FEBRUARY 2016

National DEFENSE

NDIA'S BUSINESS AND TECHNOLOGY MAGAZINE ▪ $5.00

Lockheed Targets Training Market

Homeland Missile Defense in Limbo

More Ships On the Way

Budget boost for new cutters marks turning point for the U.S. Coast Guard

"You Copy"

"Loud And Clear"

These extremely light weight booster amplifiers are no lightweights when it comes to performance. They increase the range and improve overall tactical radio communications even in extreme conditions... when a quality signal is critical. They're tough and simple to use.

AR-20 – World's Smallest 20-Watt Man-Packable Amplifier

- New JITC/IW Certified
- 20 Watts
- 30 – 512 MHz
- Available with LNA
- "Airborne Certified" version available
- Supports AM, FM, HPW, SINCGARS, IW, ANW2, SRW, WNW, ASCM, and more waveforms
- Works with multiple radios including AN/PRC-159, AN/PRC-154 Rifleman™, AN/PRC-152A, AN/PRC-148 JEM tactical radios and more

AR-50 – The Widest Range of Radio Platforms & Waveform Support

- JITC, IW and DAMA Certified
- 50 Watts
- 30 – 512 MHz
- Tested to 400G Drop Test & 4G Vibration Test
- Supports AM, FM, HPW, SINCGARS, IW, ANW2, SRW, WNW, ASCM, and more waveforms
- Works with Harris AN/PRC-117F, AN/PRC-117G, AN/PRC-152A, Thales AN/PRC-148 JEM, Raytheon AN/PSC-5D, Rockwell Collins AN/ARC-210 tactical radios and more

BATTLE TESTED

To learn more, visit us at www.arworld.us/tactical or call us at 425-485-9000.

modular rf

Other ar divisions: rf/microwave instrumentation • receiver systems • ar europe

www.arworld.us

National DEFENSE
Exclusive content on our blog
www.NationalDefenseMagazine.org/blog
Twitter.com/NationalDefense
Facebook.com/NationalDefense

February 2016

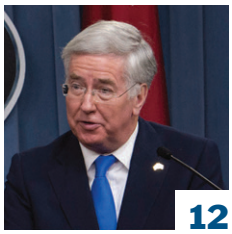
NDIA'S BUSINESS AND TECHNOLOGY MAGAZINE
VOLUME C, NUMBER 747
WWW.NATIONALDEFENSEMAGAZINE.ORG

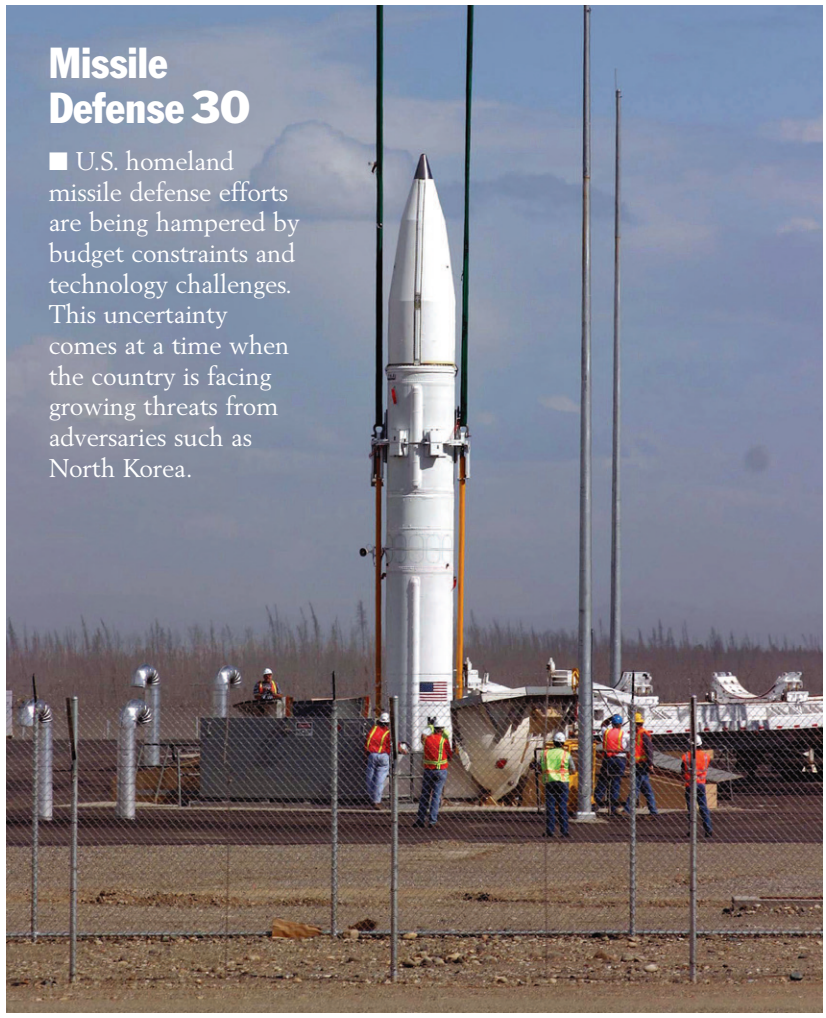
Training and Simulation 20

■ Lockheed Martin is looking to expand its training and simulation business with the expectation that demand for such systems will remain strong. The company is taking advantage of opportunities overseas and through its joint strike fighter program.

Cover Story 36

■ Congress gave the Coast Guard additional funds for acquisition accounts in fiscal year 2016. That increase will go toward a ninth national security cutter, a new polar icebreaker and funding for the offshore patrol cutter, enabling the service to more effectively carry out its missions. **Cover: National Security Cutter Stratton (Coast Guard)**





Missile Defense 30

■ U.S. homeland missile defense efforts are being hampered by budget constraints and technology challenges. This uncertainty comes at a time when the country is facing growing threats from adversaries such as North Korea.

DEPARTMENTS

National Defense FEBRUARY 2016
VOLUME C
NUMBER 747

EDITOR
Sandra I. Erwin
(703) 247-2543
SErwin@ndia.org

MANAGING EDITOR
Stew Magnuson
(703) 247-2545
SMagnuson@ndia.org

SENIOR WRITER
Jon Harper
(703) 247-2542
JHarper@ndia.org

STAFF WRITER
Yasmin Tadjdeh
(703) 247-2585
YTadjdeh@ndia.org

DESIGN DIRECTOR
Brian Taylor
(703) 247-2546
BTaylor@ndia.org

EDITORIAL ASSISTANT
Allyson Versprille
(703) 247-9469
AVersprille@ndia.org

National Defense Magazine
2111 Wilson Blvd., Suite 400
Arlington, VA 22201

CHANGE OF ADDRESS:
http://eweb.ndia.org

LETTERS TO THE EDITOR: National Defense welcomes letters—pro or con. Keep them short and to the point. Letters will be edited for clarity and length. All letters considered for Readers Forum must be signed.

Letters can be either mailed to: Editor, National Defense, 2111 Wilson Boulevard, Suite 400, Arlington, VA 22201 or e-mailed to letters@nationaldefensemagazine.org.

SUBSCRIPTION AND REPRINTS: Editorial features in National Defense can be reprinted to suit your company's needs. Reprints will be customized at your request and are available in four-color or black and white.

For information regarding National Defense subscription terms and rates, please call (703) 247-9469, or visit our web page at www.ndia.org.

NDIA MEMBERSHIP: The National Defense Industrial Association (NDIA) is the premier association representing all facets of the defense and technology industrial base and serving all military services. For more information please call our membership department at 703-522-1820 or visit us on the web at www.ndia.org/membership

National Defense (ISSN 0092–1491) is published monthly by the National Defense Industrial Association (NDIA), 2111 Wilson Blvd., Suite 400, Arlington, VA 22201–3061. TEL (703) 522–1820; FAX (703) 522–1885. **Advertising Sales:** Dino K. Pignotti, 2111 Wilson Blvd., Suite 400, Arlington, VA 22201–3061. TEL (703) 247–2541; FAX (703) 522–1885. The views expressed are those of the authors and do not necessarily reflect those of NDIA. **Membership rates** in the association are $40 annually; $15.00 is allocated to National Defense for a one-year association basic subscription and is non-deductible from dues. Annual rates for NDIA members: $40 U.S. and possessions; District of Columbia add 6 percent sales tax; $45 foreign. A six-week notice is required for change of address. Periodical postage paid at Arlington, VA and at additional mailing office. **POSTMASTER:** Send address changes to National DEFENSE, 2111 Wilson Blvd, Suite 400, Arlington, VA 22201–3061. The title National Defense is registered with the Library of Congress.

University of Phoenix®
College of Security & Criminal Justice

A degree in security can open up a wide, wide world of career possibilities for you.

In today's world, security is more important than ever. Which means there is an immense range of opportunities in the security profession. With a degree in Security Management from University of Phoenix, you can reach new heights in this growing field. We offer a Bachelor of Science in Security Management, an Associate of Arts in Security Management and certificate programs that are aligned to the Security Competency Model, written by University of Phoenix and recently validated and published by the U.S. Department of Labor.

To learn more, visit **phoenix.edu/security.**

For more information about each of these programs, including on-time completion rates, the median debt incurred by students who completed the program and other important information, please visit phoenix.edu/programs/gainful-employment.

New Blood May Stem Industry Consolidation

William J. Perry, the nation's highly respected former secretary of defense, was recently in Washington, D.C., to present his latest book, "My Journey at the Nuclear Brink." It is yet another contribution to a public career that has, by any measure, been extraordinary. I highly recommend it.

In comments he made to defense reporters in Washington, D.C., it was not Perry's observations about nuclear strategy and force structure that caught my attention; rather it was his recollections of the defense industry consolidation that occurred during his time as defense secretary in the early 1990s.

He had hoped that the restructuring of the industry, which followed his famous 1993 "last supper" with senior industry executives, would have resulted in a leaner industry rather than one consolidated into a few large firms.

These comments are conceptually consistent with others recently made by Defense Undersecretary for Acquisitions, Technology and Logistics Frank Kendall expressing his discomfort with United Technologies' (UTC) sale of its Sikorsky Helicopter unit to Lockheed Martin. Kendall observed that, "with size comes power, and the department's experience with large defense contractors is that they are not hesitant to use this power for corporate advantage."

What is the issue here? It is the concern expressed by both of these tremendous public servants that as the defense industrial base has contracted it has resulted in a structure that is — conceptually at least — less conducive to price control and technological innovation, conditions that flow from greater competition. I am sympathetic with the argument, but only to a point.

> "It is the concern ... that as the defense industrial base has contracted it has resulted in a structure that is — conceptually at least — less conducive to price control and technological innovation, conditions that flow from greater competition."

As many of my previous postings in this column have indicated, at the National Defense Industrial Association we are concerned about the shrinkage of the defense industrial base that has occurred over the past two decades. It is in the nation's best interest to have a competitive and technologically vibrant defense industry that is geographically dispersed and diverse. Our nation, along with many of its close allies around the world, relies on America's "Arsenal of Democracy."

The U.S. defense industrial base is a major strategic asset and key competitive advantage that extends U.S. influence and enhances the nation's capabilities. But this capability largely resides in the nation's private sector, and government leaders must recognize that this circumstance results in their having only indirect influence over corporate decisions.

Private sector companies that are well managed are always seeking ways to become leaner. As Heidi Shyu, the Army's former service acquisition executive, has stated, excess overhead in a company directly translates to extra costs and lower profits, making company management very "lean-conscious."

In the early 1990s, when Perry convened his "last supper," many defense companies had some excess capacity associated with programs they had committed to that were either being canceled or significantly reduced in scale. But much of their management overhead was tied to government accounting and auditing practices. Since some of it was unable to be reduced proportionately with program reductions, this meant that consolidation was the only viable pathway in the face of sharply declining acquisition spending. Company "miniaturization" was never a real choice, the result being some 50 companies — depending on whose data one uses — consolidating into five or six of today's "top tier primes."

Consolidations such as this can increase economies of scale, but increased size and market share can also shift pricing power toward the firm and away from the consumer.

This was the concern expressed by Kendall, who noted that he was "neutral" on the Lockheed-Sikorsky deal so long as, "it doesn't affect our prices much." This comment basically acknowledges that U.S. anti-trust law does not limit company size or market share. As the Supreme Court noted in the 1920 case of United States v. United States Steel Corp., "[T]he law does not make mere size an offense, or the existence of unexerted power an offense."

Where anti-trust law can come in to play is where companies are known to collude on price, or otherwise control them, by creating barriers for other firms to enter the market.

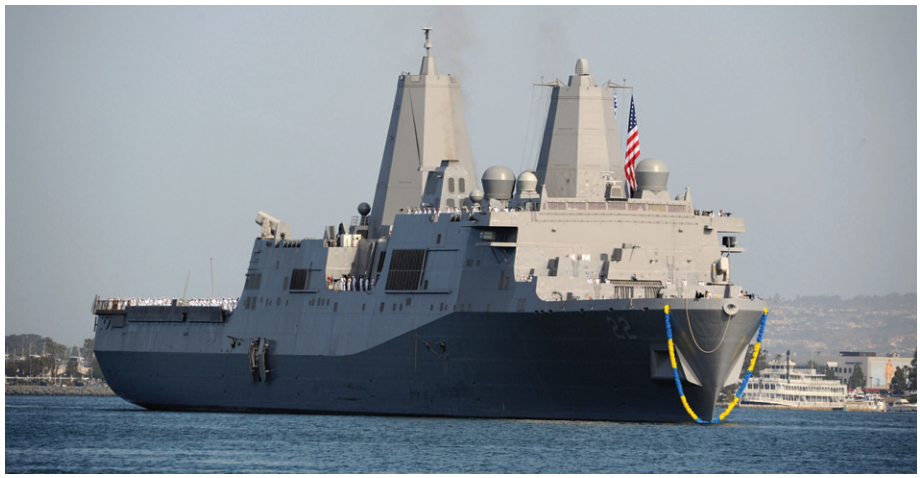
Regarding prices, this does not seem to have happened as the Pentagon recently reported that program cost growth has been greatly reduced over the past decade. And as for barriers to entry, many would argue that the Pentagon's own intrusive reporting and auditing requirements are themselves the greatest barrier to new firms entering the defense market. This seems to be the major message Silicon Valley companies have passed to the Defense Department following Secretary Ashton Carter's April 2015 outreach to them.

It may be that Perry's recent comments are intended to signal that the Defense Department remains opposed to further industry consolidation, the Pentagon's unstated position since its 1998 opposition to the proposed merger of Lockheed Martin with Northrop Grumman. If so, that is a useful clarification. As some industry experts have indicated, the government has almost no tools available to prevent a company making a strategic divestiture, such as UTC did with Sikorsky, and a tough case to make when opposing mergers on anti-trust or monopolistic grounds.

Therefore, the better focus is to attract new firms into the defense market, which means aggressively eliminating barriers to entry. But to do that, the Pentagon needs to look objectively at where those barriers are and who has created them.

Email your comments to cmckinley@ndia.org

Amphibious Transport Docks Could Host Missile Defense Systems



■ Huntington Ingalls Industries is in discussions with defense officials about potentially putting missile defense radars and laser weapons on San Antonio-class amphibious transport docks.

"You can put a lot of additional weight on the ship and you can put … some modern technologies like ballistic missile defense radars that are very heavy," Brian Cuccias, corporate vice president at HII and president of Ingalls Shipbuilding, told reporters. "We think it's a great idea."

"You have a design life margin …. on some ships that say you can only take so much more weight before you have a stability issue or, you know, you don't have your margins," he said. "When you close in the well deck of the LPD ship you expand that capability to take a lot of weight, and the stability on LPD is such you can actually put weight up high" where missile defense radars would be positioned.

One of the challenges of hosting ballistic missile defense radars is the need to power them and cool them, Cuccias noted. "You need arrangeable volume for power generation. You need arrangeable volume to have cooling," he said. "LPD allows for that. … The basic bones of the ship allow that to take place."

Cuccias would not say which officials have discussed the idea with him. "We're talking about it and so there is some interest, but that's as far as I really want to go," he said, adding that he believes interest is "growing."

READ MORE: bit.ly/1KdDTen

F-35 Ramp-Up to Present Logistics Challenge

■ As if producing cutting-edge warplanes weren't hard enough, what comes next — maintenance and logistics support — can be an even more daunting challenge.

The F-35 joint strike fighter certainly will present this test to the Pentagon as manufacturing of the U.S. military's newest combat jet ramps up from a few dozen to more than a hundred per year. The fleet is projected to grow from 154 today to more than 1,000 fighters in the next four years. And even if the Defense Department and manufacturer Lockheed Martin manage to fix all the development glitches that still dog the airplane, there are worries about the government and the industry's capacity to keep the fleet in working order after F-35 squadrons around the world start operating the planes.

The F-35 program executive officer, Air Force Lt. Gen. Christopher Bogdan, has sounded alarms in recent months about the coming logistics crunch. The plan is to triple the production and fielding rate in just three years, from about three to four dozen airplanes a year to more than 120. Bogan said the accelerated delivery gives him "some pause" and fears there could be a shortage of suppliers that can fill the spike in demand for spare parts and of skilled technicians to repair the technologically advanced airplanes. "What I most worry about, and what we most have to concentrate on, is the supply base," Bogdan said last fall.

The logistics issues associated with the introduction of a new fleet of aircraft are nothing new for the Pentagon. These are problems that the Defense Department typically encounters when it begins fielding a brand-new system, said retired Air Force Lt. Gen. Charles "CR" Davis, who served as the service's top military adviser on weapons acquisitions.

READ MORE: bit.ly/1P4Ub0s

Defense Watch By Sandra I. Erwin

CEOs Not Yet Ready to Take a Gamble

Where's the payoff?

That's the question for which defense executives don't have clear answers as they weigh investment choices in an uncertain market.

In years past, these decisions would have been relatively straightforward and shaped almost entirely by the Pentagon's five-year research, development and procurement funding plan.

The game has changed dramatically during the Obama presidency as partisan fights derailed the customary budget process and the federal government almost every year has been saved from the brink of shutdown by 11th hour deals.

In this climate, top defense contractors have opted to deploy their cash, repurchasing their stocks and paying out dividends to shareholders. So it comes as no surprise that private investments in new technology by the top firms in the aerospace and defense industry have been on a downward slope, despite the constant pressure for innovation and growth.

New data on the defense and aerospace sector from the consulting firm Deloitte shows that company-funded IRAD, shorthand for independent research and development, has declined from 4.27 percent of revenues in 2009 to 3.14 percent in 2014, a 26.5 percent drop.

The Pentagon has taken a dim view of this trend. The Defense Department's top weapons buyer Frank Kendall has called out defense CEOs for hoarding cash instead of pouring more money into next-generation technology. This is a burning concern for officials like Kendall who worry about keeping the military technologically sharp. It's not just IRAD that is coming down. Federal funding for defense research, development, testing and evaluation dipped from $79.7 billion in 2009 to $62.9 billion in 2014, a 21.08 percent decline. The Defense Department projects a further contraction of 10 percent in RDT&E funding between 2016 and 2020.

"The iconic technological innovations that characterize the sector's history have been largely dependent on funding from the U.S. government, as well as internal company sources," says Deloitte. The upshot is a likely erosion in competitiveness for defense and aerospace, analysts warn, at a time of heightened global tensions, aggressive military actions by America's adversaries and increased competition in commercial markets.

The Pentagon understandably wants contractors to give less money to shareholders and to help foot the bill for new product development. But that might be an unreasonable expectation, especially in today's climate, say Bloomberg Government analysts Robert Levinson and Jesse Holler. "While the big five defense contractors are giving a lot more money back to shareholders than they're investing in R&D, additional investments may not be justified by financial returns," they point out. "With defense spending levels locked in through fiscal 2017, investment choices probably won't change much for contractors in the near future. R&D investments may not increase at all, unless defense technologies can be leveraged into broader, possibly commercial markets."

