some difficulties in applying distinction (6.4.6.1), direct participation (6.4.6.2), proportionality (6.4.6.3), geographical scope of conflict (6.4.6.4), and the prohibition on perfidy (6.4.6.5). There are many more issues, however, these have been discussed in breadth and depth in other publications.[151]

6.4.6.1 Distinction

Some deem distinguishing military objectives from civilian and protected persons and objects to be difficult in the cyber context. As military cyber operations often make use of cyberspace, they travel through series of military and non-military infrastructures and sometimes across multiple borders. As such, faced with the intertwinement of these systems, one might argue that it is impossible to make distinction when conducting military cyber operations.

This, however, depends on the approach taken to data as object and damage (permissive, functional or restrictive). This thesis has chosen a functional approach to damage and further specified that loss of usability would constitute damage. When loss of usability manifests on systems other than the target (e.g. intermediary systems) in the area of operations this would constitute damage. Damage to the intermediary systems could potentially violate the principle of distinction if the systems are civilian or otherwise protected from attack. The permissibility of that collateral damage depends on the assessment whether the military advantage gained is not disproportionate to the collateral damage. Depending on that assessment, the military cyber operations qualifying as attack affecting civilian systems could be permissible or prohibited.

Simple transmission of data over civilian network infrastructure, not constituting damage, is not a violation of distinction.[152] Transmission of data over civilian network infrastructure resulting in loss of usability may constitute a violation of distinction, however, it could still be permissible. Thus, for those deeming cyber operations to be inherently indiscriminate, it is paramount to realise that the cyber operation requires causation of damage on a non-

[150] Henckaerts et al., Customary International Humanitarian Law. p. 224. Rule 65.

[151] See for example: Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare; Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations

[152] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 251.

military objective to become indiscriminate and even then, it may still be permissible if it is not disproportional.

6.4.6.2 *Direct participation*

An issue related to distinction is the issue of direct participation by civilians in cyber operations and as a consequence loss of protection against direct attack "for such time as they directly participate in hostilities".[153] In order to constitute direct participation, the act should fulfil three cumulative requirements: "(1) A threshold regarding the harm likely to result from the act, (2) a relationship of direct causation between the act and the expected harm, and (3) a belligerent nexus between the act and the hostilities conducted between the parties to an armed conflict".[154] As the Tallinn Manual notes, civilian systems may be used to mount the attack unbeknownst to the owner (unknowing participation) and sometimes civilians might willingly engage in attacks themselves (deliberate participation), for instance by installing software to be used in operations such as stress-testers or DDoS-tools (e.g. low-orbit ion cannon, high-orbit ion cannon or Lizzard Stresser).[155] In order to be able to make an assessment of the qualification of acts as direct participation this sub-section will briefly elaborate on the three cumulative criteria.

Firstly, the threshold of harm, the threshold can be reached by "causing harm of a specifically military nature or by inflicting death, injury, or destruction on persons or objects".[156] The damage does not have to be materialised yet; the "objective likelihood" of harm suffices to reach the threshold.[157] Harm of a military nature is understood to be not only "the killing and wounding of military personnel" and/or damaging of military materiel, it also comprises the restriction or disturbing of "deployments, logistics and communications".[158] Examples of non-lethal adversely affecting acts are: "guarding captured military personnel, [...] clearing of mines [...], interference with military computer networks [...], wiretapping the adversary's high command [and] transmitting targeting information for an attack".[159] If the act does not cause harm of a specifically military nature, it can still rise to the threshold of harm by inflicting death, injury or destruction to "persons or objects protected against direct attack".[160]

[153] Ibid. p. 118.

[154] Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. p. 46

[155] Brian Krebs, "Six Nabbed for using LizardSquad Attack Tool," krebsonsecurity.com/tag/lizard-stresser/; William Turton, "Lizard Squd's Xbox Live, PSN Attacks were a 'Marketing SCheme' for New DDoS Service," dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/ (accessed December 25, 2015).

[156] Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. p. 47.

[157] Ibid. p. 47.

[158] Ibid. p. 48.

[159] Ibid. p. 48.

[160] Ibid. p. 50.

The second cumulative requirement is direct causation, which is understood to comprise of a "causal link between a specific act and the harm likely to result" from that act.[161] The requirement is fulfilled when the "specific act in question, or a concrete and coordinated military operation of which that act constitutes an integral part – in one casual step – cause harm that reaches the required threshold".[162] Examples of acts that do not bring about harm in one causal step are: "economic sanctions"; "scientific research and design"; "production and transport of weapons and equipment"; "recruitment and training of personnel"; and "the assembly and storing of an IED in a workshop".[163] The following act do bring about harm in one causal step: "planting and detonation" of an IED; "identification and marking of targets"; "analysis and transmission of tactical intelligence to attacking forces"; and "instruction and assistance given to troops for the execution of a specific military operation".[164]

The third element that has to be fulfilled together with the threshold of harm and direct causation is the requirement of belligerent nexus. The objective likelihood of harm does not suffice; the act has to be "specifically designed to [cause harm] in support of a party to an armed conflict and to the detriment of another".[165] Belligerent nexus does not relate to "the state of mind of the person concerned", rather it pertains to the "objective purpose of the act".[166] Thus, it is not influenced by factors "such as personal distress or preferences or the mental ability or willingness of persons to assume responsibility for their conduct", however there are exceptional situations in which it can be influenced by such factors.[167] The Interpretative Guidance highlights a situation in which civilians "are totally unaware of the role they are playing in the conduct of hostilities" and hence they are not "performing an action".[168] Therefore, they retain their protected civilian status and cannot be made object of attack.

The two scenarios in the cyber context – deliberate and unknowing participation – in the light of the cumulative requirements are fairly clear. If the military cyber operations to which the civilians contribute in either one of the scenarios reach the threshold of harm, which depends on the approach taken to harm (see 6.3), then the first requirement is fulfilled. The second criterion, direct causation, is also easily fulfilled if the requisite harm is achieved, as the system of a civilian in both scenarios is used to launch an attack. The third requirement is where the scenarios diverge. In the 'deliberate' scenario the person taking part would satisfy the requirement of belligerent nexus when the act is being used

[161] Ibid. p. 51.

[162] Ibid. p. 53.

[163] Ibid.. pp. 53-54.

[164] Ibid. p. 58.

[165] Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. p. 59.

[166] Ibid. pp. 59-60.

[167] Ibid. p. 56.

[168] Ibid. p. 56.

to support a party to the conflict and to the detriment of another. In the 'unknowing' scenario, when the person is totally unaware of their role, the person would not be performing an action and hence he would not be directly participating in hostilities. Although clear in theory, distinguishing intent during conflict in these scenarios would prove nearly impossible.

6.4.6.3 Proportionality

Section 6.4.4 noted that proportionality involves assessing the potential disproportionality of collateral damage (including incidental injury) and the military advantage gained. This assessment should include direct and indirect effects, during transit and execution of an attack, however, only to the extent that the effects are foreseeable and only taking into account the information reasonably known at the time of planning, approval or execution. Collateral damage involves the traditional 'incidental loss of civilian life, injury to civilians and damage to civilian objects'. Besides the traditional elements, depending on the approach taken (see 6.3), collateral damage also includes functional damage in the specific context of military cyber operations (see 6.3.2). As this thesis uses loss of usability as threshold, if a cyber operation qualifying as attack causes loss of usability collateral to the intended target this 'damage' should be taken into account in the proportionality assessment.

Some argue that making a proportionality assessment is difficult or impossible considering the intertwined nature of cyberspace. The first order or the direct effects are relatively easy to take into account as creating these effects is the purpose of the attack. The indirect, second or n-order effects are gradually becoming more difficult to assess. The higher the n-order effect, the more complex it will get, as potential contingencies will increase exponentially. This rapidly increases to the extent that an attacker cannot be reasonably expected to foresee these types of effects. Attackers are, however, under the obligation to take into account only the reasonably foreseeable (see 6.4.4). Thus, direct and indirect effects should be taken into account, however, only to the extent that the effects are reasonably foreseeable for an attacker.

6.4.6.4 Location

Cyberspace has resulted in diminishing value of geographical space and time (see chapter three). One does not have to travel to a location, it has become increasingly easy to provide and receive services remotely. The same goes for participating in conflict: armed forces, members of armed groups and directly participating civilians do not need to travel to the theatre of war in order to create effects. As such, whilst the conflict is geographically limited to the territories of the parties to the conflict, its peripheries might span the world. Various groups not located on the territories of the belligerents may target the parties to the conflict. This results in questions as to when such a foreign actor may be attacked by a party to an armed conflict.

As mentioned in sub-section 6.4.5, should a neutral or uncommitted State be "unable or unwilling" to stop their territory from being used for those activities, then the parties may conduct operations to aim to end the activities. There are, however, certain criteria for doing so, namely: seriousness and that "the exercise of belligerent rights on neutral territory by a party to the conflict must represent an immediate threat to the security of the aggrieved party and there must be no feasible and timely alternative to taking action on neutral territory."[169] Should an act committed against a belligerent or by a belligerent from the territory of neutral party result in a serious disadvantage for the target belligerent actor, the target actor must notify the neutral party and "allow a reasonable time [...[to address the violation". [170] That is, unless the seriousness of the act demands immediate action, then the target actor may "use such immediate force as is necessary to terminate the violation."[171] In other words, although the sphere of the conflict may increase significantly and attract all sorts of non-belligerent States and groups, the original belligerents can react to cyber operations conducted from non-belligerent territories against them in such an event.

6.4.6.5 Perfidy

As mentioned in 6.4.5, perfidy is prohibited under IHL. Within the context of cyberspace and cyber operations this brings about interesting issues. Social engineering, one of the crucial cyber capabilities is entirely aimed at deceiving a target (see Chapter Four). The discipline at its most simple could be defined as "a method of gaining access to systems, data, or buildings through the exploitation of the human psychology".[172] It uses methods involving pretexting, impersonation, baiting, pressure, false authority, false credibility and many others.[173] Besides the social engineering discipline, specific methods used in the context of cyber operations aim to deceive an opponent, for instance cloned websites are often used in phishing schemes or DNS-spoofing.[174]

This begs the question when these deceptive activities transgress the permissible use of ruses and deception in IHL and become perfidious. Three of the four factors of perfidy (see 6.4.5) are easily met by any of the above methods, namely (1) inviting particular confidence by adopting the layout and format of a trustworthy site; (2) intent to betray that confidence,

[169] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 255.

[170] Ibid. p. 255.

[171] Ibid. p. 255.

[172] Reynolds, Social Engineering: The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception. p. 13; See for more defintions: Gaving Watson, Andrew Mason and Richard Ackroyd, Social Engineering Penetration Testing (Boston: Syngress, 2014). pp. 2-3.

[173] Ibid. p. 39.

[174] In the former case an attacker mimics a website that is trusted by the user by adopting its exact format and layout, after that, the attacker sends an email prompting the target to log in to some trusted service (Facebook, banking, Twitter, etc.). When the target logs in at the fake website the credentials are obtained by the attacker. DNS-spoofing or poisoning involves sending a wrong IP-address for a trusted domain. Instead of the legitimate IP-address of Facebook, the DNS resolver returns a 'false' IP-address specified by the attacker. Often this false address leads the user to a website resembling the legitimate website – with the legitimate URL 'facebook.com'. When the user logs in, their credentials are stored on the server of the attacker. Besides these examples, there are many other disciplines and methods specifically aimed at deceiving a target into trusting a service and consequently betray that trust.

for instance through stealing credentials; and (3) misusing the specific protection of civilian status. The fourth factor, intended to or causing death or injury of the adversary, however, is not as easily met. Whereas the aforementioned rules and principles regarding the conduct of hostilities often involved the syntax 'death, injury, damage or destruction', the latter two are not included in the fourth factor of perfidy. The Tallinn Manual explicitly notes: "the perfidy rule does not extend to perfidious acts that result in damage or destruction of property."[175]

Thus when the deceptive activity fails to qualify as perfidious, as it does not cause death or injury and is not otherwise specifically prohibited (e.g. misusing protective indicators of the Red Cross), the activities would not be prohibited. As these cyber capabilities are often used as stepping-stones in an operation and seldom for the actual attack potentially causing death or injury, these social engineering types of activities will hardly ever qualify as perfidious in the strict legal sense.

6.4.7 Sub-conclusion

This section has sought to answer the following sub-question: *What IHL rules and regulations apply to military cyber operations above the threshold of attack?* In order to answer the sub-question this section has first discuss the need for a weapons review (see 6.4.1). Only cyber capabilities capable of reaching the threshold of attack or methods of conducting hostilities should be subjected to such a review. After that this section has discussed the main rules governing the conduct of hostilities: distinction (see 6.4.2), precautions (see 6.4.3), proportionality (see 6.4.4) and other rules (see 6.4.5). This section then highlighted potential difficulties in applying distinction, direct participation, proportionality, the geographic scope of conflict, and perfidy to military cyber operations (6.4.6).

As to the answer to the research question, when the military cyber operation qualifies as an attack the legal framework is identical to any other form of traditional attack. The general legal framework consists of four main requirements, being: the need to review new weapons, distinguish between civilians and military objectives, take all feasible precaution to limit civilian harm and damage, and lastly that collateral damage and incidental injury must not be disproportional/excessive to the military advantage gained. Besides those, there are other specific rules on certain activities, of which the geographical scope and perfidy have been described in this section. Although there are apparent difficulties in applying, amongst other, distinction, proportionality, location and the prohibition on perfidy, military cyber operations above the threshold of attack are enveloped by a clear legal framework.

[175] Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare. p. 182.

6.5 Conclusion

This chapter has focused on answering the sub-question: *What is the IHL legal framework for employing military cyber operations above the threshold of attack during armed conflict?* In order to answer the sub-question this chapter has first addressed the applicability of IHL in general and to military cyber operations in specific (see 6.2). After specifying when IHL applies, it concluded that IHL is also applicable to military cyber operations during armed conflict. The main issue no longer is if IHL applies, instead it is how to apply IHL to military cyber operations. Consequently, this chapter has turned to the discussion on how to apply IHL to military cyber operations (see 6.3). The debate regarding IHL's application is currently in flux, there are various perspectives and approaches, some traditional and others more contemporary. As there are no clear-cut answers as to how to apply IHL to military cyber operations, anyone seeking to determine the legal framework applicable to military cyber operations during conflict is forced to select an approach or set of approaches. This chapter has qualified data as non-object, selected the functional approach, and loss of usability as threshold. After having described how IHL could be applied to military cyber operations, this chapter has discussed the contents of the legal framework applicable to military cyber operations (see 6.4). The main rules on the conduct of hostilities and particular challenges in applying these rules on military cyber operations were discussed.

The answer to the sub-question is answered by section 6.4, however, it cannot be seen in isolation from the selections made in section 6.3, nor from IHL's applicability in general in section 6.2. The selections determine the applicability of the legal framework to particular military cyber operations: whether it is a well-established framework on the conduct of hostilities above the threshold of attack or a much vaguer legal framework. As noted in 6.3.2.3, currently the main question is not what legal framework is applicable to military cyber operation above the threshold of attack – as this is evident. Instead, the main questions are when military cyber operations qualify as an attack and what legal framework applies to military cyber operations below the threshold of attack. The merits of this chapter to this discussion do not lie in describing a well-established legal framework; instead, it lies in a description of the general criteria for a military cyber operation to qualify as attack.

6.5.1 Relevance

The insights from this chapter illustrate that military cyber operations are governed by a legal framework during armed conflict. The utility of military cyber operations has a somewhat dyadic relation with this 'legal' perspective. For actors upholding international legal standards military cyber operations are enabled, in part, by the legal framework which allows for actors to engage in hostilities during armed conflict. At the same time, the potential utility of military cyber operations is limited by the IHL framework. Military cyber operations are not different from other military operations in that regard, all military operations are limited by the IHL framework. As shown in this chapter, however, there is considerable room for interpretation. The chosen interpretation would determine if a military cyber operation qualifies as conduct of hostilities and consequently whether the full IHL framework or a limited set of rules is applicable.

In a more general sense, the 'legal' perspective advanced in this chapter highlights that military cyber operations are governed by laws. This chapter has dealt exclusively with IHL during armed conflict, but as others have indicated, laws also govern military cyber operations conducted outside armed conflict.[176] Thus, laws curtail the potential uses of military cyber operations.

In the context of this research the 'legal' perspective limits how military cyber operations could be used. The previous perspectives highlighted the enabling circumstances for military cyber operations: the 'power' perspective put forward many goals actors may want to achieve, the 'society' perspective has shown that our informationised condition enables the use of 'cyber', the 'technology' perspective illustrates that there are many cyber capabilities which can be used to influence, and the 'military' perspective has shown that the military has integrated cyber capabilities in military cyber operations. The 'legal' perspective in this chapter puts a limit on how military cyber operations may be used in the light of all these enabling circumstances, and thus, the 'legal' view impacts the potential utility of military cyber operations (see Figure 32).

[176] See for example: Katharina Ziolkowski, Peacetime Regime for State Activities in Cyberspace : International Law, International Relations and Diplomacy / (Tallinn, Estonia: Tallinn, Estonia : NATO CCD COE Publications, 2013).; Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge: Cambridge University Press, 2017).

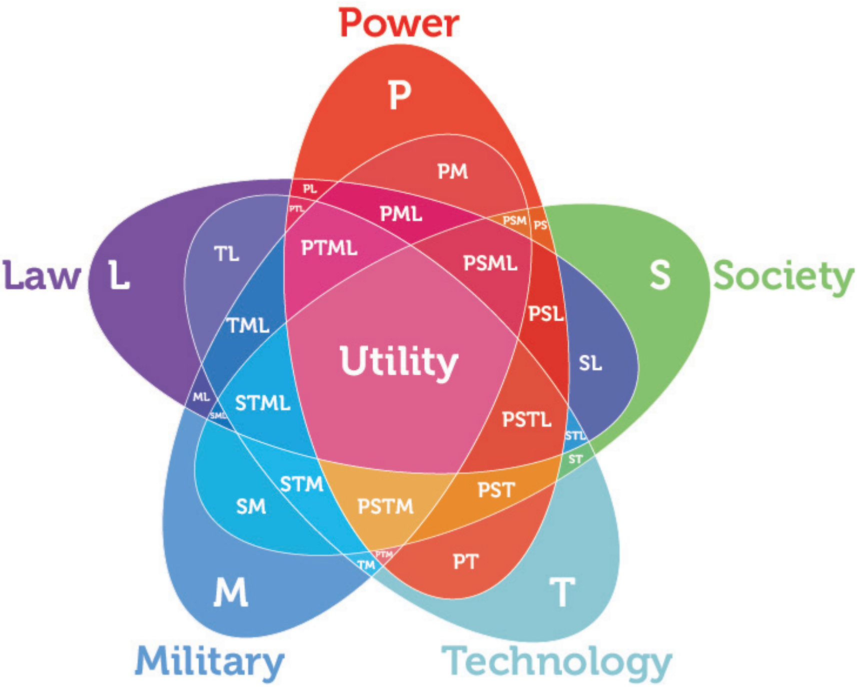

Figure 32 The 'power', 'society', 'technology, 'military', and 'legal' perspective adjoined

7

Synthesis

7 Synthesis

7.1 Introduction

7.1.1 Goal of this chapter

The goal of this research is to contribute to understanding of the utility of military cyber capabilities and has set out to do so via the following research question: *What is the utility of military cyber operations during armed conflict?* The previous chapters have covered the subjects of power, society, cyber, fighting and law. This chapter will adjoin these perspectives and provide an answer to the research question.

7.1.2 Structure

In order to structure the research this thesis has used the interdisciplinary research process (IRP) as research 'style'. Chapter one has covered steps one to three (state research question; justify using an interdisciplinary approach; identify relevant disciplines). Chapters two to six have covered steps four to six (conduct literature research; develop adequacy in each relevant discipline; analyse the problem and evaluate each insight or theory). This chapter will focus on integration and reflection, in doing so it will cover steps seven to ten (identify conflict; create common ground; construct a more comprehensive understanding; reflect on, test, and communicate the findings). Section 7.2 will provide a brief overview of the findings of this research, section 7.3 will integrate the insights from the five perspectives and answer the research question, section 7.4 will reflect on the value of the insights generated, section 7.5 will conclude this chapter.

7.2 Overview

Chapter two has argued that the notion of power needs to be addressed in order to understand how the military instrument can be employed, to what end, and how cyber capabilities can contribute to achieving this end. After conducting a theoretical literature review into the 20th century power discussion chapter two has created a framework with potential elements that impact power such as context, power concept involved, and the dimensions scope, domain and means.

Chapter three has discussed informationised society and the rise of 'cyber' therein and the effect on the notions of power. Chapter three concluded that although remaining conceptually and theoretically valid, all elements included in the power framework from chapter two are impacted by informationised society and rise of 'cyber'.

Chapter four has described the arena where cyber activities are conducted (i.e. cyberspace) and listed representative tools with which actors seek to influence each other in cyberspace (i.e. cyber capabilities). There are different conceptualisations of cyberspace, the broadest is the State conceptualisation using a layered 'cyberspace' model to highlight different aspects of networking: geographic, physical, logic and social. There are series of cyber capabilities aimed at influencing the different components of cyberspace, that is, the cyber persona (e.g. data mining, websites, social media, mail, instant messaging, text messages, forums and blog), logical network (e.g. firmware malware, authentication flaw exploitation, social engineering, vulnerability exploitation, wiretapping, denial of service, distributed denial of service, SQL injection, cross-site scripting, cross-site request forgery) and physical network components (e.g. hardware Trojans and emanation exploitations).

Chapter five has discussed how armed forces are conceptually and doctrinally organised and what the place of cyber capabilities is within that organisation. After having discussed fighting power, military operations and military cyber operations, it concluded that military cyber operations fit within the conceptual construct of military operations. Military cyber operations target entities in the information dimension of the operational environment to ultimately create an effect in the cognitive dimension.

Chapter six concluded that the debate on the IHL legal framework applicable to military cyber operations is in flux. Therefore, those seeking to derive a legal framework are forced to select their preferred approach or set of approaches. For instance, in qualifying data as object, the approach to damage and, in the case of the functional approach, the level of functional damage required to qualify as 'damaging'. Chapter six has created a framework for selecting the approach taken to data, damage, and loss of usability.

7.3 Integration

This section will integrate the 'power', 'society', 'technology', 'military' and 'law' perspectives to create a more comprehensive understanding of the utility of military cyber operations.

Many armed forces have incorporated cyber capabilities in a relatively new form of military operations called 'military cyber operations'.[1] These operations make use of the military's fifth warfighting domain: cyberspace. Cyberspace consists of cyber personas (e.g. social-media accounts), logical network components (e.g. software and protocols), and the physical network components (e.g. hardware). The military generates fighting power to be used in cyberspace vis-à-vis cyber personas, logical network components, and physical network components by organising the required conceptual (e.g. doctrine), physical (e.g.

[1] See for example: James R. Clapper, Marcel Lettre and Michael S. Rogers, Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States (Washington, D.C.: U.S. Senate Armed Services Committee, 2017). p. 5.

personnel and materiel), and moral (e.g. training) aspects. Via military cyber operations the military seeks to create an effect that results in the (partial) achievement of goals. Military cyber operations could do so stand-alone or together with other military operations in other domains such as land, sea, air, or space.

The utility of military cyber operations encompasses their fitness for achieving an end or goal, thus a sense of purpose is required to analyse their utility. This research has advanced seven examples of potential goals actors seek to achieve using their power instruments, the so-called strategic functions: anticipation, prevention, deterrence, protection, intervention, stabilisation, and normalisation. The military is merely one of the power instruments available to an actor to achieve these goals. Other power instruments are the political, informational, economical, and civil capacities. These instruments in contemporary society all have 'cyber' aspects to them, the military is not exclusively integrating cyber capabilities. Actors use their instruments to promote or protect their interests either directly against other actors or indirectly via institutions, by creating a better position for themselves in power structures or in more discursive ways. The strategic functions give direction to the utility syntax in the research question as the question consequently revolves around the contribution of military cyber operations to achieving the strategic functions.

A goal's feasibility impacts whether an activity has utility in achieving that goal. If a goal simply is unachievable irrespective of the effort spent or capabilities used, the utility of a specific capability in achieving this goal is likely marginal. The goals used as example in this research, the seven strategic functions, are subject to academic debate regarding their feasibility, for example: the human capacity to anticipate is deemed flawed, it is unclear how to best prevent crises, the effectivity of intervention is highly contested, and the current approach to stabilisation and normalisation is hardly achievable. That does not mean, however, that new technologies such as cyber capabilities cannot contribute to achieving these goals at all. Informatisation has resulted in increasingly sophisticated systems to anticipate situations, given new tools to prevent crises, resulted in new values to be protected, resulted in the re-evaluation of deterrence, created new ways for intervening, and spawned new technologies to help stabilising and normalising a situation. The issue still remains, however, that the goals are overly ambitious or complex, a problem which new technology and military cyber operations cannot solve by themselves. Thus, military cyber operations might contribute to achieving goals, however, they are not a panacea for these issues.

Whether military cyber operations successfully contribute to achieving a goal depends on the context. This research has taken a broad approach to context by considering the societal context of military cyber operations. Our current societal condition was characterised as 'informationised'. Informatisation has changed the way we generate wealth, work, commute and interact with the world around us. Society's informationised condition is the basis for the rise of 'cyber', cyber capabilities, and the receptiveness (or vulnerability) to these capabilities. By highlighting the broader context this research has highlighted the reason why cyber capabilities in general and military cyber operations in specific are potentially powerful means in contemporary society. Informationised society is the foundation for the utility of military cyber operations.

Considering the potential of cyber capabilities involved in military cyber operations and the receptiveness of contemporary society to these capabilities, it is beyond doubt that military cyber operations have potential utility. Whether they have actual utility in contributing to strategic functions depends on the specific situation. This assessment of actual utility is highly contextual and whether military cyber operations' potential is actualised is complicated by various factors.

One of the factors is the role of the military instrument in the strategy for achieving a particular goal. The military instrument is only one of the power instruments available to a State. States use different integrative strategies for employing their instruments such as smart power, the whole of government approach, comprehensive approach, or the JIMP-approach. Whether or not the military instrument has a role in achieving a certain goal depends on the chosen strategy and decision-making. Should the product of decision-making result in the military instrument not having a role, then the potential utility of military cyber operations is not actualised.

A second factor is the situational context of the military cyber operation. The situational context of military operations is complex. It is impacted by many situational variables, for instance politics (informal and formal political power distribution), military (military capabilities of enemy, friendly, and neutral actors), economy (individual and group behaviours related to producing distributing, and consuming resources), society (beliefs, values, customs, and behaviours of society), information (nature, scope, and characteristics of persons and systems that collect, disseminate, or act on information), infrastructure (facilities, services, and installations), the physical environment (e.g. geography, climate, and weather) and time. [2] These are but a few of the variables in the situational context that may thwart military cyber operations in realising their potential.

A third complicating factor is the proficiency of the military in preparing, planning, and conducting cyber operations. The military generates fighting power to conduct military cyber operations. Although this may sound relatively simple, generating the proper concepts for using military cyber operations (conceptual component), hiring qualified personnel in a competitive market (physical component), providing them with the right mindset (moral component) is a complex endeavour which does not necessarily yield the right result at first try. Also, as the discussion regarding the place of military cyber operations among other military operations has shown (e.g. their relations to EW and information operations), the military has to become familiarised with cyber capabilities

[2] United States Army, Army Doctrine Publication 5-0: The Operations Process (Washington, D.C.: Department of the Army, 2012). p. 5.

and its relations with other operations. Optimising fighting power for military cyber operations and organisational familiarisation takes time and as such may impact the military's ability to effectively utilise military cyber operations in a specific situation.

A fourth factor is the legal framework governing the use of military cyber operations. Military cyber operations can be used inside and outside armed conflict, in both cases their use is governed by a legal framework. This research has discussed the framework applicable to military cyber operations during conflict. The legal framework limits the possible uses of military cyber operations, resulting in a limit on their potential uses (e.g. indiscriminate or perfidious use). In that regard, however, military cyber operations are not different from traditional military operations.

Should these complicating factors be mitigated then military cyber operations result in effects in or through cyberspace (e.g. mislead, confuse, degrade, promote, inform, destroy and degrade) and by doing so contribute to achieving goals at various levels within the military instrument, which ultimately results in a military contribution to achieving an actor's strategic goals.

Considering the different types of military cyber operations and cyber capabilities involved therein, certain operations are potentially suited for specific goals: ISR cyber operations could serve to anticipate emerging threats by gathering intelligence (anticipation);[3] offensive cyber operations could be used in support of an information campaign or stand-alone to create or defuse crises to prevent a harmful event from occurring (prevention);[4]

[3] See for example: "The Flame: Questions and Answers," , accessed October 30, 2013, securelist.com/en/blog/208193522/.; "Dropping Elephant: Inelegant Espionage," Kaspersky, accessed June 27, 2018, kaspersky.com/blog/dropping-elephant/15149/; "Potent Skygofree Malware Packs 'Nevere-before-seen' Features," Threatpost, accessed June 27, 2018, threatpost.com/potent-skygofree-malware-packs-never-before-seen-features/129479/; "Introducing WhiteBear," Kaspersky, accessed June 27, 2018, securelist.com/introducing-whitebear/81638/; "ZooPark: New Android-Based Malware Campaign Spreading through Compromised Legitimate Website," Kaspersky, kaspersky.com/about/press-releases/2018_zoopark-new-android-based-malware; "Gauss Malware: Nation-State Cyber-Espionage Banking Trojan Related to Flame, Stuxnet," Computerworld, accessed June 27, 2018; "Duqu 2.0: The most Sophisticated Malware Ever Seen," Infosec Institute, accessed June 27, 2018, resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/; "Meet 'Flame', the Massive Spy Malware Infiltrating Iranian Computers," Wired, accessed June 27, 2018, wired.com/2012/05/flame/.

[4] See for instance: "BlackEnergy Trojan Strikes again: Attack Ukrainian Electric Power Industry," ESET, accessed February 10, 2017, welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/; "KillDisk and BlackEnergy are Not just Energy Sectory Threats," Trend Micro, accessed February 10, 2017, blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/; "Киберугроза Blackenergy2/3. История Атак На Критическую Ит Инфраструктуру Украины," Cys-Centrum, accessed February 10, cys-centrum.com/ru/news/black_energy_2_3; "Newly Discovered BlackEnergy Spear-Phishing Campaign Targets Ukrainian Entitities," Kaspersky, accessed February 10, 2017, usa.kaspersky.com/about-us/press-center/press-releases/2016/newly-discovered-blackenergy-spear-phishing-campaign-targets-uk; "BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents," Kaspersky, accessed February 10, 2017, securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/; F-Secure, BlackEnergy & Quedagh: The Convergence of Crimeware and APT Attacks (Helsinki: F-Secure,[2014]); "U.S. Confirms BlackEnergy Malware used in Ukrainian Power Plan Hack," , accessed February 25, ibtimes.com/us-confirms-blackenergy-malware-used-ukrainian-power-plant-hack-2263008; "How Russia Pulled Off the Biggest Election Hack in U.S. History," Esquire, accessed February 8, 2017, esquire.com/news-politics/a49791/russian-dnc-emails-hacked/; Nicolas Falliere, Liam O. Murchu and Eric Chien, "W32. Stuxnet Dossier," Symantec Security Response (2011); "Stuxnet Central," accessed September 15, 2014, tofinosecurity.com/stuxnet-central.

the military could communicate its capability to conduct offensive cyber operations and strike back to dissuade adversaries from attacking (deterrence);[5] enabling and defensive cyber operations can be used to protect the networks of armed forces but could also be used to protect non-military networks of other actors (protection);[6] offensive cyber operations can be used to intervene in order to enforce a change in the behaviour of an actor (intervention);[7] or military cyber operations can contribute to stabilising or normalising a situation by providing insight in the situation or quelling hostile elements (stabilisation and normalisation).[8]

In sum, the answer to the research question (‘*what is the utility of military cyber operations during armed conflict?*’) is that military cyber operations have *potential* utility during conflict. As described above, whether or not they have *actual* utility depends on the context of the use of military operations. Although to some this answer may be unsatisfactory, the insights generated by discussing the five perspectives contributes to understanding of the utility of military cyber operations. The illustrative goals, societal context, and situational context of military operations described above are complicating factors. These factors, however, can be rearticulated to ‘axioms’ for military cyber operations to actualise their potential utility:

[5] See for example: “Australia’s Offensive Cyber Capability,” Australian Strategic Policy Institute, accessed June 27, 2018, aspi.org.au/report/australias-offensive-cyber-capability.; “UK Becomes First State to Admit to Offensive Cyber Attack Capability,” Financial Times, accessed June 27, 2018, ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de.; “German Cyber Agency Calls for Authority to Hack Back: Spiegel,” Reuters, accessed June 27, 2018, reuters.com/article/us-germany-cyber/german-cyber-agency-calls-for-authority-to-hack-back-spiegel-idUSKBN1DM1XU; “DHS Secretary Promises U.S. Will Strike Back Against Cyber Adversaries,” Nextgov, accessed June 27, 2018, nextgov.com/cybersecurity/2018/04/dhs-secretary-promises-us-will-strike-back-against-cyber-adversaries/147521/; “Britain’s Cyber Security Bolstered by World-Class Strategy,” accessed June 27, 2018, gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy.