One industry player that is bucking the trend is Textron AirLand. The company a year and a half ago unveiled a commercially developed military airplane that is being watched as a bellwether. If Textron's gamble pays off, it might encourage other companies to take more risk. If it doesn't, the industry and its investors will see it as a cautionary tale.

Textron's surveillance and strike jet, the Scorpion, was developed with private funding in 23 months. There are still no signs that the Pentagon will buy it, but the company is optimistic about the international market. "We made a decision to make an investment in a commercially developed military airplane," Textron AirLand President Bill Anderson says in an interview. This past summer, he spent seven weeks in eight countries marketing the airplane.

The Pentagon asked industry to invest, and this is one company's answer to that call. "We did something completely different and completely outside the system," Anderson says. The reaction from the Defense Department has been limited so far. "The Air Force and Navy are taking a hard look at the value and capability," he says. "They are actively discussing how they could use it."

The Defense Department is accustomed to buying highly customized equipment made to stringent specs, so it remains to be seen whether it is serious about off-the-shelf procurements. "Change for big institutions takes a long time," says Anderson.

So how much patience will Textron's shareholders have? "We are actively pursuing sales globally," he adds. "We are not waiting for the DoD to respond. At this point, international sales look like they would move much faster than DoD."

There is not much appetite for big technology bets among defense contractors. For the time being, returning money to shareholders through stock buybacks and dividends seems to be the safest path. "It's easy to see why Kendall decries stock buybacks," Bloomberg analysts say. In 2014 the top five defense contractors — Lockheed Martin, Boeing, Raytheon, General Dynamics and Northrop Grumman — collectively distributed dividends and bought back stock valued at $18.6 billion, about 88 percent of their cash from operating activities that year. The same year, those five companies invested $5.2 billion in R&D.

Defense contractors are no different than other major corporations in America's civilian economy when it comes to IRAD, Bloomberg notes. "When R&D spending by the top five defense contractors is compared with that of the top five companies in the Standard & Poor's 500 Index, they have similar percentages."

The problem for defense firms is that they don't see an incentive to invest. There are fewer programs to bid for. Once a product is developed, even if it's successful, production runs are small. There is also pressure on government procurement officers to squeeze contractors' profit margins.

"Commercial companies invest heavily because there is a potential to reap huge profits at levels the government may find unpalatable," the Bloomberg analysis concludes. "When no clear future payoff exists, contractors may be deterred from making further investments in R&D. Until the model changes, government may need to pay for R&D above and beyond what the market will bear."

Planetary Defense: A New Hot Market

If there is one thing more important than national defense, it's planetary defense.

There are objects in outer space that could potentially wipe out humanity and they are not malevolent little green men in spaceships. They are asteroids and comets, and a bigger than average sized one striking Earth would be the equivalent of the United States, Russia, China and the whole rest of the "club" popping off all their nukes at once.

With little fanfare, NASA in January opened up its planetary defense coordination office with a mandate to identify potential chunks of rock hurdling toward Earth and to stop them if possible.

The 2016 budget, which was recently passed, allocated $50 million this year alone for the office, five times what has been budgeted for detection and mitigation of "near-Earth" objects in the past.

Big defense contractors — particularly those involved in space such as Boeing, Lockheed Martin, Raytheon and Northrop Grumman — will most likely be seeking contracts in this emerging new defense market. If a mission is needed to stop a killer asteroid, $50 million will be a drop in the bucket.

How real is the threat?

There are more than 13,500 near-Earth objects of various sizes that have been spotted to date. That doesn't count the ones that have not been discovered, a NASA news release states.

> "The nation doesn't want to see the day when the president calls a press conference to announce that an asteroid the size of a skyscraper is going to strike the Earth in two years."

In short, they have struck Earth before, and it's impossible to rule out that it will never happen again. The history of near-Earth objects striking Earth is writ all over the face of the planet. The Chicxulub Crater buried beneath the Yucatan Peninsula in Mexico is suspect number one as the object that killed off the dinosaurs some 66 million years ago. The crater is 100 miles long, 12 miles deep and is only the second largest one found on Earth. Scientists speculate that it caused mega-tsunamis, covered the world in ash, radically altered the atmosphere and created dust that blotted out the sun.

So is 66 million years "just a blink of an eye" in geological terms, or are we overdue for another impact?

A reminder that we are at the mercy of the cosmos arrived in Russia on Feb. 15, 2013, when the Chelyabinsk meteor came skimming across the upper atmosphere and exploded before reaching the ground. It weighed approximately 10,000 metric tons and had gone undetected. The effects of the shockwave injured more than 1,500 victims and caused widespread damage. If it had arrived at a different trajectory, the results would have been far worse.

Not more than a day later, a second previously undetected asteroid came within 17,200 miles of Earth. The two events were coincidental, scientists said. They were coming from completely different trajectories. The two incidents created a sense of urgency. Efforts to detect asteroids and possibly mitigate impacts were ad hoc and spread out in various NASA programs. The new office is a step to bring everything under one umbrella.

There is some good news. More than 90 percent of near-Earth objects larger than 3,000 feet have already been discovered, NASA said. The new office will focus on finding objects that are "slightly bigger than a football field" at 450 feet or larger. NASA relies on a global network of astronomers using ground-based telescopes as well as the space-based NEOWISE infrared telescope to find these potential killers. The spacecraft, constructed by Ball Aerospace and Lockheed Martin, was launched in 2009.

"The office … will also take a leading role in coordinating interagency and intergovernmental efforts in response to any potential impact threats," a NASA statement said.

Interagency coordination will include the Defense Department, National Science Foundation and Department of Homeland Security components such as the Federal Emergency Management Agency.

Of course, if it comes to FEMA being called in, that means bad news. FEMA would handle the preparations and response planning related to the consequences of atmospheric entry or impact to U.S. communities, the statement said.

Hopefully, it will not come to that. Part of the new office's mission will be to develop technology to stop an impact.

There are two notable programs being pursued. NASA has an "asteroid redirect mission," which will send a robot to space where it will capture and return a boulder-sized sample to place in the moon's orbit where it can be studied. A secondary goal is to explore planetary defense technologies. This mission is not expected to launch until the 2020s.

A more direct attempt to defend against asteroids is a joint European Space Agency-NASA program, the "asteroid impact and deflection assessment mission." It has actually identified a rock called 65803 Didymous that will be close enough to Earth in October 2022 to test the ability to move a near-Earth object into a different trajectory.

It will send two independent spacecraft to the asteroid. The NASA double asteroid redirection test mission led by the Johns Hopkins Applied Physics Laboratory will crash into Didymous to nudge it into a different path. An ESA spacecraft will be there to assess and observe the impact.

One hopes that the office comes up with other concepts and technologies and puts some real money into them.

The nation doesn't want to see the day when the president calls a press conference to announce that an asteroid the size of a skyscraper is going to strike the Earth in two years.

"What are the plans to stop it?" a reporter will inevitably ask.

"Well, first we're going to release a request for proposals, and then we're going to hold an industry day."

Email your comments to smagnuson@ndia.org

Carefully Tailor Codes of Conduct

Nearly every company maintains a collection of basic standards and expectations commonly referred to as a code of conduct.

Additionally, most companies maintain separate, more detailed policies that address the specific areas of professionalism, human resources rules, anti-harassment and anti-bullying, social media, confidentiality, and standards peculiar to certain industries or job functions.

But a company must be exceptionally careful about the language that it uses in describing and proscribing prohibited behavior to avoid running afoul of federal labor law.

For example, the National Labor Relations Board has determined that the following common workplace conduct rules are unlawful:

- Be respectful of others and the company.
- Do not make insulting, embarrassing, hurtful or abusive comments about other company employees online and avoid the use of offensive, derogatory or prejudicial comments.
- Do not send unwanted, offensive or inappropriate e-mails.
- Do not make personal insults, use obscenities or engage in any conduct that would be unacceptable in a professional environment.
- Material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or otherwise unlawful or inappropriate may not be sent by email.
- Misconduct includes false accusations against the company and/or against another employee or customer.

Many compliance, human resources and legal professionals are still grappling with the board's narrow view of what constitutes lawful restrictions on bad behavior.

So why did the board deem these seemingly legitimate policies unlawful? Because they prohibited — or could reasonably be read to prohibit — employees from engaging in protected concerted criticism of the company's labor policies or treatment of employees, or they prohibited employees from arguing with each other about unions, management and their terms and conditions of employment.

The National Labor Relations Board's general counsel provided the following explanation in a memorandum issued March 18, 2015, titled, "Report of the General Counsel Concerning Employer Rules."

It says: "According to the board, criticizing the company and its managers, and arguing about labor policies and workplace conditions is protected activity under Section 7 of the National Labor Relations Act. This protection applies to all employees, unionized or not."

The general counsel's memo further expounded that policies that prohibit employees from engaging in "disrespectful," "negative," "inappropriate" or "rude" conduct toward the company or its management, absent sufficient clarification or context, will usually be found unlawful. The board even interprets Section 7 to protect those employee criticisms of the company or its management that are false or defamatory. Thus, only those code of conduct rules which are narrowly tailored to prohibit "maliciously false" — i.e., "knowingly" or "recklessly" false — statements about the company or its managers are permissible.

The board recognized that employee criticism and argument about terms and conditions of employment can become quite vigorous and contentious. Nevertheless, it stated that a company may not prohibit protected speech simply because it includes "intemperate, abusive and inaccurate statements," including profanity.

The board makes clear that workplace conduct rules — including anti-harassment policies — which broadly prohibit any "negative," "inappropriate," "offensive," or even "intimidating" statements or discussions, without further clarification, will be deemed unlawful. As the board sees it, employees would likely construe that type of broad policy language to restrict their Section 7 rights.

In contrast to the narrow limits on employee misconduct policies directed at the company or its management, the board allows greater restrictions on employee misconduct directed at others. This includes co-workers as well as the company's clients, business partners, competitors and other third parties. For example, the memo states that a broad policy requiring employees to be "respectful and professional" toward co-workers and other third parties — but not the company or its managers — will "generally be found lawful." The board also allows policies that require employees to be cooperative with each other and management in the performance of their work, and those that prohibit acts of insubordination.

Furthermore, the board recognizes a company's right to prohibit employees from engaging in speech or conduct that disparages the company's products or services. However, a policy that broadly prohibits conduct that could damage or undermine the company's "reputation" would be unlawful because of the chilling effect on Section 7 rights to criticize the employer's labor policies or working conditions, including the right to do so in a public forum.

Walking the line between lawful and unlawful conduct rules is not easy. When drafting a code or other policy that addresses employee behavior, it's important to understand the board's narrow view of conduct restrictions allowed under Section 7. Companies must word policies so that employees would not reasonably interpret them as restricting their rights to criticize the company or its management regarding labor policies or work conditions, or vigorously debate such matters with each other.

And, although it seems to defy common sense, this includes the right to use disrespectful, demeaning, intimidating or profane statements — and even false accusations — in doing so. Companies should consider adding a statement that nothing in the policy is intended to limit employees' rights to engage in protected concerted activities under Section 7 of the NLRA. Although not a panacea, this type of statement should support the enforceability of policies that are reasonably well drafted.

Denise Brucker is senior counsel at Cubic Corp. The opinions expressed are solely those of the author.

 By Herb Fenster, Terra Fulham and Jason Workmaster

Don't Bank on Relief from DCAA Audits

The Truth in Negotiations Act is a statute with which defense contractors are likely familiar. It requires contractors to submit current, accurate and complete cost or pricing data when negotiating certain contracts with the government.

Gathering and producing this data can be an arduous process and can result in the inadvertent disclosure of information that does not entirely satisfy the TINA standard. In such situations, contractors often will voluntarily notify the government of the issue and seek to resolve it.

In such situations, it is only reasonable for the contractor to expect the government not to conduct a full-scope audit by the Defense Contract Audit Agency (DCAA) but rather to recognize the contractor's good-faith conduct and agree to a limited review. Such has not been the case, however, resulting in industry calls for regulatory action to rein in the agency.

On Nov. 20, the Defense Department responded to these calls and published a proposed rule to amend the Defense Federal Acquisition Regulation Supplement. The change would require contracting officers to request a limited-scope audit if a contractor voluntarily discloses that cost or pricing data was inaccurate, incomplete or not current when submitted, unless a full-scope audit is "appropriate for the circumstances." In theory, the proposed rule would give a contracting officer the flexibility to focus an audit on the inaccurate portions disclosed by the contractor. But as currently drafted, the rule offers no meaningful assurance of relief for contractors.

The proposed rule amends the DFARS to:

- Require contracting officers to request a limited-scope audit, unless a full-scope audit is appropriate under the circumstances, when a contractor voluntarily discloses inaccurate or otherwise defective pricing after contract award;
- Require the contracting officer to consult with the DCAA to determine the appropriate scope of an audit following a voluntary disclosure, based on an evaluation of the completeness of the contractor's disclosure; the accuracy of the contractor's cost impact calculation for the affected contract; and the potential impact on existing contracts, task orders, delivery orders or other proposals submitted by the contractor; and
- Clarify that voluntary disclosure of defective pricing does not waive government entitlement to the recovery of any overpayments, or the rights to pursue claims based on inaccurate, incomplete or outdated cost or pricing data.

Under TINA, a contracting officer may unilaterally adjust a contract price to exclude any significant amount by which the contract price was increased due to inaccurate pricing. The Defense Department is authorized to examine and audit "all records" related to the contract to evaluate the accuracy, completeness and currency of certified cost or pricing data required to be submitted under the act.

To avoid these contract adjustments and audits, contractors frequently resubmit certified cost or pricing data — sometimes reflecting only minor changes — because data that are frequently updated are less likely to be considered outdated or inaccurate. The resubmissions are burdensome for contractors who must conduct repeated "sweeps" for updated data.

The Defense Department initiated a study published in September to identify "unnecessary requirements for which costs exceed benefits." Among the recommended changes was a suggested return to a 1980s practice allowing contractors to voluntarily disclose inaccurate or incomplete pricing data post award and provide the Defense Department with refunds, without risk of initiating contractual adjustments or associated audits. As a result of this study's recommendations, the department directed the defense procurement and acquisition policy office to submit a revision to the DFARS to eliminate the requirement that a contracting officer must request an audit if a contractor voluntarily discloses inaccurate pricing post award.

But the proposed rule fails to adopt the suggestion for refunds without audit risk or meaningfully address contractors' underlying concerns. It provides no solid assurances to contractors about what to expect following a disclosure of inaccurate pricing information and does nothing to reduce the burden of repeated submission.

While the proposed rule allows a contracting officer the discretion to order a limited-scope audit, the standards for this determination are vague, and the incentive for the contracting officer to make this determination is unclear. It directs a contracting officer to request a limited-scope audit following a voluntary disclosure, unless a full-scope audit is "appropriate for the circumstances," based on consultation with DCAA. The proposed rule provides no guidance as to when a full-scope audit may be "appropriate," giving significant discretion to contracting officers and DCAA. The lack of guidance makes disagreement between the contracting officer and the agency likely — putting a contracting officer in the challenging, and often untenable, position of having to defy the DCAA in order to issue a limited-scope audit. The proposed rule expressly states that contractors who voluntarily disclose defective pricing may still be subject to claims based on the submission of inaccurate, incomplete or outdated pricing information, despite voluntary disclosure.

The Defense Department should amend the proposed rule before finalizing. First, the rule should provide clear guidance on what circumstances require a full audit following a voluntary disclosure, to reduce uncertainty for contractors and disagreement between contracting officers and the DCAA.

Second, the rule should guarantee contractors insight into the government's determination on the scope of an audit following voluntary disclosure.

Finally, the department should adopt the recommendation to allow contractors to voluntarily disclose inaccurate pricing data and provide it with refunds without facing the risk of contractual adjustments or the associated audits.

Herb Fenster, Terra Fulham and Jason Workmaster are partners at the government contracts group at the law firm of Covington & Burling LLP.

Budget Matters

By Jon Harper

Pentagon Chief Deals Blow to Navy's LCS

The Navy's littoral combat ship/frigate program took a major hit recently when Secretary of Defense Ash Carter suggested the service should slash planned procurement from 52 to 40 ships, a 23 percent cut.

In a Dec. 14 memo to Navy Secretary Ray Mabus, Carter criticized the service's shipbuilding plans and argued that some of the money slated for LCS and modified-LCS frigates could be better spent on other capabilities.

"For the last several years, the Department of the Navy has overemphasized resources used to incrementally increase total ship numbers at the expense of critically needed investments in areas where our adversaries are not standing still," he said. "This has resulted in unacceptable reductions to the weapons, aircraft and other advanced capabilities that are necessary to defeat and deter advanced adversaries."

The Carter memo calls on the Navy to procure eight fewer littoral combat ships and frigates over the course of the future years defense plan. The average cost of an LCS is about $450 million, according to the Navy's fiscal year 2016 budget request.

The memo also tasked the Navy to downselect to a single variant by 2019. Lockheed Martin and Austal USA are currently building littoral combat ships with different baseline designs.

Under the revised budget scheme outlined by Carter, the Navy would procure additional high-tech capabilities across the future years defense plan, including: 10 Flight III destroyers; SM-6 missiles and other advanced munitions; 31 additional F-35C joint strike fighters; an unspecified number of F/A-18 E/F Super Hornets; advanced electronic warfare capabilities; and upgrades to Flight II destroyers and attack submarines.

The Defense Department also intends to increase the Navy's budget by $1.7 billion over the course of the future years defense plan to further boost investments in such equipment, Carter said in the memo. "These choices will create a Navy that is far better postured to deter and defeat advanced adversaries."

Navy spokeswoman Lt. Cmdr. Hayley Sims acknowledged the memo but declined to address specifics.

"Shipbuilding has always been a priority for the Navy and we will continue to balance capability with capacity in our shipbuilding programs as we have always done," she said in an email. "We are aware of the memo, however budget discussions are pre-decisional. It would be inappropriate to discuss anything further until the [fiscal year] '17 budget is finalized."

The Pentagon's 2017 budget request is slated for release in early February.

In the wake of the Carter memo, Rep. Randy Forbes, R-Va., chairman of the House Armed Services seapower and projection forces subcommittee, made a case for boosting the Navy's budget.

"Secretary Carter has framed this as a choice between capability and capacity, but the undeniable reality is that our Navy needs more of both," he said in a statement. "We shouldn't have to keep making these hard choices between LCS and submarines, presence and surge capacity, modernization and readiness. … Unless we provide more resources for our Navy, it is not going to be able to keep meeting the demands that our nation and our national security strategy place upon it."

NAVY

Battle Looms Over Military Health Care Reform

■ Members of the Armed Services Committees are expected to make a push this year for military health care reform. But opposition from advocacy groups and lawmakers standing for reelection may stymie those efforts, analysts said.

In recent years, Pentagon officials have been sounding the alarm about the need to rein in personnel costs. Health care for troops, retirees and their families now costs the Pentagon about $50 billion annually, roughly 10 percent of its budget.

"One out of every 10 dollars is going to health care," said Stephen Ondra, a former military doctor and the current chief medical officer for the Health Care Service Corp., at a recent Center for a New American Security conference. "We have to do that in a more efficient way … that will give more flexibility in terms of budget dollars to the Department of Defense" for other priorities such as modernization.

In a report last year, the Military Compensation and Retirement Modernization Commission estimated that implementing its health care reform proposals — including compelling non-active duty beneficiaries to select commercial insurance plans — would save the Pentagon more than $6 billion annually.