[6] See: “The Borderless Threat: Army Cyber Command Helping Defend Nation’s Network,” U.S. Army, accessed June 27, 2018, army.mil/article/194348/the_borderless_threat_army_cyber_command_helping_defend_nations_network; “Cyber-Command may Help Protect Civilian Networks,” Washington Post, accessed June 27, 2018, washingtonpost.com/wp-dyn/content/article/2009/05/05/AR2009050504342.html.

[7] See footnote 1123.

[8] See for example: Mark Nelson Quihuis and Karen Guttieri, “Peace Technology: Scope, Scale, and Cautions,” Building Peace, no. 5 (2015), 14-16.; Orna Young and Enda Young, Technology for Peacebuilding in Divided Societies: ICTs and Peacebuilding in Northern Ireland (Belfast: Transformative Connections,[2015]).; Daniel Stauffacher et al., Communication Technology for Peace: The Role of ICT in Preventing, Responding to and Recovering from Conflict (New York: The United Nations Information and Communication Technologies Task Force, 2005).; Daniel Stauffacher et al., ed., Peacebuilding in the Information Age: Sifting Hype from Reaility (Geneva: ICT4Peace Foundation, 2011).; Sanjana Hattotuwa, “Big Data and Peacebuilding,” Stability : International Journal of Security and Development 2, no. 3 (2013).; Anne Kahl and Puig Larrauri, “Technology for Peacebuilding,” Stability: International Journal of Security & Development 2, no. 3 (2013).; Francesco Mancini, ed., New Technology and the Prevention of Violence and Conflict (New York: International Peace Institute, 2013).; Patrick T. Brandt, John R. Freeman and Philip A. Schrodt, “Real Time, Time Series Forecasting of Inter- and Intra- State Political Conflict,” Conflict Management and Peace Science 28, no. 1 (2011), 41-64.; Sanam Naraghi Anderlini and Judy El-Bushra, “Post-Conflict Reconstruction,” Inclusive Security, Sustainable Peace: A Toolkit for Advocacy and Action (2004), 51-68.

Society has to be able to create, utilise, or sustain cyber capabilities in order to be able to actualise the potential of military cyber operations.

The military must integrate these cyber capabilities to generate fighting power in cyberspace via military cyber operations.

The military's contribution to strategic goals must be clear as utility stems from purpose.

The strategic goals must not be unachievable as the ability of an activity to contribute is impacted by potential effectiviness.

The military must utilise cyber operations together with other operations or stand-alone to contribute to achieving strategic, operational, and tactical goals.

The purpose of military cyber operations at the operational or tactical level must be clear for them to have utility in contributing to operational or tactical goals.

Military cyber operations must effectively mitigate the complicating factors in the situational context.

Only when the strategic purpose of the military and the contribution of military cyber operations to the goals of the military instrument are clear and the complicating factors are mitigated then military cyber operations can actualise their utility.

Following these axioms could result in more effective use of military cyber operations: Decisionmakers could create or improve the circumstances for a society's ability to create, utilise, or sustain cyber capabilities through technical education or stimulating research and development in the private or public sector (see axiom I); decisionmakers could prompt the military to effectively integrate these cyber capabilities and other novel capabilities by giving them the means and mandate for doing so (see axiom II); decisionmakers could create an integrative strategy wherein the contribution of the various power instruments is made clear (see axiom III); decisionmakers could formulate realistic goals to which power instruments contribute (see axiom IV); the military could create conceptual clarity regarding the place of military cyber operations and familiarise the military organisation with cyber operations by using them in military exercises and deployments (see axiom V); military commanders could specify the operational or tactical goals military cyber operations have to contribute to (see axiom VI); or, in general, assist the effective conduct of military cyber operations by reducing complicating factors to a minimum, for instance by deciding on the approach taken to the legal framework (see axiom VII).

As this research has illustrated, military cyber operations have *potential* utility. This research has not unequivocally proven that military cyber operations have *actual* utility. The inability to conclusively prove that military cyber operations have actual utility, partly due to the classified nature of these operations, should not result in short-sightedly dismissing the 'cyber option' in warfighting. Many actors in the world today utilise cyber capabilities to create effects in furtherance of their goals, the only uncertainty is the extent to which cyber capabilities contribute to those goals. Our society is still undergoing rapid informatisation and increases to rely on information and communication technologies, hence cyber capabilities will increasingly be able to influence humans and machines. The field of cybersecurity increasingly receives scholarly attention, and by doing so new techniques, tools, and procedures arise to attack and mitigate the consequences of these attacks. Armed forces around the world are seeking to best integrate military cyber capabilities to gain an edge on contemporary and future battlefields. The legal discourse on the use of cyber capabilities does not longer revolve around assessing the applicability of established legal frameworks, instead it now focuses on operationalising these frameworks. As such, by taking this political, societal, technical, military and legal context of military cyber operations into consideration, it is evident that military cyber operations will actualise their potential utility. As illustrated in the axioms, this is less a matter of technical capability than the willingness to utilise these capabilities and intellectual ingenuity to integrate these capabilities.

7.4 Reflection

This section will reflect on the contribution of this thesis (7.4.1), the research method used (7.4.2), and author bias and limitations (7.4.3).

7.4.1 Contribution

The purpose of interdisciplinarity is creating a more comprehensive understanding of a complex issue that defies explanation by a single discipline; in this thesis the complex issue is the utility of military cyber operations during armed conflict. The quality of interdisciplinary work is based on creation of comprehensive understanding, that is, "new knowledge that is useful, disciplined, integrative, and purposeful."[9] There are a variety of 'tests' for assessing the quality or contribution of the understanding created through interdisciplinarity;[10] this sub-section will use parts of 'The Newell Test'.[11] The Newell Test comprises, amongst other, the following questions: [12] 'Does is it answer the research question?' and 'is it useful to practitioners, the public, or policy makers who are concerned with that particular issue?' This sub-section will argue that these two requirements of quality are fulfilled.

[9] Repko and Szostak, Interdisciplinary Research: Process and Theory. p. 358.

[10] See: Ibid. pp. 358-365.

[11] Göktuğ Morçöl, ed., *Handbook of Decision Making* (New York: CRC Press, 2007). p. 262.

[12] Ibid. p. 262.

As to the first question, this research has answered the research question with defining utility of military cyber operations during armed conflict as contextual and dependent of various aspects included in five different perspectives (power, society, technology, military and law). In other words, the answer to the research question is contextual, which is only logical considering the complex nature of the issue addressed. There is no clear-cut answer as to the utility of military cyber operations. Anyone claiming to hold such a definitive context-independent answer will most likely offer a mono-disciplinary perspective that fails to consider the complex nature of utility of military cyber operations. Therefore, the answer provided by this thesis in the form of five interrelated perspectives, factors complicating the context of military cyber operations, and axioms for their utility provides an answer to the research question within the given limitations of this research (see 7.4.3).

As to the second question, the usefulness of this research, the following paragraphs will argue that the findings contribute to more effective action for military and non-military decision- and policymakers and create more understanding in a broader audience. Should decision-makers heed the axioms, then this would allow for more effective utilisation of military cyber operations – and of any other military operation. In a more general sense this research has contributed to the understanding of military cyber operations in the *zeitgeist* of 2013 to 2018 for a general public and military public. This research may foster understanding of the broad impact of informatisation on society, spawning new cyber capabilities and creating increased vulnerability to these capabilities. Also, this research may create sensitivity regarding the different terminology used in discussions regarding 'cyber', for instance that 'cyber attack' has seven different meanings that are all equally valid, or that 'cyberspace' is accepted in governmental parlance but that in 'information security' the world of networking is perceived differently and different jargon is used. To the military public, the contribution of this research lies in an overview of potential cyber capabilities to be used in military cyber operations, placing them within the operational environment, conceptually disentangling them from other military operations, and affirming that integration of military cyber operations requires physical, moral and conceptual elements. This may contribute to the military's familiarisation with military cyber operations. Apart from these insights, as this research has taken a broad approach to context, this may create awareness of the context wherein the military instrument is used and what the impact of that context is on the utility of military operations in general and military cyber operations in specific.

7.4.2 Research method

This thesis has used the ten-step IRP as research 'style'. As argued in chapter one, the complex issue of the utility of military cyber operations necessitates an interdisciplinary approach as it defies explanation by a single discipline. This sub-section will reflect on the IRP as method adopted for the purpose of this thesis.

The purpose of selecting the IRP was creating more comprehensive understanding of the utility of military cyber operations during conflict. This thesis has followed the steps of the IRP, steps one to three were conducted chapter one; steps four, five and six were executed in chapter two to five; steps seven to ten will be completed in this chapter.

In the view of the author the IRP has resulted in the desired outcome of increased understanding of the complex issue of the utility of military cyber operations during armed conflict (see 7.3). This understanding has the potential to be helpful to decisionmakers and a wider public (see 7.4.1). Therefore, as the IRP has delivered the intended result it is considered to indeed be the appropriate method for answering the research question.

7.4.3 Author bias and limitations

Although aiming to create adequacy in the relevant insights pertaining to the problem, “one can hardly claim to have practitioner-level understanding of every insight produced and every theory or method used by the authors who have written about the problem.”[13] Logically this notion affects this thesis and its author. The timeframe available for this thesis was approximately four years (September 2013 – October 2017), hence the author’s ability to develop adequacy was limited by time. The author has received multidisciplinary pre-graduate education (bachelor War Studies, Faculty of Military Sciences) and monodisciplinary graduate education in the law discipline (master Public International Law, Utrecht University), developing adequacy in disciplines/perspectives outside this scope required considerably more attention.

The international relations perspective on power in chapter two was relatively new to the author, as was the sociological account of informationised society in chapter three. Also, the author lacks formal academic education in computer security and/or computer science, disciplines which provide some of the insights from chapter four. As such these chapters are most likely to be subjected to the author’s limitations in disciplinary education, disciplinary-specific research skills, sensitivity to disciplinary nuance, and constraints in time available to develop adequacy.

The chapters expressing military and legal perspectives are closer to the author’s educational background (War Studies and Public International Law) and professional background (former Army officer). As with all components of this thesis, however, the amount of time available for these chapters was constrained. Lastly the IRP was new to the author, hence, some time was devoted to become accustomed to this method.

The IRP has forced the author to adopt a broad interdisciplinary perspective to the utility military cyber operations and to avoid disciplinary or author bias (e.g. military or legal). This has resulted in a more nuanced and more comprehensive understanding of the utility

[13] Repko and Szostak, Interdisciplinary Research: Process and Theory. p. 355.

of military cyber operations during armed conflict. Thus overall, despite the constraints in time and other limitations, the author considers that this thesis has resulted in a novel and more comprehensive interdisciplinary understanding of the utility of military cyber operations during conflict.

7.5 Conclusion

This chapter has aimed to adjoin the insights from the previous chapters on power, society, cyber, fighting and law by conducting steps seven to ten of the IRP. Section 7.2 has provided an overview of the results of the literature reviews conducted in the five chapters of this thesis. The insights from the various chapters were integrated in section 7.3 where the five perspectives (power, society, technology, military, and legal) were adjoined to answer the research question. Military cyber operations were found to have *potential* utility, whether they have *actual* utility depends on the context. Complicating factors impacting military cyber operations were listed, including axioms for mitigating the influence of these factors on the utility of military cyber operations. After having integrated the insights produced in this research and answering the research question, section 7.4 has assessed the value of the results of this research by reflecting on its contribution to decisionmakers and the public, research method used, and author bias and limitations. By concluding steps seven to ten of the IRP, this chapter has finished the process and thereby this research.

Appendix A

Appendix A

This appendix is an addition to sub-section 4.3.3, it lists and describes the following types of servers from a software perspective: application, cache, catalogue, communications, database, file, game, mail, message, name, proxy and web servers.

Application server

First, the application server, this is a server dedicated to running applications after being provided input via a graphical user interface (GUI) or another system's process.[14] As such an application server is best defined as provider of "an environment where applications can run, no matter what the applications are or what they do".[15] Having an application server is useful because it provides a single point for maintenance (patches, updates, etc.) and distributes the load from the front-end (e.g. the GUI), via the application server, to the backend (databases). Application servers host a "variety of language systems used to query databases", these queries on databases "retrieve up-to-date data" and present it to "users via their browsers or client applications".[16] Nowadays, application servers are employed in a variety of contexts, not only database querying. A typical, although very simplified, use case would be a website utilising PHP Hypertext Processor (PHP) – an often-used scripting language on websites – to provide a user with a service, for instance finding the nearest electronics shop. In order to get this information to the user the website developer writes a PHP script taking the location of the user as input, then the PHP script queries a database of all electronics shops to match the user's location to the shop closest to that location and lastly provide the nearest shop as output. A web server (discussed later) would normally be able to serve the PHP script functionality to reasonable amounts of users, without needing an application server. However, if the number of visitors increases, the script is run more often and hence the load on the website increases, potentially resulting in a server overload. The web developer may then decide to place the PHP script or parts of it on an application server. When a user accesses the front-end of the web server he is presented with a similar GUI, but instead of the web server itself processing the script, an application programming interface (API) delegates the processing to the application server and returns the output to the web server. By delegating tasks over multiple servers, the website can serve more visitors. Popular application server software includes Apache Tomcat (Java), Zend server (PHP), Microsoft Internet Information Services (IIS) using the .NET framework, Oracle's WebLogic Application Server and IBM's Websphere (both enabling the Java Platform Enterprise Edition framework).[17]

[14] Margaret Rouse, "Application Server Definition," SearchSQLServer, searchsqlserver.techtarget.com/definition/application-server (accessed July 9, 2015).

[15] Joseph Ottinger, "What is an App Server?" TheServerSide, theserverside.com/news/1363671/What-is-an-App-Server (accessed July 20, 2015).

[16] PCMag, "Definition of: Application Server," pcmag.com/encyclopedia/term/37926/application-server (accessed July 10, 2015).

[17] Apache, "Apache Tomcat," tomcat.apache.org (accessed July 10, 2015); Oracle, "Zend Server," oracle.com/technetwork/topics/php/zend-server-096314.html (accessed July 10, 2015); Reagan Templin, "Introduction to IIS Architectures," Microsoft, iis.net/learn/get-started/introduction-to-iis/introduction-to-iis-architecture (accessed July 10, 2015); Oracle, "Oracle WebLogic Server," oracle.com/technetwork/middleware/weblogic/overview/

Cache server

Just like application servers, cache servers are trying to make the user's experience on the Internet better, faster and cheaper. Caching is the process of storing "frequently used data, and web pages […] on the local hard disk for later retrieval".[18] Caching occurs on multiple 'levels': in the user's browser, via a caching proxy server (e.g. within a companies local area network or within an ISP's network), in front of a web server via a reverse proxy caching server or by the web server itself.[19] When a website is accessed and opened via a browser on a user's machine, it makes a local copy in a special folder on the user's local disk. When a user at a later time reopens the website, the browser checks whether the online website is newer than the local, offline version. If the local, offline version is up to date, the browser prefers to use the local version which it can open faster and does not require data being sent to the Internet (which used to cost users money).[20]

The other three types of caching are server based; the server is the same in all cases only their position in the network differs. A caching server does exactly the same as the client's browser, when a client accesses a resource it makes a copy of that resource and saves it on the server. In an office environment a caching server would store the websites frequented by the employees. For instance, Alice visits a website for the first time using Internet, that website is then copied to the caching server within the office LAN. When Bob wants to visit the same website, the caching server provides him with the local copy on the cache server. This reduces the amount of Internet traffic going from the office LAN to the wide area network (WAN), makes the user experience faster (Internet traffic is slower than LAN traffic) and saves money. Such a caching service is achieved by tunnelling the outgoing data traffic of employees through a proxy cache server, the server checks if outgoing requests are already cached and caches websites not in its cache.

Apart from companies' large networks, caching servers are also used by Internet service providers (ISP's), when a user accesses a website, that website is cached within the ISP's network. When another user wants to access the same website, he is referred to the cached version on the cache server. The reason for doing this is purely financial; it reduces the costs for the ISP since they often have to pay transit fees to other ISP's for transporting data. By caching websites, the ISP prevents paying twice for the transit of the same resource. The proxy cache server is placed within the LAN of a company or ISP; the reverse proxy cache server is placed close to the webserver, i.e. the server providing a web service. It takes the load of a web server by caching most used resources, for example if a website has a file on it which is requested by many users, the reverse proxy cache makes a copy and the users

index-085209.html (accessed July 10, 2015); IBM, "WebSphere Application Server," ibm.com/software/products/en/appserv-was (accessed July 10, 2015).w

[18] Abjjijit Jana, "Exploring Caching in ASP.NET," Code Project, codeproject.com/Articles/29899/Exploring-Caching-in-ASP-NET (accessed July 10, 2015); Apple, "About Caching Service," help.apple.com/serverapp/mac/4.0/?lang=en#/apd74DDE89F-08D2-4E0A-A5CD-155E345EFB83 (accessed July 10, 2015).

[19] Ibid; Jana, "Exploring Caching in ASP.NET,"

[20] Guy Provost, "How Caching Works," HowStuffWorks, computer.howstuffworks.com/cache4.htm (accessed July 13, 2015).

are referred to that copy. This takes the load from a web server of servicing that file or any file taking up many resources. A webserver itself can also cache certain resources, for instance database information retrieved from another database or web server, be doing so it “improves the performance of sites by decreasing the round trip of data” from another server.[21] Examples of software enabling cache services on servers include Apache HTTP Server, Nginx, Polipo and Squid.[22] According

Index/catalogue servers
As third, catalogue or index servers help users to find information within a local area network or on the Internet.[23] A catalogue server indexes files and other resources into “an inverted index that maps each query word to a matching lists of documents (the hit list).”[24] Users can then query the catalogue server which presents the user with most relevant hits, which is determined “by intersecting the hit lists of the individual query words” and then computing “a relevance score for each document”.[25] Catalogue or index servers are used within intranets, but also on the Internet. Most prominently by Google, Yahoo and other search engines. Users access the web server (frontend) of Google, this server hands of the querying effort to index servers, that is, if the result is not already cached.

Communication server
Communications servers are dedicated to enabling clients to communicate with each other and with content hosted within a network – most often within a company’s local area network (LAN). As a communication server connotes most with office environments, such a server is sometimes called a business server.[26] Services provided by a communications server are, amongst other, “instant messaging, [tele]presence, conferencing, and Voice over IP telephony”,[27] but arguably also print, fax and other office environment services will fall under the ambit of communications services. Instant messaging will be covered when discussing messaging servers, telepresence, conferencing, and Voice over IP will be discussed briefly here.

Telepresence is the ability for employees to be virtually present in a place whilst being physically in a different location, for instance through video conferencing. In order to do so a communications server (sometimes called a conferencing server) allows employees to (video)call other employees. Simply put, employees engaging in video conversation

[21] Jana, “Exploring Caching in ASP.NET,” ng

[22] Apache, “HTTP Server Project,” apache.org (accessed July 13, 2015); nginx, “About,” nginx.org/en/ (accessed July 13, 2015); Polipo, “Polipo - a Caching Web Proxy,” Université Paris Diderot, pps.univ-paris-diderot.fr/~jch/software/polipo/ (accessed July 13, 2015); Squid, “Squid: Optimising Web Delivery,” squid-cache.org (accessed July 13, 2015).

[23] Microsoft, “Global Catalog Servers,” technet.microsoft.com/en-us/library/cc977998.aspx (accessed July 13, 2015).

[24] Luiz André Barroso, Jeffrey Dean and Urs Hölzle, “Web Search for a Planet: The Google Cluster Architecture,” *IEEE Micro Magazine* 23, no. 2 (2003), 22-28. p. 23.

[25] Ibid.

[26] Skype for Business, “Skype for Business Server,” Microsoft, products.office.com/en-us/skype-for-business/server-hybrid (accessed July 13, 2015).

[27] Microsoft, “Microsoft Office Communications Server,” technet.microsoft.com/en-us/office/ocs/bb267356.aspx (accessed July 13, 2015).

use software on their client (computer) to login into the conferencing application, this software authenticates the client on a communications server/service, the user can then search through the user pool on the conferencing service and invite/call other employees, these invitees authenticate themselves on the service as well and can then accept the invite/call, the client software presents the users with a graphical user interface with audio and/or video, in the background the communications server exchanges the audio and video between those participating in the conversation.

A Voice over IP (VoIP) service works in a similar way by using session initiation protocol (SIP), real-time transport protocol (RTP) and real-time transport control protocol (RTCP).[28] Voice over IP is a technique enabling sending voice over data networks instead of a using a separate and dedicated phone network, the so-called public switched telephone network (PSTN). VoIP being cheaper and easier to implement, it is slowly but steadily replacing PSTN networks in certain parts of the world.[29] A VoIP session is set-up when a user wants to call another user. First SIP discovers "the current host(s) at which the destination user is reachable".[30] Discovering the location of the destination user is accomplished via "proxy servers and redirect servers which are responsible for receiving a request, determining where to send it based on knowledge of the location of the user, and then sending it there", very much like the Domain Name System (DNS) and name servers – which will be covered later in this section.[31] The SIP protocol then creates a session between end users and voice can be streamed via the RTP protocol. The most well-known software delivering these types of service is (Microsoft's) Skype for Business, successor of Microsoft Lync Server.

Database server

Database servers, as fifth, provide data to other servers, services and users, and are frequently used in online networking. By installing database server software, also called database management system (DBMS) software, a server or a personal computer can be turned into a database server. Simply put, the software allows a server or computer to hosts a database, which is "a collection of information that is organised so that it can easily be accessed, managed, and updated" (for those non-technical looking for concrete footholds, a database online slightly resembles an excel sheet table). [32] These databases are often structured in structured query language (SQL), enabling "interactive queries" and updates.[33] Users and services can perform queries on the dataset hosted on the database and receive

[28] H. Schulzrinne et al., *Request for Comments 3550: RTP, a Transport Protocol for Real-Time Applications* (Fremont: Internet Engineering Task Force,[2003]); Askozia, "What are SIP Or VOIP Phones?" askozia.com/voip/what-are-sip-or-voip-phones/ (accessed July 13, 2015).

[29] Point Topic, *VoIP Statistics - Market Analysis* (London: Point Topic Ltd.,[2013]); Frederic Lardinois, "Ethiopian Government Bans Skype, Google Talk and all Other VoIP Services," Techcrunch, techcrunch.com/2012/06/14/ethiopian-government-bans-skype-google-talk-and-all-other-voip-services/ (accessed July 13, 2015).

[30] J. Rosenberg et al., *Request for Comments 3261: SIP, Session Initiation Protocol* (Fremont: Internet Engineering Task Force,[2002]).

[31] Ibid.

[32] Allan Leake, "Database Definition," SearchSQLServer, searchsqlserver,techtarget.com/definition/database (accessed July 13, 2015).

[33] Ibid.

output. These databases “typically contain aggregations of data records or files, such as sales transactions, product catalogs and inventories, and customer profiles”.[34] One example of using database servers is using it to store passwords, when a user wants to log in a web shop he fills in his user name and password. The front-end web server checks the provided username and password to the credentials stored on the database server. Database servers used to reside at the back-end of web servers without a front-end facing the public. Whilst still largely true, modern database servers provide users with a outward facing portal for querying databases. As with all types of servers, they increasingly become able to fulfil different roles (types of services). Common software to enable a server to host databases includes MySQL, PostgreSQL, Microsoft SQL Server and Oracle (RDBMS).[35]

File and FTP servers
Database servers host data, file servers host files. File servers can range from a small home server, also known as networks accessed storage (NAS) disk, to a dedicated server within an organisation’s network allowing employees to share files over the local area network, to cloud based file services such as Dropbox and Google Drive. There is not a single type of file that can be hosted on a file server, all types can be hosted, such as images, video, audio, back-ups, system images, documents and many more. Although there is dedicated software for managing and creating file servers, building a simple file server does not require much accept for a storage medium able of connecting to a network. File servers inside a network are accessed via standard protocols, such as Server Message Block (SMB) and Network File System (NFS). When a file server is placed outside a LAN it is called a file transfer protocol (FTP) server. FTP servers enable external users to access files, by using the FTP protocol, which is also build-in in almost every computer.

Game server
As seventh, game servers, provide gaming services to users engaging in multiplayer games. Many gaming consoles (e.g. Microsoft XBOX and Sony PlayStation), PCs and mobile gaming apps add a multiplayer element to their game. Simple games may be easy to set-up from a game developer’s perspective, graphic heavy, first person shooter (FPS) games (e.g. Call of Duty, Battlefield and Counter Strike), attracting millions of players, may stress servers considerably and hence require a specific type of server. This type of server is a game server, which manages to pull of the extraordinary feat of synchronising players engaged in a game coming from different locations, with differing Internet speeds, all giving input to the server. In the early days of multiplayer FPS gaming, the architecture was peer-to-peer; one of the players would host a game and others would join.[36] Whilst this type of architecture

[34] Allan Leake, “Database Definition”.

[35] DB-Engines, “DB-Engines Ranking,” db-engines.com/en/ranking (accessed July 13, 2015).

[36] Gaffer on Games, “What Every Programmer Needs to Know about Game Networking,” gafferongames.com/networking-for-game-programmers/what-every-programmer-needs-to-know-about-game-networking/ (accessed July 13, 2015).

is still in use today "for small groups of players in certain types of games [...]",[37] the client-server architecture has largely replaced peer-to-peer architecture in multiplayer gaming.

Users install a game on their device (e.g. console), this device – the client – is connected to the Internet, when a user wants to play a multiplayer game he selects a game he wants to join from a GUI of multiplayer games hosted on game servers. The client authenticates the user on the selected game server and the server provides the client with an ID associated with the server for administrative and networking (e.g. routing) purposes. All users in a game play the game on the game server, this server "is authoritative about world simulation, game rules, and player input processing".[38] The clients and server exchange "small data packets at a high frequency (usually 20 to 30 packets per second)",[39] for instance packets entailing the user's location or actions (e.g. shots and interaction) in the virtual gaming environment.

The primary problem game servers face is synchronisation, all users have different Internet speeds, hence when a player has a slow Internet connection, the packet comprising his actions would take longer to reach the server. This would limit his ability to compete with other players with a high-speed connection. Besides that, the user plays his game on the client, so an action is taken before it is sent to the server resulting in a temporary asynchrony between the game on the client and on the server.[40] In order to solve these problems game servers utilise "client-side prediction"[41] and "lag compensation".[42] The game software on the client processes and displays the action taken by the player locally first (prediction), so the player has a direct response to his input. The server then sends all clients "a server snapshot", an update to all clients with the actual position of all players.[43] If the position of the in-game character is off "a prediction error has occurred", when such an error occurs the server has "final authority over client-side prediction".[44] Lag compensation reduces the influence of the players' differing connection speeds, such a system "keeps a history of all recent player positions for one second [...] if a user command is executed, the server estimates at what time the command was created".[45] It then can decide whether the input of the player was received before any other input from other players. Game servers come in different shapes and sizes, there are as many varieties as there are games. The functionality offered differs per game, whether it is a resource intensive FPS, turn-based strategy game or small gaming applications. The software differs accordingly, but game servers generally consist – on top of the server platform discussed earlier – of software needed to host a game and administrative software to monitor server performance (e.g. network, updates and errors).

[37] Andrew Armstrong, *The Mammoth Dedicated Server Guidebook* (Brisbane: Mammoth Media,[2009]). p. 5.

[38] Valve, "Source Multiplayer Networking," developer.valvesoftware.com/wiki/Source_Multiplayer_Networking (accessed July 13, 2015).

[39] Ibid.

[40] Gaffer on Games, "What Every Programmer Needs to Know about Game Networking."

[41] Ibid.

[42] Valve, "Source Multiplayer Networking,"

[43] Ibid.

[44] Ibid.

[45] Ibid.

Mail server

A mail or simple mail transfer protocol (SMTP) server is a server dedicated to delivering mail services. When a user sends an email, it has a source address (the user's mail address) and a destination address. A mail server is the first stop for an email after an authenticated user has pressed the 'send' button. Mail servers are generally linked to the part coming after the '@' sign, called the domain. Often the domain is linked to a company or organisation, for instance @apple.com or @google.com. There are also mail services provided as a business model such as Outlook (formerly known as Hotmail) and Gmail, these third-party mail services result in @outlook.com or @gmail.com addresses. Thus, mail servers "can be around the world or in the same building […]" where a user works.[46]

An email has two addresses, the source/sender address and the destination/recipient address. After the user has sent the mail, the SMTP server resolves the recipient address (e.g. recipient@example.com). As with most addresses on the Internet, the domain (example.com) is translated into an Internet protocol (IP) address. In order to resolve this address the SMTP server uses the domain name system (DNS) and the name servers included within this system – DNS resolving will be discussed in the section regarding name servers. After having received the IP address belonging to example.com from a name server, the sender SMTP server sends the email to the receiving SMTP server. The receiving SMTP server then stores the received mail; the user can then access the email by using post office protocol (POP3) or Internet message access protocol (IMAP). The former downloads mails from a mail server onto the device with which the service is accessed and is then deleted on the server; IMAP allows users to access and view the mails from more than one device and the mails are "stored on a remote server".[47]

Message server

The function of a messaging server largely resembles that of mail server, it is used to facilitate communication between two or more clients. [48] As with all server types, the existence of a distinct messaging server type is somewhat arbitrary, the type of server meant could be a instant messaging or Extensible Messaging and Presence Protocol (XMPP) server or an Internet Relay Chat (IRC)server.[49] XMPP "is an application profile of the Extensible Markup Language [XML] that enables the near-real-time exchange of structured yet extensible data between any two [1:1] or more network entities."[50] In other words, XMPP enables sending simple messages wrapped in tags (e.g. <from>, <to>, <message>, etc.)

[46] Active-Server, "Differences between IMAP, POP and SMTP," active-server.com/blog/differences-between-imap-pop-and-smtp/ (accessed July 13, 2015).

[47] How-to Geek, "Email: What's the Difference between POP3, IMAP, and Exchange," howtogeek.com/99423/email-whats-the-difference-in-pop3-imap-and-exchange/ (accessed July 13, 2015); Aol., "What is the Difference between POP3 and IMAP?" help.aol.com/articles/what-is-the-difference-between-pop3-and-imap (accessed July 13, 2015); Thunderbird, "What is the Difference between IMAP and POP Protocols?" help.thunderbird.edu/content/what-difference-between-imap-and-pop-protocol (accessed July 13, 2015).

[48] Margaret Rouse, "Messaging Server," Techtarget, searchexchange.techtarget.com/definition/messaging-server (accessed July 13, 2015).

[49] XMPP Standards Foundation, "About," xmpp.org/about-xmpp/ (accessed July 13, 2015).

[50] https://tools.ietf.org/html/rfc6120

between two or more clients. Popular applications of XMPP include instant messaging (e.g. Facebook Messager, Whatsapp), groupchat (e.g. virtual classrooms, situation rooms communications) and systems control.[51] Users install particular client software on their machines and by using that software they can identify their client and "connect to a local server, which will connect directly to the server of the destination client".[52] In case of instant messaging the user sends a message using the graphical user interface (GUI) of their client software, this client translates the input to XML and this XML message is sent to a XMPP server. This server stores the XML message until the receiving user's client software 'logs in' and then sends the XML message to the client machine and removes it from the server. The receiving user's client software graphically represents the XML message to the user.

Another type of messaging server is the Internet Relay Chat (IRC) server, which – instead of XMPP – is "primarily used for group chat, using [channels]".[53] The IRC network consists of IRC servers and IRC clients, the latter being machines that have IRC client software installed (e.g. Adium, mIRC and Colloquy). A channel is "implicitly" created on the IRC server when the first user joins the channel, i.e. specifies the channel he wants to join in his client software, other users can then join that channel.[54] The channel ceases to exist after the last user has left the channel.[55] A channel serves as "a text-based, virtual meeting room [...] each channel is a virtual space where anybody connected to the Internet and IRC [software] can join by entering and talking to the other people already there."[56] When a user types a message in his IRC software the software transmits the message to the IRC server, the IRC server than echoes the message to all clients subscribed to the channel creating a seemingly real-time messaging service. Although popular in the early days of consumer Internet until the height of the Internet bubble (1988 until the early 2000s), its usage is steadily declining as a result of distributed denial of service attacks on its IRC servers, rise of peer-to-peer (P2P) networks, social-networks and instant messaging solutions.[57]

Name server

Name servers are integral to the Domain Name System (DNS), this distributed system is basically comprising "a database of host information".[58] This database contains information regarding domain names (e.g. www.example.com) and the associated Internet protocol (IP) addresses (e.g. 192.0.2.1). DNS is one of the primary systems enabling the functioning of the Internet, it makes sure addresses can be resolved, updated, managed

[51] P. Saint-Andre, Kevin Smith and Remko Troncon, *XMPP: The Definitive Guide* (Sebastopol, CA: O'Reilly, 2009). pp. 4-6.

[52] Isode, "Interconnecting XMPP and IRC," isode.com/whitepapers/interconnecting-xmpp-and-irc.html (accessed July 13, 2015).

[53] Ibid.

[54] J. Oikarinen and D. Reed, *Request for Comments 1459: Internet Relay Chat Protocol* (Fremont: Internet Engineering Task Force,[1993]).

[55] Ibid.

[56] Bill Stewart, "IRC Channels," livinginternet.com/r/rw_chan.htm (accessed July 13, 2015).

[57] Royal Pingdom, "IRC is Dead, Long Live IRC," royal.pingdom.com/2012/04/24/irc-is-dead-long-live-irc/ (accessed July 13, 2015).

[58] Cricket Liu and Paul Albitz, *DNS and Bind*, 3rd ed. (Sebastopol, CA: O'Reilly, 1998). p. 89.

and presented in a human-understandable format. (names instead of addresses). This distributed database "is indexed by domain names [...] each domain name is essentially just a path in a large inverted tree, called the domain name space."[59] There are various domain levels: the highest root domain labelled " " or "."; top-level domains (TLDs) such as .com, .org, .net, .edu and country code TLDs (.us, .nl, .de, etc.); a second-level domain "is a child of a first-level domain" (for instance example.com); a third-level is a child of a second-level domain (e.g. directory.example.com).[60]

If a user wants to navigate to example.com, his machine has to know how to get there; in other words, it has to know the address belonging to the domain name example.com. Most, if not all, machines connected to the Internet and protocols making use of the Internet (e.g. Telnet and FTP) come equipped with a "resolver", software or a process used for resolving domain names to addresses.[61] The actions this resolver performs are "querying a name server", "interpreting responses (which may be resource records or an error)" and "returning the information to the programs that requested it".[62] For regular users the name server is provided for by their ISP, companies sometimes employ their own name servers. These name servers "are adept at retrieving data form the domain name space."[63] Apart from that, name servers can search through the domain name system and give information to other name servers with regard to the "zones for which they're authoritative" (via a so-called 'start of authority' record, SOA).[64]

In the case of a user wanting to navigate to example.com, the resolver queries a name server, this name server than starts the process called "name resolution or simply resolution."[65] The name server starts with querying the root name servers for the address of the .com name servers. After having received the address of the .com name server it queries that server for the address of the example.com zone. Having received the address of the example.com name server it then queries that name server for the address of example.com. The authoritative name server for example.com then returns the record stating the address belonging to example.com (in the case of example.com the name server is a.iana-servers.net). The name server queried by the resolver then returns the address and the machine can navigate to the address. In order to limit the number of duplicate DNS queries, the resolved addresses are stored locally and on the name servers for a specific time (a so-called time to live, TTL).[66] Specialised software needs to be installed on a server for it to become a name server; this software is called Berkeley Internet Name Domain (BIND).[67]

[59] Ibid.

[60] Ibid. p. 93.

[61] Ibid. p. 104.

[62] Ibid. p. 104.

[63] Ibid. p. 105.

[64] Ibid. p. 105.

[65] Ibid. p. 105.

[66] Cricket Liu and Paul Albitz, *DNS and Bind*, 3rd ed. (Sebastopol, CA: O'Reilly, 1998). pp. 111-112.

[67] Internet Systems Consortium, "Bind," isc.org/downloads/bind/ (accessed July 13, 2015).

Proxy server

A proxy server is a type of server "that acts as an intermediary between an endpoint device, such as a computer, and another server from which a user or client is requesting a service."[68] The simplest application of a proxy server is to use it as facilitator of "communication between client and target server without modifying requests or replies."[69] This type of application is sometimes called a gateway or tunnelling proxy and is employed for bundling the traffic on a network bound for the wide-area network. The proxy server "hijacks" the connection and "represents itself as a client to the target server, requesting the resource" on behalf of the initial client.[70] The target server replies and the proxy server returns the resource to the initial client, "giving a feel [of having directly] communicated with the target server."[71] Using a proxy as gateway or tunnel to the WAN makes it easy to perform administrative tasks on the outbound and inbound traffic, the proxy could be used to "reduce bandwidth usage" (via caching web documents), "enforce network access policies", "monitor user traffic", "enhance user privacy by not exposing a user's machine directly to Internet", "filter requests", "load balance network traffic across multiple Internet connections" and "relay traffic".[72] A proxy server located in front of the target server can be used to "distribute load among different web servers to reduce load on a single server [and] empower a poorly performing web server"[73] – this type of functionality has been covered before in discussing reverse cache servers which also is called a reverse proxy.

Video server

Video servers are servers that hold video data, for instance YouTube's content servers, IPTV servers and even IP camera servers. Conventional television – i.e. the type of television that used to be broadcasted to homes – has changed. It went from being broadcasted to being requested by the viewer, users decide which video they want to watch and at what time. The facilitator for this change is IP and increasing bandwidth. Video sharing websites (such as YouTube) and IPTV architecture resembles that of most online services, clients request a server to be provided with a service, in this case streaming video. In the case of the home IPTV a set-top box is connected to a user's home network and enables streaming video to television screens. Instead of a broadcast signal entering a home "from a rooftop antenna, satellite dish, or fiber-optic cable", video is streamed, i.e., "downloaded and played almost simultaneously".[74] Another application of IPTV is watching television on any device with an Internet connection, such as smartphones, tablets and laptops. There are four functionalities of IPTV services, video on demand (the modern variant of a video rental store), time-shifted television (gives users the ability to record and replay content when desired), interactive

[68] Margaret Rouse and Matthew Haughn, "Proxy Server," Techtarget, whatis.techtarget.com/definition/proxy-server (accessed July 13, 2015).

[69] Kulbir Saini, *Squid Proxy Server 3.1: Beginner's Guide* (Birmingham: Packt Publishing, 2011). p. 7.

[70] Ibid.

[71] Kulbir Saini, *Squid Proxy Server 3.1: Beginner's Guide* (Birmingham: Packt Publishing, 2011). p. 7

[72] Ibid.

[73] Ibid.

[74] Chris Woodford, "Iptv," explainthatstuff.com/how-iptv-works.html (accessed July 13, 2015).

television (play and pause live television), and live television.[75] The functions are very much the same as conventional broadcasting, the producer creates the content and televisions stations aggregate this content. But with IPTV, instead of broadcasting it themselves, the IPTV service providers take care of the content delivery. The protocols facilitating IPTV are Internet Group Management Protocol (IGMP) for subscribing to a live stream (for live television), Protocol Independent Multicast (PIM) or alternative multicast protocols are used to multicast the content to various subscribers. For on-demand services the Real-time Transport protocol and User Datagram protocol, both mentioned earlier.

Web server

Lastly, the most prevalent and apparent of servers are web servers. These are the servers hosting web pages that we access on a daily basis. For a server to become a web server it needs to have specific software installed, this software is often composed of Linux, Apache, MySQL and PHP – the so-called LAMP stack. Linux is used as the operating system, Apache as the web server, MySQL as "the relational database management system and PHP as the object-oriented scripting language."[76] Linux may be replaced by other operating systems such as Windows, Macintosh or FreeBSD. PHP can be exchanged or complemented with Perl, Python or Ruby language and MySQL can be replaced with PostgreSQL. No matter what software, the functionality delivered is a server able of serving or answering hypertext transferable protocol (HTTP) requests coming from clients. The client "sends a request to the server in the form of a request method, URI [Uniform Resource Indicator] and protocol version". The server then responds "with a status line, including the message's protocol version and a success or error code".[77] A practical everyday application is when a user types an URL in his browser, for instance http://www.example.com. The browser then formulates a HTTP request (as specified by the "http://" syntax in the URL) for the resources in the domain www.example.com/.[78] The server then returns the requested resource which can be a Hypertext Mark-up Language page, PHP page or whatever language was used to design and code the website. The browser interprets the page and graphically represents it to the user.

[75] John Fuller, "How Internet TV Works?" HowStuffWorks, electronics.howstuffworks.com/internet-tv2.htm (accessed July 13, 2015); Alliance for Telecommunications Industry Solutions, *AITS IPTV Exploratory Group Report and REcommendation to the TOPS Council* (Washington, DC: Alliance for Telecommunications Industry Solutions,[2005]); Laws.com, "Time Shifting," copyright.laws.com/time-shifting (accessed July 13, 2015).

[76] Margaret Rouse, "LAMP (Linux, Apache, MySQL, PHP)," TechTarget, searchenterpriselinux.techtarget.com/definition/LAMP (accessed July 13, 2015).

[77] R. Fielding et al., *Internet-Draft: Hypertext Transfer Protocol -- HTTP/1.1* (Fremont: Internet Engineering Task Force,[2007]).

[78] Pavan Podila, "HTTP: The Protocol Every Web Developer must Know," code.tutsplus.com/tutorials/http-the-protocol-every-web-developer-must-know-part-1--net-31177 (accessed July 13, 2015); Sarath Pillai, "HTTP (Hypertext Transfer Protocol) Request and Response," [Root.in~] #:, slashroot.in/httphypertext-transfer-protocol-request-and-response (accessed July 13, 2015).http

Appendix B

Appendix B

This appendix is an addition to sub-section 5.3.2.2, it lists and describes the following types of information related capabilities or information activities: psychological operations; presence, posture, profile; information and operations security; military deception; electronic warfare; physical destruction; key leader engagement; cyber operations; civil-military cooperation; military information support operations; strategic communication; and other supporting and coordinating mechanisms.

Psychological operations

Psychological operations are broad in scope; they involve the use of "print, radio, television, loudspeakers, face-to-face contact, the Internet, faxes, pagers and telephone" to "influence the perceptions, attitudes and behaviour of selected individuals or groups".[79] In other words, psychological operations aim to affect psyche or audiences by using all other targets in the physical and information dimensions.

Presence, posture and profile

Presence, posture and profile (PPP) is about the effect of "mere presence of a force [on] perception".[80] Similar to psychological operations, the primary target is the psyche and audiences, but as vector this activity uses the physical form of people in the physical dimension.

Information and operations security

Information and operations security are activities aimed at protecting all components of fighting power in the physical and information dimensions, they do not seek to influence other actors, instead they focus on protecting own physical, information and cognitive assets.

Military deception

Deception is also aimed at influencing the psyche of an adversary, namely, manipulating him to misunderstand the situation at hand. The vectors for influencing the psyche can be "both information and traditional physical means and methods (such as demonstrations and show of force)". [81]

Electronic warfare

Electronic warfare (EW) focuses on creating an effect versus connected objects (e.g. command and control systems) and/or virtual objects (e.g. data in transit) "[...] so that

[79] North Atlantic Treaty Organisation, *Allied Joint Publication 3.10: Allied Joint Doctrine for Information Operations* (Brussels: North Atlantic Treaty Organisation, 2009a). p. 1-8.

[80] Ibid. p. 1-8.

[81] North Atlantic Treaty Organisation, *Allied Joint Publication 3.10: Allied Joint Doctrine for Information Operations*. p. 1-9.

critical information on which an adversary will make a decision, or the information systems for carrying such information, can be affected".[82] Electronic warfare takes place in the electromagnetic spectrum, which is a "portion of the information environment", the electromagnetic spectrum "is divided into bands ranging from radio frequencies at the low en to x-ray and gamma frequencies at the high end."[83] Physical network infrastructure often utilises the electromagnetic spectrum, for instance Wi-Fi enabled devices (using the 2.4 GHz band) and cellular devices (using the 800 and 1800 MHz frequencies). As such there is considerable overlap between cyber operations and electronic warfare.

Physical destruction

NATO's physical destruction activity under the ambit of information operations emphasises (1) the use of physical action to "destroy command and control systems [...] affecting the understanding of an adversary [and] his ability to apply will" and (2) "the strong message" that can be send via "the direct application of force through physical destruction".[84] Physical destruction's target is the psyche, as vector it uses physical assets (persons and objects) and physical network infrastructure (command and control systems).

Key leader engagement

Key leader engagement (KLE) or stakeholder engagement (SHE) is aimed at engaging and impacting "all key actors" during operations.[85] KLE is about winning the favour of these leaders or, if not easily reconciled, negate their influence in their network in order to, for instance, achieve a "change in policy or support the [commanders] objectives."[86] KLE is aimed to change the perceptions and dispositions of key leaders; hence its primary goal is influencing the psyche in the cognitive dimensions. As a vector KLE most often use the physical instance of the leaders, that is, by talking face-to-face with a leader. As network technology increasingly permeates potential conflict areas, the leaders' cyber personas may be used to this extent, which might replace or supplement face-to-face talks.

Cyber operations

"[W]hen in support of [information operations]", cyber operations aim to "deny or manipulate adversary or potential adversary decision making through targeting an information medium [...], the message itself [...], or a cyber persona".[87] According to this description cyber operations, when in support of information operations, are aimed at physical network infrastructure (information media or stored data), cyber objects (data in transit) and cyber personas (e.g. social media profiles).

[82] Ibid. pp. 1-9 to 1-10.

[83] The Joint Chiefs of Staff, *Joint Publication 3-13.1: Electronic Warfare*. p. I-1.

[84] North Atlantic Treaty Organisation, *Allied Joint Publication 3.10: Allied Joint Doctrine for Information Operations*. p. 1-10.

[85] Ibid. pp. 1-10 to 1-11.

[86] The Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*. II-13.

[87] Ibid. p. II-9.

Civil-military cooperation

Civil-military cooperation (CIMIC) or civil-military operations (CMO) aim to create meaningful relationships "between military and civil actors, including national population and local authorities, as well as international, national and non-governmental organisations and agencies [...] in support of the mission".[88] Civil-military cooperation is primarily aimed at affecting "friendly and neutral populations", but also "potential adversary audiences" may be affected.[89] By enforcing (latent) relationships between various military and non-military actors a variety of effects can be created. The primary target of civil-military cooperation is human relationships, which is a distinct cognitive capacity enclosed within the human psyche. As vector, these operations use physical people (physical dimension) tied in social and professional relations (cognitive domain), increasingly these ties also reach into the information dimension, for instance mail, social media, and other ways to foster social ties.

Military information support operations

Military information support operations (MISO) are planned to "convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organisations, groups, and individuals."[90] The target audiences for these operations include "potential and actual adversaries, but also friendly and neutral populations".[91] The purpose of military information support operations is distinctively cognitive, that is, human psyche and audiences.

Strategic communication

Strategic communication (Stratcom or SC) envelops a process "of focused [...] efforts to create, strengthen, or preserve conditions favourable for the advancement of national interests, policies, and objectives by understanding and engaging key audiences through the use of coordinated programs, plans, themes, messages, and products synchronised with the actions of all instruments of national power."[92] Strategic communication is a coordinating mechanism "driven by interagency processes and integration that are focused upon effectively communicating national strategy."[93] As such, strategic communication is about synchronising the message communicated versus all entities.

[88] North Atlantic Treaty Organisation, *Allied Joint Publication 3.10: Allied Joint Doctrine for Information Operations*. p. 1-12.

[89] The Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*. p. II-9.

[90] The Joint Chiefs of Staff, *Joint Publication 3-13: Information Operations*. p. II-10.

[91] Ibid. p. II-10.

[92] Ibid. p. II-5.

[93] Ibid. p. II-5.

Other supporting and coordinating mechanisms

United States armed forces have forwarded other coordinating mechanisms aimed at synchronising information-related capabilities: being: intelligence, public affairs, joint interagency coordination and space operations. Public affairs "comprises public information, command information, and public engagement activities directed toward both the internal and external publics" as such is can potentially conflict with information activities. Interagency coordination "occurs between [the armed forces] and other [departments] and agencies, as well as with private-sector entities, nongovernmental organisations, and critical infrastructure activities", these activities involve "the combined

Bibliography

Bibliography

"Cyber Conflict and Deterrence." *Strategic Comments* 22, no. 7 (2016): iii-v.

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention). Geneva: International Committee of the Red Cross, 1949.

"IoT List: Discover the Internet of Things." iotlist.co/.

National Plan for Information Systems Protection: An Invitation to a Dialogue, edited by United States Washington, D.C.: President of the U.S, 2000.

"National Security Decision Directive Number 145 National Policy on Telecommunications and Automated Information Systems Security ". Accessed 11/14/2013, 2013. fas.org/irp/offdocs/nsdd145.htm.

The Oxford Handbook of Modern Diplomacy. USA: USA Oxford University Press, 2013.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). Geneva: International Committee of the Red Cross, 1977.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II). Geneva: International Committee of the Red Cross, 1977.

United States Constitution.

Vienna Convention on Diplomatic Relations. Vienna: United Nations, 1961.

Vienna Convention on the Law of Treaties. Vienna: United Nations, 1969.

"Seph". "What is Cyberpunk?". Accessed October 30, 2013. cyberpunkforums.com/viewtopic.php?f=1&t=361.

111th Congress House of Representatives. "Report 111-186: Intelligence Authorization Act for Fiscal Year 2010." House of Representatives. Accessed September 3, 2017. fas.org/irp/congress/2009_rpt/hrpt111-186.html.

688th Cyberspace Wing. *A Brief History of the 688th Cyberspace Wing*. Joint Base San Antonio-Lackland: 688th Cyberspace Wing History Office, 2016.

80th Congress of the United States of America. *National Security Act of 1947*. Washington, D.C.: Department of State, 1947.

Abadi, Martín and David G. Andersen. “Learning to Protect Communications with Adversarial Neural Cryptography.” *ArXiv Preprint arXiv:1610.06918* (2016).

Ackermann, Alice. “The Idea and Practice of Conflict Prevention.” *Journal of Peace Research* 40, no. 3 (2003): 339-347.

Active-Server. “Differences between IMAP, POP and SMTP.” Accessed July 13, 2015. active-server.com/blog/differences-between-imap-pop-and-smtp/.

Adams, James. *The Next World War: Computers are the Weapons and the Front Line is Everywhere*. New York: Simon and Schuster, 2001.

Adamsky, Dima. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Stanford: Stanford University Press, 2010.

———. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US, and Israel.* Stanford University Press, 2010.

Adelman, Ken. “Not-so-Smart Power.” Foreign Policy. Accessed July 31, 2017. foreignpolicy.com/2011/04/18/not-so-smart-power/.

Advisory Council on International Affairs and Advisory Committee on Issues of Public International Law. *Cyber Warfare*. The Hague: AIV/CAVV, 2011.

Agarwal, Monika and Abhinav Singh. *Metasploit Penetration Testing Cookbook*. 2nd ed. Birmingham: Packt Publishing, 2013.

Air Intelligence Agency. “Air Force Information Warfare Center.” *Air Force Intelligence Agency Almanac* no. 97 (August, 1997).

———. “Air Force Information Warfare Center: Air Force Computer Emergency Response Team.” *Air Force Intelligence Agency Almanac* no. 97 (August, 1997).

Alabaster, Keith. “Nslookup - what is it for and when might I use it?” Expert Exchange. Accessed August 31, 2015. experts-exchange.com/articles/2110/NSLOOKUP-What-is-it-for-and-when-might-I-use-it.html.

Albanesius, Chloe. “Facebook Ireland Facing Audit Over Privacy, ‘Shadow Profiles’.” PC Magazine. Accessed July 14, 2015. pcmag.com/article2/0,2817,2395109,00.asp.

Allen, Stuart and Einar Thorsen. *Citizen Journalism: Global Perspectives*. New York: Peter Lang Publishing, 2009.

Alliance for Telecommunications Industry Solutions*. AITS IPTV Exploratory Group Report and REcommendation to the TOPS Council*. Washington, DC: Alliance for Telecommunications Industry Solutions, 2005.

Almeida, Virgilio, Demi Getschko, and Carlos Afonso. "The Origin and Evolution of Multistakeholder Models." *IEEE Internet Computing* 19, no. 1 (2015): 74-79.

Ampère, Antoine. *Essai Sur La Philosophie Des Sciences Ou Exposition Analytique d'Une Classification Naturelle De Toutes Les Connaissances Humaines*. Paris: Bachelier, 1843.

Anderlini, Sanam Naraghi and Judy El-Bushra. "Post-Conflict Reconstruction." *Inclusive Security, Sustainable Peace: A Toolkit for Advocacy and Action* (2004): 51-68.

Anderson, Ross. *Security Engineering: A Guide to Building Dependable Distributed Systems*. 2nd ed. Indianapolis: Wiley Publishing, Inc., 2008.

Anderson, Chris. *Makers: The New Industrial Revolution*. 1st ed. New York: Crown Business, 2012.

Andress, Jason and Steve Winterfeld. *Cyber Warfare: Techniques and Tools for Security Practitioners*. 1st ed. Waltham: Syngress, 2011.

———. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. 2nd ed. New York: Syngress, 2014.

Anthony, Sebastian. "The First Human Brain-to-Brain Interface has been Created. in the Future, Will we all be Linked Telepathically?". Accessed January 14, 2015. extremetech.com/extreme/188883-the-first-human-brain-to-brain-interface-has-been-created-in-the-future-will-we-all-be-linked-telepathically.

Antoci, Angelo, Fabio Sabatini, and Mauro Sodini. "See You on Facebook: The Effect of Social Networking on Human Interaction." *European Research Institute on Cooperative and Social Enterprises* (2010).

Aol. "What is the Difference between POP3 and IMAP?". Accessed July 13, 2015. help.aol.com/articles/what-is-the-difference-between-pop3-and-imap.

Apache. "Apache Tomcat.". Accessed July 10, 2015. tomcat.apache.org.

———. “HTTP Server Project.”. Accessed July 13, 2015. apache.org.

Appeals Chamber. “Prosecutor v. Dusko Tadic Aka “Dule” (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction).” International Criminal Tribunal for the former Yugoslavia. Accessed May 12, 2016. icty.org/x/cases/tadic/acdec/en/51002.htm.

Apple. “About Caching Service.”. Accessed July 10, 2015. help.apple.com/serverapp/mac/4.0/?lang=en#/apd74DDE89F-08D2-4E0A-A5CD-155E345EFB83.

Armstrong, Andrew*. The Mammoth Dedicated Server Guidebook*. Brisbane: Mammoth Media, 2009.

Armstrong, Gary and Philip Kotler. *Marketing: An Introduction*. 12th ed. London: Pearson Education, 2015.

Army, US. “FM 100-6: Information Operations.” *Washington: GPO* (1996).

Arnett, Eric H. “Welcome to Hyperwar.” *The Bulletin of Atomic Scientists* 48, (1992): 14.

Arquilla, John and Douglas A. Borer, eds. *Information Strategy and Warfare: A Guide to Theory and Practice*. New York: Routledge, 2007.

Arquilla, John and David Ronfeldt. “Cyberwar is Coming!” *Comparative Strategy* 12, no. 2 (1993): 141-165.

———. *In Athena’s Camp: Preparing for Conflict in the Information Age*. Washington, D.C.: Rand corporation, 1997.

———. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica: RAND National Defense Research Institute, 2001.

Ash, Robert B. *Information Theory*. Mineola: Dover Books, 1990.

Askozia. “What are SIP Or VOIP Phones?”. Accessed July 13, 2015. askozia.com/voip/what-are-sip-or-voip-phones/.

Asonov, D. and R. Agrawal. “Keyboard Acoustic Emanations.” Berkeley, IEEE, 12 May, 2004.

Association of the U. S. Army (AUSA) and Center for Strategic and International Studies (CSIS)*. Post-Conflict Reconstruction: Task Framework*. Washington, D.C.: CSIS, 2002.

AudienceGain. "Social Media Marketing that really Works!". Accessed February 227, 2016. audiencegain.com/.

Bacevich, A. J. "New Rules: Modern War and Military Professionalism." *Parameters* (December, 1990).

Bachrach, Peter and Morton S. Baratz. "Two Faces of Power." *The American Politcal Science Review* 56, no. 4 (1962): 947-952.

Bachrach, Peter and Morton S. Baratz. "Decisions and Nondecisions: An Analytical Framework." *The American Political Science Review* 57, no. 3 (1963): 632-642.

Bagley, Bruce M., Jonathan D. Rosen, and Hanna S. Kassab, eds. *Reconceptualizing Security in the Americas in the Twenty-First Century*. London: Lexington Books, 2015.

Bailey, Michael, Evan Cooke, Farnam Jahanian, Yunjing Xu, and Manish Karir. "A Survey of Botnet Technology and Defenses." Washington, D.C., March 3-4, 2009.

Baldwin, David A. "The Concept of Security." *Review of International Studies; Rev.Int. Stud.* 23, no. 1 (1997): 5-26.

———. *Economic Statecraft*. New Jersey: Princeton University Press, 1985.

———. "Power and International Relations." In *Handbook of International Relations*, edited by Carlsnaes, Walter, Thomas Risse and Beth A. Simmons, 177-191. London: Sage, 2002.

———. "Power and International Relations." In *Handbook of International Relations*, edited by Carlsnaes, Walter, Thomas Risse-Kappen and Beth A. Simmons. 2nd ed., 273-297. Los Angeles: SAGE, 2013.

Baldwin, David A. "Power Analysis and World Politics: New Trends Versus Old Tendencies." *World Politics* 31, no. 2 (1979): 161-194.

Ballman, Bastian. *Understanding Network Hacks: Attack and Defense with Python*. Berlin: Springer-Verlag, 2015.

Bammer, Gabriele. *Disciplining Interdisciplinarity: Integration and Implementation Sciences for Researching Complex Real-World Problems*. Canberra: Australian National University E Press, 2013.

Banga, Mainak. “Partition Based Approaches for the Isolation and Detection of Embedded Trojans in ICs.” Master, Virginia Polytechnic Institute, 2008.

Banks, Ken and Erik Hersman. “FrontlineSMS and Ushahidi - a Demo.” Doha, IEEE, 17-19 April, 2009.

Barnett, Michael and Raymond Duvall. “Power in International Politics.” *International Organisation* 59, no. 1 (2005): 39-75.

Barroso, Luiz André, Jeffrey Dean, and Urs Hölzle. “Web Search for a Planet: The Google Cluster Architecture.” *IEEE Micro Magazine* 23, no. 2 (2003): 22-28.

Bass, Frank M. “A New Product Growth for Model Consumer Durables.” *Management Science* 15, no. 5 (1969): 215-227.

———. “A New Product Growth for Model Consumer Durables.” 50, no. 12 (2004): 1825-1832.

Bauman, Zygmunt. *Liquid Modernity*. Cambridge: Polity Press, 2006.

BBC. “Crimea Power Blackout: Russia Accuses Ukraine of Sabotage.” BBC. Accessed February 10, 2017. bbc.com/news/world-europe-34967093.

———. “Email ‘most Common Internet Activity’ in Britain.” BBC. Accessed February 15, 2018. bbc.com/news/technology-40812692.

Beagle, T. W. “Effect-Based Targeting: Another Empty Promise?” Master thesis, Air University School of Advanced Airpower Studies, 2000.

Bell, Daniel. *The Coming of Post-Industrial Society: A Venture in Social Forecasting*. New York: Basic Books, 1973.

Bell, Melissa. “Sohaib Athar’s Tweets from the Attack on Osama Bin Laden.”. Accessed January 9, 2014. washingtonpost.com/blogs/blogpost/post/sohaib-athar-tweeted-the-attack-on-osama-bin-laden--without-knowing-it/2011/05/02/AF4c9xXF_blog.html.

Bellofiore, R. (Riccardo), Guido Starosta, and Peter D. Thomas. *In Marx’s Laboratory : Critical Interpretations of the Grundrisse* Brill, 2013.

Bemis, Jim and Grayson Morgan. “Exposing the Information Domain Myth.” *Air & Space Power Journal* 22, no. 3 (2008): 19-21.

Bennet, Shea. “28% of Time Spent Online is Social Networking.” SocialTimes. Accessed July 9, 2015. adweek.com/socialtimes/time-spent-online/613474.

Berenskoetter, Felix. “Unity in Diversity? Power in World Politics.” Turin, ECPR Standing Group on International Relations, September 12-15, 2009.

Berger, Jonah and Katy Milkman. “Social Transmission, Emotion, and the Virality of Online Content.” *Wharton Research Paper* (2010).

Berghel, Hal. “On the Problem of (Cyber) Attribution.” *Computer* 50, no. 3 (2017): 84-89.

Betker, Michael R., John S. Fernando, and Shaun P. Whalen. “The History of the Microprocessor.” *Bell Labs Technical Journal* 2, no. 4 (1997): 29-56.

Betz, David and Tim Stevens. *Cyberspace and the State: Toward a Strategy for Cyber-Power*. London: Routledge, 2011.

Bill Chavez, Rebecca. “The Rule of Law and Courts in Democratizing Regimes.” In *The Oxford Handbook of Law and Politics*, edited by Caldeira, Gregory A., R. Daniel Kelemen and Keith E. Whittington. Oxford: Oxford University Press, 2008.

Blitz, James. “UK Becomes First State to Admit to Offensive Cyber Attack Capability.” Financial Times. Accessed June 27, 2018. ft.com/content/9ac6ede6-28fd-11e3-ab62-00144feab7de.

Bodeau, Deborah, Richard Graubart, and William Heinbockel. “Characterizing Effects on the Cyber Adversary.” *MTR130432, MITRE Corporation, November* (2013).

Boebert, W. Earl. “Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.” Washington, D.C., National Academies Press, June 10-11, 2010.