The commission "provided a nice pathway," said Tina Jonas, former Pentagon comptroller, at a recent Center for Strategic and International Studies conference. "I don't know how far they [lawmakers] will go but … it could provide a nice potential relief" for modernization accounts.

But advocacy groups are lining up against potential changes to the TRICARE system.

"Proposals earlier this year recommended … forcing beneficiaries into plans similar to those of federal civilians, imposing significantly higher fees, and means-testing … benefits so beneficiaries with higher incomes would pay even more," the Military Officers Association of America, a non-profit group, said in a December statement. "All of those and others could be on the table again in 2016," it warned.

MOAA leaders will be "storming the Hill" this spring to pressure lawmakers not to approve reforms that the group opposes, the statement said. It encouraged likeminded individuals to send a "barrage" of correspondence to members of Congress.

"We've seen from years of experience … when legislators get tons of mail on a topic, the vast majority aren't going to ignore their constituents," the statement said.

Phillip Carter, director of the Military, Veterans and Society Program at CNAS, said concerns about personnel costs "don't trump the very effective and very powerful groups in Congress and in Washington that stand up for people" who receive military benefits.

Ondra said approving major health care reforms in 2016 would be difficult politically. "In an election year I'm not overly optimistic, but I think that we can start the conversation."

AIR FORCE

Air Force Facing Budgetary Train Wreck

■ Absent a major increase in topline funding, the Air Force acquisition budget will experience a crunch in the 2020s, analysts said.

The service is projected to spend more than $67 billion in fiscal years 2016 through 2020 on its top three priorities — the F-35 joint strike fighter, KC-46 tanker and long-range strike bomber — as well as C-130 cargo aircraft and unmanned aerial vehicles, according to the Congressional Research Service.

Budget plans for this period also include initial funding for: joint surveillance target attack radar system recapitalization; a new combat rescue helicopter; a presidential aircraft replacement; and a new advanced T-X trainer aircraft.

These programs, if carried to fruition, are all likely to be in the procurement stage in the 2020s. The Air Force is therefore facing a modernization "bow wave" unless plans are modified, budget experts said.

"Procurement spending on established programs will continue to be substantial," Jeremiah Gertler, a military aviation specialist with the Congressional Research Service, said in a December report, "The Air Force Aviation Investment Challenge."

"How will the future Air Force procurement budget accommodate the new programs as well?"

Todd Harrison, a defense budget expert at the Center for Strategic and International Studies, said procuring just "the big three" — F-35, KC-46 and long-range strike bomber — would be a major modernization burden. "All of those programs will be at or ramping up to full-rate production in the next decade," he noted at a recent CSIS conference. "But … you've got several other major programs that are supposed to be ramping up at the same time."

The Air Force may need to defer or delay programs or find other sources of funding, Gertler said in the report. Steps the service could potentially take include: reducing annual quantities of the F-35; retarding the growth of research-and-development programs; deferring the KC-Y follow-on tanker; or securing funding for the new bomber through a non-Air Force budget account.

The Air Force is not preparing for the bow wave, Harrison said. "We're not even really dealing with it yet. We're not even seeing it yet" in budget documents.

Gertler said projecting program budget requirements 10 years out instead of five in the Defense Department's future years defense plans "could more tangibly illustrate the resource decisions required today to avoid budgetary 'train wrecks' in the future."

Email your comments to jharper@ndia.org

United Kingdom Creating Defense Innovation Cell

The United Kingdom is investing more than $1 billion to fund cutting edge defense technology, said the country's secretary of state for defense.

"At a time of growing threats — nuclear, conventional, state-based or terrorist — the United Kingdom is stepping up with bigger and stronger defense," said Michael Fallon. "We are increasing our defense budget. We are increasing the size and power of our armed forces so that we can do more to protect our security. And in so doing, we aim to become an even stronger partner of our most steadfast ally, the United States."

The United Kingdom will put $1.5 billion into an innovation fund that will help it secure an operational advantage in the future, he said during a December speech at the Atlantic Council, a Washington, D.C.-based think tank.

Taking a page out of the United States' book, the country wants to create its own version of the Defense Innovation Unit - Experimental, he said. U.S. Secretary of Defense Ash Carter established DIUx in 2015 to better tap into the work being done in Silicon Valley.

"We will be launching our Emerging Technology and Innovation Analysis Cell to help identify game changing technologies. We are setting up a new center to pool the intelligence of the best brains in British business, academia and the public sector," Fallon said.

The U.K. government — currently being led by the Conservative Party — has pledged to spend 2 percent of its GDP on defense. Over the next decade, it intends to allocate more than $265 billion to new equipment, he said.

The country wants to work more closely with the United States on defense innovation, he noted. The United Kingdom plans to tighten links between the two nations and work together on emerging technology demonstrators, participate in joint war games to test ideas and adapt new operating concepts, Fallon said.

"We want to learn from you and to collaborate more with you," he said. "I've been impressed by the way in which you've been able to tap into some of the fizz, if I can call it that, of the smaller high-tech companies and bring their applications to bear on defense solutions."

Traditionally, when the United Kingdom needs a new piece of equipment, be it an airplane or a frigate, it sends out a request for proposals to industry, Fallon said. "What we've not said to our high-tech center is, 'You come and tell us what solutions you've got for some of the challenges, some of the technologies that our adversaries are employing.'"

The nation also plans to make more investments in small businesses, he noted. It intends to spend 25 percent of its defense dollars on small- to medium-sized companies to "try and attract more of this brain power into defense," he said.

The United Kingdom plans to work with organizations such as Glasgow University, the University of Strathclyde, Amethyst Research and Helia Photonics, all of which are based in Scotland, a Ministry of Defence statement said.

The ministry said more details about the innovation center and other technology initiatives would be available later in 2016.

— Yasmin Tadjdeh ▪ ytadjdeh@ndia.org

DEFENSE DEPT

Army Tests Counter Drone Technology

■ To combat the increased use of small drones by adversaries, the Army is looking to develop technology that will more effectively counter them.

Over 90 countries and non-state actors operate drones today, including at least 30 that employ or are developing armed drones, according to a June 2015 Center for a New American Security report titled, "A World of Proliferated Drones: A Technology Primer."

"We've been in this environment where improvised explosive devices … have proven very, very lethal to U.S. forces," said Paul Scharre, senior fellow at CNAS, a Washington, D.C. think tank. Now "we're looking at a world where instead of worrying about running into IEDs, the IEDs are coming [and] looking for us."

The threat posed by the proliferation of drones is a "game changer," affecting the way that U.S. ground forces think about protection, he said. They "have been able to fight for the last 50 years — basically the last half a century — without worrying about threats from the air" because the U.S. Air Force has been so dominant, Scharre said. "This begins to change that."

Even if the Air Force has superiority up at 30,000 feet, smaller drones will be able to come in below the radar, which makes them harder to detect. Additionally, the U.S. military is not going to use an F-22 to shoot down a hobbyist drone, he said.

Soldiers and Marines are most susceptible to the threat because they are fighting in more congested, urbanized areas where adversaries, including actors like the Islamic State, might choose to use such vehicles, Scharre noted.

Northrop Grumman has developed a system called "Venom" that could address this growing problem, according to a company executive.

The system is currently being tested under a contract with the Army, said Charles Michaels, business development manager for laser systems at Northrop.

Venom demonstrated the ability to identify and track small unmanned aerial systems and provide precision targeting on the move at the Army Maneuver-Fires Integrated Experiment exercise held at Fort Sill, Oklahoma, in July, Michaels said.

The core of the system is an enhancement to the company's lightweight laser designator rangefinder (LLDR), a current Army program of record. The system can recognize targets in day, night and obscurant conditions, a December press release said. Northrop began delivering LLDR in 2004, and the service has fielded more than 2,700 systems.

Venom positions the rangefinder on a stabilized, gimbaled vehicle mount, Michaels said. It has a vehicle-agnostic design, meaning it can be installed on a wide range of Army platforms, he added.

— Allyson Versprille ▪ aversprille@ndia.org

NORTHROP GRUMMAN, MUTUALINK

Wearable Device to Assist First Responders

■ A new device called the "Wearable Smart Gateway" can connect sensors — such as body cameras, heart rate monitors and locator beacons — worn by first responders or members of the military and feed that data back to a command center.

The device, which was developed by Mutualink, a Wallingford, Connecticut-based communication and multimedia company, can be used to give agencies and commanders better situational awareness, said one executive.

"A remote agency can see the data, how a soldier or a first responder is feeling by their biologic measurements [and] what they're seeing from real-time body cameras," said Michael Wengrovitz, vice president of innovation for Mutualink.

Data is sent securely and instantly to a cloud-based network, which can be accessed by a command center, he said. It can be viewed through a browser on a computer, a tablet or a smartphone.

The device is powered by Intel's Edison chip, he said. "It's basically a computer, which is the size of a postage stamp, that runs off a small battery. … It hardly takes any energy at all."

It can be used for a variety of situations, including monitoring a person's vital signs, Wengrovitz said.

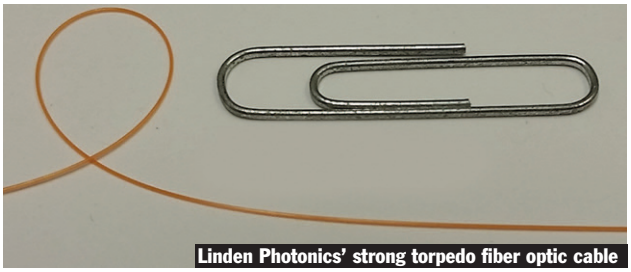
For example, if a first responder is out in the field and doing a strenuous mission, sensors on his or her body could alert a commander to an elevated heart rate, he said.

"The heart rate changes colors on the display when it gets above a certain threshold," he said. It can also set off an audible alarm that will notify the responder and the commander.

That commander could then send in a replacement or call an ambulance. Data from the wearable sensor can then be transferred directly to the hospital, Wengrovitz said.

The Wearable Smart Gateway comes in two different versions. One is tiny enough to fit into a vest or coat pocket and the other is a ruggedized device that can snap onto the back of a cell phone.

— Yasmin Tadjdeh ▪ ytadjdeh@ndia.org



Linden Photonics' strong torpedo fiber optic cable

Emergency Military Network to Go Under Sea

■ Military scientists are developing a rapidly deployable undersea network, which could restore tactical military communications that are compromised by adversaries.

In September, the Defense Advanced Research Projects Agency awarded a $1.9 million contract to LGS Innovations, a networking and communications solutions company, for phase one of the tactical undersea network architectures (TUNA) program.

The company has two partners for the project: Linden Photonics, which specializes in high-strength fiber optic cables, and Tethers Unlimited, a private aerospace company. The team aims to "develop the world's strongest neutrally buoyant undersea cable" for the network, an LGS press release said.

"Such technologies will allow the DoD to maintain an information advantage, even in contested areas," said Bob Beyers, technical director of applied research and technology at LGS Innovations.

The initial phase of the TUNA program is focused on concept and technology development in three areas: system design, small fiber optic cable systems and buoy nodes, the press release said. The buoys would function as signal relay points for the network.

One of the main challenges "is the development of an undersea microcable that simultaneously possesses small size, high strength, low optical loss and neutral-buoyancy, and is producible in long cable lengths," Beyers said in an email. DARPA requires that TUNA technologies be capable of surviving deployment and operation in the ocean for at least 30 days. To date, most undersea cables are big, heavy and expensive, he noted.

The cable LGS has proposed is based on a commercial offering by Linden Photonics called "strong torpedo fiber optic cable," Beyers said. LGS proposed changes in design and fabrication that would enable the product to better meet the military's needs, he said. The cable uses a highly resistant liquid crystal polymer to improve strength.

Phase one of the program will last 15 months. LGS will provide model simulations, design and analysis as well as scaled development and demonstration for the technology over that period. DARPA has plans for a second phase focused on the implementation of an integrated end-to-end network prototype.

— Allyson Versprille ▪ aversprille@ndia.org

DARPA Investing in Vanishing Air Vehicles

■ Air vehicles delivering critical supplies to ground troops could soon simply disappear into thin air after dropping their payload, reducing troops' environmental footprint.

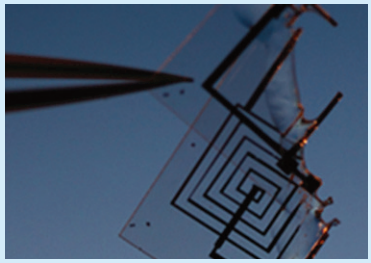
The project, which is being spearheaded by the Defense Advanced Research Projects Agency, is known as the "inbound, controlled, air-releasable, unrecoverable systems" (ICARUS) program.

"The main goal is to be able to deliver supplies whether they … [are] things like batteries, water, medical supplies to teams of either military or humanitarian personnel," Troy Olsson, ICARUS' program manager, told National Defense.

The vehicle, after dropping off its payload, would then disappear after being triggered by an operator or environmental factors, such as sunlight or temperature.

While the idea may seem too futuristic to be true, ICARUS builds off a previous DARPA project known as the "vanishing programmable resources" (VAPR) program, Olsson said.

"The goal of the VAPR program is to build transient or vanishing microsystems, so think of small-scale wireless sensor devices that can vanish on command," he said. "Part of that program was to make things like circuit boards [and] packaging."



One approach to that was a vanishing polymer, he said.

DARPA worked with the University of Illinois, Cornell and Georgia Tech on VAPR. Recently, there have been major advancements in the program that led agency officials to believe creating a disappearing delivery vehicle was feasible, he said.

The University of Illinois several years ago developed circuit boards that could sublimate from a solid into a gas when exposed to ultraviolet light. Georgia Tech recently piggybacked off that development and demonstrated it could generate the same result with visible light, he said.

"They basically have figured out a way to tailor the wavelength at which that vanishing of the polymer occurs all the way up to 600 nanometers," he said. "In the context of ICARUS, you might think this might be something like sunlight, for example."

Additionally, Cornell University recently demonstrated that it could increase the stiffness of the polymers from something on the order or a rubber band to a piece of Tupperware, he said.

While Olsson is optimistic that DARPA will develop a variety of air vehicles for ICARUS, he said it is unlikely that the technology is mature enough to produce a drone.

"There's nothing precluding a powered aircraft from the ICARUS program," he said. "I can't envision one, but that doesn't mean somebody else can't."

ICARUS is a two-phase program that will last 26 months with total funding of about $8 million. DARPA published a broad agency announcement in October and bids were due in late November.

— Yasmin Tadjdeh ▪ ytadjdeh@ndia.org

LINDEN PHOTONICS, DARPA

3D Database to Improve Simulated Flight Training

■ Rockwell Collins has unveiled a synthetic database to model environments across the globe that will reduce simulated training costs while improving military readiness, according to a company executive.

The synthetic environment is the newest version of the company's WholeEarth product line, which was first introduced over 15 years ago. The enhanced environment combines geo-specific imagery data, 3D models and "geo-typical" imagery — swatches that are generic but still representative of a particular region's topography. The product creates more realistic training scenarios for service members who will eventually fly in a variety of locations, said Lance Moss, principal product manager for simulation and training solutions at Rockwell Collins.

The product is unique because it can deliver global representations at any altitude, during any point in the day, in both the summer and winter seasons, and at all wavelengths with 0.5m resolution, he said.

The product is currently in an "alpha state" with the official release happening in May. "From now until then we will be finalizing initial content — mostly the continental United States," Moss said.

"Then, over the next two years we will be tailoring the entire rest of the Earth with different content in those regions so it looks like Asia and Africa and Europe and Australia and so on."

The company plans to have follow-on releases twice a year — in November and May — over that two-year period. After that time, it hopes to have the entire globe represented, he said.

The WholeEarth product already has two international customers in the Asia region, according to Moss. They've "placed preorders and are waiting for that May release," he said. Though the initial product launch will focus on U.S. content, the company is also going to provide tailored data for those two customers, he said.

Updated regions moving forward will depend on need and demand. "Right now, the needs are Western and Eastern Europe, the Middle East … and some Asian" regions, he said.

The product is being touted as a "ready made," low-cost option because it uses nonspecific geographic representations, while also giving customers the flexibility to add high-resolution, photo-exact insets if there is an area where they want more precise imagery. The inset can be placed on top of the Rockwell Collins' dataset and "it will be integrated seamlessly on a real-time rendering" without additional costs for blending and integration, Moss said.

The WholeEarth synthetic environment has "a relatively small cost compared to building your own data," he said.

The Rockwell Collins database would cost less than $10,000 for annual maintenance and updates, and the standard option for the WholeEarth solution would be in the "tens of thousands at most," Moss said.

— Allyson Versprille ▪ aversprille@ndia.org

ROCKWELL COLLINS

Finance, Health Care, Agriculture Play Key Roles in Critical Infrastructure Protection

By Chris Wiedemann

Of the major agencies of the federal government involved in critical infrastructure protection, the Department of Homeland Security and the Department of Defense receive the most attention.

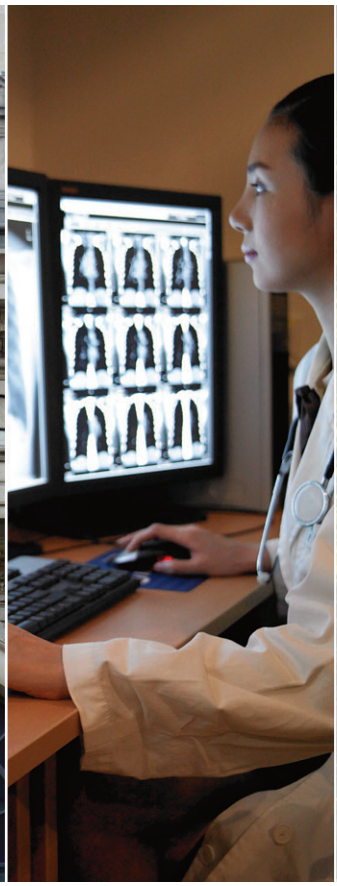
But there are three less discussed, but equally important, elements of the nation's critical infrastructure: the financial sector — banks and the technology they rely on — health care and public health, where critical infrastructure constitutes hospitals, medical transport and drug supplies; and food and agriculture — farms, supporting infrastructure, and financial systems.

When Presidential Policy Directive 21 (PPD-21) broadened the critical infrastructure segments and definitions originally outlined in Homeland Security Policy Directive 7 (HSPD-7), it created new responsibilities for a number of federal departments, termed sector-specific agencies.

They are responsible for developing and disseminating infrastructure protection requirements to states, local authorities and industry.

While there is little opportunity to sell explicitly security-related technologies to the government — the market for those rests with the infrastructure owners themselves — sector-specific agencies have requirements around information sharing and dissemination that industry can help meet. And anyone looking to support the mission of critical infrastructure protection outside of DHS should be reaching out to the Departments of Treasury, Health and Human Services, and Agriculture.

> "Understanding where the pockets of protection responsibility lie will enable industry to provide real value to both the government and the American public."



THINKSTOCK

The responsibilities of the sector-specific agencies entrusted with infrastructure issues are diverse.

The agency for financial services is the Treasury Department, and those looking to assist their critical infrastructure mission should look to the office of critical infrastructure protection and compliance policy, under the direction of the assistant secretary for financial institutions. The office coordinates the development and implementation of financial infrastructure protection requirements, which revolve primarily around data privacy and redundancy. These requirements are intended to ensure that a successful attack against a major system does not shut down the nation's financial infrastructure.

The office also facilitates information sharing between the federal government, state and local regulators and the financial sector.

In this capacity, it will have industry requirements for tools and services enabling information exchange and coordinating activities between geographically disparate stakeholders. This office is also involved in shaping policy around financial privacy; as such, those in the data protection industry need to keep an eye on the latest developments coming out of OCIP.