Boniface, Pascal. “What Justifies Regime Change?” *The Washington Quarterly* 26, no. 3 (2003): 59-71.

Boot, Max. *War made New: Technology, Warfare, and the Course of History 1500 to Today*. New York: Gotham Books, 2006.

Bothe, Michael, Karl Josef Partsch, and Waldemar A. Solf. *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*. Dordrecht: Martinus Nijhoff Publishers, 1982.

Bousquet, Antoine. “Chaoplexic Warfare Or the Future of Military Organisation.” *International Affairs* no. No. 84 (2008): 915-929.

Brandt, Patrick T., John R. Freeman, and Philip A. Schrodt. “Real Time, Time Series Forecasting of Inter- and Intra- State Political Conflict.” *Conflict Management and Peace Science* 28, no. 1 (2011): 41-64.

Brevini, Benedetta, Arne Hintz, and Patrick McCurdy. *Beyond WikiLeaks: Implication for the Future of Communications, Journalism and Society*. New York: Palgrave MacMillan, 2013.

Breylan Communications. “What are some of the Different Kinds of Servers?”. Accessed July 9, 2015. breylancommunications.com/productsupport/5/what_are_some_of_the_different_kinds_of_servers.php.

British Army. “77th Brigade.”. Accessed February 27, 2016. army.mod.uk/structure/39492.aspx.

———. *Army Doctrine Publication: Operations*. Shrivenham: Development, Concepts and Doctrine Centre, 2010.

British Army Headquarters Land Warfare Centre. *Doctrine Note 07/08: The Coordination of Key Leader Engagement*. Warminster: Land Warfare Centre, 2008.

Brownsword, Roger, Eloise Scotford, and Karen Yeung, eds. *The Oxford Handbook of Law, Regulation and Technology*. 1st ed. Oxford: Oxford University Press, 2017.

Buchanan, Ben. “Cyber Deterrence Isn’t MAD; it’s Mosaic.” *Georgetown Journal of International Affairs* (2014): 130-140.

———. “Cyber Deterrence Isn’t MAD; it’s Mosaic.” *Georgetown Journal of International Affairs* (2014): 130-140.

Bunk, Joost R. H. “The Protection of Intellectual Property in Cyber-Space Under International Humanitarian Law during Cyber Operations.” Master, Leiden Law School, 2016.

Bush, George W. “The National Security Strategy of the United States of America.”. state.gov/documents/organisation/63562.pdf.

Butler, Lee. “At the End of the Journey: The Risks of Cold War Thinking in a New Era.” *International Affairs (Royal Institute of International Affairs 1944-)* 82, no. 4 (2006): 763-769.

Buzan, Barry and Lene Hansen. *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, 2009.

Cabinet Office United Kingdom. “Britain’s Cyber Security Bolstered by World-Class Strategy.”. Accessed June 27, 2018. gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy.

———. *A Strong Britain in an Age of Uncertainty: The National Security Strategy*. London: The Stationary Office, 2010.

Campen, Alan D. *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax: AFCEA International Press, 1992.

Carden, Michael J. “Cyber Task Force Passes Mission to Cyber Command.”. Accessed November 14, 2013. defense.gov/News/NewsArticle.aspx?ID=60755.

Carment, David and Albrecht Schnabel, eds. *Conflict Prevention: Path to Peace Or Grand Illusion?*. New York: United Nations University Press, 2003.

Carr, Edward H. *The Twenty Years’ Crisis 1919-1939: An Introduction to the Study of International Relations*. 2nd ed. London: MacMillan & Co. Ltd., 1946.

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. 2nd ed. Farnham: O’Reilly, 2012.

Carrier, Richard. “Some Reflections on the Fighting Power of the Italian Army in North Africa, 1940– 1943.” *War in History* 22, no. 4 (2015): 503-528.

Casengo. “How to WhatsApp Your Way into Extraordinary Customer Service.”. Accessed August 26, 2015. casengo.com/blog/how-to-whatsapp-your-way-into-extraordinary-customer-service/.

Cassese, Antonio, ed. *Realizing Utopia: The Future of International Law*. Oxford: Oxford University Press, 2012.

Castells, Manuel. *The Information Age: Economy, Society, and Culture*. 2nd ed. 2010.

———. *The Rise of the Network Society, the Information Age: Economy, Society, and Culture*. Chichester: Wiley-Blackwell, 2010.

Castells, Manuel. “Globalisation, Networking, Urbanisation: Reflections on the Spatial Dynamics of the Information Age.” *Urban Studies* 47, no. 13 (2010): 2737.

CDU/CSU Parliamentary Group. “A Security Strategy for Germany Presented at the CDU/CSU Security Conference.” Berlin, May 7, 2008.

Center for Strategic and International Studies (CSIS)*. The Cyber Index: Interantional Security Trends and Realities*. Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2013.

———.. *Net Losses: Estimating the Global Cost of Cybercrime*. Washington, D.C.: Center for Strategic and International Studies (CSIS), 2014.

———. “Significant Cyber Incidents since 2006.” CSIS. Accessed May 24, 2018. csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity.

Chairman of the Joint Chiefs of the Staff. *Memorandum of Policy no. 30: Command and Control Warfare* 1993.

Chandler, Daniel and Rod Munday. *A Dictionary of Media and Communication*. Oxford: Oxford University Press, 2011.

Chang, Frederick R. “Computer Science. is Your Computer Secure?” *Science (New York, N.Y.)* 325, no. 5940 (2009): 550.

Chapman, Gary. “An Introduction to the Revolution in Military Affairs.” *XV Amaldi Conference on Problems in Global Security* (2003).

Chen, Adrian. “The Agency.” The New York Times. Accessed February 27, 2016. nytimes.com/2015/06/07/magazine/the-agency.html?_r=0.

Cheyre, Juan Emilio. “Defence Diplomacy.” In *The Oxford Handbook of Modern Diplomacy*, edited by Cooper, Andrew F., Jorge Heine and Ramesh Thakur. Oxford: Oxford University Press, 2013.

Chong, Alan. “Smart Power and Military Force: An Introduction.” *Journal of Strategic Studies* 38, no. 3 (2015): 233-244.

Christensen, Christian. “Discourses of Technology and Liberation: State Aid to Net Activists in an Era of “Twitter Revolutions”.” *The Communication Review* 14, no. 3 (2011): 233-253.

Cisco. “Designing MPLS Extensions for Customer Edge Routers, no. 1575.” Cisco. Accessed July 9, 2015. cisco.com/en/US/products/hw/routers/ps259/prod_bulletin09186a00800921d7.html#wp30266.

———. “Understanding the Ping and Traceroute Commands.”. Accessed August 31, 2015. cisco.com/c/en/us/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html.

Clapper, James R., Marcel Lettre, and Micahel S. Rogers. *Joint Statement for the Record to the Senate Armed Services Committee: Foreign Cyber Threats to the United States*. Washington, D.C.: U.S. Senate Armed Services Committee, 2017.

Claude, Inis L. *Power and International Relations*. New York: Random House, 1962.

Claude, Inis L. “The Balance of Power Revisited.” *Review of International Studies* 15, no. 2 (1989): 77-85.

Clausewitz, Carl von. *On War*, edited by Howard, Michael, Peter Paret [Vom Kriege]. Translated by Howard, Michael and Peter Paret. Princeton: Princeton University Press, 1976.

Clifford, Catherine. “Top 10 Apps for Instant Messaging.” Entrepreneur. Accessed August 26, 2015. entrepreneur.com/article/230335.

Clingendael Conflict Research Unit*. CRU Policy Brief: How to make the Comprehensive Approach Work*. The Hague: Clingendael, 2012.

Clinton, William J. “Executive Order 13010: Critical Infrastructure Protection.” *Federal Register* 61, no. 138 (1996): 37347-37350.

———. “Presidential Decision Directive 63.” *The White House, Washington, DC* (1998).

Cohen, Eliot A. “The Mystique of U.S. Air Power.” *Foreign Affairs* 73, no. 1 (1994): 109-124.

———. “A Revolution in Warfare: Impact of Military Technologies in the Reshaping of the Armed Forces.” *Foreign Affairs* 75, no. 2 (1996): 37.

Cohn, Chuck. “A Beginner’s Guide to Establishing an Online Presence on a Budget.” Forbes. Accessed August 24, 2015. forbes.com/sites/chuckcohn/2015/03/13/a-beginners-guide-to-establishing-an-online-presence-on-a-budget/.

Coleman, Gabriella E. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. New York: Verso, 2014.

Commission du Livre Blanc sur la Défense et la Sécurité Nationale. *The French White Paper on Defence and National Security*. New York: Odile Jacob Publishing Corp., 2008.

Committee III. *Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts*. Vol. XIV. Bern: Federal Political Department, 1978.

Computer History Museum. “Fairchild’s Approach: The Planar Process.” computerhistory.org/revolution/digital-logic/12/329. Accessed October 6, 2014.

Condliffe, Jamie. “Even if You Don’t use Social Networks, they Still Know Stuff about You.” Gizmodo. Accessed July 14, 2015. gizmodo.com/even-if-you-dont-use-social-networks-they-still-know-s-1643246882.

Connolly, William E. “Taylor, Foucault, and Otherness.” *Political Theory* 13, no. 3 (1985): 365-376.

Constatin, Lucian. “Design Flaw in Intel Processors Opens Door to Rootkits Researcher Says.” PCWorld. Accessed August 31, 2015. pcworld.com/article/2965872/components-processors/design-flaw-in-intel-processors-opens-door-to-rootkits-researcher-says.html#tk.rss_security.

Consumer Reports. “Big Brother is Watching.”. Accessed July 17, 2015. consumerreports.org/cro/money/consumer-protection/big-brother-is-watching/overview/index.htm.

Cooper, Jeffrey E. “Another View of the Revolution in Military Affairs.” Carisle Barracks, U.S. Army War College, April, 1994.

Cordray III, Robert and Marc Romanych. “Mapping the Information Environment.” *Iosphere* no. Summer (2005).

Core Security. “Core Impact.” Core Security. Accessed August 10, 2017. coresecurity.com/core-impact.

Corral, Ernesto. “#badbios.” Security Artwork. Accessed August 31, 2015. securityartwork.es/2013/10/30/badbios-2/?lang=en.

Corrin, Amber. “The Other Syria Debate: Cyber Weapons.”. Accessed 30 October, 2013. fcw.com/articles/2013/09/04/cyber-weapons-syria.aspx.

Counter-Terrorism Implementation Task Force*. Report of the Working Group on Countering the use of the Internet for Terrorist Purposes*. New York: United Nations, 2009.

Coyle, Cheryl L. and Heather Vaughn. “Social Networking: Communication Revolution Or Evolution?” *Bell Labs Technical Journal* 13, no. 2 (2008): 13-17.

Crawford, James. *The International Law Commission’s Articles on State Responsibility: Introduction, Text and Commentaries*. Cambridge: Cambridge University Press, 2002.

Cronin, Blaise and Holly Crawford. “Information Warfare: Its Application in Military and Civilian Contexts.” *The Information Society* 15, no. 4 (1999).

Cull, Nicholas J. “WikiLeaks, Public Diplomacy 2.0 and the State of Digital Public Diplomacy.” *Place Branding and Public Diplomacy* 7, no. 1 (2011): 1-8.

Cyberspace, Defending America’s. “National Plan for Information Systems Protection: An Invitation to a Dialogue.” (2000).

Cys-Centrum. “Киберугроза blackenergy2/3. история атак на критическую ит инфраструктуру украины.” Cys-CentrumFebruary 10. cys-centrum.com/ru/news/black_energy_2_3.

Dahl, Robert A. “The Concept of Power.” *Behavioral Science* 2, no. 3 (1957): 201-215.

Dahl, Robert A. “A Critique of the Ruling Elite Model.” *The American Political Science Review* 52, no. 2 (1958): 463-469.

Dalton, Richard. “WikiLeaks: Diplomacy as Usual.” *The World Today* 67, no. 1 (2011): 12-13.

David, G. J. and T. R. McKeldin III, eds. *Ideas as Weapons: Influence and Perception in Modern Warfare*. Washington, D.C.: Potomac Books, 2009.

Davis, Paul K. *Effects-Based Operations: A Grand Challenge for the Analytical Community*. Santa Monica: RAND, 2001.

Davis, Paul K. “Deterrence, Influence, Cyber Attack, and Cyberwar.(Navigating Deterrence: Law, Strategy, and Security in the Twenty-First Century).” *New York University Journal of International Law and Politics* 47, no. 2 (2015): 327-355.

DB-Engines. “DB-Engines Ranking.”. Accessed July 13, 2015. db-engines.com/en/ranking.

de Neuilly, Yves Buchet. “Wikileaks, the Media, and Diplomacy.” *Genèses* 94, no. 1 (2014): 140-158.

Dekkers, Patrick, A.P, Chris Benten, and Han Dijkstra. *Advisory Report: Information as Weapon, Vector and Target*. The Hague: Ministry of Defence, 2016.

Denning, Dorothy E. “Rethinking the Cyber Domain and Deterrence.” *Joint Force Quarterly* 77, no. 2nd Quarter (2015): 8-15.

Dennys, Christian. “For Stabilisation.” *Stability: International Journal of Security & Development* 2, no. 1 (2013).

Department of Defense. *Defense Science Board Task Force on High Performance Microchip Supply*. Washington, D.C.: Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, 2005.

Department of the Air Force. *Operational Cyberspace Command “Go do” Letter*. Washington, D.C.: Office of the Chief of Staff, 2006.

Department of the Army. *Field Manual 3-12: Cyberspace and Electronic Warfare Operations*. Washington, D.C.: Department of the Army, 2017.

Department of the Army Headquarters. *Field Manual 3-38: Cyber Electromagnetic Activities*. Washington, DC.: Department of the Army, 2014.

Department of the Navy. *Forward... from the Sea: Anytime, Anywhere.* Vol. Chapter VIII: Programs 1998.

Deptula, David A. “Toward Restructuring National Security.” *Air Force Research Institute Strategic Studies Quarterly* no. Winter (2007).

Development, Concepts and Doctrine Centre. *Joint Doctrine Publication 04: Understanding*. Shrivenham: Ministry of Defence, 2010.

———. *Joint Doctrine Publication 5-00: Campaign Planning*. 2nd ed. The Development, Concepts and Doctrine Centre, 2008.

DeYoung, Karen, Ellen Nakashima and Emily Rauhala. “Trump Signed Presidential Directive Ordering Actions to Pressure North Korea.”. Accessed May 23, 2018.

Di Marzio, Giulio. “The Targeting Process: This Unknown Process (Part 1).” *NATO Rapid Deployable Corps Italy Magazine* no. 13 (2009): 11-13.

Difference Between. “Difference between Cyberspace and Internet.”. Accessed May 24, 2018. differencebetween.info/difference-between-cyberspace-and-internet.

Digeser, Peter. “The Fourth Face of Power.” *The Journal of Politics* 54, no. 4 (1992): 977-1007.

Dinstein, Yoram. *War, Aggression and Self-Defence*. 5th ed. Cambridge: Cambridge University Press, 2011.

Dixon, Robyn. “Kenyan Chief’s Twitter Feed Helps Round Up Stolen Cows and Lost Phones.” Los Angeles Times. Accessed December 23, 2015. latimes.com/world/great-reads/la-fg-c1-kenya-twitter-20150901-story.html.

Dobuzinskis, Alex and Jim Finkle. “California Hospital Makes Rare Admission of Hack.”. reuters.com/article/us-california-hospital-cyberattack-idUSKCN0VS05M.

Donner, M. “Cyberassault on Estonia.” *IEEE Security and Privacy* 5, no. 4 (2007): 4-4.

Donohue, Brian. “How Much does a Botnet Cost?” Threatpost. Accessed December 25, 2015. threatpost.com/how-much-does-botnet-cost-022813/77573/.

Dörmann, Knut. “Applicability of the Additional Protocols to Computer Network Attack.” Stockholm, ICRC, November 17-19, 2004.

———. “The Legal Situation of “Unlawful/Unprivileged Combatants”.” *Internation Review of the Red Cross* 85, no. 849 (2003).

Doverspike, Robert D., K. K. Ramakrishnan, and Chris Chase. “Structural Overview of ISP Networks.” In *Guide to Reliable Internet Services and Applications*, edited by Kalmanek, Charles R., Sudip Misra and Yang Richard Yang. London: Springer, 2010.

Drew, Dennis M. and Donald M. Snow. *Making Strategy: An Introduction to National Security Processes and Problems*. 8th ed. Maxwell Air Force Base: Air University Press, 2002.

Droege, Cordula. “Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.” *International Review of the Red Cross* 94, no. 886 (2012): 533-578.

Drucker, Peter Ferdinand. *The Age of Discontinuity: Guidelines to our Changing Society*. 3rd ed. London: Transaction Publishers, 2000.

Ducheine, PAL and Jelle Van Haaster. “Fighting Power, Targeting and Cyber Operations.” *Amsterdam Law School Research Paper* no. 2014-10 (2014).

Ducheine, Paul A. L. “The Notion of Cyber Operations.” In *Research Handbook on International Law and Cyberspace*, edited by Tsagourias, Nicholas and Russell Buchan, 211-232. Cheltenham: Edward Elgar Publisching, 2015.

Ducheine, Paul A. L., Michael N. Schmitt, and Frans P. B. Osinga. *Targeting: The Challenges of Modern Warfare*. The Hague: Asser Press, 2016.

Ducheine, Paul A. L., Jelle van Haaster, and Richard van Harskamp. “Manoeuvring and Generating Effects in the Information Environment.” In *Netherlands Annual Review of Military Studies 2017: Winning without Killing, the Strategic and Operational Utility of Non-Kinetic Capabilities in Crises*, edited by Ducheine, Paul A. L. and Frans P. B. Osinga, 155-179. The Hague: Asser Press, 2017.

Ducheine, Paul A. L. and Jelle van Haaster. “Fighting Power, Targeting and Cyber Operations.” *Cyber Conference 2014 Proceedings* (forthcoming 2014).

Ducheine, Paul Alphons Leo and Eric H. Pouw. *ISAF Operaties in Afghanistan: Oorlogsrecht, Doelbestrijding in Counterinsurgency, ROE, Mensenrechten & Ius Ad Bellum* Wolf Legal Publishers, 2010.

Ducheine, Paul and Jelle Van Haaster. “Cyber-Operaties en Militair Vermogen.” *Militaire Spectator* 182, no. 9 (2013).

———. “Fighting Power, Targeting and Cyber Operations.” Talinn, NATA CCD COE, 3-6 June, 2014.

Ducheine, Paul Alphons Leo. *Cyber Warfare : Critical Perspectives /*. ‘S-Gravenhage: ‘S-Gravenhage : T.M.C. Asser Press, 2012.

Dunlap Jr, Charles J. “Lawfare Today: A Perspective.” *Yale Journal of International Affairs* 3, (2008): 146.

Dutch Department of Defence. *Land Doctrine Publicatie Militaire Doctrine Voor Het Landoptreden (LDP-1)*. Amersfoort: Opleidings- en Trainingscentrum Operatiën, 2009.

Dutch Ministry of Defence. *The Defence Cyber Strategy*. The Hague: Dutch Ministry of Defence, 2012.

———. *Netherlands Defence Doctrine*. Den Haag: Ministerie van Defensie, 2013.

Dynel, Marta and Jan Chovanec. “Researching Interactional Forms and Participant Structures in Public and Social Media.” In *Participation in Public and Social Media Interactions*, edited by Dynel, Marta and Jan Chovanec. Amsterdam: John Benjamins Publishing Company, 2015.

Echevarria II, Antulio J. *Clausewitz and Contemporary War*. Oxford: Oxford University Press, 2007.

———. *Fourth-Generation War and Other Myths*. Carlisle Barracks: Strategic Studies Institute U.S. Army War College, 2005.

Eijndhoven, Don. “On Dutch Banking Woes and DDoS Attacks.”. Accessed January 8, 2014. argentconsulting.nl/2013/04/on-dutch-banking-woes-and-ddos-attacks/.

Electrospaces. “The Phones of the Dutch Prime Minister.”. Accessed February 27, 2016. electrospaces.blogspot.nl/2014/11/the-phones-of-dutch-prime-minister.html.

Ellis, Blake. “The Banks’ Billion-Dollar Idea.” CNN. Accessed July 17, 2015. money.cnn.com/2011/07/06/pf/banks_sell_shopping_data/.

Entrepreneur. “5 Server Operating Systems for Your Business.”. Accessed July 9, 2015. entrepreneur.com/article/200856.

Erickson, Kate. “7 Ways to Build Your Online Presence Now.”. Accessed August 24, 2015. eofire.com/7-ways-to-build-your-online-presence/.

Ernst, Douglas. “Terrorist ‘Moron’ Reveals ISIS HQ in Online Selfie.”. washingtontimes.com/news/2015/jun/4/air-force-bombs-islamic-state-hq-building-after-te/.

European Commission. *Digital Economy and Society Index*. Brussels: European Commission, 2017.

Europol. "The Relentless Growth of Cybercrime." Europol. Accessed February 15, 2018. europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime.

Eurostat. "Living Online: What the Internet is used for." Eurostat. Accessed Februar 15, 2018. ec.europa.eu/eurostat/cache/infographs/ict/bloc-1b.html.

Evans, Dave and Jake McKee. *Social Media Marketing: The Next Generation of Business Engagement*. Indianapolis: Wiley Publishing, Inc., 2010.

Everard, Jerry. *Virtual States: The Internet and the Boundaries of the Nation-State*. New York: Routledge, 2000.

Exploit Database. "Windows Exploits.". Accessed March 14, 2014. exploit-db.com/platform/?p=windows.

Facebook. "Platform Insights: Measure and Optimize Your Facebook Page Or Domain.". Accessed July 17, 2015. developers.facebook.com/docs/platforminsights.

Falliere, Nicolas, Liam O. Murchu, and Eric Chien. "W32. Stuxnet Dossier." *Symantec Security Response* (2011).

Farwell, James P. "The Media Strategy of ISIS." *Survival* 56, no. 6 (2014): 49-55.

Farwell, James P. and Rafal Rohozinski. "The New Reality of Cyber War." *Survival* 54, no. 4 (2012): 107-120.

Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. "From Data Mining to Knowledge Discovery in Databases." *AI Magazine* 17, no. 3 (1996): 37.

Federal Ministry of Defence. *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*. Bonn: Federal Ministry of Defence, 2006.

Feldman, Brian. "An Incomplete List of Every Person, Place and Institution upon which Anonymous has 'Declared War'." New York Magazine. Accessed July 27, 2017. nymag.com/selectall/2016/03/everything-upon-which-anonymous-has-declared-war.html.

Feldman, Maryann P. and Richard Florida. "The Geographic Sources of Innovation: Technological Infrastructure and Product Innovation in the United States." *Annals of the Association of American Geographers* 84, no. 2 (1994): 210-229.

Ferguson, Niall. “Power.” *Foreign Policy* no. 134 (2003): 18.

Fielding, R., J. Gettys, J. Mogul, H. Fystyk, L. Masinter, P. Leach, T. Berners-Lee, Y. Lafon, and J. F. Reschke*. Internet-Draft: Hypertext Transfer Protocol -- HTTP/1.1*. Fremont: Internet Engineering Task Force, 2007.

Financial Times*. FT Global 500*. London: Financial Times, 2017.

———.. *FT Global 500*. London: Financial Times, 2010.

———.. *FT Global 500*. London: Financial Times, 2003.

———.. *FT Global 500*. London: Financial Times, 1996.

Fingleton, Eamonn. “America the Innovative?” The New York Times. Accessed October 12, 2017. nytimes.com/2013/03/31/sunday-review/america-the-innovative.html.

Finn, Peter. *Cyber Assaults on Estonia Typify a New Battle Tactic* 2007.

Finnemore, Martha. *The Purpose of Intervention: Changing Beliefs about the use of Force*. London: Cornell University Press, 2004.

Fischer, Joan. “Protecting Electronic Borders.” *U.S. Army Intelligence and Security Command Journal* 20, no. 2 (1997).

Fisher, Tim. “Firmware.”. Accessed July 9, 2015. pcsupport.about.com/od/termsf/g/firmware.htm.

———. “Router: Everyting You Need to Know about Routers.” About Tech. Accessed July 9, 2015. pcsupport.about.com/od/componentprofiles/p/router.htm.

Fitzgerald, Mary C. “Marshal Ogarkov on Modern War: 1977-1985.” *Center for Naval Analyses* Professional Paper 443.10, (1987).

Fitzpatrick, Alex. “Facebook Monitors Your Chats for Criminal Activity [REPORT].” Mashable. Accessed July 17, 2015.

Fiverr. “Results for ‘Google Review”.”. Accessed February 27, 2016. fiverr.com/search/gigs?acmpl=1&sub_category=67&category=2&utf8=%E2%9C%93&search_in=category&source=guest-hp&locale=en&query=google+review&page=1&layout=auto.

Fleck, Dieter. *The Handbook of International Humanitarian Law*. 2nd ed. Oxford: Oxford University Press, 2006.

———. *The Handbook of International Humanitarian Law*. 3rd ed. Oxford: Oxford University Press, 2013.

Floor, J. M. G. and W. F. Van Raaij. *Marketingcommunicatiestrategie*. 5th ed. Groningen: Wolters-Noordhoff, 2006.

Forouzan, Behrouz A. *Data Communications and Networking*. 4th ed. New York: McGraw-Hill, 2007.

Foster, Richard N. *Innovation: The Attacker's Advantage*. London: MacMillan, 1986.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. 2nd ed. New York: Random House, 1995.

Fox, Liam. "Why the UK is Investing £1.9bn in Cyber Security." NewStatesman. Accessed October 31, 2018. newstatesman.com/spotlight/cyber/2018/05/why-uk-investing-19bn-cyber-security.

French, David. *Raising Churchill's Army : The British Army and the War Against Germany, 1919-1945*. Oxford: Oxford University Press, 2000.

Friedman, Thomas L. *The World is Flat: A Brief History of the Twenty-First Century*. New York: Farrar, Straus and Giroux, 2007.

Friedman, Thomas L. *The World is Flat: A Brief History of the Twenty-First Century*. 3rd ed. New York: Picador, 2007.

Frodeman, Robert, Julie Thomson Klein, Carl Mitcham, and J. Britt Holbrook, eds. *The Oxford Handbook of Interdisciplinarity*. New York: Oxford University Press, 2010.

FrontlineSMS. "The FrontlineSMS Platform." FrontlineSMS. Accessed August 11, 2017. frontlinesms.com/product.

F-Secure*. BlackEnergy & Quedagh: The Convergence of Crimeware and APT Attacks*. Helsinki: F-Secure, 2014.

———.. *The Duke: 7 Years of Russian Cyberespionage*: F-Secure, 2015.

Fuchs, Christian. *Social Media: A Critical Introduction*. Los Angeles: SAGE, 2014.

Fuchs, Christian, author. *Social Media: A Critical Introduction /*. Second edition. ed. Los Angeles: Sage, 2017.

———. *Social Media: A Critical Introduction /* Los Angeles: SAGE, 2014.

Fuller, J. F. C. *The Generalship of Ulysses S. Grant*. New York: Dodd, Mead and Company, 1929.

Fuller, John. "How Internet TV Works?" HowStuffWorks. Accessed July 13, 2015. electronics.howstuffworks.com/internet-tv2.htm.

Fung, Brian. "Cyber Command's Exploding Budget." The Washington Post. Accessed December 23, 2015. washingtonpost.com/news/the-switch/wp/2014/01/15/cyber-commands-exploding-budget-in-1-chart/.

———. "How Many Cyberattacks Hit the United States Last Year." Nextgov. Accessed January 1, 2017. nextgov.com/cybersecurity/2013/03/how-many-cyberattacks-hit-united-states-last-year/61775/.

Fung, Brian and Andrea Peterson. "The Centcom 'Hack' that Wasn't.". washingtonpost.com/news/the-switch/wp/2015/01/12/the-centcom-hack-that-wasnt/.

Gaffer on Games. "What Every Programmer Needs to Know about Game Networking.". Accessed July 13, 2015. gafferongames.com/networking-for-game-programmers/what-every-programmer-needs-to-know-about-game-networking/.

Galdi, Theodor W. "Revolution in Military Affairs? Competing Concepts, Organisational Responses, Outstanding Issues." 11. iwar.org.uk/rma/resources/rma/crs95-1170F.htm.

Gallangher, Sean. "Opposite of OPSEC: Russian Soldier Posts Selfies - from Inside Ukraine.". arstechnica.com/tech-policy/2014/08/opposite-of-opsec-russian-soldier-posts-selfies-from-inside-ukraine/.

Gallie, W. "Essentially Contested Subjects." *Proceedings of the Aristotelian Society* 56, (1956): 167.

Galrahn. "Electronic War in IAF Strike in Syria.". informationdissemination.net/2007/10/electronic-war-in-iaf-strike-in-syria.html.

Garland, H. “Design Innovations in Personal Computers.” *Computer* 10, no. 3 (1977): 24-27.

Gates, Bill. *The Internet Tidal Wave*. Redmond: Microsoft, 1995.

Gates, Robert M. *The Ultimate Insiders Story of Five Presidents and how they Won the Cold War*. New York: Touchstone, 1996.

Gaus, Gerald F. *Expert Political Judgment: How Good is it? how can we Know?*. Vol. 5 2007.

Gavin, Francis J. “Same as it Ever was: Nuclear Alarmism, Proliferation, and the Cold War.” *International Security* 34, no. 3 (2009): 7-37.

Geers, Kenneth. “The Challenge of Cyber Attack Deterrence.” *Computer Law and Security Review: The International Journal of Technology and Practice* 26, no. 3 (2010): 298-303.

Genkin, Daniel, Adi Shamir, and Eran Tromer. *RSA Key Extraction Via Low-Bandwidth Acoustic Cryptanalysis*. Tel Aviv: Tel Aviv University, 2013.

Gerbaudo, Paolo. *Tweets and the Streets: Social Media and Contemporary Activism*. London: Pluto Press, 2012.

Gertz, Bill. “User Suspended: Twitter Blocks Multiple Accounts of Somali Al-Qaeda Group during Kenya Attack.”. Accessed January 8, 2014. freebeacon.com/user-suspended/.

Gervais, Michael. “Cyber Attacks and the Laws of War.” *Berkeley Journal of International Law* 30, no. 2 (2012): 579.

Geuss, Megan. “On Average, American Get 189 Cable TV Channels and Only Watch 17.”. Accessed October 16, 2014. arstechnica.com/business/2014/05/on-average-americans-get-189-cable-tv-channels-and-only-watch-17/.

Gibbons, Glen. “FCC Fines Operator of GPS Jammer that Affected Newark Airport GBAS.” Engineering Solutions from the Global Navigation Satellite System Community. Accessed February 28, 2016. insidegnss.com/node/3676.

Gibson, William. “Burning Chrome.” *Omni* (July, 1982): 72-107.

———. *Neuromancer*. New York: Berkley Publishing Group, 1984.

Gill, Terry D. and Paul A. L. Ducheine. "Anticipatory Self-Defense in the Cyber Context." *United States Naval War College International Law Studies* 89, (2013): 438-471.

Gill, Terry D. and Dieter Fleck, eds. *The Handbook of the International Law of Military Operations*. Oxford: Oxford University Press, 2011.

Gill, Terry D., Jelle van Haaster, and Mark P. Roorda. "Some Legal and Operational Considerations regarding Remote Warfare: Drones and Cyber Warfare Revisited." In *Research Handbook on Remote Warfare*, edited by Ohlin, Jens David. Northampton: Edward Elgar Press, forthcoming 2016.

Gilpin, Robert. *War and Change in World Politics*. Cambridge: Cambridge University Press, 1983.

Gilsinan, Kathy and Krishnadec Calamur. "Did Putin Direct Russian Hacking? and Other Big Questions." The Atlantic. Accessed January 6, 2017. theatlantic.com/international/archive/2017/01/russian-hacking-trump/510689/.

Giridharadas, Anand. "Africa's Gif to Silicon Valley: How to Track a Crisis." The New York Times. Accessed December 23, 2015. nytimes.com/2010/03/14/weekinreview/14giridharadas.html.

Computer Security Act 1987, 100th Congress (1987 - 1988) H.R.145 (1987): 1.

Goel, Sharad, Jake M. Hofman, and M. Irmak Sirer. "Who does what on the Web: A Large-Scale Study of Browsing Behavior." Dublin, Association for the Advancement of Artificial Intelligence Press, June 4-7, 2012.

Goel, Sharad, Jake M. Hofman, and M. Irmak Sirer. "Who does what on the Web: A Large-Scale Study of Browsing Behavior."2012.

Golbeck, Jennifer, Cristina Robles, and Karen Turner. "Human Factors in Computing Systems CHI '11 Extended Abstracts." *Chi Ea '11* (2011): 253-262.

Goldberg, Donald. "The National Guards." *Omni Magazine* 9, no. 8 (May, 1987).

Goldstone, Jack A., Robert H. Bates, David L. Epstein, Ted Robert Gurr, Michael B. Lustik, Monty G. Marshall, Jay Ulfelder, and Mark Woodward. "A Global Model for Forecasting Political Instability." *American Journal of Political Science* 54, no. 1 (2010): 190-208.

Goodin, Dan. “Meet “badBIOS,” the Mysterious Mac and PC Malware that Jumps Airgaps.” Ars Technica. Accessed August 31, 2015. arstechnica.com/security/2013/10/meet-badbios-the-mysterious-mac-and-pc-malware-that-jumps-airgaps/.

Goodin, Robin E. and Hans-Dieter Klingemann. *A New Handbook of Political Science*. Oxford: Oxford University Press, 1996.

Goodin, Robert E. *The Oxford Handbook of Political Science*. Oxford: Oxford University Press, 2011.

Google. “Measure Learn and Grow.”. Accessed July 17, 2015. google.com/analytics/standard/.

Gorobets, Oleg. “Dropping Elephant: Inelegant Espionage.” Kaspersky. Accessed June 27, 2018. kaspersky.com/blog/dropping-elephant/15149/.

Gostev, A. “The Flame: Questions and Answers.”. Accessed October 30, 2013. securelist.com/en/blog/208193522/.

Gouré, Dan. “Is there a Military-Technical Revolution in America’s Future?” *The Washington Quarterly* 16, no. 4 (1993): 175-192.

Graham, Robert. “Sniffing.” WindowsSecurity. Accessed September 5, 2015. windowsecurity.com/whitepapers/misc/Sniffing_network_wiretap_sniffer_FAQ_.html.

Gralla, Preston and Michael Troller. *How the Internet Works*. 8th ed. Indiana: Que, 2006.

Grant, Tim J., Hein S. Venter, and Jan H. P. Eloff. “Simulating Adversarial Interactions between Intruders and System Administrators using OODA-RR.”ACM, 2007.

Gray, Chris Hables. *Post-Modern War: The New Politics of Conflict*. New York: The Guilford Press, 1997.

Gray, Colin. *Strategy for Chaos*. London: Frank Cass, 2002.

Gray, Colin S. “RMAs and the Dimensions of Strategy.” *Joint Force Quarterly* no. Autumn/Winter (1998).

———. *War, Peace and International Relations: An Introduction to Strategic History*. Oxford: Routledge, 2007.

Gray, Colin S. *Hard Power and Soft Power: The Utility of Military Force as an Instrument of Policy in the 21st Century*. Carlisle: Strategic Studies Institute, 2011.

GReAT. “Equation: The Death Star of Malware Galaxy.” Securelist. Accessed August 31, 2015. securelist.com/blog/research/68750/equation-the-death-star-of-malware-galaxy/.

———. “Introducing WhiteBear.” Kaspersky. Accessed June 27, 2018. securelist.com/introducing-whitebear/81638/.

———. “Poseidon Group: A Targeted Attack Boutique Specializing in Global Cyber-Espionage.”. securelist.com/blog/research/73673/poseidon-group-a-targeted-attack-boutique-specializing-in-global-cyber-espionage/.

Greenberg, Andy. “Darpa Turn Oculus into a Weapon for Cyberwar.” Wired. Accessed January 14, 2015. wired.com/2014/05/darpa-is-using-oculus-rift-to-prep-for-cyberwar/.

———. “Shopping for Zero-Days: A Price List for Hackers’ Secret Software Exploits.” Forbes. Accessed March 14, 2014. forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/.

Greenhouse, Linda. “Computer Security Shift is Approved by Senate.” *The New York Times* (December 24, 1987).

Greenwald, Glenn. “How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations.” The Intercept. Accessed March 1, 2014. firstlook.org/theintercept/2014/02/24/jtrig-manipulation/.

Greenwald, Glenn and Andrew Fishman. “Controversial GCHQ Unit Engaged in Domestic Law Enforcement, Online Propaganda, Psychology Research.”. Accessed February 27, 2016. theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/.

Greenwood, Christopher. “Scope of Application of Humanitarian Law.” In *The Handbook of International Humanitarian Law*, edited by Fleck, Dieter. 2nd ed., 45-78. Oxford: Oxford University Press, 2011.

Greenwood, Christopher. “The Concept of War in Modern International Law.” *International and Comparative Law Quarterly* 36, no. 2 (1987): 283-306.

Griffiths, Martin. *Fifty Key Thinkers in International Relations*. New York: Routledge, 1999.

Grimes, Roger A. “Why Internet Crime Goes Unpunished.”. infoworld.com/article/2618598/cyber-crime/why-internet-crime-goes-unpunished.html.

Group of Experts on a New Strategic Concept for Nato. *NATO 2020: Assured Security; Dynamic Engagement*. Brussels: NATO, 2010.

gsmmasten.nl. “Waar Staan De GSM En UMTS Masten in Nederland?”. Accessed February 27, 2016. gsmmasten.nl.

Guo, Jingzhi, Ham Lam Jok, Jeong Lei, Xin Guan, Hin Iong Pei, and Chao Ieong Meng. “Alibaba International: Building a Global Electronic Marketplace.” Shanghai, IEEE, 24-26 October, 2006.

Gupta, Sunil. “Impact of Sales Promotions on when, what, and how Much to Buy.” *Journal of Marketing Research : JMR* 25, no. 4 (1988): 342-355.

Guttal, Shalmali. “The Politics of Post- War/ Post- Conflict Reconstruction.” *Development* 48, no. 3 (2005): 73.

Guzzini, Stefano. “On the Measure of Power and the Power of Measure in International Relations.” *DIIS Working Paper* no. 28 (2009).

Guzzini, Stefano. “Structural Power: The Limits of Neorealist Power Analysis.” *International Organisation* 47, no. 3 (1993): 443-478.

Haas, Ernst B. “The Balance of Power: Prescription, Concept, Or Propaganda.” *World Politics* 5, no. 4 (1953): 442-477.

Haelig, Carlton G. “Contemporary Armerican Military Innovation.” *Small Wars Journal* (2017).

Hafner, Katie and John Markoff. *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. New York: Touchstone, 1992.

Hall, Todd. “An Unclear Attraction: A Critical Examination of Soft Power as an Analytical Category.” *Chinese Journal of International Politics* 3, no. 2 (2010): 189-211.

Hannah, Andrian. “Packet Sniffing Basics.” Linux Journal. Accessed September 5, 2015. linuxjournal.com/content/packet-sniffing-basics.

Hanson, Fergus and Tom Uren. “Australia’s Offensive Cyber Capability.” Australian Strategic Policy Institute. Accessed June 27, 2018. aspi.org.au/report/australias-offensive-cyber-capability.

Hanspach, Michael and Michael Goetz. “On Covert Acoustical Mesh Networks in Air.” *Journal of Communications* 8, no. 11 (2013): 758.

Harden, Leland and Bob Heyman. *Digital Engagement*. New York: Amacom, 2009.

Harris, Michael. *The End of Absence: Reclaiming what we’Ve Lost in a World of Constant Connection*. New York: Current, 2014.

Harrison Dinniss, Heather. *Cyber Warfare and the Laws of War*. Cambridge: Cambridge University Press, 2012.

———. “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives.” *Israel Law Review* 48, no. 1 (2015): 1-16.

Hart, Jeffrey. “Three Approaches to the Measurement of Power in International Relations.” *International Organisation* 30, no. 2 (1976): 289-305.

Harvey, Jan V. *Space: The Fourth Military Dimension*. Carlisle Barracks: U.S. Army War College Strategic Studies Institute, 1988.

Hathaway, Melissa and Francesca Spidalieri. *The Netherlands Cyber Readiness at a Glance*. Arlington: Potomac Institute for Policy Studies, 2017.

Hattotuwa, Sanjana. “Big Data and Peacebuilding.” *Stability : International Journal of Security and Development* 2, no. 3 (2013).

Hawkinson, J. and T. Bates*. Request for Comments 1930: Guidelines for Creation, Selection, and Registration of an Autonomous System (AS)*. Fremont: Internet Engineering Task Force, 1996.

Hayden, Michael V. “The Future of Things “Cyber”.” *Strategic Studies Quarterly* no. Spring (2011).

Heftye, Erik. “Multi-Domain Confusion: All Domains are Not Created Equal.” RealClear Defense. Accessed August 28, 2017. realcleardefense.com/articles/2017/05/26/multi-domain_confusion_all_domains_are_not_created_equal_111463.html.

Heim, Michael. *The Metaphysics of Virtual Reality*. Oxford: Oxford University Press, 1993.

Held, David and Kyle McNally, eds. *Lessons from Intervention in the 21st Century: Legality, Feasibility and Legitimacy*. Chichester: Global Policy Journal, 2015.

Henckaerts, Jean-Marie, Louise Doswald-Beck, Carolin Alvermann, Knut Dörman, and Baptiste Rolle. *Customary International Humanitarian Law*. Vol. 1: Rules. Cambridge: Cambridge University Press, 2005.

Herridge, Catherine. "Army Warns US Military Personnel on Threat to Family Members." Fox News. Accessed November 15, 2016. foxnews.com/politics/2014/10/02/army-warns-us-military-personnel-on-isis-threat-to-family-members.html.

Hess, Kenneth. "Top 10 Linux Distributions of 2015." ServerWatch. Accessed July 9, 2015. serverwatch.com/columns/article.php/3900711/The-Top-10-Linux-Server-Distributions.htm.

Hewitt, John. "New Brain Implant Tech from Blackrock is Making 'Mind Over Matter' a Reality.". Accessed January 14, 2015. extremetech.com/extreme/194935-new-brain-implant-tech-from-blackrock-is-making-mind-over-matter-a-reality.

———. "We can Now Remotely Control Paralyzed Rats, Letting them Walk again: Humans are Next.". Accessed January 14, 2015. extremetech.com/extreme/190882-we-can-now-remotely-control-paralyzed-rats-letting-them-walk-again-humans-are-next.

Hilbert, Martin*. Quantifying the Data Deluge and the Data Drought: Background Note for the World Development Report 2016*. Washington D.C.: World Bank, 2015.

Hilbert, M. and P. Lopez. "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part I: Results and Scope." *International Journal of Communication* 6, (2012): 956-979.

———. "How to Measure the World's Technological Capacity to Communicate, Store, and Compute Information Part II: Measurement Unit and Conclusions." *International Journal of Communication* 6, (2012): 936-955.

Hilbert, Martin and Priscila López. "The World's Technological Capacity to Store, Communicate, and Compute Information." *Science* 332, no. 6025 (2011): 60.

Hinkle, Katharine C. "Countermeasures in the Cyber Context: One More Thing to Worry about." *Yale Journal of International Law Online, 37, 11* 21, (2011).

Hirvelä, Arto. "Discovering how Information Warfare Distorts the Information Environment." In *Proceedings of the 5th European Conference on Information*

Warfare and Security, edited by Remenyi, Dan. Reading: Academic Conferences Limited, 2006.

Hoerni, J. A. "Method of Manufacturing Semiconductor Devices (U. S. Patent no. 3,025,589)." *IEEE Solid-State Circuits Newsletter* 12, no. 2 (2007): 41-42.

Hoffman, Frank and Michael C. Davies. "Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework." Small Wars Journal. Accessed August 28, 2017. smallwarsjournal.com/jrnl/art/joint-force-2020-and-the-human-domain-time-for-a-new-conceptual-framework.

Hofmans, Tijs. "Teenager Suspected of Crippling Dutch Banks with DDoS Attacks." Computer Weekly2018. computerweekly.com/news/252434665/Teenager-suspected-of-crippling-Dutch-banks-with-DDoS-attacks.

House, White. "Defending America's Cyberspace: National Plan for Information Systems Protection Version 1.0." (2000).

———. "Presidential Decision Directive/NSC-63, Critical Infrastructure Protection." *Retrieved August* 21, (1998): 2010.

How-to Geek. "Email: What's the Difference between POP3, IMAP, and Exchange.". Accessed July 13, 2015. howtogeek.com/99423/email-whats-the-difference-in-pop3-imap-and-exchange/.

Hruska, Joel. "How L1 and L2 CPU Caches Work, and Why they're an Essential Part of Modern Chips.". Accessed July 9, 2015. extremetech.com/extreme/188776-how-l1-and-l2-cpu-caches-work-and-why-theyre-an-essential-part-of-modern-chips.

Hsu, Kimberly and Craig Murray. *China and International Law in Cyberspace*. Washington, D.C.: U.S.-China Economic and security Review Commission Staff Report, 2014.

Hudson, Trammel, Xeno Kovah, and Corey Kallenberg. *Thunderstrike 2 Sith Strike: A MacBook Firmware Worm* 2015.

Hudspeth, Allen. "Computer Programming: From Machine Language to Artificial Intelligence.". Accessed July, 8, 2015. techopedia.com/2/28245/development/programming-tools/computer-programming-from-machine-language-to-artificial-intelligence.

Hughes, Chris. “Jihadis Threaten to Slaughter British Soldiers’ Wives and Families as Police Issue Social Media Warning.” Mirror. Accessed November 15, 2016. mirror.co.uk/news/uk-news/jihadis-threaten-slaughter-british-soldiers-6173859.

Hughes, Thomas P. “Technological Momentum.” In *Does Technology Drive History? the Dilemma of Technological Determinism*, edited by Smith, Merrit Roe and Leo Marx. 4th ed., 101-114. Cambridge: Massachusetts Institute of Technology, 1994.

Huntley, Wade L. “Rebels without a Cause: North Korea, Iran and the NPT.” *International Affairs* 82, no. 4 (2006): 723-742.

Hutchins, Eric M., Michael J. Cloppert, and Rohan M. Amin. “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.” Washington, D.C., Academic Conferences and Publishing International Limited, 17-18 March, 2011.

Ianelli, Nicholas and Aaron Hackworth. “Botnets as a Vehicle for Online Crime.” *CERT Coordination Center* 1, (2005): 15-31.

Iasiello, Emilio. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7, no. 1 (2014): 54-67.

———. “Is Cyber Deterrence an Illusory Course of Action?” *Journal of Strategic Security* 7, no. 1 (2014): 54-67.

IBM. “WebSphere Application Server.”. Accessed July 10, 2015. ibm.com/software/products/en/appserv-was.

Immunity. “Canvas.” Immunity. Accessed August 10, 2017. immunityinc.com/products/canvas/.

Indiana University. “What is Spam?”. Accessed August 26, 2015. kb.iu.edu/d/afne.

InetDaemon. “Interior Vs. Exterior Routing Protocols.”. Accessed July 9, 2015. inetdaemon.com/tutorials/internet/ip/routing/interior_vs_exterior.shtml.

Infobyte. “Evilgrade.” infobyte. Accessed August 10, 2017. github.com/infobyte/evilgrade.

Information Office of the State Council. “China’s National Defense in 2010.”. Accessed June 23, 2014. english.gov.cn/official/2011-03/31/content_1835499.htm.

———. *The Diversified Employement of China's Armed Forces*. Beijing: Information Office of the State Council, 2013.

International Committee of the Red Cross. *Commentary on the First Geneva Convention*. 2nd ed. Cambridge: Cambridge University Press, 2016.

———. *International Humanitarian Law*. Geneva: International Committee of the Red Cross, 2015.

———. *International Humanitarian Law*. Geneva: ICRC, 2015.

International Court of Justice. *Advisory Opinion of 8 July 1996: Legality of the Threat Or use of Nuclear Weapons*. The Hague: International Court of Justice, 1996.

International Criminal Tribunal for the Former Yugoslavia. *Prosecutor v Dragoljub Kunarac, Radomir Kovac and Zoran Vukovic (Judgement)*, edited by Appeals Chamber. The Hague: United nations, 2002.

International Law Association. *Final Report on the Meaning of Armed Conflict in International Law*. The Hague: International Law Association, 2010.

International Law Commission. *Draft Articles on Responsibility of States for Internationally Wrongful Acts, with Commentaries*. New York: United Nations, 2001.

International Telecommunication Union (ITU). "ICT Development Index 2017." ITU. Accessed June 25, 2018. itu.int/net4/ITU-D/idi/2017/index.html.

———. *Measuring the Information Society Report*. Vol. 1. Geneva: International Telecommunication Union, 2017.

———. *The World in 2013: ICT Facts and Figures*. Geneva: ICT Data and Statistics Division Telecommunication Development Bureau, 2013.

Internet Systems Consortium. "Bind.". Accessed July 13, 2015. isc.org/downloads/bind/.

Isode. "Interconnecting XMPP and IRC.". Accessed July 13, 2015. isode.com/whitepapers/interconnecting-xmpp-and-irc.html.

Jabareen, Yosef. "Conceptualizing " Post- Conflict Reconstruction" and " Ongoing Conflict Reconstruction" of Failed States." *International Journal of Politics, Culture, and Society* 26, no. 2 (2013): 107-125.

Jablonsky, David. *The Owl of Minerva Flies at Twilight: Doctrinal Change and Continuity and the Revolution in Military Affairs*. Carlisle Barracks: U.S. Army War College, 1994.

Jachec-Neale, Agnieszka. *The Concept of Military Objectives in International Law and Targeting Practice*. London: Routledge, 2014.

Jachtenfuchs, Markus. "The Monopoly of Legitimate Force: Denationalization, Or Business as Usual?" *European Review* 13, no. 1 (2005): 37-52.

Jana, Abjijit. "Exploring Caching in ASP.NET." Code Project. Accessed July 10, 2015. codeproject.com/Articles/29899/Exploring-Caching-in-ASP-NET.

Janczewski, Lech. *Cyber Warfare and Cyber Terrorism* IGI Global, 2007.

Janczewski, Lech J. and Andrew M. Colarik. *Cyber Warfare and Cyber Terrorism*. Hershey: Information Science Reference, 2008.

Jayaswal, Kailash. *Administring Data Centers: Servers, Storage, and Voice Over IP*. Indianapolis: Wiley Publishing, Inc., 2006.

Jenkins, Ryan. "Is Stuxnet Physical? does it Matter?" *Journal of Military Ethics* 12, no. 1 (2013): 68-79.

Jobe, Nicole. *Instituionalizing the Human Domain: Being Penny Wise and Pound Wise*. Fort Eustis: United States Army Training and Doctrine Command, 2014.

John Hopkins School of Advanced International Studies. "Conflict Prevention." John Hopkins School of Advanced International Studies. Accessed May 4, 2017. sais-jhu.edu/content/conflict-prevention.

Johnson, Barnabas. "The Cybernetics of Society: The Governance of Self and Civilization.". Accessed October 30, 2013. jurlandia.org/cybsocsum.htm.

Johnson, Thomas R. *American Cryptology during the Cold War, 1945-1989: Book II Centralizations Wins, 1960-1972*. Fort Meade: National Security Agency Center for Cryptologic History, 1995.

———. *American Cryptology during the Cold War, 1945-1989: Book IV Cryptologic Rebirth, 1981-1989*. Fort Meade: National Security Agency Center for Cryptologic History, 1995.

Joint Centre for Concepts, Doctrines and Experimentations. *Joint Concept (FRA) 01: Capstone Concept for Military Operations*. Paris: Joint Centre for Concepts, Doctrines and Experimentations, 2013.

Joint Chiefs of Staff. *Joint Publication 1: Doctrine for the Armed Forces of the United States*. Washington, DC: Joint Chiefs of Staff, 2013.

Juniper Networks. "OSPF Areas and Router Functionality Overview.". Accessed July 9, 2015. juniper.net/documentation/en_US/junos12.1/topics/concept/ospf-routing-understanding-ospf-areas-overview.html#id-11620170.

Kahl, Anne and Puig Larrauri. "Technology for Peacebuilding." *Stability: International Journal of Security & Development* 2, no. 3 (2013).

Kali. "Kali.". Accessed August 31, 2015. kali.org.

Kali Linux. "Kali Linux Tools: Passwords.". Accessed September 1, 2015. tools.kali.org/tag/passwords.

———. "What is Kali Linux.". Accessed August 31, 2015. docs.kali.org/introduction/what-is-kali-linux.

Kallenberg, Corey and Xeno Kovah. *How Many Million BIOSes would You Like to Infect?* Legbacore, 2015.

Kamal, Ahmad. *The Law of Cyber-Space an Invitation to the Table of Negotiations*. 1st ed. Geneva: United Nations Institute for Training and Research, 2005.

Kampmark, Binoy. "Cyber Warfare between Estonia and Russia." *Contemporary Review* 289, no. 1686 (2007): 288.

Kane, Ziad M. "Newsweek in 1995: Why the Internet Will Fail.". Accessed October 9, 2014. thenextweb.com/shareables/2010/02/27/newsweek-1995-buy-books-newspapers-straight-intenet-uh/.

Kaplan, Abraham. *The Conduct of Inquiry*. 4th ed. New Brunswick: Transaction Publishers, 2009.

Kaplan, Caren. "Air Power's Visual Legacy: Operation Orchard and Aerial Reconnaissance Imagery as Ruses De Guerre." *Critical Military Studies* 1, no. 1 (2015): 61-78.

Kaplan, Andreas M. and Michael Haenlein. “Users of the World, Unite! the Challenges and Opportunities of Social Media.” *Business Horizons* 53, no. 1 (0, 2010): 59-68.

Kaplan, Robert D. “The Coming Anarchy.” *World Policy Journal* 17, no. 2 (2000): 95-96.

Karim, Ahmad, Rosli Salleh, Muhammad Shiraz, Syed Shah, Irfan Awan, and Nor Anuar. “Botnet Detection Techniques: Review, Future Trends, and Issues.” *Journal of Zhejiang University SCIENCE C* 15, no. 11 (2014): 943-983.

Kaspersky. “Adwind: Malware-as-a-Service Platform that Hit More than 400.000 Users and Organisations Globally.”. kaspersky.com/about/news/virus/2016/Adwind.

———. “BlackEnergy APT Attacks in Ukraine Employ Spearphishing with Word Documents.” Kaspersky. Accessed February 10, 2017. securelist.com/blog/research/73440/blackenergy-apt-attacks-in-ukraine-employ-spearphishing-with-word-documents/.

———. “Collateral Damage: 26% of DDoS Attacks Lead to Data Loss.” Kaspersky. Accessed December 25, 2015. kaspersky.com/about/news/business/2015/Collateral-damage-26-per-cent-of-DDoS-attacks-lead-to-data-loss.

———. “Newly Discovered BlackEnergy Spear-Phishing Campaign Targets Ukrainian Entitities.” Kaspersky. Accessed February 10, 2017. usa.kaspersky.com/about-us/press-center/press-releases/2016/newly-discovered-blackenergy-spear-phishing-campaign-targets-uk.

———. “ZooPark: New Android-Based Malware Campaign Spreading through Compromised Legitimate Website.” Kaspersky. kaspersky.com/about/press-releases/2018_zoopark-new-android-based-malware.

Kavanagh, D. and D. Richards. “Departmentalism and Joined-Up Government.” *Parliamentary Affairs* 54, no. 1 (2001): 1-18.

Kelly, Heather. “The Power of One Wrong Tweet.” CNN. Accessed March 1, 2014. edition.cnn.com/2013/04/23/tech/social-media/tweet-ripple-effect/.

Kelly, Seán. *Customer Intelligence: From Data to Dialogue*. Chichester: John Wiley & Sons Ltd, 2006.

Kelly, Tim and David Souter. *The Role of Information and Communication Technologies in Postconflict Reconstruction*. Washington, D.C.: World Bank, 2014.

Khandelwal, Swati. "Here's how Hackers Stole $80 Million from Bangladesh Bank." The Hacker News. Accessed February 14, 2018. thehackernews.com/2016/03/bank-hacking-malware.html.

Khara, Kanika. "Different Types of Servers." Buzzle. Accessed July 9, 2015. buzzle.com/articles/different-types-of-servers.html.

Kitzen, Martijn. "Close Encounters of the Tribal Kind: The Implementation of Co-Option as a Tool for De-Escalation of Conflict–The Case of the Netherlands in Afghanistan's Uruzgan Province." *Journal of Strategic Studies* 35, no. 5 (2012): 713-734.

Kleffner, Jann K. "Human Rights and International Humanitarian Law: General Issues." In *The Handbook of the International Law of Military Operations*, edited by Gill, Terry D. and Dieter Fleck. Oxford: Oxford University Press, 2011.

Klout. "The Klout Score.". Accessed August 20, 2015. klout.com/corp/score.

Knibbs, Kate. "What's a Facebook Shadow Profile, and Why should You Care?" Digital Trends. Accessed July 14, 2015. digitaltrends.com/social-media/what-exactly-is-a-facebook-shadow-profile/.

Knight, Mark. "Reversing the Stabilisation Paradigm: Towards an Alternative Approach." *Stability: International Journal of Security & Development* 5, no. 1 (2016).

Knorr, Klaus. *The Power of Nations: The Political Economy of International Relations*. New York: Basic Books, 1975.

Knorr, Klaus 1911-1990. *The Power of Nations : The Political Economy of International Relations / Klaus Knorr*. New York: New York : Basic Books, 1975.

Koot, André. "Ditch Cyber Campaign.". Accessed October 30, 2013. id-use.blogspot.nl.

Korzak, Elaine. "UN GGE on Cybersecurity: The End of an Era?" The Diplomat. Accessed February 20, 2018. thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/.

Kosur, Heather M. "The Definition of a Network Router for the Non-Technical Person." Bright Hub. Accessed July 9, 2015. brighthub.com/computing/hardware/articles/51073.aspx.

Kotler, Philip and Gary Armstrong. *Principles of Marketing*. 14th ed. New York: Pearson Education, 2010.

Kovacs, Eduard. “DDOS Attack on DigiD Impacts 10 Million Dutch Users.”. Accessed October 30, 2013. news.softpedia.com/news/DDOS-Attack-on-DigiD-Impacts-10-Million-Dutch-Users-348791.shtml.

Kozierok, Charles M. “OSPF Hierarchical Topology, Areas and Router Roles.”. Accessed July 9, 2015. tcpipguide.com/free/t_OSPFHierarchicalTopologyAreasandRouterRoles-2.htm.

———. “TCP/IP Architecture and the TCP/IP Model.”. Accessed January 28, 2015. tcpipguide.com/free/t_TCPIPArchitectureandtheTCPIPModel.htm.

Krebs, Brian. “Six Nabbed for using LizardSquad Attack Tool.”. krebsonsecurity.com/tag/lizard-stresser/.

Krepinevich, Andrew F., Jr. *The Military-Technical Revolution: A Preliminary Assessment*. Washington, D.C.: Center for Strategic and Budgetary Assessments, 1992.

Krieg, Christian, Andrian Dabrowski, Heidelinde Hobel, Katharina Krombholz, and Edgar Weippl. “Hardware Malware.” In *Synthesis Lectures on Information Security, Privacy, & Trust*, edited by Bertino, Elisa and Ravi Sandhu: Morgan&Claypool Publishers, 2013.

Kuehl, Dan. “Joint Information Warfare: An Information-Age Paradigm for Jointness.” *Strategic Forum Institute for National Strategic Studies* no. 105 (March, 1997).

Kuen and Mike. “Paros.”. Accessed August 11, 2017. sourceforge.net/p/paros/wiki/Home/.

Kuhn, Markus G. “Optical Time- Domain Eavesdropping Risks of CRT Displays.” Berkeley, IEEE, 12-15 May, 2002.

Kurzweil, Ray. *The Singularity is Near: When Humans Transcend Biology*. London: Viking Penguin, 2005.

Laasme, Haly. “Estonia: Cyber Window into the Future of NATO.” *Joint Force Quarterly* no. 63 (2011): 58.

Lachow, Irving. “Cyber Terrorism: Menace Or Myth?” In *Cyber Power and National Security*, edited by Kramer, Franklin D., Stuart H. Starr and Larry K. Wentz. 1st ed., 437. Dulles: National Defense University Press, 2009.

Lancaster, Shirley J. “DIME Elements of Jihad.” Master thesis, U.S. Army War College, 2011.

Lardinois, Frederic. “Ethiopian Government Bans Skype, Google Talk and all Other VoIP Services.” Techcrunch. Accessed July 13, 2015. techcrunch.com/2012/06/14/ethiopian-government-bans-skype-google-talk-and-all-other-voip-services/.

Laswell, Harold D. and Abraham Kaplan. *Power and Society: A Framework for Political Inquiry*. New Haven: Yale University Press, 1950.

Latham, Robert, ed. *Bombs and Bandwith: The Emerging Relationship between Information Technology and Security*. New York: The New Press, 2003.

Lawand, Kathleen, Robin Coupland, and Peter Herby. *A Guide to the Legal Review of Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*. Geneva: International Committee of the Red Cross, 2006.

Laws.com. “Time Shifting.”. Accessed July 13, 2015. copyright.laws.com/time-shifting.

Lawson, Sean. “Just how Big is the Cyber Threat to the Department of Defense?” Forbes. Accessed January 3, 2017. forbes.com/sites/firewall/2010/06/04/just-how-big-is-the-cyber-threat-to-dod/#7dd5408175e3.

Lawson, Ewan. “Deterrence in Cyberspace: A Silver Bullet or a Sacred Cow?” *Philosophy & Technology* (2017).

Leake, Allan. “Database Definition.” SearchSQLServer. Accessed July 13, 2015. searchsqlserver,techtarget.com/definition/database.

Lécuyer, Christophe. “The Planar Process.” Nobelprize.org: The Official Web site of the Nobel Prize. Accessed October 6, 2014. nobelprize.org/nobel_prizes/themes/physics/lecuyer/planar.html.

Leslie, Andrew, Peter Gizewski, and Michael Rostek. “Developing a Comprehensive Approach to Canadian Forces Operations.” *Canadian Military Journal* 9, no. 1 (2007).

Levin, Nathan P. “Computational Logic.” *The Journal of Symbolic Logic* 14, no. 3 (1949): 167-172.

Levy, Jack S. “War and Peace.” In *Handbook of International Relations*, edited by Carlsnaes, Walter, Thomas Risse and Beth A. Simmons, 350-368. London: Sage, 2002.

Li, Nan. “The PLA’s Evolving Campaign Doctrine and Strategies.” In *The People’s Liberation Army in the Information Age*, edited by Mulvenon, James C. and Richard H. Yang, 146-174. Santa Monica: RAND, 1999.

Liang, Qiao and Wang Xiangsui. *Unrestricted Warfare*. Beijing: People’s Liberation Army Literature and Arts Publishing House, 1999.

Libicki, Martin. “What is Information Warfare?” *National Defense University ACIS Paper 3* (1995).

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation, 2009.

Liff, Adam P. “Cyberwar: A New ‘Absolute Weapon’? the Proliferation of Cyberwarfare Capabilities and Interstate War.” *Journal of Strategic Studies* 35, no. 3 (2012): 401-428.