Protection of the health care and public health sector is the responsibility of Health and Human Services, specifically the critical infrastructure program under the assistant secretary for preparedness and response.

That program is the federal presence on a coordinating body known as the healthcare sector coordinating council, which is focused this year on the second stage of their critical infrastructure plan. Having successfully identified which elements of the health care and public health infrastructure are mission critical, the focus has shifted to risk management tools that can help infrastructure owners protect the critical systems they control from system failure or external attack.

The Health and Human Services crit-

ical infrastructure program serves in a coordinating capacity in this effort, and requires the same information sharing capabilities needed by other agencies to facilitate communication and collaboration between stakeholders across the country. There are also needs for data analytics and visualization capabilities at the federal level to enable more effective decisions driven by stakeholder-provided data.

With responsibilities over areas ranging from water and food transportation to farm-specific financial systems, the food and agriculture sector is perhaps the broadest of the identified 16 critical infrastructure sectors. Consequently, responsibility is split between the Department of Agriculture — specifically the national security policy staff at the office of homeland security and emergency coordination – and the Food and Drug Administration, which is primarily involved in researching and developing food safety technologies that are critical to food and agriculture's protection responsibilities.

Both of these agencies are heavily involved in research and development of infrastructure-protecting technologies, and industry has an opportunity to assist. Specifically, FDA's center for food safety and applied nutrition is leading efforts to develop and disseminate new technologies that safeguard the country's food supply, with a particular focus on responding to terrorist actions.

PPD-21 created protection mandates that extend far beyond information systems and "traditional" infrastructure.

This opens up wide swathes of the government to industry engagement, particularly around information sharing, analytics, and research support. Understanding where the pockets of protection responsibility lie, and acting on that information, will enable industry to provide real value to both the government and the American public by helping to ensure that the nation's critical infrastructure remains safe. **ND**

Chris Wiedemann is a senior analyst with immixGroup, an Arrow company. He can be reached at Chris_Wiedemann@immxgroup.com, or connect with him on LinkedIn at www.linkedin.com/in/ccwiedemann.

COMMENTARY

Naval Energetics Research Needs Renewed Focus

By Ashley Johnson

While other nations are making strides in energetic material development, the United States has remained dormant. The result is a surface fleet that lacks weapons with the range to attack aircraft, ships and submarines outside enemy anti-ship cruise missile range, according to one analyst.

The Navy deemphasized sea control in the 25 years since the end of the Cold War because U.S. maritime supremacy was essentially unchallenged, wrote Bryan Clark, an analyst at the Center for Strategic and Budgetary Assessments. "Less investment went into surface fleet anti-submarine warfare and surface warfare capabilities or next-generation anti-air warfare weapons." Similarly, the Defense Department saw no peer competitors and its energetics research and development spending dropped precipitously.

Lack of evolution in this field isn't unique to the surface fleet. It impacts every domain of the naval enterprise: surface, undersea, air and ground. A renewed focus in energetic materials — research, development, testing and evaluation of energetics materials and systems — is required to regain the technological advantage and to provide solutions for emerging anti-access/area

> "We can recapture technical superiority with organic, in-house talent and capability."

NAVY

denial challenges.

Energetics are energy releasing materials — explosives, propellants, pyrotechnics, reactive materials, related chemicals and fuels — as well as their application in propulsion and ordnance systems engineered to optimize their effects. These complex materials are core to weapon development and help determine performance — range, speed, lethality and other effects. Energetic materials get weapons to the intended target, and ensure maximum lethality once they arrive.

Previous generations of these materials enabled U.S. technological superiority. Nitrocellulose propellants, Explosive D and fuzing extended naval gunfire's range and effects. Solid propellants in tough, lightweight, composite casings enabled submarine and ship-launched missiles; and thermobarics engineered for shoulder-launched munitions crumbled buildings at Fallujah.

But remaining on top requires continuous devotion, discipline, proficiency and technical rigor. Talent, novel concepts, capability and capacity are readily available within the Defense and Energy Departments, academia and industry. When there is appropriate interest and funding, new solutions are always possible. Examples include:

• Re-establishing a U.S. source of triamino-trinitrobenzene (TATB), an energetic material used in the booster and fuzing systems for missiles, bombs and artillery warheads. For decades, there had not been a continental U.S. source, and the United Kingdom source had not produced the material for nearly 10 years. Prior to the TATB working group's efforts, DoD had been forced to utilize stockpile material, which had been nearly exhausted.

• Developing a Lead-Azide replacement to reduce environmental concerns and meet Environmental Protection Agency requirements. The "Green Primary Explosives team" at the Naval Surface Warfare Center developed, tested and qualified an environmentally benign, drop-in replacement. The new compound is the first primary explosive qualified by the Navy in more than 90 years, and will reduce the amount of lead used in detonators and fuzes by thousands of pounds a year.

• Using microelectromechanical systems, or MEMS, to increase munitions system reliability and meet DoD unexploded ordnance requirements. After 2018, U.S. forces will be required to employ only cluster munitions that do not result in more than one percent of them being unexploded. The Navy's early research using MEMS fuzes to reduce failure rates led to funding from the Office of Naval Research.

While these are impressive examples, they are also reactionary. For more than 15 years, the nation has accepted risk in this area by reducing research and testing investments, while others increased theirs. Today, naval energetics can make only limited contributions to advanced component development and prototypes.

"It is inconceivable that the United States should be anything but at the cutting edge of energetics," wrote former U.S. Marine Corps Commandant Gen. Michael Hagee. The inconceivable has occurred. The Navy accepted risks regarding energetic materials and systems, due to a variety of factors.

Reduced workforce was another factor. According to the naval research advisory committee's 2010 Summer Study, the naval R&D workforce dropped 50 percent in 15 years. The energetics workforce took its cuts, too. In 1994, Naval Surface Warfare Center Indian Head had 13 personnel conducting energetic material molecular design. Today, there are just four.

While the energetics workforce and research funding decreased, the naval warfare centers' workload increased 25 percent in the decade following 9/11 to meet increased operational tempo demanded by homeland security needs and the wars in Iraq and Afghanistan.

There is a misconception that rail guns and directed energy systems negate future energetics-based weapons. "By equipping ships with rail guns rather than standard artillery, the Navy could eliminate the hazards of having high explosives on board ships," stated Scientific American. Directed energy technology will offer tremendous capabilities. Yet there are fiscal and operational barriers, and an all-electric Navy doesn't address the host of other energetic materials systems currently out there to fight wars. Warheads, rocket motors, propulsion systems, and cartridge and propellant-actuated devices — all energetics-based — touch every part of the fleet and its wings.

Additionally, these electric weapon systems have no role in the underwater domain, where continued dominance should remain a high priority.

BrahMos is the world's fastest cruise missile.

There is a misperception that energetic materials have little left to offer. Investments had dropped significantly by 2008 and continued to decline for another reason. "The consensus in the DoD scientific community is that traditional explosives and energetics performance ... has likely peaked," wrote a senior Navy official.

We are far from reaching the limit in this field as evidenced by the progress of a few internal R&D efforts:

• Densified propellants for shoulder-launched assault weapons: Due to the large overpressure produced by shoulder-launched weapon systems, they cannot safely be fired from an enclosure, requiring the operator to leave cover, increasing exposure to enemy fire.

By developing a system inspired by a recoilless rifle, this advancement will keep Marines alive by drastically reducing overpressure and fireball; reducing peak-sound, pressure-level by more than 10 decibels; and increasing impulse, or push forward, by up to 35 percent per unit volume, allowing a reduction in propulsion system size and weight.

• High-density reactive materials that replace inert steel in warhead casings: This effort significantly increases the lethality of weapon systems against an increasingly harder target set. While conventional munition casings fragment after impact, HDRM casings release additional incendiary energy to dramatically increase explosive force.

ANURAG

• Hybrid rocket fuel that matches solid fuel performance while creating a safer system that can be stopped and restarted in flight: The new boron-based system overcomes traditional difficulty of inefficient combustion with boron by elimination of hydrogen in the composition. The increased performance was demonstrated using a sub-scale rocket motor test stand constructed at the command.

The United States treated energetic materials and systems as a technologically frozen commodity, but other nations did not.

Development of the BrahMos missile is recounted in "The Path Unexplored" by India's BrahMos Corp. CEO A. Sivathanu Pillai. Meeting with Russian missile developer NPO Mashinostroyenia, Pillai said India sought a missile superior to the U.S. Navy's Tomahawk missile. "This was to be our magical first-strike weapon," wrote Pillai. The Russians stated they already had a liquid ramjet engine intended for a supersonic missile. A Russia-India venture resulted in reportedly the world's fastest cruise missile, with Mach 2.8 speed and 290 kilometer range.

"Chinese scientists have become more active on the world stage in the field of energetic materials," stated the Journal of Energetic Materials. Between 1991 and 2011, Chinese scientists published 6,415 technical papers on energetics – compared to the 5,720 published by U.S. scientists.

Such energetic materials and systems enable advanced weapons, many of which are easily available on the global market and challenge current U.S. capabilities. Twelve surface-launched missiles outrange the U.S. Navy's Harpoon antiship cruise missile. Not only longer-ranging, other nations' ASCMs are precision guided, sea-skimming, maneuverable, and can accelerate in terminal approaches to Mach 2.9, reducing reaction times.

Now consider the future. News media reported that Russia seeks to develop a new fuel that will power Mach 5 hypersonic missiles. Documents also evidence quests for "super-cavitating" undersea weapons, with speeds of more than 200 mph — a capability greatly dependent on propellants. Additionally, Indian news broadcasts reported their country's development of CL-20 explosive — created, but not pursued, by the United States — which is four times more powerful than standard RDX explosive.

Foreign weapon advances in multiple domains are improving and expanding.

"The combination of these rapidly-proliferating approaches permits adversaries to attack from close in or at great distance — concentrated in time and space with unprecedented precision," wrote then Vice Adm. John Richardson and Lt. Joel Ira Holwitt in the June 2012 issue of the U.S. Naval Institute's Proceedings magazine. "Our Navy's traditional standoff ranges have become less and less protective."

The challenges go beyond anti-access/area denial. Non-state actors are acquiring other nations' advanced weapons to engage in hybrid warfare.

Deputy Secretary of Defense Robert Work recognized the implications.

"We have seen in Ukraine the state-backed proxy separatists have access to advanced capabilities. ... They're backed by modern fire and counter-fire capability that the Army and the Marine Corps simply [have] not had to consider since the end of the Cold War," said Work. "Our enemies have gone to school on us at least since 1991 Desert Storm, and they have adapted with a vengeance. They spent the past few decades investing heavily in capabilities that counter our own."

While the nation has invested heavily in enhanced platforms over the past 15 years, investments in weapon systems have not maintained pace.

We can recapture technical superiority with organic, in-house talent and capability. Our naval energetics renaissance must begin now because developing the next generation of enhanced capabilities depends on a broad expanse of science and engineering disciplines that, like all things in the acquisition cycle, takes time.

This specialized work is unique to the Defense Department. Industry has minimal involvement in the field due to environmental and safety risks, long-term investments and limited commercial applications. Scientists must first conduct basic research to explore the first principles of chemistry, physics and thermodynamics. Scientists and engineers can then test hypotheses to explore concept feasibility, ultimately leading to the development, test and evaluation of prototype systems.

The 2014 Defense Innovation Initiative seeks to advance military superiority. This initiative must include a plan to increase energetic materials and systems research and testing. Warfighters are demanding weapons go farther, go faster, hit harder, have tailored effects and get smaller. The quest for smaller enables existing platforms and personnel to carry more, and accommodates miniaturized weapons being delivered by increasingly smaller, unmanned systems.

We need to address limitations of our weapon systems with respect to range, speed, size, weight, lethality, signature, accessibility and insensitivity across all domains. These calls imply requests for new weapons with new energetic materials and systems — not simply modifying weapons developed 50 years ago.

To meet these demands and fulfill our responsibilities, more subject matter experts are required. After years of cuts and attrition, there are few left and the majority of those that do remain are in the twilight years of their careers.

A 30-year naval energetics-based systems technology plan is needed for the current fleet, the fleet in construction and the fleet in planning. These fleets require state-of-the-art energetic materials and systems, initially to address capability gaps and pursue countermeasures and advantages, but ultimately to regain the nation's full spectrum dominance against any and all potential adversaries. **ND**

Ashley Johnson is the technical director of the Naval Surface Warfare Center Indian Head explosive ordnance disposal technology division.

Lockheed Expands Training And Simulation Enterprise

By Allyson Versprille

Lockheed Martin is increasing investments in training and simulation technologies with the expectation that international and domestic demand for such systems will remain strong, said executives for the defense contractor.

"In general, we're seeing continued demand out of the U.S. for training," said David Scott, vice president of business development and strategy for training and logistics solutions at Lockheed. "While there is a scaleback in the overall budgets or a flattening of budgets, there is a recognition that training is an essential component to have a force that is ready to fight."

Michael Blades, a senior analyst at the market research and consulting firm Frost & Sullivan, said the training and simulation market is attractive because while other programs in the defense budget are experiencing cuts, funding for training remains stable. Blades projected that the combined annual growth rate from fiscal year 2015 to fiscal year 2020 for total spending on training and simulation would increase about 1.7 percent per year. That number is close to the rate of inflation, which means training and simulation is a steady market, he said.

Another reason companies like Lockheed would be interested in investing in such systems is because militaries in general want to do more with less, he said. "They want to be able to do more training for readiness with the same amount of dollars."

One solution to that problem is using immersive virtual training as opposed to expensive live training, Blades said.

Scott said demand for training and simulation capabilities is even stronger overseas, especially in areas like the Middle East. "They are proceeding into operations there, and they recognize and now have a stronger need for training," he said. There is a "general recognition that it's not just owning an airplane or a ship or a tank, but you have to have the trained crew to operate it."

One of the main focuses of Lockheed's business strategy is what the company refers to as its "turn-key solutions." Such programs offer a performance-based approach where end-to-end training is delivered as a service.

One of the company's model programs is the Republic of Singapore Air Force Basic Wings Course. Through the course, Lockheed Martin-led "Team 21" — a partnership with Pilatus Aircraft and Hawker Pacific — has delivered 50,000 flying hours and trained more than 300 pilots since 2008.

The Basic Wings Course program falls under a 20-year service provision contract. Through the agreement, Lockheed and its teammates supply the aircraft, sustainment engineering, maintenance support and a ground-based training system, which includes several simulators, part task trainers and a complete desktop training environment, said Tom Quelly, director of business development at Lockheed Martin Mission Systems and Training.

The contractor also delivers the courseware, monitors and upgrades obsolescent parts, and supplies ground-based instructors for the simulators, he noted. The Singaporean government is responsible for providing the flight instructors in addition to logistics and training IT management systems, he said.

These types of partnerships offer benefits to both Lockheed and its customers, Quelly noted. By integrating all of the

MAJOR TURN-KEY PROGRAMS

- **Republic of Singapore Air Force Basic Wings Course program**

- **United Kingdom Military Flying Training System program**

- **Australia's AIR 5428 Pilot Training System project**

F-35 JOINT STRIKE FIGHTER TRAINING PROGRAM

components of the training system and tailoring them to a specific country's needs, turn-key arrangements result in higher-quality graduates, shorter training terms and reduced costs, he said. Past programs have saved 15 to 20 percent over traditional acquisitions, he noted.

Another benefit for the customer is a steady cost for the duration of the contract, which is typically delivered over a long period of time — about 20 to 25 years — at a fixed price, Quelly added.

Through these fixed-price arrangements, the company assumes a lot of risk and is incentivized to offer the service in the most efficient manner, at the lowest cost. "If we manage that risk well, we meet our financial metrics," Quelly said. "If we don't, we're at risk."

For Lockheed, such contracts provide the company with long-term stability and growth. "They're very predictable as far as our business metrics," he said. "They give us a very good opportunity to build and grow a stable workforce of training experts."

Additionally, long, sustained partnerships enable the company to remain close to its foreign customers to better identify their needs and where to target internal research and development, Quelly said. "On the training programs we've had — the Singapore program or the U.K. MFTS [Military Flying Training System program] — they've allowed us to become aware of requirements and needs that we've in turn put investments against." MFTS is a turn-key program that Ascent — a 50/50 joint venture between Lockheed Martin and Babcock International — secured in 2008. That contract spans 25 years.

In December, Lockheed-led Team 21 was awarded a contract for approximately $850 million for an initial seven-year program to train the next generation of Australian military pilots. "Performance-based options for up to 25 years will provide the opportunity to extend the length and increase the value of the total contract," a company press release said.

Through the AIR 5428 Pilot Training System project, Lockheed will be responsible for delivering an integrated training solution for all future pilots in the Australian air force, navy and army, the release said.

The company is also in ongoing discussions with Qatar to potentially

LOCKHEED MARTIN

Singapore's Basic Wings Course program uses Pilatus' PC-21 trainer.

implement such a program there, Quelly noted.

Another key component of Lockheed's training and simulation portfolio is the F-35 joint strike fighter.

By early January, 251 pilots from six nations — the United States, Italy, the United Kingdom, the Netherlands, Norway and Australia — had been taught on Lockheed's F-35 training system. The centerpiece of the system is the company's full mission simulator, a high-fidelity 360-degree visual dome.

"The code that flies in the F-35 is the code that flies in the trainer," said John Leonhardt, F-35 technical operations director at Lockheed. "That gives you the fidelity and the seamless training back and forth. About 50 percent of missions could actually be trained in the simulator."

For previous aircraft, only 40 percent of missions could be trained on such devices, he said. "Taking 10 percent of that training and moving it into the … simulator is a huge sustainment cost [saver] in terms of fuel, air time, and wear and tear on the physical aircraft."

Using simulators for training is important because they can replicate difficult environments that are impossible to test against in a live aircraft, Leonhardt said. "Simulation allows you to do that using real-world physics-based models and weapons-based models, and bringing them together in a classified way to test the limits of the aircraft." Such an environment is safer for both the platform and the pilot, he added.

Tactically the F-35 will fight in a formation of four aircraft. To enable pilots to rehearse missions in a more realistic setting, four full-mission simulators can be linked together allowing airmen to train side by side in real time. This gives them the ability to hone their tactical skills for employing the joint strike fighter against ground and airborne threats, a company press release said. The U.S. Air Force began training on these simulators in December at Hill Air Force Base, Utah. The first Air Force squadron will reach combat readiness in August.

Lockheed also provides the maintenance training for the joint strike fighter. By early January the company had trained 2,445 personnel from the aforementioned countries on its aircraft systems maintenance trainer.

The defense prime is currently delivering on the system development and demonstration contract for the F-35 program. This includes aircraft testing, low-rate initial production, initial pilot and maintainer training, and sustainment, a company spokesperson said in an email. That phase will conclude in 2017 with the delivery of Block 3 capabilities.

Lockheed is in the process of negotiating the next steps in the F-35 program with the joint program office and the military services as it prepares for full-rate production, Block 4 capabilities and global training and sustainment, the spokesperson said.

After 2017, "we are competing for each of those next increments," Leonhardt said. "Each LRIP [low-rate initial production] we will compete and put our formal bid in, and we'll leave it up to the JPO to select the best bidder."

Blades said it could be difficult for Lockheed to maintain its role providing the training and the sustainment on the F-35 in years to come. They have the advantage up front because they are the original equipment manufacturer, he said. However, as training becomes more virtual and open sourced "it's going to be more and more competitive. It's going to be harder to keep that contract" past the initial agreement.

Wearality's virtual reality glasses

This will be especially true in the foreign market, he noted. "They're going to want to be able to do their own training … and not count on Lockheed Martin to do it."

Another area of interest for the defense prime is developing training and simulation devices that are mobile, lightweight and reconfigurable, executives told National Defense.