Lillemose, Jacob and Mathias Kryger. “The (Re)Invention of Cyberspace.” Kunstkritikk. Accessed October 18, 2017. kunstkritikk.com/kommentar/the-reinvention-of-cyberspace/.

Limnél, Jarno. “What is Real in Cyberhype?”. Accessed October 30, 2013. infosecisland.com/blogview/23393-What-is-Real-in-Cyberhype.html.

Lind, William S., Keith Nightengale, John F. Schmitt, Joseph W. Sutton, and Gary I. Wilso. “The Changing Face of War: Into the Fourth Generation.” *Marine Corps Gazette* (October, 1989): 22-26.

Lindoff, Jenny and Magdalena Granasen. *Challenges in Utilising Key Leader Engagement in Civil-Military Operations*. Stockholm: Swedish Defence Research Agency, 2011.

Liphshiz, Cnaan. “Israeli Vice Prime minister’s Facebook, Twitter Accounts Hacked .”. Accessed January 8, 2014. jta.org/2012/11/21/news-opinion/israel-middle-east/israeli-vice-prime-ministers-facebook-twitter-accounts-hacked.

Lipovsky, Robert and Anton Cherepanov. “BlackEnergy Trojan Strikes again: Attack Ukrainian Electric Power Industry.” ESET. Accessed February 10, 2017. welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/.

Liu, Cricket and Paul Albitz. *DNS and Bind*. 3rd ed. Sebastopol, CA: O'Reilly, 1998.

Lloyd, J. W., ed. *Computational Logic Symposium Proceedings*. London: Springer-Verlag, 1990.

Lombardi, Olimpia. "What is Information?" *Foundations of Science* 9, no. 2 (2004): 105-134.

———. "What is Information?" *Foundations of Science* 9, no. 2 (2004): 105-134.

Long, Colleen. "Feds in NYC: Hackers Stole $45M in ATM Card Breach.". Accessed October 30, 2013. washingtontimes.com/news/2013/may/9/feds-nyc-hackers-stole-45m-atm-card-breach/?page=all.

Loughry, Joe and David Umphress. "Information Leakage from Optical Emanations." *ACM Transactions on Information and System Security (TISSEC)* 5, no. 3 (2002): 262-289.

Lovley, Erika. "Cyberattack Explode in Congress." Politico. Accessed January 3, 2017. politico.com/story/2010/03/cyberattacks-explode-in-congress-033987.

Lowe, Donald and Simon Ng. "Effects-Based Operations: Language, Meaning and the Effect-Based Approach." San Diego, Department of Defense Command and Control Research Program, June 2004, 2004.

Lowe, Vaughan and Antonios Tznakopoulos. "Humanitarian Intervention." Oxford Public International Law. Accessed June 6, 2018. opil.ouplaw.com/view/10.1093/law:epil/9780199231690/law-9780199231690-e306.

Lowther, Adam B. *Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century*. New York: Palgrave MacMillan, 2012.

Lukes, Steven. *Power: A Radical View*. Hong Kong: MacMillan Education Ltd, 1974.

Mac Ginty, Roger. "Against Stabilisation." *Stability: International Journal of Security & Development* 1, no. 1 (2012).

Mačák, Kubo. "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects Under International Humanitarian Law." *Israel Law Review* 48, no. 1 (2015).

Macdonald, Scot. *Propaganda and Information Warfare in the Twenty-First Century*. Oxford: Routledge, 2007.

Mack, Daniel C. and Craig Gibson, eds. *Interdisciplinarity and Academic Libraries*. Chicago: Association of College and Research Libraries, 2012.

MacLennan, Bruce J. *Principles of Programming Languages: Design, Evaluation, and Implementation*. 3rd ed. New York: Oxford University Press, 1999.

Malenkovich, Serge. "Indestructible Malware by Equation Cyberspies is Out there - but Don't Panic (Yet).". Accessed Augst 31, 2015. blog.kaspersky.com/equation-hdd-malware/7623/.

Mancini, Francesco, ed. *New Technology and the Prevention of Violence and Conflict*. New York: International Peace Institute, 2013.

Mancini, Francesco and Marie O'Reilly. "New Technology and the Prevention of Violence and Conflict." *Stability : International Journal of Security and Development* 2, no. 3 (2013): Art. 55.

Mandiant*. APT1: Exposing One of China's Cyber Espionage Units*. Milpitas: Mandiant, 2013.

Mann, Michael. "Authoritarian and Liberal Militarism: A Contribution from Comparitative and Historical Sociology." In *International Theory: Positivism and Beyond*, edited by Smith, Steve, Ken Booth and Marysia Zalewski, 221-239. Cambridge: Cambridge University Press, 1996.

———. "The Autonomous Power of the State: Its Origins, Mechanisms and Results." *European Journal of Sociology* 25, no. 2 (1984): 185-213.

———. *The Sources of Social Power: A History of Power from the Beginning to A.D. 1760*. Vol. I. Cambridge: Cambridge University Press, 1986.

———. *The Sources of Social Power: Global Empires and Revolution 1890-1945*. Vol. III. Cambridge: Cambridge University Press, 2012.

———. *The Sources of Social Power: Globalizations 1945-2011*. Vol. IV. Cambridge: Cambridge University Press, 2013.

———. *The Sources of Social Power: The Rise of Classes and Nation-States 1760-1914*. Vol. II. Cambridge: Cambridge University Press, 1993.

Mann, Michael. "The Autonomous Power of the State: Its Origins, Mechanisms and Results." In *State/Space: A Reader*, edited by Brenner, Neil, Bob Jessop, Martin Jones and Gordon MacLeod, 53-64. Oxford: Blackwell Publishing, 2003.

———. “The Sources of My Sources.” *Contemporary Sociology: A Journal of Reviews* 42, no. 4 (2013): 499-502.

Manovich, Lev. “New Media from Borges to HTML.” *The New Media Reader* (2002): 13-28.

Mansfield-Devine, Steve. “Anonymous: Serious Threat Or Mere Annoyance?” *Network Security* January, (2011): 4-10.

Marbach, William D. “Beware: Hackers at Play.” *Newsweek, September* 6, (1983): 42-48.

Marks, Joseph. “DHS Secretary Promises U.S. Will Strike Back Against Cyber Adversaries.” Nextgov. Accessed June 27, 2018. nextgov.com/cybersecurity/2018/04/dhs-secretary-promises-us-will-strike-back-against-cyber-adversaries/147521/.

Marks, Joseph. “DHS is Reshaping Federal Cybersecurity with a $1 Billion Contract.” Defense One. Accessed October 31, 2018. defenseone.com/business/2018/08/dhs-reshaping-federal-cybersecurity-1-billion-contract/150775/.

Martin, Jonathan and Alan Rappeport. “Debbie Wasserman Schultz to Resign D.N.C. Post.” The New York Times. Accessed February 8, 2017. nytimes.com/2016/07/25/us/politics/debbie-wasserman-schultz-dnc-wikileaks-emails.html.

Mastapeter, Craig W. “The Instruments of National Power: Achieving the Strategic Advantage in a Changing World.” Master, Naval Postgraduate School, 2008.

Mather, Lynn. “Law and Society.” In *The Oxford Handbook of Law and Politics*, edited by Caldeira, Gregory A., R. Daniel Kelemen and Keith E. Whittington. Oxford: Oxford University Press, 2008.

Matlack, Carol. “Cyberwar in Ukraine Falls Far Short of Russia’s Full Powers.” Bloomberg Business Week. Accessed March 11, 2014. businessweek.com/articles/2014-03-10/cyberwar-in-ukraine-falls-far-short-of-russias-full-powers.

Mattern, Janice Bially. *The Concept of Power and the (Un) Discipline of International Relations* Oxford University Press, 2008.

———. “The Concept of Power and the (Un)Discipline of International Relations.” In *The Oxford Handbook of International Relations*, edited by Reus-Smit, Christian and Duncan Snidal, 691-697, 2008.

McClelland, Charles A. “The Anticipation of International Crises: Prospects for Theory and Research.” *International Studies Quarterly* 21, no. 1 (1977): 15-38.

McCracken, Harry. “The New Klout: A Warmer, Fuzzier Bottom Line on Your Online Reputation.” Time. Accessed February 28, 2014. techland.time.com/2012/08/14/the-new-klout-a-warmer-fuzzier-bottom-line-on-your-online-reputation/.

McDonnell, John P. “National Strategic Planning: Linking DIMEFIL//PMESII to a Theory of Victory.” Master, Joint Forces Staff College: Joint Advanced Warfighting School, 2009.

McGee, Matt. “Google Analytics is Installed on More than 10 Million Websites.” Marketing Land. Accessed July 17, 2015. marketingland.com/google-analytics-is-installed-on-more-than-10-million-websites-9935.

McHugh, John and Raymond Odierno. *Army Strategic Planning Guidance*. Washington, D.C.: United States Army Headquarters, 2013.

McLeary, Paul. “Dempsey Lays Out various US Military Options in Syria.”. Accessed 30 October, 2013. defensenews.com/article/20130722/DEFREG02/307220026/Dempsey-Lays-Out-Various-US-Military-Options-Syria.

McLuhan, Marshall and Quentin Fiore. *The Medium is the Massage: An Inventory of Effects*. 3rd ed. Corte Madera, CA: Gingko Press, 2001.

Mcnamara, Robert S. “Apocalypse Soon.” *Foreign Policy* no. 148 (2005): 29-35.

Mearsheimer, John J. *The Tragedy of Great Power Politics*. New York: WW Norton & Company, 2001.

Media Temple. “What is a Whois Search?”. Accessed August 31, 2015. mediatemple.net/community/products/grid/204644530/what-is-a-whois-search.

Meinel, C. and H. Sack. “The Foundation of the Interenet: TCP/IP Reference Model.” In *Internetworking*, 29-61. Berlin: Springer-Verlag, 2013.

Melzer, Nils. “Cyberwarfare and International Law.” *United Nations Institute for Disarmament Research Resources* (2011).

———. *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. Geneva: International Committee of the Red Cross, 2009.

Menn, Joseph. “Special Report: U.S. Cyberwar Strategy Stokes Fear of Blowback.” Reuters. Accessed December 23, 2015. reuters.com/article/usa-cyberweapons-idINDEE9490AX20130510.

Merriam-Webster Dictionary. “Ability.”. Accessed November 14, 2013. merriam-webster.com/dictionary/ability.

———. “Constructive.”. Accessed August 21, 2015. merriam-webster.com/dictionary/constructive.

———. “Definition of Capability.” Merriam-Webster. Accessed August 8, 2017. merriam-webster.com/dictionary/capability.

———. “Definition of Capable.” Merriam-Webster. Accessed August 8, 2017. merriam-webster.com/dictionary/capable.

———. “Definition of Utility.” Merriam-Webster. Accessed March 8, 2017. merriam-webster.com/dictionary/utility.

———. “Destructive.”. Accessed August 21, 2015. merriam-webster.com/dictionary/destructive.

———. “Diplomatic.”. Accessed July 22, 2014. merriam-webster.com/dictionary/diplomatic.

———. “Political.”. Accessed July 22, 2014. merriam-webster.com/dictionary/diplomatic.

———. “Politics.”. Accessed July 22, 2014. merriam-webster.com/dictionary/diplomatic.

———. “Willingness.”. Accessed November 14, 2013. merriam-webster.com/dictionary/willingness.

Metz, Steven. “Strategic Landpower Task Force Research Report.”. Accessed February 18, 2015. strategicstudiesinstitute.army.mil/index.cfm/articles/STRATEGIC-LANDPOWER-TASK-FORCE/2013/10/3.

Michael Mann. “An Anatomy of Power: The Social Theory of Michael Mann.” In , edited by Hall, John A. and Ralph Schroeder, 343-396. Cambridge: Cambridge University Press, 2006.

Microsoft. “Global Catalog Servers.”. Accessed July 13, 2015. technet.microsoft.com/en-us/library/cc977998.aspx.

———. “How to use TRACERT to Troubleshoot TCP/IP Problems in Windows.”. Accessed August 31, 2015. support.microsoft.com/en-us/kb/314868.

———. “Microsoft Office Communications Server.”. Accessed July 13, 2015. technet.microsoft.com/en-us/office/ocs/bb267356.aspx.

———. “Parts of a Computer.”. Accessed July 9, 2015. windows.microsoft.com/en-us/windows/computer-parts#1TC=windows-7.

———. “Seven Ways to Get Customer Email Addresses.”. Accessed August 26, 2015. microsoft.com/en-us/business/articles/seven-ways-to-get-customer-email-addresses.

Military Tribunal V. *“Hostage Case”, the United States of America Against Wilhelm List, Et Al. (Case no. 7).* Vol. XI. Washington: United States Government Printing Office, 1950.

Miller, Daniel and Don Slater. *The Internet: An Ethnographic Approach*. Oxford: Berg, 2000.

Miller, Greg. “Is this Mind-Controlled Exoskeleton Science of Spectacle?” Wired. Accessed January 14, 2015. wired.com/2014/05/world-cup-exoskeleton-demo/.

Mimoso, Michael. “Inside NLS_933W.DLL, the Equation APT Persistence Module.” Threat Post. Accessed August 31, 2015. threatpost.com/inside-nls_933w-dll-the-equation-apt-persistence-module/111128.

Ministry of Defence. *Joint Doctrine Publication 0-01: British Defence Doctrine*. 4th ed. Shrivenham: Development, Concepts and Doctrine Centre, 2011.

Ministry of Defence (Netherlands). *Future Policy Survey: Summary and Conclusions*. The Hague: Ministry of Defence, 2010.

Ministry of Defence (United Kingdom). *Cyber Primer*. 1st ed. Shrivenham: The Development, Concepts and Doctrine Centre, 2013.

———. *Cyber Primer*. 2nd ed. Shrivenham: The Development, Concept and Doctrine Centre, 2016.

———. *Joint Doctrine Publication 0-01: UK Defence Doctrine*. 5th ed. Shrivenham: Ministry of Defence, 2014.

Ministry of Defence of the Russian Federation. *Aktual'nyye Zadachi Razvitiya Vooruzhënnykh Sil Rossiyskoy Federatsii* [The priority tasks of the development of the Armed Forces of the Russian Federation]. Moscow: Ministry of Defence of the Russian Federation, 2003.

———. *Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space* [концептуальные взгляды на деятельность вооруженных сил российской федерации в информационном пространстве]. Translated by NATO Cooperative Cyber Defence Centre of Excellence 2011.

Ministry of Foreign Affairs Security Policy Department. "A Secure Netherlands in a Secure World." Government of the Netherlands. Accessed June 23, 2014. government.nl/documents-and-publications/notes/2013/06/21/international-security-strategy.html.

Ministry of the Interior and Kingdom Relations. *The Constitution of the Kingdom of the Netherlands*. The Hague: Ministry of the Interior and Kingdom Relations, 2008.

Mitchell, Bradley. "Introduction to Client Server Networks.". Accessed May 28, 2018. lifewire.com/introduction-to-client-server-networks-817420.

Mitra, Ananda. *Digital Security: Cyber Terror and Cyber Security*. New York: Infobase Publishing, 2010.

Mohamad Johan Bin Mohd, Nasir. "A Journey through Programming Language Generations." Imperial College of Science, Technology and Medicine. Accessed July 8, 2015. doc.ic.ac.uk/~nd/surprise_96/journal/vol2/mjbn/article2.html.

Moore, G. E. "Cramming More Components onto Integrated Circuits." *Proceedings of the IEEE* 86, no. 1 (1998): 82-85.

Morçöl, Göktuğ, ed. *Handbook of Decision Making*. New York: CRC Press, 2007.

Morell, Michael and Suzanne Kelly. "Former CIA Acting Director Michael Morell: "this is the Political Equivalent of 9/11"." The Cipher Brief. Accessed February 8,

2017. thecipherbrief.com/article/exclusive/fmr-cia-acting-dir-michael-morell-political-equivalent-911-1091.

Morgenthau, Hans J. *Politics among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf, 1948.

Morgenthau, Hans J. *Dilemmas of Politics*. Chicago: University of Chicago Press, 1958.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. New York: PublicAffairs, 2011.

Morris, Kevin. “Russia’s Spy Agency Invests $1 Million in Spam-Bot Army.” The Daily Dot. Accessed February 27, 2016. dailydot.com/news/svr-spy-agency-storm-13-propaganda-bots/.

Mortimer, Caroline. “NATO to Spend 2.6 Billion on Satellites, Cyber Security and Drones.” Independent. Accessed October 31, 2018. independent.co.uk/news/world/politics/nato-to-spend-three-billion-euros-on-satellites-cyber-security-and-drones-a7651966.html.

Nakashima, Ellen. “Cyber-Command may Help Protect Civilian Networks.” Washington Post. Accessed June 27, 2018. washingtonpost.com/wp-dyn/content/article/2009/05/05/AR2009050504342.html.

Namestnikov, Yuri. “The Economics of Botnets.” *Kapersky Lab* (2009).

———. “The Economics of Botnets.” *Analysis on Viruslist.Com, Kapersky Lab* (2009).

National Coordinator for Security and Counterterrorism. *Cyber Security Assessment Netherlands 2017*. The Hague: National Coordinator for Security and Justice, 2017.

NATO Cooperative Cyber Defence Centre of Excellence. “2015 UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law.” CCD COE. Accessed July 27, 2016. ccdcoe.org/2015-un-gge-report-major-players-recommending-norms-behaviour-highlighting-aspects-international-l-0.html#footnote6_e3nqd0e.

Navy Information Operations Command. “NIOC Norfolk’s History.” United States Navy. Accessed February 8, 2016. public.navy.mil/fcc-c10f/niocnorfolk/Pages/NIOCNorfolkHistory.aspx.

William Gibson: No Maps for these Territories. Directed by Neale, Mark. New York: Docurama Films, 2000.

Nederland ICT. “Infrastructuur.”. Accessed February 27, 2016. destaatvantelecom.nl/#infrastructuur.

Negroponte, Nicholas. *Being Digital*. London: Hodder & Stoughton, 1995.

Netherlands Coordinator for Security and Counterterrorism. *Cyber Security Assessment Netherlands 2017*. The Hague: Netherlands Coordinator for Security and Counterterrorism, 2017.

Netherlands Ministry of Defence*. [Dutch] Eindrapport Verkenningen: Houvast Voor De Krijgsmacht Van De Toekomst*. Den Haag: Ministerie van Defensie, 2010.

Netherlands Ministry of Foreign Affairs*. International Security Strategy: A Secure Netherlands in a Secure World*. The Hague: Ministry of Foreign Affairs, 2013.

NetMarketShare. “Desktop Top Operating System Share Trend.”. Accessed July 9, 2015. netmarketshare.com.

———. “Mobile/Tablet Operating System Market Share.”. Accessed July 9, 2015. netmarketshare.com.

Nevill, Liam and Zoe Hawkins*. Deterrence in Cyberspace: Different Domain, Different Rules*. Barton: The Australian Strategic Policy Institute, 2016.

New, Catherine. “Beyond Card Fees: Banks Look to Sell Your Data.” Daily Finance. Accessed July 17, 2015. dailyfinance.com/2011/10/25/beyond-card-fees-banks-look-to-sell-your-data/.

Ng, Eddy, Linda Schweitzer, and Sean Lyons. “New Generation, Great Expectations: A Field Study of the Millennial Generation.” *Journal of Business and Psychology* 25, no. 2 (2010): 281-292.

nginx. “About.”. Accessed July 13, 2015. nginx.org/en/.

Nighswander, Tyler, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley. “GPS Software Attacks.” Raleigh, ACM, October 16-18, 2012.

Nmap. “About.”. Accessed March 11, 2014. nmap.org.

———. “Ncat Users’ Guide.” Nmap. Accessed August 10, 2017. nmap.org/ncat/guide/.

North Atlantic Council. The Prague Summit and NATO´s Transformation: A Reader’s Guide. Brussels: NATO Public Diplomacy Division, 2003.

North Atlantic Treaty Organisation. *Allied Administrative Publication 06: NATO Glossary of Terms and Definitions (English and French)*. Brussels: NATO Standardization Agency, 2014.

———. *Allied Administrative Publication 06: NATO Glossary of Terms and Definitions (English and French)*. Brussels: NATO Standardization Agency, 2012.

———. *Allied Joint Doctrine for Information Operations*. Edition A Version 1 ed. Brussels: NATO, 2015.

———. *Allied Joint Publication 1(D): Allied Joint Doctrine*. Brussels: Nato Standardization Agency, 2010.

———. *Allied Joint Publication 1(D): Allied Joint Doctrine*. Brussels: Nato Standardization Agency, 2017.

———. *Allied Joint Publication 3.10: Allied Joint Doctrine for Information Operations*. Brussels: North Atlantic Treaty Organisation, 2009.

———. *Allied Joint Publication-5: Allied Joint Doctrine for Operaitonal-Level Planning*. Shrivenham: The Development, Concepts and Doctrine Centre, 2013.

———. *ATP 3.2.1: Allied Land Tactics*. Brussels: North Atlantic Treaty Organisation, 2009.

———. *Bi-SC NATO Information Operations Reference Book*. Brussels: NATO, 2010.

———. "Bucharest Summit Declaration Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Bucharest on 3 April 2008.". Accessed June 30, 2014. nato.int/cps/en/natolive/official_texts_8443.htm.

———. *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*. Brussels: NATO, 2010.

Nunes, Eric, Paulo Shakarian, Gerardo I. Simari, and Andrew Ruef. *Artificial Intelligence Tools for Cyber Attribution*. New York: Springer, 2018.

Nunes, Eric, Paulo Shakarian, Gerardo I. Simari, and Andrew Ruef. "Argumentation Models for Cyber Attribution." (2016).

Nunes, Mark. "Jean Baudrillard in Cyberspace: Internet, Virtuality, and Postmodernity." *Style* 29, no. 2 (1995): 314-327.

Nurnberger, Andreas, Rudolf Seising, and Constanze Wenzel. “On the Fuzzy Interrelationships of Data, Information, Knowledge and Wisdom.” Cincinnati, The 28th North American Information Processing Society Annual Conference, June 14-17, 2009.

Nye, Joseph S. *Soft Power: The Means to Success in World Politics*. New York: PublicAffairs, 2004.

Nye, Joseph S. *Cyber Power*. Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs, 2010.

———. *The Future of Power*. 1st ed. New York: Public Affairs, 2011.

———. “Hard, Soft, and Smart Power.” In *The Oxford Handbook of Modern Diplomacy*, edited by Cooper, Andrew F., Jorge Heine and Ramesh Thakur. Oxford: Oxford University Press, 2013.

Nye, Joseph S. “Deterrence and Dissuasion in Cyberspace.” *International Security* 41, no. 3 (2016): 44-71.

———. “The Regime Complex for Managing Global Cyber Activities.” *Global Commission on Internet Governance Paper Series* 1, (2014): 5-16.

———. *Soft Power : The Means to Success in World Politics*. 1st ed. New York: PublicAffairs, 2004.

O’brien, Sean P. “Crisis Early Warning and Decision Support: Contemporary Approaches and Thoughts on Future Research.” *International Studies Review* 12, no. 1 (2010): 87-104.

Obama, Barack. *National Security Strategy of the United States*. Darby: Diane Publishing Co., 2010.

———. *National Security Strategy of the United States*. Darby: Diane Publishing Co., 2015.

Ofcom. “Time Spent Online Doubles in a Decade.” Ofcom Independent Regulator and Competition Authority for the UK Communications Industries. Accessed July 9, 2015. media.ofcom.org.uk/news/2015/time-spent-online-doubles-in-a-decade/.

Offensive Security. “Sslstrip.” Offensive Security. Accessed August 10, 2017. tools.kali.org/information-gathering/sslstrip.

———. “What is Kali Linux?” Offensive Security. Accessed August 10, 2017. docs.kali.org/introduction/what-is-kali-linux.

Office of the Chief of Naval Operations. *OPNAV Instruction 3430.26: Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W)* 1995.

———. *OPNAV Instruction 3430.26: Implementing Instrution for Information Warfare/Command and Control Warfare (IW/C2W)*. Washington, D.C.: Department of the Navy, 1995.

Ogarkov, Nikolai Vasilyevich. *Military Encyclopedic Dictionary* [военный энциклопедический словарь]. Moskow: Voyenizdat, 1983.

O’Hanlon, Micahel E. *The Science of War: Defense Budgeting, Military Technology, Logistics, and Combat Outcomes*. Princeton: Princeton University Press, 2009.

Oikarinen, J. and D. Reed*. Request for Comments 1459: Internet Relay Chat Protocol*. Fremont: Internet Engineering Task Force, 1993.

Olsthoorn, A. C. J. M. and J. H. Van der Velden. *Elementaire Communicatie*. Utrecht: ThiemeMeulenhoff, 2007.

Onderzoeksraad voor Veiligheid*. Mortierongeval Mali*. Den Haag: OVV, 2017.

Oomkes, Frank R. *Communicatieleer*. 8th ed. Amsterdam: Boom, 2003.

Open Web Application Security Project. “OWASP WebScarab Project.” OWASP. Accessed August 11, 2017. owasp.org/index.php/Category:OWASP_WebScarab_Project.

———. “OWASP Zed Attack Proxy Project.” OWASP. Accessed August 11, 2017. owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

Oppenheim, A. N. “Psychological Aspects.” In *International Relations: A Handbook of Current Theory*, edited by Light, Margot and A. J. R. Groom. 1st ed., 201-213: Bloomsbury Publishing, 2016.

Oracle. “Oracle WebLogic Server.”. Accessed July 10, 2015. oracle.com/technetwork/middleware/weblogic/overview/index-085209.html.

———. “Zend Server.”. Accessed July 10, 2015. oracle.com/technetwork/topics/php/zend-server-096314.html.

Orenstein, David. "Brown Unveils Novel Wireless Brain Sensor.". Accessed January 14, 2015. news.brown.edu/articles/2013/02/wireless.

Organisation for Economic Co-operation and Development. *Policy Coherence and Whole Government Approaches in Fragile States*. Paris: OECD, 2005.

———. *Whole of Government Approaches to Fragile States*. Paris: OECD, 2006.

Ornaghih, Alberto, Marco Valleri, Emilio Escobar and Eric Milam. "Welcome to the Ettercap Project.". Accessed August 10, 2017. ettercap.github.io/ettercap/index.html.

Osinga, Frans P. B. *Science, Strategy and War: The Strategic Theory of John Boyd*. Delft: Eburon Academic Publishers, 2005.

Osnos, Evan. "Hacking with Chinese Characteristics.". Accessed October 30, 2013. newyorker.com/online/blogs/evanosnos/2013/01/hacking-with-chinese-characteristics.html.

Ottinger, Joseph. "What is an App Server?" TheServerSide. Accessed July 20, 2015. theserverside.com/news/1363671/What-is-an-App-Server.

Owens, William and Edward Offley. *Lifting the Fog of War*. New York: John Hopkins University Press, 2001.

Owyang, Jeremiah. "Diagram: How the Air Force Responds to Blogs.". Accessed August 25, 2015. web-strategist.com/blog/2008/12/31/diagram-how-the-air-force-response-to-blogs/.

Oxford Dictionaries. "Operation.". Accessed July 14, 2015. oxforddictionaries.com/definition/english/operation.

Pagaini, Pierluigi. "Duqu 2.0: The most Sophisticated Malware Ever seen." Infosec Institute. Accessed June 27, 2018. resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/.

Paganini, Pierluigi. "Duqu 2.0: The most Sophisticated Malware Ever seen." Infosec Institute. Accessed February 25, 2016. resources.infosecinstitute.com/duqu-2-0-the-most-sophisticated-malware-ever-seen/.

Page, Mark and J. E. Spence. "Open Secrets Questionably Arrived at: The Impact of Wikileaks on Diplomacy." *Defence Studies* 11, no. 2 (2011): 234-243.

Palan, Ronen. *Global Political Economy: Contemporary Theories*. London: Routledge, 2000.

Palo Alto Networks. “What is a Denial of Service Attack (DoS)?” Palo Alto Networks. Accessed August 10, 2017. paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.

Pamphlet, Air Force. “Pamphlet 14-210.” *USAF Intelligence Targeting Guide* 1, (1998).

Paris, Roland. *At War’s End*. Cambridge: Cambridge University Press, 2004.

———. *At War’s End: Building Peace After Civil Conflict*. Cambridge: Cambridge University Press, 2004.

Paris, Roland and Timothy D. Sisk, eds. *The Dilemmas of Statebuilding: Confronting the Contradiction of Postwar Peace Operations*. New York: Routledge, 2009.

PCMag. “Definition of: Application Server.”. Accessed July 10, 2015. pcmag.com/encyclopedia/term/37926/application-server.

Pettman, Ralph. “Human Security as Global Security: Reconceptualising Strategic Studies.” *Cambridge Review of International Affairs* 18, no. 1 (2005): 137-150.

Pfleeger, Charles and Shari Pfleeger. *Security in Computing*. 4th ed. Boston: Pearson Education, 2006.

Pictet, Jean S. *The Geneva Conventions of 12 August 1949: Commentary.* Geneva: International Committee of the Red Cross, 1952.

Pildes, Richard H. “The Legal Structure of Democracy.” In: *The Oxford Handbook of Law and Politics*, edited by Caldeira, Gregory A., R. Daniel Kelemen and Keith E. Whittington. Oxford: Oxford University Press, 2008.

Pillai, Sarath. “HTTP (Hypertext Transfer Protocol) Request and Response.” [Root. in~] #:. Accessed July 13, 2015. slashroot.in/httphypertext-transfer-protocol-request-and-response.

Pilloud, Claude, Yves Sandoz, Christophe Swinarski, and Bruno Zimmermann. *Commentary on the Additional Protocols: Of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: Martinus Nijhoff Publishers, 1987.

Pirker, Benedikt. “Territorial Sovereignty and Integrity and the Challenges of Cyberspace.” In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by Ziolkowski, Katharina, 189-216. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014.

Plato. "Ἀλκιβιάδης." In *Plato with an English Translation VII*, edited by Lamb, W. London: William Heinemann Ltd., 390-342 B.C.

Podila, Pavan. "HTTP: The Protocol Every Web Developer must Know.". Accessed July 13, 2015. code.tutsplus.com/tutorials/http-the-protocol-every-web-developer-must-know-part-1--net-31177.

Poggi, Gianfranco. *Forms of Power*. Oxford: Blackwell Publishers Ltd, 2001.

Point Topic. *VoIP Statistics - Market Analysis*. London: Point Topic Ltd., 2013.

Polipo. "Polipo - a Caching Web Proxy." Université Paris Diderot. Accessed July 13, 2015. pps.univ-paris-diderot.fr/~jch/software/polipo/.

Pollard, A. F. "The Balance of Power." *Journal of the British Institute of International Affairs* 2, no. 2 (1923): 51-64.

Polsby, Nelson W. *Community Power and Political Theory*. New Haven: Yale University Press, 1963.

Polsby, Nelson W. "How to Study Community Power: The Pluralist Alternative *." *The Journal of Politics* 22, no. 3 (1960): 474-484.

PortSwigger. "Burp Suite." PortSwigger. Accessed August 11, 2017. portswigger.net/burp.

Postel, Jon. *Internet Engineering Note #2: Comments on Internet Protocol and TCP* 1977.

Powell, Colin L. "Information-Age Warriors." *Byte* no. July (1992).

Powell, Colin. "U.S. Forces: Challenges Ahead." *Foreign Affairs* 71, no. 5 (1992): 32.

Pras, Aiko, Anna Sperotto, Giovane Moura, Idilio Drago, Rafael Barbosa, Ramin Sadre, Ricardo Schmidt, and Rick Hofstede. *Technical Report 10.41: Attacks by "Anonymous" WikiLeaks Proponents Not Anonymous*. Enschede: University of Twente, Centre for Telematics and Information Technology, 2010.

Press, Larry. “Analogy between the Postal Network and TCP/IP.” California State University. Accessed July 9, 2015. bpastudio.csudh.edu/fac/lpress/471/hout/netech/postofficelayers.htm.

Pritchard, Duncan. *What is this Thing Called Knowledge?*. New York: Routledge, 2006.

Pro_girl. “Viral Promotion to 5.000.000.” Fiverr. Accessed February 27, 2016. fiverr.com/pro_girl/tweet-your-game-to-3-250-000-facebook-320k-twitter?context=advanced_search&context_type=rating&pos=4&funnel=8758f0c5-68f5-4a78-b6f6-cd8125734a82;.

Provost, Guy. “How Caching Works.” HowStuffWorks. Accessed July 13, 2015. computer.howstuffworks.com/cache4.htm.

Pufeng, Wang. “The Challenge of Information Warfare.” *Chinese Views of Future Warfare* (1997): 322-323.

———. “The Challenge of Information Warfare.” In *Chinese Views of Future Warfare*, edited by Pillsbury, Michael, 317-326. Washington: National Defense University Press, 1998.

Puri, Ramneek. “Bots & Botnet: An Overview.” *SANS Institute 2003* (2003).

Qiang, Li, Yang Ze-Ming, Liu Bao-Xu, and Jiang Zheng-Wei. “A Reasoning Method of Cyber-Attack Attributions Based on Threat Intelligence.” *International Journal of Computer and Systems Engineering* 10, no. 5 (2016).

Quester, George H. “Crises and the Unexpected.” *The Journal of Interdisciplinary History* 18, no. 4 (1988): 701-719.

Quihuis, Mark Nelson and Karen Guttieri. “Peace Technology: Scope, Scale, and Cautions.” *Building Peace* no. 5 (2015): 14-16.

Radio Free Europe/Radio Liberty. “Pylon ‘Blown Up’ in Ukraine, Causing Crimea’s Blackout.” Radio Free Europe/Radio Liberty. Accessed February 10, 2017. rferl.org/a/ukraine-crimea-black-out-state-of-emergency/27379758.html.

Raduege, Harry D. “Future Defense Department Cybersecurity Builds on the Pas.” *Signal* (February, 2008).

Ragalado, Antonio. “Military Funds Brain-Computer Interfaces to Control Feelings.” MIT Technology Review. Accessed January 14, 2015. technologyreview.com/news/527561/military-funds-brain-computer-interfaces-to-control-feelings/.

Rajnovic, Damir. “Cyberspace - what is it?”. Accessed May 24, 2018. blogs.cisco.com/security/cyberspace-what-is-it.

Rapid 7. “The Attacker’s Playbook: Test Your Network to Uncover Exploitable Security Gaps with Metasploit.”. Accessed March 14, 2014. rapid7.com/products/metasploit/.

Rathbun, Brian C. “Uncertain about Uncertainty: Understanding the Multiple Meanings of a Crucial Concept in Internetaional Relations Theory.” *International Studies Quarterly* 51, (2007): 533-557.

Rayner, Alex. “Can Google’s Deep Dream Become an Art Machine?” The Guardian. Accessed November 9, 2016. theguardian.com/artanddesign/2016/mar/28/google-deep-dream-art.

RCRWireless. “MPLS PE the Provider Edge.”. Accessed July 9, 2015. rcrwireless.com/20140513/wireless/mpls-pe.

Readhead, Harry. “Your Facebook, Twitter and Blog are about to be Monitored for References to the Government.” Metro. Accessed July 17, 2015. metro.co.uk/2015/06/05/your-facebook-twitter-and-blog-are-about-to-be-monitored-for-references-to-the-government-5232639/.

Recknagel, Charles. “Five Things You should Know about Syria and Russia’s S-300 Missile System.”. rferl.org/content/explainer-russia-syria-s-300-missile-system-/25003647.html.

Recorded Future. “#ColumbianChemical Hoax: Trolling the Gulf Coast for Deceptive Patterns.”. Accessed February 27, 2016. recordedfuture.com/columbianchemicals-hoax-analysis/.

Regidi, Asheeta. “Internet Immunity?”. firstpost.com/india/internet-immunity-why-does-india-have-an-abysmal-0-7-conviction-rate-for-cyber-crimes-2566380.html.

Reith, Mark, Clint Carr, and Gregg Gunsch. “An Examination of Digital Forensic Models.” *International Journal of Digital Evidence* 1, no. 3 (2002): 1-12.

Rekhter, Y., T. Li, and S. Hares*. Request for Comments 4271: A Border Gateway Protocol 4 (BGP-4)*. Fremont: Internet Engineering Task Force, 2006.

Repko, Allen F. *Interdisciplinary Research: Process and Theory*. 1st ed. London: Sage, 2008.

Repko, Allen F. and Rick Szostak. *Interdisciplinary Research: Process and Theory*. 3rd ed. Thousands Oaks: Sage, 2017.

Reuters. “German Cyber Agency Calls for Authority to Hack Back: Spiegel.” Reuters. Accessed June 27, 2018. reuters.com/article/us-germany-cyber/german-cyber-agency-calls-for-authority-to-hack-back-spiegel-idUSKBN1DM1XU.

———. “Ukrainian Authorities Suffer New Cyber Attacks.” Reuters. Accessed March 11, 2014. reuters.com/article/2014/03/08/us-ukraine-cricis-cyberattack-idUSBREA270FU20140308.

Reynolds, Vince. *Social Engineering: The Art of Psychological Warfare, Human Hacking, Persuasion, and Deception*. North Charleston: CreateSpace, 2016.

Rheingold, Howard. *Smart Mobs: The Next Revolution*. New York: Basic Books, 2002.

———. *The Virtual Community: Homesteading on the Electronic Frontier*. Reading: Addison-Wesley Publishing Company, 1993.

Richardson, John. “Stuxnet as Cyberwarfare: Distinction and Proportionality on the Cyber Battlefield.”. Accessed February 16, 2017. globalinvestmentwatch.com/wp-content/uploads/2011/07/Stuxnet-as-Cyberwarfare-Distinction-and-Proportionality-on-the-Cyber-Battlefield.pdf.

Rid, Thomas. “How Russia Pulled Off the Biggest Election Hack in U.S. History.” Esquire. Accessed February 8, 2017. esquire.com/news-politics/a49791/russian-dnc-emails-hacked/.

Rid, Thomas and Marc Hecker. *War 2.0: Irregular Warfare in the Inforamtion Age*. London: Praeger Security International, 2009.

Rid, Thomas and Ben Buchanan. “Attributing Cyber Attacks.” *Journal of Strategic Studies* (2014): 1-34.

Riordan, M. “The Lost History of the Transistor.” *IEEE Spectrum* 41, no. 5 (2004): 44-49.

Robert, Roe A. *Report to Accompany H.R. 145*. Washington: Committee on Science, Space, and Technology, 1987.

Roberts, Paul. “Homeland Security Warns SCADA Operators of Internet-Facing Systems.”. threatpost.com/homeland-security-warns-scada-operators-internet-facing-systems-121211/75990/.

Romanych, Marc and Robert Cordray III. “Objectives in the Information Environment.” *Iosphere* no. Winter 2006 (2006).

Rona, Thomas P. “Weapon Systems and Information War.” *Boeing Aerospace Co., Seattle, WA* (1976).

Ronfeldt, David and John Arquilla. “Networks, Netwars and the Fight for the Future.” *First Monday* 6, no. 10 (2007).

Roscini, Marco. *Cyber Operations and the use of Force in International Law*. Oxford: Oxford University Press, 2014.

Roscini, Marco. “Identifying the Problem and the Applicable Law.” In *Cyber Operations and the use of Force in International Law*. Oxford: Oxford University Press, 2014.

Rosen, Stephen Peter. “After Proliferation: What to do if More States Go Nuclear.” *Foreign Affairs* 85, no. 5 (2006): 9.

Rosenberg, J., H. Schulzrinne, G. Camarillo, A. Johnston, J. Perterson, R. Sparks, M. Handley, and E. Schooler*. Request for Comments 3261: SIP, Session Initiation Protocol*. Fremont: Internet Engineering Task Force, 2002.

Rosenzweig, Paul. *Cyber Warfare: How Conflicts in Cyberspace are Challenging America and Changing the World*. Santa Barbara: Praeger, 2013.

Rotmann, Philipp. “Toward a Realistic and Responsible Idea of Stabilisation.” *Stability: International Journal of Security & Development* 5, no. 1 (2016).

Rotmann, Philipp and Léa Steinacker*. Stabilisation: Doctrine, Organisation and Practice Lessons from Canada, the Netherlands, the United Kingdom and the United States*. The Hague: Global Public Policy Institute, 2013.

Rouse, Margaret. “Application Server Definition.” SearchSQLServer. Accessed July 9, 2015. searchsqlserver.techtarget.com/definition/application-server.

———. “Business Capability.” TechTarget. Accessed August 8, 2017. searchmicroservices.techtarget.com/definition/business-capability.

———. “Customer Intelligence (CI).” Techtarget. Accessed July 16, 2015. searchbusinessanalytics.techtarget.com/definition/customer-intelligence-CI.

———. “LAMP (Linux, Apache, MySQL, PHP).” TechTarget. Accessed July 13, 2015. searchenterpriselinux.techtarget.com/definition/LAMP.

———. “Messaging Server.” Techtarget. Accessed July 13, 2015. searchexchange.techtarget.com/definition/messaging-server.

———. “Software.” TechTarget. Accessed August 13, 2017. searchmicroservices.techtarget.com/definition/software.

———. “System Software.” Tech Target. Accessed August 9, 2017. whatis.techtarget.com/definition/system-software.

Rouse, Margaret and Matthew Haughn. “Proxy Server.” Techtarget. Accessed July 13, 2015. whatis.techtarget.com/definition/proxy-server.

Rowley, Jennifer. “What is Information?” *Information Services & use* 18, no. 4 (1998): 243.

Royal Pingdom. “IRC is Dead, Long Live IRC.”. Accessed July 13, 2015. royal.pingdom.com/2012/04/24/irc-is-dead-long-live-irc/.

Rubenking, Neil, J. “Flame Malware: Cybergeddon Or Old News?”. Accessed October 30, 2013. securitywatch.pcmag.com/security-spyware/298405-flame-malware-cybergeddon-or-old-news.

Rummel, Rudolph J. *Dimensions of Conflict Behavior within and between Nations*. Evanston: Northwestern University, 1963.

Russel, Andrew L. “OSI: The Internet that was Not.”. Accessed February 2, 2015. spectrum.ieee.org/computing/networks/osi-the-internet-that-wasnt.

Russia Today. “State of Emergency, Blackout in Russia’s Crimea After Transmission Towers in Ukraine Blown Up.”. Accessed February 10, 2017. rt.com/news/323012-crimea-blackout-lines-blown-up/.

Russian Ministry of Defense. *Conceptual Views regarding the Activities of the Armed Forces of the Russian Federation in the Information Space*. Translated by NATO Cooperative Cyber Defence Centre of Excellence. Moscow: Department of the Ministry of Defence, 2012.

Ryan, Damian and Calvin Jones. *The Best Digitial Marketing Campaings in the World: Mastering the Art of Customer Engagement*. London: KeganPage, 2011.

Safko, Lon. *The Social Media Bible: Tactics, Tools and Strategies for Business Success*. 3rd ed. New Jersey: John Wiley & Sons, 2012.

Sageman, Marc. *Leaderless Jihad: Terror Networks in the Twenty-Frist Century*. Philadelphia: University of Pennsylvania Press, 2008.

Saini, Kulbir. *Squid Proxy Server 3.1: Beginner's Guide*. Birmingham: Packt Publishing, 2011.

Saint-Andre, P. *Request for Comments 6120: Extensible Messaging and Presence Protocol (XMPP)*. Fremont: Internet Engineering Task Force, 2011.

Saint-Andre, P., Kevin Smith, and Remko Troncon. *XMPP: The Definitive Guide*. Sebastopol, CA: O'Reilly, 2009.

Salesforce Radian6. "Marketing Cloud: Radian6 Introduction.". Accessed August 20, 2015. esources.docs.salesforce.com/rel1/radian6/en-us/static/pdf/MarketingCloudRadian6Introduction.pdf.

Sanger, David E. "Iran Fights Malware Attacking Computers.". nytimes.com/2010/09/26/world/middleeast/26iran.html?_r=0.

———. "U.S. Decides to Retaliate Against China's Hacking." The New York Times. Accessed December 23, 2015. nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?_r=0.

Sarigol, Emre, David Garcia, and Frank Schweitzer. "Online Privacy as a Collective Phenomenon." Dublin, Conference on Online Social Networks, October 1-2, 2014.

Sassen, Saskia. *The Global City: New York, London, Tokyo*. Princeton, N.J: Princeton University Press, 1991.

Sathi, Arvind. *Big Data Analytics: Disruptive Technologies for Changing the Game*. Boise: MC Press, 2012.

Sauer, Frank. *Atomic Anxiety: Deterrence, Taboo and the Non-use of U.S. Nuclear Weapons*. New York: Palgrave Macmillan, 2015.

Saul, Ben and Kathleen Heath. "Cyber Terorism." In *Research Handbook on International Law and Cyberspace*, edited by Tsagourias, Nicholas and Russell Buchan, 147-167. Cheltenham: Edward Elgar Publishing, 2015.

Savage, Charlie and Emmarie Huetteman. “Manning Sentenced to 35 Years for a Pivotal Leak of U.S. Files.” The New York Times. Accessed July 27, 2017. nytimes.com/2013/08/22/us/manning-sentenced-for-leaking-government-secrets.html.

Savvius. “Ethernet Protocols and Packets.”. Accessed July 9, 2015. wildpackets.com/resources/compendium/ethernet/ethernet_packets.

Sawicki, Jana. *Disciplining Foucault: Feminism, Power, and the Body*. New York: Routledge, 1991.

Schell, Roger R. “Computer Security.” *Air University Review* (1979).

Schelling, Thomas C. *Arms and Influence: With a New Preface and Afterword*. Yale: New Haven and London Yale University Press, 2008.

Schleicher, Charles P. *Introduction to International Relations*. Englewood Cliffs: Prentice-Hall, 1954.

Schmelze, Cord. “Evaluating Governance: Effectiveness and Legitimacy in Areas of Limited Statehood.” *SFB-Governance Working Paper Series* 26, (2011).

Schmitt, Eric and Thom Shanker. “U.S. Debated Cyberwarfare in Attack Plan on Libya.”. Accessed October 30, 2013. nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html?_r=0.

Schmitt, Michael N. “Computer Network Attack and the use of Force in International Law: Thoughts on a Normative Framework.” *Columbia Journal of Transnational Law* 37, (1999): 1998-1999.

———. “The Law of Cyber Warfare: Quo Vadis?” *Stanford Law & Policy Review* 25, (2014).

———. “The Law of Cyber Warfare: Quo Vadis?” *Stanford Law & Policy Review* 25, (2014).

———. “Rewired Warfare: Rethinking the Law of Cyber Attack.” *International Review of the Red Cross* 96, no. 893 (2014): 189-206.

———. “The State of Humanitarian Law in Cyber Conflict.”. Accessed July 27, 2016. justsecurity.org/18891/state-humanitarian-law-cyber-conflict/.

———. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

———. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 2013.

———. "The" use of Force" in Cyberspace: A Reply to Dr Ziolkowski." In *Proceedings of the 4th International Conference on Cyber Conflict*, edited by Czosseck, Christian, Rain Ottis and Katharina Ziolkowski, 311-317. Tallinn: NATO CCDCOE, 2012.

———. "Wired Warfare: Computer Network Attack and Jus in Bello." *International Review of the Red Cross* 84, no. 846 (2002).

———. "Classification of Cyber Conflict." *Journal of Conflict and Security Law* 17, no. 2 (2012): 245-260.

Schnaubelt, Christopher M. "The Illusions and Delusions of Smart Power." In *Towards a Comprehensive Approach: Integrating Civilian and Military Concepts of Strategy*, edited by Schnaubelt, Christopher M. Rome: NATO Defense College, 2011.

Schneider, Gerald, Nils Petter Gleditch, and Sabine Carey. "Forecasting in International Relations." *Conflict Management and Peace Science* 28, (2011): 5-14.

Schneier, Bruce. *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*. Indianapolis: John Wiley, 2012.

Schrodt, Philip A., James Yonamine, and Benjamin E. Bagozzi. "Data-Based Computational Approaches to Forecasting Political Violence." In *Handbook of Computational Approaches to Counterterrorism*, 129-162. New York: Springer, 2013.

Schroeder, Ralph. "An Anatomy of Power: The Social Theory of Michael Mann." In , edited by Hall, John A. and Ralph Schroeder, 1-16. Cambridge: Cambridge University Press, 2005.

Schulzrinne, H., S. Casner, R. Frederick, and V. Jacobsen*. Request for Comments 3550: RTP, a Transport Protocol for Real-Time Applications*. Fremont: Internet Engineering Task Force, 2003.

Schwartz, Mathew J. "Blackhole Botnet Creator Buys Up Zero Day Exploits." Information Week. Accessed March 14, 2014. informationweek.com/security/vulnerabilities-and-threats/blackhole-botnet-creator-buys-up-zero-day-exploits/d/d-id/1108075?.

Scottish Qualifications Authority. “Types of Network Server.”. Accessed July 9, 2015. sqa.org.uk/e-learning/HardOSEss04CD/page_33.htm.

Sebastian, Z. “Security 1:1: Various Types of Network Attacks.” Symantec. Accessed September 5, 2015. symantec.com/connect/articles/security-11-part-3-various-types-network-attacks.

Second International Peace Conference. *Convention (III) Relative to the Opening of Hositlities*. The Hague: International Conferences (The Hague), 1907.

———. *Convention (IV) Respecting the Laws and Customs of War on Land*. The Hague: International Conferences (The Hague), 1907.

Security Council of the Russian Federation. “The Military Doctrine of the Russian Federation.”. Accessed June 23, 2014. scrf.gov.ru/documents/33.html.

———. *Military Doctrine Russian Federation* [ОЕННАЯ ДОКТРИНА РОССИЙСКОЙ ФЕДЕРАЦИИ]. Moscow: Security Council of the Russian Federation, 2010.

———. “Russia’s National Security Strategy to 2020.”. Accessed June 23, 2014. rustrans.wikidot.com/russia-s-national-security-strategy-to-2020.

Security Service MI5. “Cyber.” Security Service MI5. Accessed July 3, 2017. mi5.gov.uk/cyber.

Security.nl. “17-Jarige KPN-Hacker Bekent Schuld.”. Accessed October 30, 2013. security.nl/posting/35861/17-jarige+KPN-hacker+bekent+schuld.

Seese, Michael. *Scrappy Information Security*. Silicon Valley: Scrappy About, 2009.

Selyukh, Alina and Jim Finkle. “Some U.S. Utilities Say they’re Under Constant Cyber Attack.”. Accessed October 30, 2013. reuters.com/article/2013/05/21/us-cybersecurity-utilities-idUSBRE94K18V20130521?feedType=RSS&feedName=technologyNews&utm_source=feedly.

Shackelford, Scott and Amanda Craig. “Beyond the New’Digital Divide’: Analyzing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity (Forthcoming).” *Stanford Journal of International Law* 50, no. 119 (2014).

Shakarian, Paulo. “The 2008 Russian Cyber Campaign Against Georgia.” *Military Review* 91, no. 6 (2011): 63.

Shamsie, Kamila. “Malala Yousafzai: ‘it’s Hard to Kill. Maybe that’s Why His Hand was Shaking’.” The Guardian. Accessed March 1, 2014. theguardian.com/world/2013/oct/07/malala-yousafzai-hard-to-kill-taliban.

Shane, Scott and Michael S. Scmidt. “Hillary Clinton Emails Take Long Path to Controversy.”. nytimes.com/2015/08/09/us/hillary-clinton-emails-take-long-path-to-controversy.html.

Shannon, C. E. “A Mathematical Theory of Communication.” *Bell System Technical Journal* 27, no. 3 (1948): 379-423.

Shannon, Claude E. and Warren Weaver. *The Mathematical Theory of Communication*. Champaign: University of Illinois Press, 1949.

Shear, Michael D. and Matthew Rosenberg. “Released Emails Suggest the D.N.C. Derided the Sanders Campaign.” The New York Times. Accessed February 8, 2017. nytimes.com/2016/07/23/us/politics/dnc-emails-sanders-clinton.html.

Shearlaw, Maeve. “From Online Trolling to Death Threats - the War to Defend Eritrea’s Reputation.” The Guardian. Accessed June 25, 2018. theguardian.com/world/2015/aug/18/eritrea-death-threats-tolls-united-nations-social-media.

Sheftick, Gary. “TRADOC: Strategic Landpower Concept to Change Doctrine.”. Accessed February 18, 2015. army.mil/article/118432/TRADOC__Strategic_Landpower_concept_to_change_doctrine/.

Shellman, Stephen M., Brian Levey, and H. Leonard. “Countering the Adversary: Effective Policies Or a DIME a Dozen?” Chantilly, Human Social Culture Behavior Modeling Program, February 8-10, 2011.

Shirey, R. *Request for Comments 4949: Internet Security Glossary Version 2*. Fremont: Internet Engineering Task Force, 2007.

———.. *Request for Comments 4949: Internet Security Glossary, Version 2*: Internet Engineering Task Force, 2007.

Shodan Exploits. “Windows XP Exploits.” Shodan HQ. Accessed March 14, 2014. exploits.shodan.io/?q=windows+xp.

Siddique, Haroon. “Taliban and Nato-Led Forces Engage in War of Words on Twitter.” The Guardian. Accessed March 1, 2014.

Simmons, Beth. “International Law and International Relations.” In *The Oxford Handbook of Law and Politics*, edited by Caldeira, Gregory A., R. Daniel Kelemen and Keith E. Whittington. Oxford: Oxford University Press, 2008.

Simonds, Frank H. and Brooks Emeny. *The Great Powers in World Politics: International Relations and Economic Nationalism*. New York: American Book Company, 1937.

Singer, P. W. and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press, 2014.

Singer, J. D. and Melvin Small. “The Composition and Status Ordering of the International System: 1815-1940.” *World Politics* 18, no. 2 (1966): 236-282.

Sizer, Richard A. “Land Information Warfare Activity.” *Military Intelligence Professional Bulletin* (January-March, 1997).

Skaržauskienė, Aelita and Marius Kalinauskas. “The Future Potential of Internet of Things.” *Social Technologies* no. 2(1) (2012): 102-113.

Skype for Business. “Skype for Business Server.” Microsoft. Accessed July 13, 2015. products.office.com/en-us/skype-for-business/server-hybrid.

Smith, Anton K. *Turning on the Dime: Diplomacy’s Role in National Security*. Carlisle: U.S. Army War College Strategic Studies Institute, 2007.

Smith, Edward, A. *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*. Washington, D.C.: Department of Defense Command and Control Research Program, 2002.

Smith, Merrit Roe and Leo Marx. *Does Technology Drive History? the Dilemma of Technological Determinism*. 4th ed. Cambridge: Massachusetts Institute of Technology, 1994.

Smith, Rupert. *The Utility of Force: The Art of War in the Modern World*. New York: Alfred A. Knopf, 2007.

Social Engineer, inc. “Maltego.” Social Engineer, inc. Accessed August 10, 2017. social-engineer.org/framework/se-tools/computer-based/maltego/.

———. “The Social Engineering Framework.” Social Engineer, inc. Accessed August 10, 2017. social-engineer.org/framework/se-tools/computer-based/social-engineer-toolkit-set/.

Soeters, Joseph, Paul C. van Fenema, and Robert Beeres, eds. *Managing Military Organisations: Theory and Practice*. Abingdon: Routledge, 2010.

Sood, Ashish, Gareth M. James, Gerard Tellis J., and Ji Zhu. “Predicting the Path of Technological Innovation: SAW Vs. Moore, Bass, Gompertz, and Kryder.” *Marketing Science* 31, no. 6 (2012): 964-979.

Spencer, Neil. “How Much Data is Created Every Minute.”. Accessed October 30, 2013. visualnews.com/2012/06/19/how-much-data-created-every-minute/.

———. “How Much Data is Created Every Minute.”. Accessed October 30, 2013. visualnews.com/2012/06/19/how-much-data-created-every-minute/.

Spring, Michael B. “Client/Server Technology.”. Accessed May 28, 2018. encyclopedia.com/computing/news-wires-white-papers-and-books/clientserver-technology.

Spring, Tom. “Potent Skygofree Malware Packs ‘Nevere-before-seen’ Features.” Threatpost. Accessed June 27, 2018. threatpost.com/potent-skygofree-malware-packs-never-before-seen-features/129479/.

Sprout, Harold Hance and Margaret Tuttle Sprout. *Foundations of International Politics*. New Jersey: Van Nostrand, 1962.

Sputnik International. “UN Cybersecurity Report Compromises on Self-Defense Issue - Russian Official.”. Accessed July 28, 2016. sputniknews.com/politics/20150817/1025819426/UN-cybersecurity-report-compromises-on-self-defence.html.

Spykman, Nicholas John. *America’s Strategy in World Politics: The United States and the Balance of Power*. 2nd ed. New Jersey: Transaction Publishers, 2007.

Squid. “Squid: Optimising Web Delivery.”. Accessed July 13, 2015. squid-cache.org.

Standage, Tom. *Writing on the Wall: Social Media-the First 2,000 Years*. New York: Bloomsbury Publishing, 2013.

Statista. “Most Popular Online Activities of Adult Users in the Unites States 2015.”. Accessed February 15, 2018. statista.com/statistics/183910/internet-activities-of-us-users/.

Stauffacher, Daniel, William Drake, Paul Currion, and Julia Steinberger. *Communication Technology for Peace: The Role of ICT in Preventing, Responding* *to and Recovering from Conflict*. New York: The United Nations Information and Communication Technologies Task Force, 2005.

Stauffacher, Daniel, Barbara Weekes, Urs Gasser, Colin Maclay, and Michael Best, eds. *Peacebuilding in the Information Age: Sifting Hype from Reaility*. Geneva: ICT4Peace Foundation, 2011.

Steger, Manfred B. *Globalization: A very Short Introduction*. 3rd ed. Oxford: Oxford University Press, 2013.

Sterling, Bruce. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam Books, 1994.

Sterling, Greg. “Nielsen: More Time on Internet through Smartphones than PCs.” Marketing Land. Accessed July 9, 2015. marketingland.com/nielsen-time-accessing-internet-smartphones-pcs-73683.

Stewart, Bill. “IRC Channels.”. Accessed July 13, 2015. livinginternet.com/r/rw_chan.htm.

Stoll, Christopher. “The Internet? Bah!” *Newsweek* 125, no. 9 (1995): 41.

Stone, Jeff. “U.S. Confirms BlackEnergy Malware used in Ukrainian Power Plan Hack.”. ibtimes.com/us-confirms-blackenergy-malware-used-ukrainian-power-plant-hack-2263008.

Storm, Darlene. “Gauss Malware: Nation-State Cyber-Espionage Banking Trojan Related to Flame, Stuxnet.” Computerworld. Accessed June 27, 2018.

———. “Macs can be Remotely Infected with Firmware Malware that Remains After Reformatting.” Computerworld. Accessed August 31, 2015. computerworld.com/article/2955641/cybercrime-hacking/macs-can-be-remotely-infected-with-firmware-malware-that-remains-after-reformatting.html.

Strate, Lance. “The Varieties of Cyberspace: Problems in Definition and Delimitation.” *Western Journal of Communication (Includes Communication Reports)* 63, no. 3 (1999): 382-412.

Stuttard, Dafydd and Marcus Pinto. *The Web Application Hacker’s Handbook: Finding an Exploiting Security Flaws*. 2nd ed. Indianapolis: John Wiley & Sons, Inc., 2011.

Suits, Devon L. “The Borderless Threat: Army Cyber Command Helping Defend Nation’s Network.” U.S. Army. Accessed June 27, 2018. army.mil/

article/194348/the_borderless_threat_army_cyber_command_helping_defend_nations_network.

Sun Tzu. “The Art of War.” The Internet Classics Archive. Accessed August 30, 2017. classics.mit.edu/Tzu/artwar.html.

Supreme Court of the United States. *David Leon Riley, Petitioner v. California; United States, Petitioner v. Birma Wurie*, edited by Chief Justice Roberts. Vol. Nos. 18-132 and 13-212. Washington, D.C.: Supreme Court of the United States, 2014.

Suzuki, Tohru, Keita Inaba, and Junichi Takeno. “Conscious Robot that Distinguishes between Self and Others and Implements Imitation Behavior.”Springer, 2005.

Szafranski, Richard. “A Theory of Information Warfare: Preparing for 2020.” *Airpower Journal* (Spring, 1995).

Taddeo, Mariarosaria. “The Limits of Deterrence Theory in Cyberspace.” *Philosophy & Technology* (2017).

Tanase, Stefan. “Satellite Turla: APT Command and Control in the Sky.”. securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/.

Tanenbaum, Andrew S. *Modern Operating Systems*. 2nd ed. Upper Saddle River: Prentice Hall, 2001.

Tarakanov, Dmitry. “Shamoon the Wiper: Further Details (Part II).”. securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii/.

Taub, Amanda. “’Kompromat’ and the Danger of Doubt and Confusion in a Democracy.” The New York Times. Accessed February 8, 2017. nytimes.com/2017/01/15/world/europe/kompromat-donald-trump-russia-democracy.html.

TechTerms. “Firmware.”. Accessed July 9, 2015. techterms.com/definition/firmware.

Templin, Reagan. “Introduction to IIS Architectures.” Microsoft. Accessed July 10, 2015. iis.net/learn/get-started/introduction-to-iis/introduction-to-iis-architecture.

Tetlock, Philip E. *Expert Political Judgment: How Good is it? how can we Know?*. Princeton: Princeton University Press, 2005.

The Archive Team. “Friendster Snapchot Collection.” Internet Archive. Accessed July 14, 2015. archive.org/details/archive-team-friendster.

The Chairman of the Joint Chiefs of Staff. *National Military Strategic Plan for the War on Terrorism*. Washington, D.C.: The Joint Chiefs of Staff, 2006.

———. *The National Military Strategy for Cyberspace Operations*. Washington, DC: Office of the Chairman, 2006.

The CNN Wire Staff. “Congressman: A Hacker Placed Lewd Photo on Twitter Account.” CNN. Accessed March 1, 2014. edition.cnn.com/2011/POLITICS/05/30/weiner.photo/index.html.

The Comptroller General. *Report to the Chairman Committee on Government Operations House of Representatives, NORAD’s Missile Warning System: What Went Wrong?*
. Gaithersburg: United States General Accounting Office, 1981.

The Development, Concepts and Doctrine Centre. *Joint Doctrine Publication 3-45.1: Media Operations*. Shrivenham: The Development, Concepts and Doctrine Centre, 2007.

The Economist. “Economics A-Z.” The Economist. Accessed May 7, 2018. economist.com/economics-a-to-z/w.

The Guardian. “Al-Sweady Inquiry: Iraqis Mistreated but UK Troops did Not Murder Insurgents.” The Guardian. Accessed Febuary 28, 2016. theguardian.com/uk-news/2014/dec/17/al-sweady-inquiry-uk-troops-mistreated-iraqi-prisoners-not-murder.

———. “US Government Hack Stol Fingerprints of 5.6 Million Federal Employees.”. theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints.

————. “US Military’s Joint Staff Hacked as Official Point the Finger at Russia.”. theguardian.com/technology/2015/aug/06/us-military-joint-chiefs-hacked-officials-blame-russia.

The Intercept. “Snowden Archive.” The Intercept. Accessed July 27, 2017. theintercept.com/snowden-sidtoday/.