Service officials have stated they need gear that can be easily deployed with troops for training "on the go." They have also asked for systems that can be altered to enable service members to train on multiple platforms at once.

To meet this demand Lockheed has been evolving its multi-function training aid (MFTA). The system is used to help servicemembers familiarize themselves with the displays and controls inside of a cockpit and better understand procedural training concepts, said Atul Patel, director of advanced technology at Lockheed.

In order to increase efficiency and affordability for the military customer, the aid is reconfigurable. "One day you can have this trainer set up to be a C-130. The next you could have it set up to be an H-60 helicopter," Patel said.

MFTA is currently being used by the Air Force to train its special operations and C-130 aircrews, he noted.

The company is working on expanding to other platforms and customers to include aircraft like the V-22 Osprey and the H-60 Black Hawk, as well as ground vehicles, Patel said.

To reconfigure the system, it typically takes less than two hours, he noted. "The biggest time constraint is the actual controls," he said. When "going from a C-130 to an Osprey obviously you've got to get the different yokes and sticks integrated in there."

The company has also been developing wearable gear in order to meet the demand for more mobile training devices. In January 2015, Lockheed partnered with a Silicon Valley start-up called Wearality. The duo is working to develop more refined immersive virtual reality glasses, Patel said.

A user can attach a smartphone or tablet to the headgear and view the screen using the device's 3D lenses. Lockheed gave Wearality access to its patented lens technology, and the small startup has taken it to the commercial market, he said. The company hopes to take lessons learned and progress made in the commercial sphere and transfer that knowledge to its defense products.

One of the main advantages of the glasses is the wide field of view, Patel said. "Having a wider field of view gives you the opportunity for the peripheral vision to come into play and it helps to mitigate motion sickness, which you would otherwise get with a very tight field of view." ND

Email your comments to aversprille@ndia.org

WEARALITY

Authentication Among Top Cybersecurity Trends for 2016

By Bill Becker

Cybersecurity will underscore most of the federal government's military and civilian initiatives in 2016. That's understandable considering data breaches are rampant and the government maintains essentially the world's largest collection of IT networks. There's a real need to ensure data security in various applications, both within and across agencies.

Many security professionals are predicting that the top cybersecurity trends for 2016 will focus on data breach prevention — that is, thwarting the hacks from the get-go. While this is a valid outlook, as breach prevention is absolutely a critical competent of a robust cybersecurity strategy, it is not the be-all and end-all.

There are three trends that are likely to be the hottest topics among federal security professionals this year: authentication, "roots of trust" and simplified security management through shared services.

Thanks to growing insider threats, the password is no longer strong enough to protect systems. Data identity and authentication technologies will evolve and flourish in 2016.

In our app- and cloud-centric culture, almost every user has privileged rights previously reserved for administrative users. Trends like the Internet of Things, Bring Your Own Device, and federal mandates such as the Office of Management and Budget's 30-day Cybersecurity Sprint and the Cybersecurity Strategy and Implementation Plan (CSIP) have put greater emphasis on identity and authentication technologies. In fact, the CSIP calls for derived credentials solutions and other strong authentication solutions for mobile devices as a critical component of a broader effort to improve mobile device management.

It's true that mature applications and workflows still require the use of public key infrastructure (PKI) credentials. Smartcards are a robust form of authentication for traditional endpoints. Enterprise computing has matured so that smartcard-based encryption and authentication are routinely used from end users' laptop and desktop computers for applications such as secure email, virtual private network access, PKI-enabled web servers and network smartcard logon.

Unfortunately, PKI credentials on smartcards do not translate efficiently to mobile devices. Today's endpoint landscape has shifted to a variety of devices: laptops, desktops, thin clients, smartphones, tablets and more. Users now expect access to information anytime, anywhere while still protecting their data with PKI-based security. Many find it cumbersome, or even impossible, to use smartcards with PKI credentials on mobile endpoints.

Recent attempts to solve this problem are still too complex. Smartcard readers can be cumbersome, microSD cards can be easily lost, embedded PKI only works on specific smartphones and software credentials must be replicated onto every device owned by a user. Additionally, each of these approaches usually comes with its own management solution, which is an administrative and security nightmare.

What is really needed is a solution that is compatible with today's variety of endpoints and is secure, interoperable and easy to use. Hence, authentication technologies will be of particular interest in the federal security arena this year.

The Internet of Things is built on a network of uniquely identifiable devices with digital certificates. These certificates identify devices, sign firmware/software updates and facilitate encrypted communications with cryptographic key information.

Security for the Internet of Things depends on identifying devices and their masters — for example, device manufacturers, cloud service providers or Internet solution providers — and protecting the data managed and shared by those devices and masters. Unfortunately, the diverse set of devices that make up the Internet of Things means that not all of the private keys, that must be kept secret and used for information decryption can be maintained in trustworthy storage.

To solve this issue, Internet of Things keys will be cryptographically linked to keys maintained in a "root of trust," a term used by the U.S. National Institute of Standards and Technology to define components that can be trusted to perform one or more security-critical functions. These functions include protecting cryptographic keys, performing device authentication or verifying software. Ideally, roots of trust must use tamper-resistant hardware.

As the Internet of Things grows in both civilian and federal agency usage, the term "root of trust" will be heard more frequently in 2016's security conversations.

Today, data encryption is a necessity, not a luxury. Data encryption is becoming ubiquitous. It's built in to various applications and infrastructure elements, which has led to an explosion in the encryption keys that need to be managed.

Most organizations can't afford to have dedicated key management solutions for each application. Consequently, these organizations are moving to common key management, instead of managing encryption keys for each encryption system.

To simplify key management, new cybersecurity shared services will be emphasized. Enterprise IT teams will be able to offer their organizations centralized key management, encryption and tokenization, including auditing and compliance capabilities as an IT service.

Taking advantage of the "as-a-service" concept to make data encryption as simple as possible, IT departments can combine resources to provide their customers the ability to manage encryption and meet their data security and compliance requirements simply and securely. These shared services will work across different solutions, data centers, geographies or IT environments.

As efforts are consolidated in a "one-stop-shop" service, "build once" solutions can be replicated effectively and overlapping encryption solutions can be avoided.

Of course, many other security-related topics will bubble to the surface as we move further into 2016. For the most part, however, listen for these big three to dominate security discussions through the year. They're the ones that make the biggest difference for the greatest number of agencies and programs. ND

Bill Becker is technical director for SafeNet AT. He can be reached at Bill.Becker@safenetat.com

DHS Opens Silicon Valley Office in Search of Innovation

By Stew Magnuson

The Department of Homeland Security in January opened an office in the heart of Silicon Valley seeking innovation at companies that don't normally do business with the federal government.

The initiative follows in the footsteps of the Defense Department's Defense Innovation Unit-Experimental office, which is also hoping to tap into new ideas found in a region known as the heart of the U.S. information technology industry.

"This is our way of trying to get their ideas into the government, get their capabilities and use them so we can perform our mission better," said Melissa Ho, managing director of the department's Silicon Valley office, which is under the Science and Technology Directorate.

Ho will be a one-person operation for the time being.

"We felt that Silicon Valley, as well as a number of the innovation corridors around the country and around the world, have great ideas to share that we haven't been tapping into very well. We haven't been getting their interest," Ho told National Defense.

There has been some coordination between herself and the Defense Innovation Unit-Experimental office. "We have talked with them and are sharing notes: who they have been talking to; who we have been talking to. We are definitely coordinating on that front," Ho said.

To kick off the initiative, the Science and Technology Directorate in December released its first solicitation targeted at Silicon Valley firms. It focuses on cybersecurity and the "Internet of Things (IoT)."

As devices other than computers are becoming connected to the Internet — such as cars, thermostats and industrial equipment — there have been dire warnings from experts that security is not being "baked into" the systems from the beginning. For example, hackers have been able to take control of cars that were put on the road with software vulnerabilities.

"There are devices out there that are network-enabled, that affect consumers as well as the government, pipelines and other critical infrastructure end users," Ho said.

The solicitation was aimed at "nontraditional performers such as technology startups," the announcement read. It "marks an important milestone in how we do business at S&T," DHS Under Secretary for Science and Technology Reginald Brothers said in a statement. "We want to remove the barriers that limit the nation's innovators from considering us as a technology partner. The [solicitation] will help engage some of the best minds on the most difficult homeland security problems."

Ho said the process for selecting ideas is being made as simple as possible and forgoes the traditional DHS and Defense Department acquisition processes.

Applicants are being asked to fill out a seven-page document and then send it as an attachment to an email address. There won't be any need to navigate a government portal. If the office is interested in the idea, it will call in the company for a 15-minute pitch. They will receive an answer as to whether they can proceed with their proposal on the spot, she said.

"We are definitely trying to mirror the way that Silicon Valley and the other investment communities handle things, which is why we have an application process rather than a white paper followed by wimpy evaluation panels. After the 15-minute pitch, we make a decision right there," Ho said.

The office is hoping to shrink the time needed — from responding to the solicitation to the first award — down to four months, "which is a lot quicker I think, than most traditional contractors are used to," she said.

As for the first solicitation, DHS is seeking technology to detect, authenticate and update devices that are part of critical infrastructure systems.

Detecting is the ability to know what Internet-of-Things devices and components are connected to a given network or system. Authenticating is the ability to verify the provenance of their components and prevent and detect spoofing. And programs must include the ability to securely maintain and update these components.

"The diverse and widely distributed nature of IoT and the numerous ways in which devices and networks can connect with IoT systems significantly complicates the security challenge," the solicitation stated. "The first and most far reaching complication is that IoT relies on the Internet to connect and control widely distributed devices."

The office has up to $20 million to spend on this and other programs, Ho said. As for the Internet-of-Things solicitation, participants can receive $50,000 to $200,000 for each of four development phases.

After a company is chosen, it will have three to six months in the first phase to demonstrate its product. There will then be a "demo day" where DHS personnel are on hand to make evaluations.

The office's intentions are to have DHS personnel there who will be using the products during both the selection and testing processes so they are invested in the technology's development. Following the demo day, companies will have an opportunity to refine their prototype and get it ready for pilot programs.

If agents or personnel working for one of DHS' 22 components have been part of the evaluation and refinement process, they will want the end product, Ho said. It is hoped that this will avoid the so-called Valley of Death, when products are developed but they ultimately find

THINKSTOCK

no long-term customers and never make it out of the prototype phase or laboratories.

"We are trying to streamline the acquisition process so by the time [DHS components] are ready to buy the [product], they have all the necessary documentation so they can buy in bulk," she said.

John Verrico, Science and Technology Directorate spokesman, said: "The DHS components may not be the end user of what comes out of this. It may very well be industry ultimately becoming the end user, or first responders be the end users. The market is much broader than just DHS."

The next solicitation will focus less on information technology and more on the needs of Secret Service officers, Ho said.

"They have got a number of different missions — investigation, protection — so our goal is to be able to articulate to the community what their days look like and what their challenges are, and if an innovator has an idea that they think can meet that need, then we are open to an application against those challenges," Ho said.

The office will most likely host an industry day in the Valley, where Secret Service program managers can spell out their needs to the community, she said. Ho declined to say what will come after the Secret Service solicitation, but said there will be more at the end of the second quarter of fiscal year 2016. It's the office's intention to be a benefit for all of the DHS components, she said.

Most of what it is interested in will be commercial off-the shelf technology, she added.

"Our expectations are that these are going to be commercial products and we're just tailoring the technology so the government can use it, too. We're buying off the shelf. We're just trying to shape that shelf a little," Ho said.

A second goal of the office will be to recruit executives who are willing to come to Washington, D.C. to work at the department. DHS Secretary Jeh Johnson, when announcing the Silicon Valley initiative at the 2015 RSA Conference in San Francisco, said: "We want to convince some of the talented workforce here in Silicon Valley to come to Washington. … This will build capacity on all fronts. I hope some of you listening will consider a tour of service for your country."

Verrico said this "tour of duty" would probably be part of the DHS loaned executive program. It allows industry experts to come work for the government for terms of up to 120 days. The volunteers are paid by their private sector employers, who give them a leave of absence to work in the government. The S&T Directorate has not yet participated in this, and there isn't one on the table for cyber yet.

Meanwhile, being on the ground in Silicon Valley is important, Ho said.

"I think it sends a good message. We are meeting people where they are. And that's important and particularly in a community that isn't necessarily interested in getting business with the government. We're showing that we are interested in them," she said.

And the concept may expand, she added. There are innovation hubs all over the nation.

"Silicon Valley is one innovation hub, but we are looking to see how this works out and to see if there are other areas around the country where it might be useful to replicate this. There is certainly a lot of innovation going on in Austin, Boston, Denver, Chicago, etc.," Ho said.

ND

Email your comments to smagnuson@ndia.org

Defense Department Moving Slowly on 'Internet of Things'

By Jon Harper

Defense Department leaders have identified the "Internet of Things" as a key component of the military's modernization strategy. But the Pentagon is behind the curve due to security concerns and other impediments, cyber experts said.

There is a fear that without proper safeguards, this linkage of systems could be compromised with disastrous consequences.

The Internet of Things (IoT) refers to "networks of objects that communicate with other objects and with computers through the Internet," the Congressional Research Service said in a recent report about the concept. "'Things' may include virtually any object for which remote communication, data collection or control might be useful" such as vehicles, appliances, medical devices, electric grids, transportation infrastructure, manufacturing equipment or building systems.

$700 MILLION PER YEAR

Potential energy savings if military facilities used smart thermostats

The technology concept is made possible by the integration of sensors, Internet connectivity, digital analytics and automation, explained William Carter, co-author of a Center for Strategic and International Studies report released in September, "Leveraging the Internet of Things for a More Efficient and Effective Military."

The private sector has embraced the Internet of Things as a way to improve operations, using it to monitor machines, track supply chains and automate business and industrial processes. The economic impact of the technologies will be between $2.7 trillion and $6.2 trillion per year by 2025, the report said.

But the Pentagon has failed to fully leverage them despite the potential benefits, according to analysts and defense officials.

"The military continues to lead in the development of some high-end applications of IoT technologies such as surveillance and reconnaissance drones, advanced sensors and satellite communications systems, but the development and deployment of the vast majority of IoT applications are driven by the commercial sector with the military severely lagging behind," the CSIS report said.

The Internet of Things is as much about networking machines and human-machine interfaces as it is developing new platforms or systems, said retired Marine Gen. James Cartwright, former vice chairman of the joint chiefs of staff.

"This is not an invention that's required. … It is an organizational issue," he said during a recent conference at CSIS. "While we have networks out there today and we act and react to those networks and what they sense and what they tell us … most of that activity is really networking people. The next evolution in this is to bring the 'things' into it."

In a constrained budget environment, the Defense Department has opportunities to take advantage of the Internet of Things by adopting practices from the commercial sector, the CSIS report said. The military could retrofit its vehicle fleet with onboard sensors to monitor engine performance and parts status, facilitate condition-based maintenance and reduce unanticipated failures. Using sensors to track geolocation, status, fuel efficiency, weight and cargo could reduce fuel costs by as much as 25 percent and increase fleet utilization by 20 percent, the report said.

"What's happening with the Internet of Things … is we're doing every point in that supply chain and everything is an entity unto itself," said Chris Smith, vice president of technology at AT&T Government Solutions. "Instead of replacing batteries, let's say every two years because we know they're going to wear out, you can actually [monitor] each battery and each set of brakes and every component within there and say, 'No, we're starting to see the [problem] factor on this vehicle. Go replace it now so you don't break down somewhere and have to send another convoy out to pick that up.'"

Deploying radio frequency identification tags and standardized barcodes to track individual supplies down to the tactical level could provide real-time supply chain visibility and allow the military to order parts and supplies on demand, the CSIS report said.

The Internet of Things also provides opportunities to cut costs by reducing energy consumption. Smart thermostats have saved commercial consumers as much as 10 to 15 percent on heating and cooling. Even half those efficiency gains could save the Pentagon $700 million on energy per year if they were installed at military facilities, the report said.

For troops out in the field, limited Internet connectivity is a hindrance, noted Curtis Dukes, director of the information assurance division at the National Security Agency, which is tasked with protecting Pentagon communications and information systems from penetration and disruption.

"You want to have a great sensor network … but it's a bandwidth constrained environment," he said. "That's one area where there is a distinct difference between the Defense Department and the commercial sector."

Pushing connectivity out to the tactical edge in large volumes is going to require investment in new generations of communications drones and small satellites, as well as leveraging commercial satellites, Carter said.

Smith views "smart vehicles" as potential delivery platforms for connectivity. "These are mobile hot spots," he said. "Think about the field uses out there where we couldn't push the network in the past because of the cost, because of the remoteness of it. Now if all vehicles are connected you have kind of a mobile, meshed network running out there."

But the lack of common standards and protocols complicates efforts to integrate systems.

"I think we've started to lag a bit in adopting [the] Internet of Things," Dukes said. "There's a lack of standards when it comes to how you actually securely communicate with everything being Internet aware and also how that communication stream looks."

"We really haven't thought through what the security model looks [like] for this Internet of Things, and I think that's the first step. And then the second one is codifying those security parameters into standards for that," he added.

The need to develop common standards extends to commercial devices that the Defense Department would be interested in using, Carter noted.

Cultural barriers add another obstacle, analysts said.

"The risk aversion of many military figures is based on the fact that if systems fail, people die," Carter said. "Nobody wants to be calling IoT support from a foxhole saying, … 'My smartphone isn't working [and] I can't accomplish my mission.'"

Security concerns are the main issue holding back the military's use of the Internet of Things, said officials, analysts and members of industry. Some potential adversaries have advanced cyber and electronic warfare capabilities, and everything connected to the Internet is potentially vulnerable to attack, they noted.

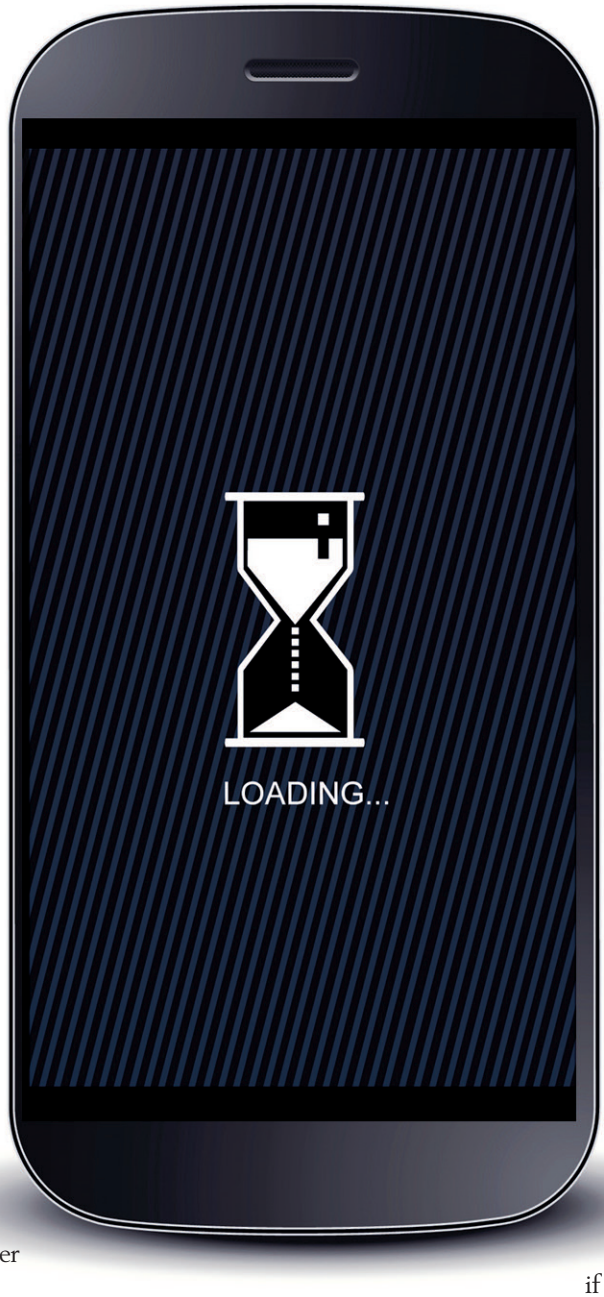
"Everybody today likes to talk about the Internet of Things … [but] I look at it as the Internet of threats," said Paul Geraci, senior director of U.S. intelligence and national security programs at OSIsoft, a California-based company that provides IoT-related software to the federal government and the private sector. "While many may look at it as a beautiful thing that we're all interconnected … it's an asymmetric threat now. It's a constant threat, and it's a constant risk."

Budget constraints and the Defense Department's approach to spending hinder the pursuit of Internet of Things technologies, Carter said. "The military does not spend dollars today to save dollars tomorrow, which is in many ways how industry has developed real value from IoT," he said. "You invest in a new system today and [then] you save on the efficiencies you generate over time."

The Defense Department has not invested enough money in cybersecurity for facilities that use Internet of Things technologies, said John Conger, former acting assistant secretary of defense for energy, installations and environment, who is now the Pentagon's principal deputy comptroller.

The Defense Department owns 300,000 buildings, some of which have hundreds of Internet access points that could be vulnerable, he noted at a recent Federal Facilities Council conference.

"While cyber threats are getting a lot of attention at the department and [U.S. Cyber Command] is getting plenty of money, the facilities are not," Conger said.



"At some point we're going to have to spend real money" to address the problem, he said. "It's not just the fact that [adversaries] might turn off the lights. … What if you have a critical system that's hooked up to all this and … you can't turn the chillers back on when the computer systems are going to overheat and that's going to shut down the network? Or what happens when they actually use that to get into some other network?"

The art of deception can be employed against machines as well as people, noted Richard Hale, deputy chief information officer for cybersecurity at the Defense Department. "The Internet of Things, especially as we get more and more autonomous and more of this is real-time control system sort of stuff — it's going to make really bad decisions if information isn't right or if it's not coming from a genuine, trustworthy" component, he said. "Non-spoofable … identity is going to be a fundamental characteristic" of the Pentagon's future IoT systems.

Dukes said "lightweight" cryptography would be needed to secure smartphones and other devices that don't have the processing capability of traditional devices. That could entail creating cryptographic tools and protocols that require less energy or less software code to execute.

In a constrained budget environment, priorities will need to be set when it comes to securing the Internet of Things, officials said.

"We don't want to have all of our money spent on some insignificant cybersecurity problem," Hale said. "Nuclear command-and-control ought to have more cybersecurity … than the thermostat in my house or in a DoD building perhaps."

The department will need to set different standards for a wide range of Internet of Things systems, from nuclear and aircraft systems on the high end to logistics and administrative activities on the lower end, Cartwright noted.

Industry needs to be a partner in these efforts, Dukes said. "As you move to these Internet of Things, if we're not careful and if we don't think about building security into those devices … an adversary would be able to connect onto that and actually see what's going on," he said. "It really is forcing industry to actually start baking or building security into this process." ND

Email your comments to jharper@ndia.org

THINKSTOCK

New Generation of Commercial Satellites to Benefit Military

By Stew Magnuson

Commercial satellite communications providers are in the process of launching a new generation of high-capacity spacecraft that will be a boon for their military customers.

Government users will have a variety of services to choose from with throughput measured in gigabytes rather than megabytes and narrower, steerable spot beams that will help prevent enemy jamming, all with no development costs to taxpayers.

"Industry is certainly leading the way with tremendous capacity — terabytes in orbit — and if DoD isn't in line to access that, that is a problem," Joe Vanderporten, director of the Air Force Space and Missile Systems Center's Pathfinder office, said at a recent Washington Space Business Roundtable panel discussion on comsat providers and the military.

The big providers such as Eutelsat, Intelsat General, SES Government Solutions and Inmarsat for the past 15 years have been selling their services to the military on year-long contracts because demand has far outpaced military satellite communications capacity. Now, they are asking that their relationship to the Defense Department evolve into more of a partnership.

One of the new satellite constellations is the O3b Network, which is operated by SES Government Solutions. At a demonstration day in Bristow, Virginia, company representatives showed how they could set up a high-capacity satellite link within hours using equipment and dishes that fit into a few easily transportable boxes.

The system connects to eight satellites that are constantly moving in a medium orbit — about 4,100 miles above the Earth — as opposed to standard communications satellites, which operate in fixed geostationary orbits at about 22,000 miles, said P. Glenn Smith, vice president of business development for SES Government Solutions.

The closer proximity means a much lower latency compared to satellites that are in fixed orbits. Smith said speeds were comparable to undersea fiber-optic cables. The satellites have steerable spot beams that cover smaller swaths of about 430 miles wide. Previous beams might cover entire continents.

That gives the system some inherent protection against jamming, Smith said.

The military operates two types of communications satellites. One is the Advanced EHF, highly protected satellites designed to work in the event of a nuclear war. Commercial satellite providers, whose main customers are telecommunications companies and television broadcasters, have no need to build battle-hardened spacecraft.

The Air Force also operates the Wideband Global Satcom satellites, which are intended to provide broadband communications to U.S. forces, but do not have as much protection.

Smith said the smaller beams make it harder for enemies to jam communications. To do so, they have to attempt it within the beam's radius. In addition, they would have to have the ability to track O3b's constantly moving satellites, which is also a difficult proposition.

"The difference is you used to point a dish at a satellite and you were on that satellite for months, maybe years. With O3b, you're on all eight of the satellites about four times per day. They are constantly moving around."

The steerable beams are now being used to provide broadband connectivity to cruise ships as they sail. That could translate to providing the same service for a Navy battle group, he said.

Another company, Inmarsat, in December completed the launching of its Global Xpress constellation with its third spacecraft.

"The final one is for Asia-Pacific. It provides coverage in that very challenging area," said Rebecca M. Cowen-Hirsch, senior vice president of government strategy and policy at Inmarsat Inc.

The new high-throughput satellites have roughly 20 times more capacity than their Inmarsat predecessors and also feature steerable spot beams for commercial or military customers. The new system is also compatible with any terminal capable of connecting to the Air Force's WGS satellites or any DoD certified waveform, she said.

"We have put a high degree of focus on cybersecurity for Global Xpress ... We have type 1 [National Security Agency] command-and-control encryption to ensure that no one controls our satellites but us," she said.

The flexible beams also have some inherent jamming protection. The waveforms they use allow the spacecraft to quickly change beams if it detects man-made or natural interference, she added. An enemy attempting to jam a signal wouldn't have any idea that the user had switched to a different beam, she said.

Hughes Network Systems LLC has internally developed a new waveform to make equipment more compatible with WGS and the new wave of high-throughput satellites. During a joint U.S.-Australian military exercise, Talisman Sabre, Hughes Defense and Intelligence Systems' division successfully demonstrated higher satellite performance using its advanced TDMA waveform technology.

Dan Losada, senior director at the Hughes division, said the company has been in the high-throughput satellite business for more than a decade with its Spaceways system, which is now used for satellite TV services.

While most of its business is now providing ground systems and modems for satellite connectivity, its new Jupiter high-capacity satellites are expected to provide coverage over most of the Americas by the end of 2016. Jupiter I is in orbit and Jupiter II will be in place by the end of the year, he said.

The TDMA waveform it developed with its own funding is available in the DoD waveform information repository, which means it can be freely applied to any military system, he said.

"High-throughput systems are more of an ecosystem than a stovepiped system. The more people you have that already share your technology, share your vision and allow you to interoperate, the better the experience it is going to be," Losada said.

"My challenge is to bring that to bear for the defense departments of the world so that they can leverage this huge amount of capacity that is going to be available," he said. Australia, for example, paid for one of the Air Force's WGS satellites so it could participate in the global system. The TDMA waveform is helping

it tap into that system.

Another high-throughput system in the works is Intelsat General's Epic series. The first spacecraft is slated to be launched at the end of January, said Kay Sears, the company's president.

It will feature wide and spot beam coverage in the same bands for increased flexibility. "It really is built for mobility applications and small terminals, all the things the government needs," she said.

Epic will have four to six times the bandwidth of a WGS satellite. "So already in the satellites we're launching in 2016, we have already seen a [leap] in technology in terms of throughput, power and flexibility. And that will continue," she said.

Sears is one of the leading industry voices asking that the Defense Department allow commercial satellite providers to have a seat at the table when it comes to planning for the future. The new wave of satellites should be considered a permanent part of the space-based communications architecture, she said.

If that were the case, industry could do a better job of building the kinds of features the military needs into their spacecraft.

WGS is based on 15-year-old technology, she said in an interview. Being a program of record, it is hard for the Air Force to insert the latest technology into each satellite it launches. Commercial providers do not have that problem. They are constantly sending new systems to orbit with the most up-to-date technology, she said.

"What we believe is that we will have 100 times the capability the WGS has in orbit or with their full constellation, not just megabytes, but real flexibility with steerable, reconfigurable beams," she said.

"We don't get a lot of help understanding the requirements and the future direction," she said. If the military wants more jamming protection for its satellites, for example, it can have it.

"Any kind of protection they can buy from a manufacturer, we can buy from a manufacturer," she said.

The Air Force is kicking off an analysis of alternatives for its next-generation communications satellites and has been conducting a series of Pathfinder studies to help it inform its decisions.

Global Xpress

INMARSAT

Meanwhile, the Air Force and the Defense Information Systems Agency continue to buy capacity on the spot market in one-year contracts using overseas contingency operations funding.

The post-WGS architecture must include the commercial provider industry, and clearly define its role and responsibilities for providing wideband communications, Sears said.

Cowen-Hirsch said the Defense Department should be looking for new and inventive ways to acquire capacity "rather than buying the same old things they bought in slightly different ways."

There is an opportunity for the Pathfinder studies to demonstrate this government-commercial integrated architecture and inform the new wideband alternatives going forward, she said. "We are hearing from the top down a real focus to drive towards that integrated architecture."

Government representatives at the panel discussion were somewhat optimistic that change was in the air.

"Some analysis suggests that some of the newer satellites are near WGS capacity," Vanderpoorten acknowledged.

"A purpose-built [government] satellite does more things," he said. How commercial and government-owned systems will line up "is a big conversation. I think it will be a mix. How big of a mix remains to be seen."

Winston Beauchamp, Air Force undersecretary for space, said: "I think there is a real convergence on the technology side. The key is to get convergence on the policy side so that we can operate more seamlessly."

Leonor Tomero, a staffer at the House Armed Services Committee, said: "The future looks bright for increasing use of commercial and I think certainly from affordability and flexibility, it has shifted, and we are seeing DoD lean more forward to take advantage of more commercial."

Meanwhile, all these new high-throughput commercial satellite systems coming online means that prices are coming down when the government buys capacity on the spot market, Sears said.

Peter Hoene, president and CEO of SES Government Solutions, said: "Government estimates were that commercial satellite services cost four times that of a WGS. Now, with high-throughput satellites, the cost is becoming more equal."

Sears agreed that prices are coming down because of the increased capacity but maintained that they could come down even more if her vision of a more cooperative relationship between the Defense Department and the comsat providers comes to fruition.

"It will bring the prices down considerably," she said. **ND**

Email your comments to smagnuson@ndia.org

Homeland Missile Defense Projects Remain in Limbo

By Jon Harper

Uncertainty surrounds the future of homeland missile defense at a time of budget constraints and technology challenges.

Efforts to protect the United States from ballistic missile attacks are being driven by North Korea's pursuit of long-range rockets and concerns that Iran is moving in the same direction, U.S. officials have said. Pyongyang has already conducted three atomic bomb tests, and recently claimed that it tested an even more powerful hydrogen bomb. The Pentagon is worried that North Korean intercontinental ballistic missiles could potentially be armed with nuclear warheads.

"Those threats continue to put at risk the peace and security … of the United States," Secretary of Defense Ash Carter said during a recent trip to South Korea.

The Defense Department is in the process of beefing up its missile shield by adding more ground-based interceptors to the existing site at Fort Greely, Alaska. Additional interceptors are located at Vandenberg Air Force Base, California. But the Pentagon has yet to endorse lawmakers' proposals for the creation of a third missile defense site in the eastern United States.

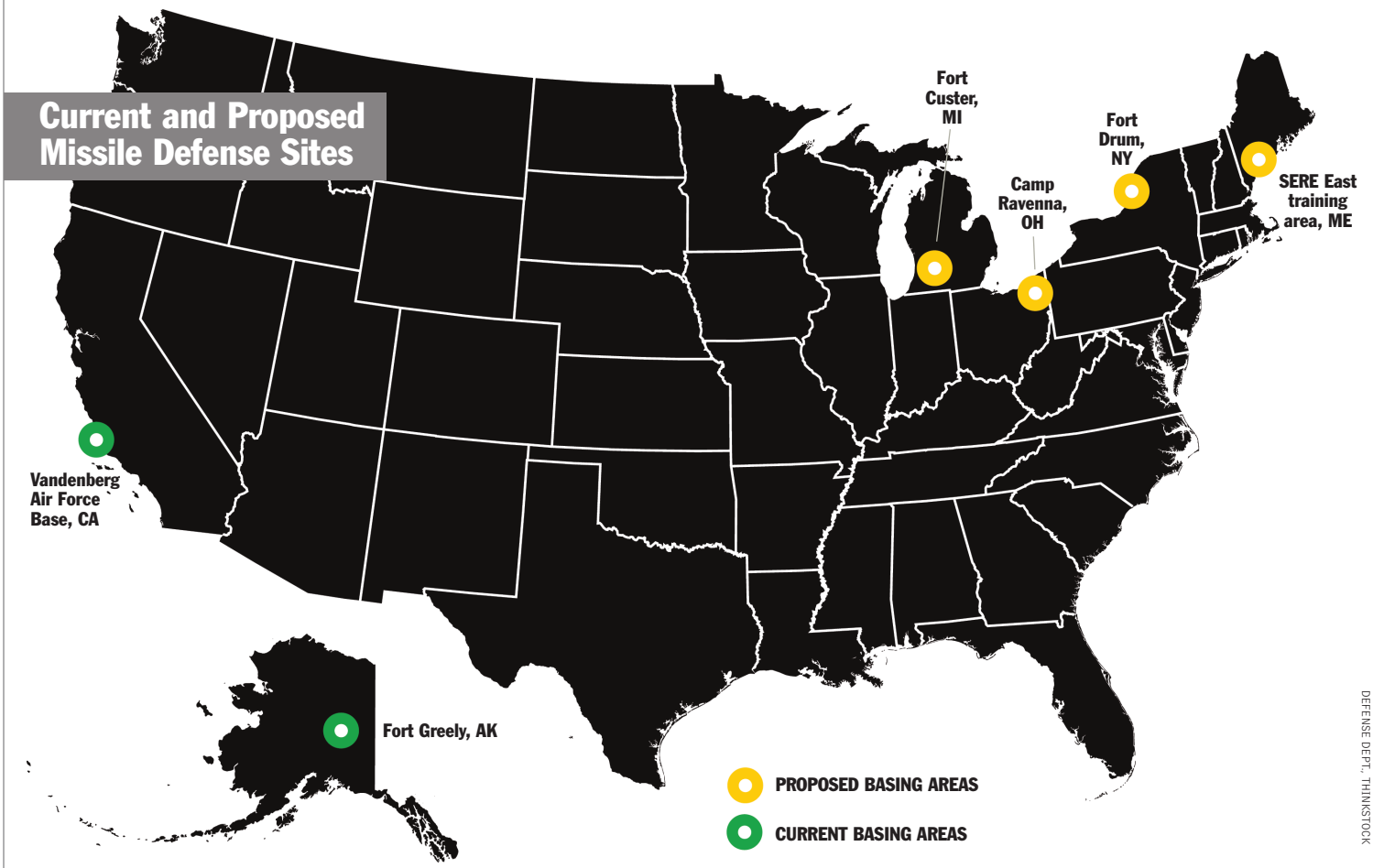
Under congressional prodding, the department has been conducting environmental impact studies of four potential basing areas: Fort Drum, New York; Fort Custer training center in Michigan; Camp Ravenna joint military training center in Ohio; and the SERE East [survival, evasion, resistance and escape] training area in Maine. That work is expected to wrap up in 2016, and the Missile Defense Agency has been tasked by Congress to select a preferred location in case policymakers decide to move forward with the project.

Having a site in the eastern United States would offer some operational advantages because it would buy time and space for intercepts, experts said.

It "allows for the opportunity of shoot-look-shoot," said retired Air Force Brig. Gen. Kenneth Todorov, former deputy director of the Missile Defense Agency, during a recent panel discussion at the Center for Strategic and International Studies. "It gives you a second shot opportunity should you have the means to determine that you … didn't hit [the incoming missile] on the first try" after using the interceptors in Alaska.

But defense officials have balked at the expected price tag. The Congressional Budget Office estimated that the cost would exceed $3 billion, and Pentagon officials have argued that the money could be better spent on other projects.

"It comes at a significant cost," said retired Lt. Gen. Richard Formica, former commanding general of U.S. Army Space and Missile Defense Command. "It was my recommendation then and would remain my opinion today that [with] the limited missile defense dollars that we have available to us, priority is on [improving ground-based intercep-



DEFENSE DEPT.; THINKSTOCK

tor] reliability" as well as enhancing sensors and doing more testing.

Missile defense budgets have been relatively flat in recent years, as the Pentagon has grappled with constraints on its topline funding.

Thomas Karako, director of the Missile Defense Project at CSIS, said it is anyone's guess as to whether or not a third site will be built.

"The only honest answer there is, 'I don't know,' and if somebody tells you they know, don't believe them," he said. "Is the budget there? And what kind of predictions do you have about the future [threat]?"

U.S. officials aren't just worried about ballistic missiles. Cruise missiles — such as the ones that Russia has developed — are also raising red flags. The Russian military recently launched such weapons from ships stationed in the Mediterranean and Caspian Seas against militants in Syria.

"They were making a point," said retired Navy Rear Adm. Archer Macy, former director of the joint integrated air and missile defense organization. "I think this was an opportunity for the Russians … to demonstrate a capability that, 'Hey, you know we've had these things, they really work … [and] we're going to use our stuff'" when it is advantageous.

The joint land attack cruise missile defense elevated netted sensor system, known as JLENS, is viewed by some officials and analysts as a promising tool for countering cruise missiles fired at Washington, D.C.

Built by Raytheon, it features radar and other electronics attached to tethered blimps that have been stationed at Aberdeen Proving Ground, Maryland. The system, which was recently going through testing and evaluation, was designed to detect airborne threats and relay that information to military aircraft or other defense assets that could destroy them. The large aerostats — which are nearly as long as a football field — can fly at 10,000 feet and stay aloft for up to 30 days, according to Raytheon.

"It allows us to look over the horizon farther and … is persistent," Adm. Bill Gortney, commander of U.S. Northern Command and North American Aerospace Defense Command, said in an interview with National Defense. He envisions JLENS as potentially "a critical piece of the system of systems that we need to defend the National Capital Region against the cruise missile threat [like the weapons] that the Russians shot in Syria."

Missile defense complex at Fort Greely, Alaska

But the program was suspended in November after one of the blimps broke loose from its tether and drifted away to Pennsylvania, where it eventually landed after damaging civilian property. The incident inspired mocking Internet memes that went viral on social media. Twitter users referred to it as #Blimpgate and used other unflattering hash tags.