The International Committee of the Red Cross. *31st International Conference of the Red Cross and Red Crescent: International Humanitarian Law and the Challenges* *of Contremporary Armed Conflicts*. Geneva: The International Committee of the Red Cross, 2011.

The Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: Joint Chiefs of Staff, 2017.

———. *Joint and National Intelligence Support to Military Operations*. Washington, D.C.: The Joint Chiefs of Staff, 2012.

———. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. Washington, D.C.: The Joint Chiefs of Staff, 2014.

———. *Joint Publication 2-0: Joint Intelligence*. Washington, D.C.: The Joint Chiefs of Staff, 2013.

———. *Joint Publication 3-0: Joint Operations*. Washington, D.C.: The Joint Chiefs of Staff, 2017.

———. *Joint Publication 3-12 (R): Cyberspace Operations*. Washington, D.C.: The Joint Chiefs of Staff, 2013.

———. *Joint Publication 3-13.1: Electronic Warfare*. Washington, D.C.: The Joint Chiefs of Staff, 2007.

———. *Joint Publication 3-13.1: Electronic Warfare*. Washington, D.C.: The Joint Chiefs of Staff, 2012.

———. *Joint Publication 3-13: Information Operations*. Washington, D.C.: The Joint Chiefs of Staff, 20 November 2014.

———. *Joint Publication 3-13: Information Operations*. Washington, D.C.: The Joint Chiefs of Staff, 2006.

———. *Joint Publication 3-13: Joint Doctrine for Information Operations*. Washington, D.C.: The Joint Chiefs of Staff, 1998.

———. *Joint Publication 3-51: Joint Doctrine for Electronic Warfare*. Washington, D.C.: The Joint Chiefs of Staff, 2000.

———. *Joint Publication 3-60: Joint Targeting*. Washington, DC: The Joint Chiefs of Staff, 2007.

———. *Joint Publication 3-60: Joint Targeting*. Washington, DC: The Joint Chiefs of Staff, 2013.

———. *Joint Publication 5-0: Joint Operation Planning*. Washington, D.C.: The Joint Chiefs of Staff, 2011.

———. “Joint Vision 2020: America’s Military - Preparing for Tomorrow.” *Joint Force Quarterly* (2000): 57-76.

———. *Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directorates: Joint Terminology for Cyberspace Operations*. Washington, D.C.: The Joint Chiefs of Staff, 2010.

———. *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow*. Washington, DC: Office of the Chairman, 2004.

The Joint Doctrine & Concepts Centre. *Joint Warfare Publication 3-80: Information Operations*. Shrivenham: Ministry of Defence, 2002.

The Rackspace. “Five Function of Effective Social Marketing Strategy.”. Accessed August 25, 2015. rackspace.com/blog/social-marketing-strategy/.

The Secretary of the Air Force. *Air Force Mission Statement*. Washington, D.C.: Chief of Staff, United States Air Force, 2005.

———. *Establishment of and Operational COmmand for Cyberspace*. Washington, D.C.: Chief of Staff, United States Air Force, 2006.

The United States House of Representatives Committee on Appropriations. “Fiscal Year 2014 Omnibus - Department of Defense Appropriations.” The United States House of Representatives Committee on Appropriations. Accessed December 23, 2015. appropriations.house.gov/uploadedfiles/01.13.14_fy_2014_omnibus_-_defense_-_summary.pdf.

The White House. *Securing America’s Cyberspace, National Plan for Information Systems Protection: An Invitation to a Dialogue*. Washington, DC: The White House, 2000.

The World Bank. “GDP (Current US$).”. Accessed July 25, 2017. data.worldbank.org/indicator/NY.GDP.MKTP.CD?year_high_desc=true.

Thompson, Carolyn. “Innocent Man Accused of Child Pornography After Neighbor Pirates His Wifi.” The Associated Press. Accessed February 28, 2016.

huffingtonpost.com/2011/04/24/unsecured-wifi-child-pornography-innocent_n_852996.html.

Thunderbird. “What is the Difference between IMAP and POP Protocols?”. Accessed July 13, 2015. help.thunderbird.edu/content/what-difference-between-imap-and-pop-protocol.

TIbbs, Hardin*. The Global Cyber Game: Achieving Strategic Resilience in the Global Knowledge Society*. Shrivenham: Defence Academy of the United Kingdom, 2013.

Toffler, Alvin. *Powershift: Knowledge, Wealth and Violence at the Edge of the 21st Century*. New York: Bantam Books, 1990.

———. *The Third Wave: The Classic Study of Tomorrow*. New York: Bantam Books, 1980.

Toffler, Alvin and Heidi Toffler. *War and Anti-War*. London: Little, Brown and Company Limited, 1993.

Tofino Security. “Stuxnet Central.”. Accessed October 30, 2013. tofinosecurity.com/stuxnet-central.

———. “Stuxnet Central.”. Accessed September 15, 2014. tofinosecurity.com/stuxnet-central.

Tor, Uri. “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence.” *Journal of Strategic Studies* (2015): 1-26.

———. “‘Cumulative Deterrence’ as a New Paradigm for Cyber Deterrence.” *Journal of Strategic Studies* (2015): 1-26.

Torgerson, Jason W. “The Campaign of 1777: Examination of a Turning Point using DIME.” Master, U.S. Army Command and General Staff College, 2009.

Townsend, Kevin. “U.S. Cyber Command Launched DDoS Attack Against North Koreau: Report.” Security Week. Accessed 23 May, 2018. securityweek.com/us-cyber-command-launched-ddos-attack-against-north-korea-report.

Trappl, Robert. “Preface: The Cybernetics and Systems Revival.”. Accessed November 11, 2013. osgk.ac.at/emcsr/00/preface98.html.

Trenche, Emmanuel. "5 Ways to Get Customer Intelligence for Free." Business 2 Community. Accessed July 17, 2015. business2community.com/customer-experience/5-ways-get-customer-intelligence-free-0686435.

Trial Chamber. "Prosecutor v. Ramush Haradinaj, Idriz Balaj, Lahi Bahimaj (Judgement)." International Criminal Tribunal for the former Yugoslavia. Accessed June 14, 2018. icty.org/x/cases/haradinaj/tjug/en/080403.pdf.

Triggs, Rob. "What is SMS and how does it Work." Android Authority. Accessed August 28, 2015. androidauthority.com/what-is-sms-280988/.

Triggs, Robert. "What is SMS and how does it Work?" Android Authority. Accessed August 14, 2017. androidauthority.com/what-is-sms-280988/.

Tsagourias, Nicholas and Russell Buchan, eds. *Research Handbook on International Law in Cyberspace*. Cheltenham: Edward Elgar Publishing, 2015.

Tsagourias, Nicholas. "Cyber Attacks, Self- Defence and the Problem of Attribution." *Journal of Conflict and Security Law* 17, no. 2 (2012): 229-244.

Turton, William. "Lizard Squd's Xbox Live, PSN Attacks were a 'Marketing SCheme' for New DDoS Service.". Accessed December 25, 2015. dailydot.com/crime/lizard-squad-lizard-stresser-ddos-service-psn-xbox-live-sony-microsoft/.

Tweede Kamer der Staten Generaal. "Wifi-Netwerk." Tweede Kamer der Staten-Generaal. Accessed February 27, 2016. jaarverslag2011.tweedekamer.nl/informatiseren/wifi-netwerk.

Tzifakis, Nikolaos. "Post-Conflict Economic Reconstruction." Princeton. Accessed May 21, 2017. pesd.princeton.edu/?q=node/260.

U.S. Department of Defense. "Joint Task Force on Computer Network Defense Now Operational." *Office of the Assistant Secretary of Defense (Public Affairs)* no. 658-98 (December 30, 1998).

U.S. Department of Homeland Security ICS-CERT. "Alert (IR-ALERT0H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure." ICS-CERT. Accessed February 10, 2017. ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Uckelmann, Dieter, Mark Harrison, and Florian Michahelles. *Architecting the Internet of Things*. New York: Springer, 2011.

Ukraine Today. “Inside Kremlin Propaganda Machine: Russian Blogger Exposes Russia’s Internet Troll Factory.”. Accessed February 27, 2016. youtube.com/watch?v=L5w3Ib1cyJM.

Ullman, Richard H. (Richard Henry). “Redefining Security.” *International Security* 8, no. 1 (1983): 129-153.

United Nations. *Charter of the United Nations*. New York: United Nations, 1945.

United Nations Department of Economic and Social Affairs*. World Population Prospects: The 2017 Revision*. New York: United Nations, 2017.

United Nations Development Programme*. Issue Brief: Using Technologies for Conflict Prevention*. New York: United Nations Development Programme, 2012.

United Nations General Assembly*. A/70/174: Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations, 2015.

———.. *A/RES/68/243: Developments in the Field of Information and Telecommunications in the Context of International Security*. New York: United Nations, 2014.

United Nations Office on Drugs and Crime*. The use of the Internet for Terrorist Purposes*. New York: United Nations, 2012.

United States Air Force. “Air Force Pamphlet 14-210: Intelligence Targeting Guide.”. Accessed January 8, 2014. fas.org/irp/doddir/usaf/afpam14-210/part01.htm.

United States Army. *Army Doctrine Publication 3.0: Unified Land Operations*. Washington, D.C.: Department of the Army Headquarters, 2011.

———. *Army Doctrine Publication 5-0: The Operations Process*. Washington, D.C.: Department of the Army, 2012.

———. *Cyberspace Operations Concept Capability Plan 2016 2028*. Fort Eustis: The United States Training and Doctrine Command, 2010.

———. *Field Manual 3-38: Cyber Electromagnetic Activities*. Washington, D.C.: Department of the Army Headquarters, 2014.

———. *Field Manual no. 100-6: Information Operations*. Washington, DC: U.S. Government Printing Office, 1996.

United States Army Intelligence and Security Command. “The INSCOM Story.” INSCOM History Office. Accessed February 8, 2016. inscom.army.mil/organisation/History.aspx.

United States Army Training and Doctrine Command. *Handbook Number 1: A Military Guide to Terrorism in the Twenty-First Century*. Fort Leavenworth: United States Army Training and Doctrine Command, 2007.

———. *TRADOC Pamphlet 525-69: Military Operations Concept for Information Operations*. Fort Monroe: Department of the Army, 1995.

———. *The U.S. Army Study of the Human Dimension in the Future*. Ford Eustis: United States Army Training and Doctrine Command, 2008.

United States Army and United States Marine Corps. *Army Field Manual 3-24/ Marine Corps Warfighting Publication 3-33.5: Counterinsurgency*. Washington, DC: United States Army, 2006.

United States Army, United States Marine Corps, and the United States Special Operations Command. *Strategic Landpower: Winning the Clash of Wills*. Washington, D.C.: United States Army; United States Marine Corps; the United States Special Operations Command, 2013.

United States Computer Emergency Response Team. “Security Tip (ST04-015): Understanding Denial-of-Service Attacks.” US-CERT. Accessed August 10, 2017. us-cert.gov/ncas/tips/ST04-015.

United States Department of Defense. *Department of Defense Strategy for Operating in Cyberspace*. Washington DC: United States Department of Defense, 2011.

———. *Information Operations Roadmap*. Washington, D.C.: Department of Defense, 2003.

———. *Strategy for Operating in Cyberspace* 2011.

United States Department of the Air Force*. Broad Agency Announcement: Cyberspace Warfare Operations Capabilitites*, 2012.

United States General Accounting Office. *NORAD’s Missile Warning System: What Went Wrong?*. Washington: United States General Accounting Office, 1981.

Subcommittee of the Committee on Government Operations. *Special Inquiry on Invasion of Privacy.* Eighty-Ninth Congress, First sess., 1965.

United States Joint Forces Command. *Commander's Handbook for Strategic Communication and Communication Strategy*. Suffolk: U.S. Joint Warfighting Center, 2010.

United States Marine Corps Combat Development Command. *A Concept for Information Operations*. Quantico: United States Marine Corps, 2002.

United States Office of the Director of National Intelligence*. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. Washington, D.C.: United States Office of the Director of National Intelligence, 2017.

United States Presidential National Security Decision Directive 145. *National Policy on Telecommunications and Automated Information Systems Security* 1984.

United States Strategic Command. "Fact File: Joint Task Force - Computer Network Operations.". Accessed November 14, 2013. iwar.org.uk/iwar/resources/JIOC/computer-network-operations.htm.

University of Southern California. "Organizing Your Social Sciences Research Paper: The Literature Review." University of Southern California. Accessed June 1, 2017. libguides.usc.edu/c.php?g=235034&p=1559822.

Valentino-DeVries, Jennifer, Lam T. Vo and Danny Yadron. "Cataloging the World's Cyberforces." The Wall Street Journal. Accessed July 28, 2017. graphics.wsj.com/world-catalogue-cyberwar-tools/.

Valve. "Source Multiplayer Networking.". Accessed July 13, 2015. developer.valvesoftware.com/wiki/Source_Multiplayer_Networking.

Van Beijnum, Iljitch. *Bgp*. Sebastopol, CA: O'Reilly, 2002.

———. "What is BGP, Anyway?". Accessed July 9, 2015. bgpexpert.com/what.php.

Van Creveld, Martin. *The Changing Face of War: Lessons of Combat, from the Marne to Iraq*. New York: Ballantine Books, 2006.

———. *The Rise and Decline of the State*. Cambridge: Cambridge University Press, 1999.

van den Bosch, Bart. "Non-Kinetic Capabilities and the Threshold of Attack in the Law of Armed Conflict." In *Netherlands Annual Review of Military Studies 2017: Winning without Killing, the Strategic and Operational Utility of Non-Kinetic*

Capabilities in Crises, edited by Ducheine, Paul A. L. and Frans P. B. Osinga, 255-273. The Hague: Asser Press, 2017.

———. "War without Violence: An Analysis of Rules of International Humanitarian Law Applicable to the Military Cyber Operations Below the Threshold of Attack." Ph.D., Netherlands Defence Academy and University of Amsterdam, 2018.

Van Dijk, Jan. *The Network Society*. 2nd ed. London: SAGE Publications LtD, 2006.

van Haaster, Jelle. "Assessing Cyber Power." Tallinn, NATO CCD COE, 2016.

van Haaster, Jelle, Rickey Gevers, and Martijn Sprengers. *Cyber Guerilla*. Boston: Syngress, 2016.

van Haaster, Jelle and Mark P. Roorda. "D-Day's Demise: The Impact of Hybrid Warfare on Traditional Operational Rationale." *Militaire Spectator* 185, no. 4 (2016): 175-185.

vBulletin. "Forums, Topics and Posts.". Accessed August 26, 2015. vbulletin.com/forum/help?faq=vb3_board_usage#faq_vb3_forums_threads_posts.

Veldt, David. "Is LinkedIn the Creepiest Social Network?" Gizmodo. Accessed July 14, 2015. gizmodo.com/is-linkedin-the-creepiest-social-network-498946693.

Ventre, Daniel. *Information Warfare*. 2nd ed. London: Wiley, 2016.

Vergun, David. "Operators Shift to Cyber Electromagnetic Activities." U.S. Army. Accessed November 25, 2016. army.mil/article/165494.

Voetelink, J. "Lawfare." *Militair Rechtelijk Tijdschrift* 106, no. 3 (2013): 69-79.

Vogt, Ryan, John Aycock, and Michael J. Jacobson Jr. "Army of Botnets." *Network and Distributed System Security Symposium* no. February (2007).

Volchek, Dmitry and Daisy Sindelar. "One Professional Russian Troll Tells all." Radio Free Europe Radio Liberty. Accessed February 27, 2016. rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html.

Wachanga, D. N. "Participatory Culture in an Emerging Information Ecosystem: Lessons from Ushahidi." *South African Journal for Communication Theory and Research* 38, no. 2 (2012): 195-212.

Walter, Chip. "Kryder's Law." *Scientific American* 293, no. 2 (2005): 32.

Warner, Michael. “Cybersecurity: A Pre-History.” *Intelligence and National Security* 27, no. 5 (2012): 781-799.

Watson, Gaving, Andrew Mason, and Richard Ackroyd. *Social Engineering Penetration Testing*. Boston: Syngress, 2014.

Watts, Barry D. *The Maturing Revolution in Military Affairs*. Washington, D.C.: Center for Strategic and Budgetary Assessments, 2011.

Weaver, Warren. “The Mathematics of Communication.” In *Communication Theory*, edited by Mortensen, David C. 2nd ed., 27-38. New Brunswick: Transaction Publishers, 2008.

Weber, Max. “Politics as a Vocation.” Chap. Hans H. C. Wright Mills, In *From Max Weber: Essays in Sociology*, edited by Gerth, Hans H. and Charles Wright Mills. London: Routledge, 1918.

Webster, Frank. *Theories of the Information Society*. 4th ed. London: Routledge, 2014.

Wedgwoord, Janet E., Alicia Ruvinsky, and Timothy Siedlecki. “What Lies Beneath: Forecast Transparency to Foster Understanding and Trus in Forecast Models.” In *Advances in Human Factors and Ergonomics Series*, edited by Salvendy, Gavriel and Waldemar Karwowski, 64-73. New York: CRC Press, 2010.

Wei, Wang. “Hackers Steal $60 Million from Taiwanese Bank; Two Suspects Arrested.” The Hacker News. Accessed February 14, 2018. thehackernews.com/2017/10/swift-bank-hacking.html.

Weinberger, Sharon. “How Israel Spoofed Syria’s Air Defense System.”. wired.com/2007/10/how-israel-spoo/.

West, Richard and Lynn H. Turner. *Understanding Interpersonal Communication: Making Choices in Changing TImes*. 2nd ed. Boston: Wadsworth Cengage Learning, 2009.

Wetteroth, Debbra. *Reference Model for Telecommunications*. New York: McGraw-Hill, 2003.

What Is RSS. “RSS Explained.”. Accessed August 28, 2015. whatisrss.com.

White, Stephen K. “Foucault’s Challenge to Critical Theory.” *The American Political Science Review* 80, no. 2 (1986): 419-432.

Wiener, Norbert. *The Cybernetics of Society: The Governance of Self and Civilization*. Cambridge: M.I.T. Press, 1948.

Wight, Martin. *Power Politics*, edited by Bull, Hedley, Carsten Holbraad. 2nd ed. London: Bull, Hedley; Holbraad, Carsten, 1986.

WikiLeaks. "Hillary Clinton Email Archive." WikiLeaks. Accessed February 8, 2017. wikileaks.org/clinton-emails/.

———. "The Podesta Emails." WikiLeaks. Accessed February 8, 2017. wikileaks.org/podesta-emails/.

———. "What is WikiLeaks." WikiLeaks. Accessed July 27, 2017. wikileaks.org/What-is-Wikileaks.html.

Wilhoit, Kyle. "KillDisk and BlackEnergy are Not just Energy Sectory Threats." Trend Micro. Accessed February 10, 2017. blog.trendmicro.com/trendlabs-security-intelligence/killdisk-and-blackenergy-are-not-just-energy-sector-threats/.

Wilson, Mark. "LightEater Malware Attack Places Millions of Unpatched BIOSes at Risk." Beta News. Accessed August 31, 2015. betanews.com/2015/03/21/lighteater-malware-attack-places-millions-of-unpatched-bioses-at-risk/.

Winston, Brian. *Media, Technology and Society, a History: From the Telegraph to the Internet*. London: Routledge, 1998.

Wolfers, Arnold. "" National Security" as an Ambiguous Symbol." *Political Science Quarterly : PSQ ; the Journal Public and International Affairs* 67, no. 4 (1952): 481-502.

———. "The Pole of Power and the Pole of Indifference." *World Politics* 4, no. 1 (1951): 39-63.

Wolff, Francis, Chris Papachristou, Swarup Bhunia, and Rajat S. Chakraborty. "Towards Trojan-Free Trusted ICs: Problem Analysis and Detection Scheme." Munich, ACM, March 10-14, 2008.

Woodford, Chris. "Iptv.". Accessed July 13, 2015. explainthatstuff.com/how-iptv-works.html.

Worley, Robert D. *Orchestrating the Instruments of Power: A Critical Examination of the U.S. National Security System*. Raleigh: Lulu Press, 2012.

Wright, Quincy. *A Study of War: Volume II*. Chicago: The University of Chicago Press, 1942.

———. *A Study of War: Volume II.* Chicago: The University of Chicago Press, 1942.

Wyler, Grace. "AP Twitter Hacked, Claims Barack Obama Injured in White House Explosions

.". Accessed January 8, 2014. businessinsider.com/ap-hacked-obama-injured-white-house-explosions-2013-4.

XMPP Standards Foundation. "About.". Accessed July 13, 2015. xmpp.org/about-xmpp/.

Yapp, Chris. "What is Information?" *Itnow* 53, no. 2 (2011): 18-18.

Yoshimi, Shunya. "Information." *Theory, Culture & Society* 23, no. 2 (2006): 271.

Young, Orna and Enda Young*. Technology for Peacebuilding in Divided Societies: ICTs and Peacebuilding in Northern Ireland*. Belfast: Transformative Connections, 2015.

Young, Peg and J. K. Ord. "Model Selection and Estimation for Technological Growth Curves." *International Journal of Forecasting* 5, no. 4 (1989): 501-513.

YouTube. "YouTube Analytics Basics.". Accessed July 17, 2015. support.google.com/youtube/answer/1714323?hl=en.

Zeleny, Milan. "Management Support Systems: Towards Integrated Knowledge Management." *Human Systems Management* 7, no. 1 (1987): 59-70.

Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired. Accessed February 10, 2017. wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

———. "Meet 'Flame', the Massive Spy Malware Infiltrating Iranian Computers." Wired. Accessed June 27, 2018. wired.com/2012/05/flame/.

———. "Mossad Hacked Syrian Official's Computer before Bombing Mysterious Facility." Wired. Accessed June 5, 2018. wired.com/2009/11/mossad-hack/.

Zhang, Li. "A Chinese Perspective on Cyber War." *Internation Review of the Red Cross* 94, no. 886 Summer 2012 (2012).

Ziolkowski, Katharina. “Ius Ad Bellum in Cyberspace – some Thoughts on the “Schmitt-Criteria” for use of Force.” In *Proceedings of the 4th International Conference on Cyber Conflict*, edited by Czosseck, Christian, Rain Ottis and Katharina Ziolkowski. Tallinn: NATO CCD COE, 2012.

Ziolkowski, Katharina. “Peacetime Cyber Espionage: New Tendencies in Public International Law.” In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by Ziolkowski, Katharina, 425-464. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014.

Ziolkowski, Katharina. *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*. Tallinn, Estonia: Tallinn, Estonia : NATO CCD COE Publications, 2013.

Zyck, S. A. and M. “Preparing Stabilisation for 21st Century Security Challenges.” *Stability: International Journal of Security & Development* 4, no. 1 (2015).

ОКеям Нет. “Россия снова Агрессор.”. Accessed February 27, 2016. youtube.com/watch?v=JLesB4EQQrI.

Summary

Summary

On Cyber: The Utility of Military Cyber Operations During Conflict

There is a lacuna in the understanding of the utility of military cyber operations at all levels of warfighting. This results in hesitant use of military cyber operations during conflict. Before States are able to employ military cyber operations with utility, however, a thorough understanding is required of their strategic, societal, technological, military and legal context. This thesis addresses these five perspectives in order to create a more comprehensive understanding of the utility of military cyber operations.

Chapter two has argued that the notion of power needs to be addressed in order to understand how the military instrument can be employed, to what end, and how cyber capabilities can contribute to achieving this end. After conducting a theoretical literature review into the 20th century power discussion chapter two has created a framework with potential elements that impact power such as context, power concept involved, and the dimensions scope, domain and means. Whether or not an actor is able of achieving its interests depends on the context of an actor's action, an action in a specific context may have different consequences in another context. The scope of an activity epitomises the ends sought after with a certain activity (e.g. anticipation, prevention, deterrence, protection, intervention, stabilisation or normalisation), the domain involves the type of actor subjected to the activity (e.g. State or non-State actor), and the means comprise the instruments used for conducting the activity (e.g. political, informational, economic, military or civil capacities). The power concept characterises the mechanism through which power is effectuated (compulsory, institutional, structural or productive). The elements included in the power framework impact the potential utility of any activity conducted to influence in international relations, including military cyber operations.

Chapter three has discussed informationised society and the rise of cyber therein and the effect on the notions of power. Chapter three concluded that although remaining conceptually and theoretically valid, all elements included in the power framework from chapter two are impacted by informationised society and rise of cyber (i.e. context, mechanisms, and dimensions). Although informationised society proved to be a contested construct, Chapter three characterised this type of society by series of changes in technological, economical, occupational, spatial and cultural areas. Within informationised society 'cyber' has arisen, first as fiction and later as a reality within international relations. Informationised society and the rise of cyber affect the power framework produced in chapter two.

Chapter four has described the arena where cyber activities are conducted (i.e. cyberspace) and listed representative tools with which actors seek to influence each other cyberspace (i.e. cyber capabilities). There are different conceptualisations of cyberspace, the broadest is the State conceptualisation using a layered 'cyberspace' model to highlight different aspects of networking: geographic, physical, logic and social. The logical and physical network layers are described in more detail in the technical perspective on 'the Internet'. Chapter four has discussed series of cyber capabilities aimed at influencing the different components of cyberspace, that is, the cyber persona (e.g. data mining, websites, social media, mail, instant messaging, text messages, forums and blog), logical network (e.g. firmware malware, authentication flaw exploitation, social engineering, vulnerability exploitation, wiretapping, denial of service, distributed denial of service, SQL injection, cross-site scripting, cross-site request forgery) and physical network components (e.g. hardware Trojans and emanation exploitations).

Chapter five has discussed how armed forces are conceptually and doctrinally organised and what the place of cyber capabilities is within that organisation. After having discussed fighting power, military operations and military cyber operations, chapter five concluded that military cyber operations fit within the conceptual construct of other military operations. Military cyber operations target entities in the information dimension of the operational environment to ultimately create an effect in the cognitive dimension contributing to a certain goal.

Chapter six concluded that the debate on the IHL legal framework applicable to military cyber operations is in flux. Therefore, those seeking to derive a legal framework are forced to select their preferred approach or set of approaches. For instance, in qualifying data as object, the approach to damage and, in the case of the functional approach, the level of functional damage required to qualify as damaging. Chapter six has created a framework for selecting the approach taken to data, damage, and loss of usability.

Chapter seven has concluded this thesis with defining the utility of military cyber operations as dependent on the purpose, the context wherein they are used, the cyber capabilities involved therein, the military proficiency in utilising the cyber capabilities and the legal framework governing that specific context. As such utility lies at the intersection of all five perspectives described in this thesis: power, society, technology, military, and law. Utility depends on all five perspectives and cannot be seen from a mono-disciplinary perspective, utility defies explanation by a single discipline and doing so would result in a misrepresentation of the complexity of utility in the context of military cyber operations.

Summary in Dutch (‘samenvatting’)

Summary in Dutch ('samenvatting')

Over Cyber: Het Nut van Militaire Cyberoperaties Tijdens Conflict

Op de verschillende niveaus van oorlogvoering is gebrek aan begrip van het nut van militaire cyberoperaties tijdens conflict. Dit resulteert in terughoudendheid bij het gebruik van dit type operaties. Om het nut van militaire cyberoperaties te begrijpen is context nodig. De context wordt gevormd door de volgende vijf perspectieven: macht, maatschappij, technologie, militaire operaties en recht. Dit proefschrift adresseert deze vijf perspectieven in vijf hoofdstukken.

Hoofdstuk twee gaat in op de academische discussie over macht en heeft als doel begrip creëren van de context van de inzet van het militaire instrument. In hoofdstuk twee is een model gecreëerd met de elementen die invloed hebben op machtsverhoudingen zoals context, gebruikte machtsconcepten en machtsdimensies zoals toepassingsgebied, toepassingsbereik en middelen. Het toepassingsgebied gaat over het doel van een activiteit (bijvoorbeeld anticiperen, voorkomen, afschrikken, beschermen, interveniëren, stabiliseren en normaliseren), het toepassingsbereik gaat over de actoren die betrokken zijn bij de activiteit (zoals Statelijke of niet-Statelijke actoren) en middelen gaat over de instrumenten waar gebruik van gemaakt wordt (bijvoorbeeld diplomatieke, informationele, militaire, economische of civiele instrumenten). Deze elementen beïnvloeden de effectiviteit van activiteiten tussen actoren, bijvoorbeeld militaire cyberoperaties.

Hoofdstuk drie beschrijft de informatisering van de maatschappij, dit is noodzakelijk aangezien deze de context vormt voor alle beïnvloedingsactiviteiten en heeft geresulteerd in de opkomst van cyber. Informatisering heeft effect op de maatschappij in technologische, economische, beroepsmatige, ruimtelijke en culturele zin. Binnen deze geïnformatiseerde maatschappij is cyber opgekomen, eerst in fictie en later als reële factor van invloed binnen internationale betrekkingen. Hoofdstuk drie concludeert dat het model van machtselementen uit hoofdstuk 2 conceptueel valide blijft maar dat de inhoud alle elementen beïnvloed wordt door informatisering en de opkomst van cyber.

Hoofdstuk vier gaat in op de technische aspecten van militaire cyber operaties, namelijk de arena waar cyberactiviteiten uitgevoerd worden ('cyberspace') en de middelen waar actoren dat mee doen ('cyber capaciteiten'). Cyberspace wordt op verschillende manieren geconceptualiseerd, de meest omvattende is cyberspace als gelaagd model dat geografische, fysieke, logische en sociale factoren van netwerken benadrukt.
Een ander model is het 'Internet model', dat zich met name toespitst op de fysieke en logische componenten binnen het 'cyberspace model'. Hoofdstuk vier heeft verder cyber capaciteiten benoemt die gericht zijn op de 'cyber persona' component (bijvoorbeeld datamining, websites, social media, mail, instant messaging, sms, forums en blogs); 'logic

network' component (zoals firmware malware, exploitatie van authenticatiefouten, social engineering, exploitatie van kwetsbaarheden, afluisteren, denial of service, distributed denial of service, SQL injectie, cross-site scipting en cross-site request forgery); en 'physical network' component (bijvoorbeeld hardware Trojans en exploitatie van emissies).

Hoofdstuk vijf legt uit hoe de krijgsmacht conceptueel en doctrinair georganiseerd is en wat de plaats van cyber capaciteiten is binnen deze organisatie. Na het bespreken van militair vermogen, militaire operaties en militaire cyberoperaties wordt geconcludeerd dat militaire cyberoperaties passen binnen het denken over militaire operaties. Militaire cyberoperaties zijn gericht tegen entiteiten in de informatiedimensie van de operationele omgeving, om uiteindelijk een effect te creëren in de cognitieve dimensie.

In hoofdstuk zes wordt geconcludeerd dat het juridische raamwerk van toepassing op militaire cyber operaties tijdens gewapend conflict aan discussie onderhevig is. Om het juridische raamwerk van toepassing op dit type operaties te kunnen deduceren moeten keuzes gemaakt worden in de benaderingswijze inzake de kwalificatie van data als object, schade en de benodigde mate van functionele schade. In hoofdstuk zes is een raamwerk gecreëerd voor het selecteren van de benaderingswijze inzake eerdergenoemde zaken en de gevolgen daarvan op het juridische raamwerk dat van toepassing is.

Hoofdstuk zeven definieert het nut van militaire cyberoperaties. Dit type operaties heeft nut afhankelijk van hun gewenste doel, de context waarin ze gebruik worden, de cybercapaciteiten die gebruikt worden in de operatie, de kunde van de krijgsmacht in het gebruik van deze capaciteiten en het juridische raamwerk dat van toepassing is in de specifieke context van de cyberoperatie. Met andere woorden, het nut van militaire cyberoperaties bevindt zich op het snijvlak van de vijf perspectieven beschreven in dit proefschrift.