The program will remain on hold until investigators figure out what went wrong. After that, its future is uncertain.

"You look for the root cause of what happened … you look for mitigation measures that you can put in place, and then you make a risk-based decision on whether you want to go flying again," Gortney said. "That's where we are."

"I'm confident we will come up to a solution … [and] un-pause the test to see if this is going to be able to fill a critical capability gap for us," he added.

The NORTHCOM/NORAD chief did not provide a timeline for when the investigation would be completed.

Raytheon declined an interview request to discuss the program. "The investigation into the Oct. 28 JLENS


JLENS

incident is ongoing and, unfortunately, we won't be able to comment further until it wraps up," Keri Connors, a communications manager at Raytheon, said in an email.

Some observers see great value in JLENS' sensing potential, but question the use of a tethered blimp.

"I love the capability that it brings [but] I don't really love the platform that it's brought on," Todorov said. "What happened to JLENS was unfortunate. … It gets a lot of bad press and people you know yucking it up a little bit over the balloon that flew away. I get it that the platform is not great but … let's focus on the capabilities that are brought by the platform."

Karako said the Pentagon should consider other options for deploying the sensors, including long-endurance unmanned aerial vehicles. "There's probably a variety of ways that this kind of elevated sensor looking down can be positioned," he said. "I think at this point we ought to be agnostic about the platform … and getting back to completing the test of the sensor and looking for various ways to mount it — maybe it's an aerostat and maybe it's something else."

The Missile Defense Advocacy Alliance, a non-profit group, said JLENS might need to be jettisoned. It called for the development of an alternative cruise missile defense system if that scenario comes to fruition.

"If the JLENS cannot be assured to stay tethered or deflate automatically should the tether break, then it simply should not be deployed or made operational," the group's Chairman Riki Ellison said in a written statement after the aerostat came loose. "Abandoning the JLENS program should these efforts to fix the system seem unattainable or perhaps unaffordable would still require the U.S. government to develop, test and eventually deploy another solution for the 360-degree air defense of the National Capital Region."

The Defense Department has spent about $2.7 billion on JLENS. Despite the recent embarrassment, and lingering questions about the program's cost and capabilities, some experts believe the system should be given more time to prove its worth.

"I just thank God that we didn't stop the first time that Orville and Wilbur Wright crashed … an airplane," Formica said. "I'm not suggesting that JLENS is going to become the next airplane, but I am suggesting that we don't throw the capability away because it had an unfortunate problem. Let's fix that problem and then … test that capability, [see] what it provides and then make a decision based on that."

If JLENS resumes and performs well in testing, moving forward with it could force tradeoffs if missile defense budgets remain relatively flat.

"If at some point we determine that it is a useful system, it just becomes another part of that tension because it means more investment in capability, force structure, manpower — and someone has got to pay that bill," Formica said.

Macy said the next presidential administration will likely conduct a comprehensive missile defense review to assess threats, consider options for countering them and determine the best path forward.

The CSIS panelists supported the Defense Department's ongoing efforts to improve the "hit-to-kill" vehicles that are responsible for destroying incoming warheads by colliding with them at high speeds. But they were wary of relying solely on that technology to defend the homeland from ICBMs. The United States needs to be looking at other technologies and operational concepts including taking out enemy missiles "left of launch" before they are fired, they said.

"There will never be enough interceptors" to guarantee that all incoming enemy missiles would be shot down, Formica said. Interceptors are also expensive to build, he noted.

Technologies that could contribute to the mission include non-kinetic tools such as cyber and electronic warfare, the panelists said. "Left of launch is far more than just Scud hunting," Formica said, referring to U.S. efforts to locate and bomb mobile Iraqi missile launchers during the First Gulf War.

Karako believes there will be new opportunities for industry in the coming years. "The missile threat isn't going away. Everybody pretty much recognizes that," he said. "The set of industry solutions to that problem I suspect are not going anywhere either. … The next hill, if you will, is how to do it differently … in addition to staying the course on what we're doing now."

Directed energy technologies could have transformative missile defense applications, he said. "Modestly-sized directed energy weapons on the spine of a high flying, persistent UAV … really have the potential to revolutionize our concept of operations and our capacity for dealing with foreign missile threats."

It "appears that they're making some pretty interesting progress" in this field, he added. "In doing so you really begin to move toward a pretty interesting solution set for these problems that have really occupied such a significant amount of our energy over the last several decades." ND

Yasmin Tadjdeh contributed to this story.

Email your comments to jharper@ndia.org

DEFENSE DEPT.

Navy Focuses on Maritime Superiority In Complex World

By Yasmin Tadjdeh

The U.S. Navy is juggling many missions around the globe. It is challenging the Islamic State in the Middle East and is increasing its presence in the Asia-Pacific region as China continues to intimidate its neighbors. At the same time, other nations — such as Iran and North Korea — remain concerns.

To maintain its global dominance, Navy leadership released in January a strategy called, "A Design for Maintaining Maritime Superiority," that is intended to guide the sea service as the world grows more complex, said Chief of Naval Operations Adm. John Richardson.

"The character of the entire game has changed," he said during a speech in January. "In particular, the pace of things has become so accelerated. … If we do not respond to those changes, if we do not recognize and adapt to the changing character of the game, we are a Navy that is at risk of falling behind … our competitors."

While the world was once more black and white with only two superpowers — the United States and the Soviet Union — it now faces a more congested playing field, he said. Competitors include Russia, China, North Korea, Iran and terrorist organizations.

"For the first time in what I would say is roughly 25 years, the United States is back to an era of great power competition," he said. "When I was deployed in 1983 … it was a different world. When the Soviet Union dissolved, the Cold War ended, we really entered a period where we were not … challenged at sea, not in a very meaningful way. That era is over."

As outlined in the Navy's new strategy, some of these actors are seeking to exploit what Richardson calls the three global forces: traffic in the ocean, the global information system and the increasing rate of innovation.

"I'm focusing on three forces that for the Navy are sort of defining our way forward. The three forces that are causing our world to be more used, more trafficked, more stressed, more important and perhaps, most interestingly, more competed than ever," he said.

The maritime domain looks physically the same, but it is becoming more crowded. Since 1992, maritime traffic has increased by a factor of four. Technology is making previously unreachable parts of the ocean floor accessible. That is opening up certain areas to mineral, oil and gas exploration, he said.

The global information system is also rapidly expanding, Richardson said. Undersea cables, satellites and wireless networks connect the globe. Citing data from IBM, Richardson said 2.5 quintillion bytes — that's 18 zeroes — of data are created every day. Ninety percent of the data available in the world today was created in the last two years.

There are also rapid advancements in technology, such as material science, robotics and artificial intelligence. "It is coming at us faster and faster and they are being adopted by society just as fast," he said.

Adm. John Richardson

NAVY

Potential adversaries are exploiting all three of these forces, he said. To respond, the Navy has identified four lines of effort — "warfighting, learning faster, strengthening our Navy team and building partnerships," according to the strategy.

The effort includes maintaining and modernizing the undersea leg of the nuclear triad, it said.

Additionally, the Navy must develop concepts and capabilities to "provide more options to national leaders, from non-conflict competition to high-end combat at sea," it said.

"Operations short of conflict should be designed to contain and control escalation on terms favorable to the United States.

USS Ronald Reagan

Combat at sea must address 'blue-water' scenarios far from land and power projection ashore in a highly 'informationalized' and contested environment," the strategy said.

These concepts would be validated through wargaming, fleet exercises, unit training, certification, and modeling and simulations.

The service must also "advance and ingrain information warfare" as well as explore alternative fleet designs "including kinetic and non-kinetic payloads, and both manned and unmanned systems," the strategy said.

The document also called for an organizational examination of U.S. Fleet Forces Command, Commander of Pacific Fleet and subordinate commands to "better support clearly defining operational and warfighting demands and then to generate ready forces to meet those demands."

The strategy comes on the heels of a December memo by Secretary of Defense Ash Carter where he criticized the Navy for over-prioritizing fleet size and neglecting capability.

"The Navy has overemphasized resources used to incrementally increase total ship numbers at the expense of critically-needed investments in areas where our adversaries are not standing still, such as strike, ship survivability, electronic warfare and other capabilities," the memo addressed to Secretary of the Navy Ray Mabus said. "This has resulted in unacceptable reductions to the weapons, aircraft and other advanced capabilities that are necessary to defeat and deter advanced adversaries."

The Navy's latest program submission — which exceeds the service's 308-ship requirement — is "unbalanced" and creates too much warfighting and technical risk, he said.

In the memo, Carter announced that he would slash the number of littoral combat ship purchases from 52 to 40. "This plan reduces, somewhat, the number of LCS available for presence operations, but that need will be met by higher-end ships, and it will ensure that the warfighting forces in our submarine, surface and aviation fleets have the necessary capabilities and posture to defeat even our most advanced potential adversaries," he said.

During a December speech at a defense forum hosted by the U.S. Naval Institute prior to the release of the memo, Sen. John McCain, R-Ariz., chairman of the Senate Armed Services Committee, said the United States "is confronting the most diverse and complex array of global crises since the end of World War II," but at the same time does not have enough resources to meet the increased demand.

"Now more than ever a strong Navy is central to our nation's ability to deter adversaries, assure allies and defend our national interest," he said. "And yet, by any measure, today's fleet … is too small to address these critical security challenges. The Navy's requirement is 308 ships. The Bipartisan National Defense Panel calls for a fleet of 323 to 346 ships and our combat commanders say they require 450 ships."

While current vessels are more capable than their predecessors, more are still needed, he said. "The size of our fleet translates directly to presence, which is essential to protecting shipping lanes, responding to crises and deterring aggression. And we cannot be present with the ships we don't have."

The military must be willing to reimagine the Navy, he said. He noted that six months after the attacks at Pearl Harbor, the U.S. Navy had a major victory at Midway, which was a turning point in the war in the Pacific.

"That victory was not the work of six months, but of many years before the war began. The U.S. Navy in the 1930s adapted itself — despite fervent opposition at times both internally and externally — from an organization built around the battleship to one organized around carrier aviation," he said.

The government must reconsider whether or not naval forces are postured for success, he said. Additionally, leadership must take a hard look at studies that suggest adding forward bases or stationing more forces in the Western Pacific, such as a second aircraft carrier or an amphibious ready group.

NAVY

The Navy and Marine Corps currently maintain two maritime hubs, one in the Pacific and one in the Middle East, McCain said. The United States should consider establishing one in Europe because of recent aggressive behavior by Russia, he said.

"Given Russia's behavior in the past three years, a third hub, centered on an aircraft carrier strike group, may now be necessary in the Mediterranean to protect U.S. and allied interests while enabling prompt response options," he said.

Additionally, there must be a greater focus on technological innovation, McCain said. "We have to face the reality that America's military technological advantage is eroding and eroding fast. Assumptions we have made about the battlefield, such as having unfettered access to the sea and sky, have led to operational and programmatic decisions which are no longer appropriate for the global security environment [in] which we find ourselves," he said.

Richardson said the sea service is tackling the innovation issue. He called for the Navy to "fast track" technologies to help it maintain an edge over adversaries.

"In many ways our most challenging competitors are very close, in terms of capability, to us. We've got to be very mindful of that, be cleared eyed about that," he said. "We've got to spend some time recapturing the momentum, and picking up the pace and moving faster."

The Navy wants to create an acquisition "HOV lane" where certain mature technologies can be fast tracked.

He would also facilitate more experimentation on ships. "The amount of creativity that is out there in the fleet is tremendous," he said. "The real magic happens when you put … developers [on ships] and they meet with sailors out there and they watch their ideas come to life," he added.

It is more important to begin working on innovation immediately but deliberately, rather than trying to guess what might be needed decades from now, Richardson said.

"I don't want to put a big a bet on something 20 years down the road. I want to put a bet on something I can get started on now and I will learn my way into the future," he said.

The Navy's new maritime strategy comes at a time of global changes, experts have said. Ronald O'Rourke, naval affairs specialist at the Congressional Research Service, said the world is now entering a new strategic era.

"Many observers starting in late 2013 have concluded that we have undergone a shift in strategic eras, from the familiar post-Cold War Era of the last 20 or 25 years, to a new and different strategic era, entering renewed great power competition and challenges to key elements of the U.S.-led international order that has operated since World War II," he said.

This strategic shift has been difficult for some to recognize, he said during the forum. For example, the markers of it are less abrupt than the ones that heralded in the shift from the Cold War to the post-Cold War era. Additionally, this shift is "less pleasant than the one that Americans were presented with at the end of the Cold War," in which they won the war. In this case it is harder to accept, he said.

This new era has yet to be named, O'Rourke said. That could be damaging because it makes it harder for citizens to recognize and subsequently adapt to the changes. **ND**

Email your comments to ytadjdeh@ndia.org

Congress Boosts Coast Guard Budget

By Yasmin Tadjdeh

The Coast Guard has often been characterized as perennially underfunded, but thanks to Congress, the service received a major boost to its acquisition accounts for fiscal year 2016.

In the recently passed omnibus budget, Congress allocated the Coast Guard nearly $928 million more in acquisition, construction and improvement funding than it asked for in the president's fiscal year 2016 budget request. That will go toward a ninth national security cutter, a new polar icebreaker and increased funding for the offshore patrol cutter.

The funding increase comes at a time of growing missions for the service. Over the past year, it has taken on a larger role in patrolling the Western hemisphere as smugglers attempt to bring drugs into the United States. Additionally, as sea ice melts in the Arctic and opens up new waterways, the service — which operates the nation's polar icebreakers — will play a greater role in the region, officials have said.

The service in January issued a solicitation for a new icebreaker.

"The Coast Guard appreciates the tremendous support of Congress in addressing the service's priorities of both investing in future capabilities as well as preserving today's frontline operations," said Eric Nagel, a spokesman for the sea service. "[This] demonstrates Congress' recognition of the Coast Guard's role to secure the homeland and safeguard lives and property in the maritime domain."

Ashley Godwin, senior defense advisor for the Shipbuilders Council of America, a Washington, D.C.-based advocacy group, said the increased budget would help the Coast Guard meet many of its future acquisition requirements.

"The administration has been doing a lot of lip service to increasing the Coast Guard's budget but the money hasn't been there," she said. "Congress basically said, 'Well, if you're not going to do it, we're going to do it.' So the increase was dramatic."

Congress allocated a total of $743.4 million for the national security cutter program — $652 million more than the service asked for in the president's budget. The bulk of it — $640 million — will go toward the acquisition of a ninth NSC, one more than the program of record called for. Twelve million dollars will go toward top-side engineering design work to deploy small unmanned aerial systems off the ship.

In an interview with National Defense prior to the finalization of the omnibus budget, Rear Adm. Joseph M. Vojvodich, the Coast Guard's assistant commandant for acquisition and chief acquisition officer, said the service was proud of the work it had done procuring the new cutter. It recently christened the sixth NSC, which will be delivered by the end of 2016. The eighth will be delivered in 2018.

Brian Slattery, a defense and security policy analyst at the Heritage Foundation, a Washington, D.C.-based think tank, said the extra national security cutter was one of the Coast Guard's biggest wins in the budget. It also came as somewhat of a surprise.

"It did come out of the blue a little bit, but it will definitely be a win for the Coast Guard as long as the subsequent funding for personnel and all the other associated assets that go into that vessel are implemented as well," he said.

The additional NSC was put into the budget by Sen. Thad

Cochran, R-Miss., Slattery said.

"That appropriation has gotten a little bit of flack from certain media outlets for being an earmark or being excessive because the Coast Guard technically isn't asking for it," he said. However, two studies have previously suggested that a ninth NSC was necessary in order for the Coast Guard to perform its missions, he said.

"Even though the Coast Guard program of record is only for eight, that eight number was forced under budget constraints … and nine is certainly a more appropriate number," he said. "That is going to be very big in terms of the national security cutter being able to provide more capacity and more days at sea in the overall fleet."

Godwin said she didn't consider the ninth NSC to be an earmark. Ingalls Shipbuilding in Pascagoula, Mississippi is building the ships.

"The naysayers can say, 'Oh, it's an earmark,' but suppliers for shipbuilding are in all 50 states. It's more than just one shipyard, one state. Shipbuilding is so large. It permeates throughout the U.S.," she said. "This is good for many, many states [and] many, many employers."

Congress also appropriated $89 million toward the offshore patrol cutter, $70.5 million above what the service asked for in the president's budget. The extra funds will go toward commencing phase two of the OPC acquisition process, which would include a downselect to one vendor.

Commandant of the Coast Guard Adm. Paul Zukunft has said the offshore patrol cutter is the service's top priority. The program calls for a total of 25 vessels to be procured, which will replace aging medium-endurance cutters.

Vojvodich said: "It's really a priority for us because the medium-endurance cutters are really a workhorse for the fleet … [and] we're experiencing some reliability issues with that fleet. At some point you've got to recapitalize."

Currently, Bollinger Shipyards Lockport LLC, Eastern Shipbuilding Group Inc. and General Dynamics-Bath Iron Works are vying for the contract. In 2014, the Coast Guard awarded them each a firm fixed-price contract for the preliminary and contract design of the vessel.

Technical proposals were due in January, Vojvodich said. By mid-March all submissions should be complete, and the Coast Guard will begin an evaluation of the technical and pricing data. A downselect will be made by the end of fiscal year 2016, he said. Construction begins in fiscal year 2018 and delivery of the first vessel is slated for fiscal year 2021.

In an effort to save money, the program doesn't ask industry to produce new, cutting-edge technology, he noted.

"We've made that program affordable through … a lot of industry engagement," he said. "We're using state-of-the-market technology, so there are no research proj-

$743 million allocated for the national security cutter program

$89 million allocated for the offshore patrol cutter

VIGOR INDUSTRIAL (OPC CONCEPT), COAST GUARD

ects included in that. We made some tough decisions in terms of the capability that we're going to have."

For example, both the national security cutter and the fast response cutter have stern-launch capability, which allows small boats to enter and exit from the stern. "To make the thing more affordable, we're not going to ask industry to do that. We're not asking industry to have some unique material or some unique hull design. It's just going to be basic shipbuilding," he said.

In order to bring costs down the offshore patrol cutter does not have ballistic protection, he said.

Before the budget was released, Godwin said she thought the Coast Guard would have to pick between the offshore patrol cutter and national security cutter. "But they didn't. They gave them money for both," she said.

The bill also boosted spending to accelerate the acquisition of a new polar icebreaker. It allocated $2 million more than what was requested in the president's budget.

The Coast Guard has a statutory requirement to maintain and operate the nation's polar icebreakers. Currently, only two — the Polar Star, a heavy-duty vessel, and the Healy, a medium-duty vessel primarily used for scientific research — are operational. A third, the Polar Sea, was mothballed after the heavy-duty icebreaker suffered a massive engine failure in 2010.

During remarks in Seward, Alaska, in September, President Barack Obama called for the nation to invest in more icebreakers.

"After World War II, we had seven icebreakers — four under the Navy, three under the Coast Guard. Today, in part because we haven't been reinvesting, although we technically have three, operationally we really only have two and only one heavy icebreaker," he said. "Just to give you a sense of contrast, Russia has about 40, and 11 icebreakers either planned or under construction."

The Polar Star

The administration proposed to accelerate the acquisition of a replacement heavy icebreaker to 2020 from 2022. Coast Guard leaders have estimated it will cost $1 billion to build a new icebreaker over 10 years.

However, language in the omnibus budget said the Obama administration was not doing enough.

"The growth of global commerce, scientific research, tourism and other activity in the Arctic region requires a multi-mission icebreaker to sustain a U.S. presence, maintain domain awareness and furnish critical search and rescue capabilities," the bill said.

"Unfortunately, the Coast Guard's current fleet of heavy icebreakers is not adequate to meet this expanding mission. Although the administration has now proposed accelerating the acquisition of the first replacement heavy icebreaker, the funding proposed for the Coast Guard's icebreaker program in fiscal year 2016 inadequately supports this plan," it said.

Having a sufficient number of polar icebreakers is critical to national security, Vojvodich said. "Without having these heavy icebreakers, we're going to lose … global access throughout the world."

The Coast Guard has noted that any funding for a new icebreaker must come from above its topline, he said. "It has been pretty clear that it doesn't fit," he said. "We've estimated that thing costing over $1 billion, and if you look at our budget, that crowds out just about everything else."

The Coast Guard is also conducting a study to see whether it is possible to refurbish the Polar Sea, Vojvodich said. The vessel is currently in preservation dry dock to prevent further deterioration.

Zunkunft said the solicitation would help lock down requirements. An industry day is expected in March.

"While we do that work, we're doing a level of assessment right now in terms of its condition — the hull, the machinery, the piping, the sewage, all the things that come with it," he said. "We'll have a fuller picture of what it would take to reactivate that."

At the moment, it would be speculative to say whether or not it is possible to refurbish Polar Sea, he said.

Both the Polar Star and Polar Sea are 40 years old. Early this decade, the Polar Star was refurbished, giving it an extra seven to 10 years of life. However, parts of the Polar Sea were used during Star's recapitalization, potentially making it even harder to bring Polar Sea back to service, experts have said.

Slattery suggested the Coast Guard consider purchasing an icebreaker from a foreign country.

"There are a number of foreign nations who build similar vessels, although it is possible that they don't meet the same capability requirements that … the U.S. is looking for," he said. "Other than Russia, it appears that many nations are not necessarily building vessels that rise to the level of capability in terms of icebreaking and in terms of sustaining polar weather conditions and things of that nature [as the Polar Star and Polar Sea]."

Many countries — including Finland and South Korea — have "relatively comparable" vessels for "upwards of a third of the cost of what the estimate is for the one to be built in the United States," he said.

The Coast Guard also plans to make investments in drones. It is currently undergoing a study to assess whether the service should procure unmanned aerial systems and if so, what type, Vojvodich said. The study is looking at Group 2 systems, which weigh 21 to 55 pounds.

"We're analyzing the technology. We're certainly trying to understand our need and our requirement — so making sure that we're not acquiring technology for the sake of the technology," he said. "We want to make sure we're solving a problem, filling a gap in terms of our capability."

UAS could be used for wide-area surveillance over the horizon, he said. Systems must, however, be affordable and sustainable.

The service currently does not own any UAS but partners with a variety of government entities and flies their systems, including those of the Navy and Customs and Border Protection.

In 2014, it worked with the National Oceanic and Atmospheric Association to simulate an oil spill using oranges, peat moss and environmentally safe green dye. AeroVironment Puma systems — which weigh 13 pounds — were then used for tests. ND

Email your comments to ytadjdeh@ndia.org

COAST GUARD

I/ITSEC Sees Record Attendance, Participation

By James Robb

The Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) 2015 was a spectacular success by every measure.

With almost 15,000 in attendance, the event saw increases in every category of registration. Throughout 2015, senior government leaders re-emphasized the value of bringing government and industry together to discuss requirements, debate trends and demonstrate new capabilities.

With virtually all the leaders in the training community at one site, I/ITSEC provided one-stop shopping for meeting, market research and next-generation technology.

This year's outpouring from the government side was remarkable. Not only did government registrations increase by almost 650 attendees, service chief level participation and the number of senior leaders and decision makers present was the highest ever. The National Training and Simulation Association, an affiliate of the National Defense Industrial Association, will continue to work government attendance issues, but the trend is up and the outlook for I/ITSEC 2016 is extremely bright.

Reps. Bobby Scott, R-Va., and John Mica, R-Fla., reported in keynote speeches that there is great support for defense in Congress and that they are working hard to stabilize funding. Vice Adm. William F. "Bill" Moran, deputy chief of naval operations, highlighted the Navy's substantial effort to revolutionize its training.

Waymon Armstrong, founder and CEO of Engineering & Computer Simulations, gave an inspiring talk on the need to take risks in pursuit of next-generation technologies.

The flag/general officer panel noted that we have not "played hurt" — engaged in combat with degraded systems or communications — for a long time and that we need to continually analyze asymmetric ways enemies will engage us at home and abroad.

Marine Corps Commandant Gen. Robert B. Neller and a dream team of Marine Corps senior leaders discussed the service's training vision and implementation. Their message was clear — synthetic environments are a key element of the future USMC training strategy.

I/ITSEC panels included the topics of joint strike fighter training, cyber, energy and medical simulation. We also had a robust international agenda with speakers from around the globe featuring panels from Europe and new participation from the Asia Pacific Simulation Alliance. There were also lessons learned from Exercise Trident Juncture, the largest NATO exercise held since the Cold War.

I/ITSEC 2015 featured a number of groundbreaking special events that addressed the most significant national security challenges faced today. The first was Operation Blended Warrior that brought together capabilities from over 30 government and industry entities in a live-virtual-constructive network on the exhibit floor as they fought their way through challenging scenarios.

EPNAC PHOTOGRAPHY

The second major theme was Black Swan. Black Swans are low probability but extremely high impact events that have or will dramatically affect the global condition. We had a great kickoff for this theme that will continue into 2016 with Black Swan technical papers, special presentations and dynamic discussions on how modeling and simulation can literally save the world.

The I/ITSEC exhibition hall hosted more than 470 companies and organizations again this year. The international presence continues to be strong with new exhibitors from Austria and Saudi Arabia and increased presence from Israel, France and Turkey. In addition, we saw continued strong participation in international pavilions with the European Training and Simulation Association, Brazil, the Netherlands and Canada all being represented by separate facilities on the exhibit floor. The program included opportunities for international attendees to schedule meetings with government and industry.

The world remains a very dynamic and dangerous place and support for warriors and first responders has never been more important. At the same time, the nation's economy, communications, critical infrastructure and social structures are being attacked in virtual ways, and training and simulation capability must adapt and adjust to these trends.

With this in mind, we will continue to expand the scope of I/ITSEC 2016 to include training and simulation related to defending and improving the transportation, energy, manufacturing, business and education domains. The demand for integration of virtual, constructive, gaming and analysis into our core workforce skillsets has never been more important.

Next year is I/ITSEC's 50th birthday so we are planning something special to celebrate a half century of training and simulation.

We continue the training and simulation discussion March 9 when NTSA hosts the Modeling and Simulation Congressional Caucus led by Rep. Randy Forbes, R-Va., in Chesapeake, Virginia, and at our multi-domain modeling and simulation event, MODSIM World 2016, April 26-29 at the Virginia Beach Convention Center.

Retired Navy Rear Adm. James Robb is president of the National Training and Simulation Association.

NDIA Calendar

February

3
Trusted Microelectronics Workshop
Arlington, VA
www.ndia.org/meetings/6290

8
Georgia Chapter
Annual Awards Dinner
Atlanta, GA
www.ndia-ga.org

9-10
2016 Human Systems Conference
Springfield, VA
www.ndia.org/meetings/6350

11
Tennessee Valley Chapter
Membership Dinner
Huntsville, TN
www.ndiatvc.org

11
TRIAD
Orlando, FL
www.ndia.org/meetings/614T

29-March 4
2016 Pacific Operational
Science & Technology Conference
Honolulu, HI
www.ndia.org/meetings/6540

March

1-2
Michigan Chapter
Cybersecurity Defense
Sector Summit
Troy, MI
www.ndia-mich.org

1
Live Fire Test & Evaluation
McLean, VA
www.ndia.org/meetings/6390
See our ad on p. 42

2-3
31st Annual National
Test & Eval Conference
McLean, VA
www.ndia.org/meetings/6190
See our ad on p. 42

2-3
Ground Robotics Capabilities
Conference and Exhibition
Springfield, VA
www.ndia.org/meetings/6380
See our ad on p. 42

8
2016 Women In Defense
Annual HORIZONS
Scholarship Dinner
Arlington, VA
www.ndia.org/meetings/6WI1

9
2016 Women In
Defense Annual
National Conference
Arlington, VA
www.ndia.org/meetings/6WID

9
2016 M&S
Leadership Summit
Chesapeake, VA
www.trainingsystems.org

10
NMSC Annual Meeting
Chesapeake, VA
www.trainingsystems.org

15-16
2016 Precision Strike Annual Review
Springfield, VA
www.precisionstrike.org
See our ad on p. 42

17-18
Greater Los Angeles Chapter
66th Annual West Coast
Dinner & Acquisition Forum
Marina del Ray, CA
www.ndia-lachapter.org

22
Michigan Chapter
Networking Social
Dearborn, MI
www.ndia-mich.org

29-31
Munitions Executive Summit
Parsippany, NJ
www.ndia.org/meetings/6650
See our ad on p. 43

April

5-6
Insider Threat Program Workshop
Springfield, VA
www.ndia.org/meetings/6800

8
Michigan Chapter
58th Annual ROTC
Awards Banquet
Troy, MI
www.ndia-mich.org

11-13
Joint Undersea Warfare
Technology Spring Conference
San Diego, CA
www.ndia.org/meetings/6260
See our ad on p. 43

18-20
32nd Annual National
Logistics Forum
Washington, DC
www.ndia.org/meetings/6730
See our ad on p. 43

For more information and online registration, visit our website: www.ndia.org. Or contact our Operations Department at (703) 247-9464.

19-20
Medical Research, Development and Acquisition in Support of the Warfighter
Ellicott City, MD
www.ndia.org/meetings/6310
See our ad on p. 43

25-28
2016 Armament Systems Forum
Fredericksburg, VA
www.ndia.org/meetings/6610

27-28
Michigan Chapter Defense Exposition (MDEX)
Warren, MI
www.ndia-mich.org

26-28
MODSIM World 2016
Virginia Beach, VA
www.trainingsystems.org

May

3-5
59th Annual Fuze Conference
Charleston, SC
www.ndia.org/meetings/6560

9-11
Annual Tactical Wheeled Vehicles Conference
Reston, VA
www.ndia.org/meetings/6530

9-13
29th International Symposium on Ballistics
Edinburgh, Scotland
www.ndia.org/meetings/6210

12
NDIA Annual Award Dinner & Eisenhower Award Presentation (Black Tie)
McLean, VA
www.ndia.org/meetings/6130

16
Washington, D.C. Chapter Benefit Golf Outing for USO-Metro
Suitland, MD
www.ndia.org/washdc

23-26
SOFIC
Tampa, FL
www.ndia.org/meetings/6890

24-26
Iowa-Illinois Chapter Midwest Small Business Government Contracting Symposium
Moline, IL
www.ndia-ia-il.org

June

1-2
DI2E Plugfest
Fairfax, VA
www.di2eplugfest.org

8-9
Tennessee Valley Chapter Missile Defense Agency Small Business Programs Conference
Huntsville, AL
www.ndiatvc.org

9
WID Service to The Flag Award Program & Reception
Arlington, VA
www.womenindefense.net

July

14
Integrated Air & Missile Defense Symposium
Laurel, MD
www.ndia.org/meetings/6100

TRAINING & PROFESSIONAL DEVELOPMENT COURSES

Defense Systems Acquisition Management Course (DSAM)
Defense Acquisition University instructors present an intense week of acquisition program management knowledge and processes.

- **March 21-25**
  Denver, CO
  www.ndia.org/meetings/602B
- **June 20-25**
  Phoenix, AZ
  www.ndia.org/meetings/602C

Mastering Business Development Workshop
An educational and professional development program focusing on the thinking, process and discipline needed for professional BD.

- **February 9-10**
  Orlando, FL
  www.ndia.org/meetings/607B
- **April 5-6**
  Washington, DC
  www.ndia.org/meetings/607C
- **June 22-23**
  Boston, MA
  www.ndia.org/meetings/607D

How Washington Works
A fast-paced overview of the decision support systems, organizations and procedures underlying the defense acquisition process. Ideal for those who are new to or routinely do business with the DoD.

- **February 3-4**
  Reston, VA
  www.ndia.org/meetings/643B
- **May 11-12**
  Reston, VA
  www.ndia.org/meetings/643C
- **July 27-28**
  Reston, VA
  www.ndia.org/meetings/643D

For more information and online registration, visit our website: www.ndia.org. Or contact our Operations Department at (703) 247-9464.

Live Fire Test & Evaluation

"Live Fire Test and Evaluation: Applying Technology and Innovation to Efficiently Address Current and Future Threats"

Held at the SECRET/U.S. Only level
March 1, 2016
Topics to include:

- New and Emerging Technologies in LFT&E
- LFT&E and the Acquisition Process
- Statistics in LFT&E
- Support for Armed Conflict

* To occur in conjunction with the 31st Annual National T&E Conference

McLean, VA • March 1, 2016
www.ndia.org/meetings/6390

31st Annual National Test & Eval Conference

"The Future of T&E: Technology Excellence and Innovation"

The 31st Annual National Test And Evaluation Conference Returns to DC in the Spring!

Sessions to include:
- Proper roles of T&E in our defense acquisition system
- New & Emerging Technologies
- Big Data and Knowledge Management
- Other key T&E issues such as Reliability, Statistic, Early Involvement, Sustainability & Cyber Security

McLean, VA • March 2-3, 2016
www.ndia.org/meetings/6190

Ground Robotics Capabilities Conference and Exhibition

"Realizing the Robotic & Autonomous Systems Vision"

Strategic overview of the current needs and requirements related to ground robotic technology research and development.

Springfield, VA • March 2-3, 2016
www.ndia.org/meetings/6380

2016 Precision Strike Annual Review

PSA
PRECISION STRIKE ASSOCIATION

"Precision Engagement Acquisition Strategy to Support 3rd Offset"

As we near the edge of the technical envelope, it behooves both Government and Industry to work cooperatively in the new "better, faster, cheaper" acquisition environment to anticipate, get ahead and develop the next new thing in precision.

Springfield, VA • March 15-16, 2016
www.precisionstrike.org/Events/6PPR

2016 Munitions Executive Summit and Advance Planning Briefing to Industry

This annual event will be attended by key leaders in the U.S. Government acquisition, program management and technology sectors and industry leaders in the U.S. Munitions Industrial Base.

Parsippany, NJ • March 29-31, 2016
www.ndia.org/meetings/6650

Joint Undersea Warfare Technology Spring Conference

"Assuring Undersea Dominance in an Era Of Major Power Competition"

Secret/U.S. Only

This annual conference focuses on the Navy's key undersea warfare missions of countering submarine and mine threats to sea lines of communication and protecting and facilitating power projection from the sea.

San Diego, CA • April 11-13, 2016
www.ndia.org/meetings/6260

32nd Annual National Logistics Forum

"Readiness Today, Innovation for the Future: Delivering the Realm of the Possible"

The National Logistics Forum will assemble ...
- Senior Pentagon-based logistics policy officials
- Senior government logistics practitioners
- Industry leaders and logistics providers

To address ...
- Challenges facing delivery of logistics capabilities and services in a resource-constrained environment
- Opportunities and future impacts of known and anticipated fiscal constraints

Washington, DC • April 18-20, 2016
www.ndia.org/meetings/6730

Medical Research, Development and Acquisition in Support Of The Warfighter

"Military Medicine in a Complex Environment"

The 2nd Annual NDIA USAMRMC Conference expands this year to include the medical research, development, test and evaluation (RDTE) missions across the Department of Defense (DoD), and will include perspectives from Army, Navy, Air Force and the Defense Health Agency!

Ellicott City, MD • April 19-20, 2016
www.ndia.org/meetings/6310

Next Month

Navy Priorities

■ Secretary of Defense Ash Carter is pushing the Navy to rethink its investment priorities, including cutbacks in the procurement of the Littoral Combat Ship. He argues that the service should prioritize resources in other capabilities. What is the outlook for the Navy's budget plans? And what types of systems does the service need to invest in to win wars against advanced adversaries?

In the next issue of National Defense, service leaders, analysts and members of industry discuss the potential consequences of future LCS decisions on the Navy's capabilities and the shipbuilding workforce.

Autonomous Systems

■ Pentagon leaders have identified autonomous systems as a key element of its "third offset strategy." The strategy calls for investing in capabilities that will enable the U.S. military to maintain its technological edge over potential adversaries. How does the Defense Department hope to integrate and exploit autonomy? And what are the challenges that lie ahead?

Navy Bomb-Disposal Robots

■ After years of delays, the Navy is moving ahead with its family of explosive ordnance disposal robots. It has issued contracts to begin building a small back-packable robot. As the executive agent for EOD technology, the Navy must field these life saving machines for the other services. But the Air Force and Army appear to have run out of patience.

Smart Munitions

■ The Air Force wants to build munitions that fly in a group to attack targets. It also wants to be able to communicate with them after launch so they can be ordered to change direction if needed. These expendable robots are the result of years of research looking into swarming technology.

FEBRUARY 2016 Index of Advertisers

Interact with the companies whose products and services are advertised in National Defense.

National DEFENSE International Advertising Headquarters

For information on advertising in National Defense, contact the International Advertising Headquarters or your regional advertising office.

VICE PRESIDENT, ADVERTISING
Dino K. Pignotti
(703) 247–2541
Fax: (703) 522-4602
dpignotti@ndia.org

Advertising Headquarters is located at:
2111 Wilson Blvd., Suite 400
Arlington, VA 22201
Advertising Fax: (703) 522-4602

ADVERTISING REGIONAL OFFICES

▪ **Northeastern United States & Canada**
(CT, DE, MA, ME, NH, NJ, NY, PA, RI, VT)

Dino K. Pignotti
(703) 247–2541
Fax: (703) 522-4602
dpignotti@ndia.org

2111 Wilson Blvd., Suite 400
Arlington, VA 22201

▪ **Southeastern United States and Metro DC Area** **(AL, FL, GA, KY, MD, MS, NC, SC, TN, VA, WV & DC)**

Barros Sales
Jim Barros & Mark Horowitz
(805) 584-2130
Fax: (805) 584-3796
jim@barrossales.com

6480 Katherine Road # 72
Simi Valley, CA 93063

▪ **South Central United States**
(AR, KS, LA, MO, OK, TX)

Dino K. Pignotti
(703) 247–2541
Fax: (703) 522-4602
dpignotti@ndia.org

2111 Wilson Blvd., Suite 400
Arlington, VA 22201

▪ **Western and North Central United States**
(AK, AZ, CA, CO, HI, IA, ID, IL, IN, MI, MN, MT, ND, NE, NM, NV, OH, OR, SD, UT, WA, WI, WY)

Barros Sales
Jim Barros & Mark Horowitz
(805) 584-2130
Fax: (805) 584-3796
jim@barrossales.com

6480 Katherine Road # 72
Simi Valley, CA 93063

GET MORE NATIONAL DEFENSE

NationalDefenseMagazine.org

Exclusive Online Content

Read daily breaking news stories and full-length features in our blog and archived magazine content.

Digital Magazine

View the latest issue online, anytime at: digital.nationaldefensemagazine.org

Podcast

Listen to summaries of top stories from National Defense at: nationaldefense.libsyn.com

Newsletters

Sign up for our Weekly Insider and Defense Watch newsletters at: bit.ly/NDsignup

Social Media

Follow us and share our stories on Twitter, Facebook and Google+

Twitter.com/NationalDefense

Facebook.com/NationalDefense

BUILT TO SURVIVE

Off-road or on, experience counts. Trust expertly engineered and mission-proven Battelle Armored Vehicles for superior protection and reliability through every turn.

Get there safely – go with a Battelle.

800.201.2011 | solutions@battelle.org | www.battelle.org

Battelle
The Business of Innovation