# DefenseNews

www.defensenews.com

A GANNETT COMPANY


**SPECIAL REPORT**

**HOMELAND SECURITY** 9


April 27, 2015


EUROPE

## Budget Boost Expected

With a new pro-military coalition taking office in May, Finland's defense spending is sure to rise. *Page 16*



NORTH AMERICA

## BAE IT Selloff?

BAE Systems is considering shedding parts of its US-based business. *Page 3*



ASIA & PACIFIC RIM

## Communications Delay

Procedural disputes are hampering development of the Indian Army's Tactical Communication System. *Page 16*

INTERVIEW

## Vernon Coaker

The UK Labour Party's shadow defense secretary discusses the strategic defense and security review, budget cuts and the future of the Successor submarine program. *Page 22*

# Pentagon's Cyber Strategy Relies on Deterrence, Industry

By AARON MEHTA

**WASHINGTON** — The Pentagon's new cyber strategy emphasizes deterrence, a shift that analysts say is a subtle, but important, change for the future of the department.

It also sets up a reliance on the commercial technology sector, which comes with a new push to strengthen ties between Silicon Valley and the Pentagon.

The new strategy, released April 23, represents the first update to the Pentagon's cyber strategy since 2011 — a veritable lifetime given the speed at which technology has developed.

The overall focus of the strategy falls into three categories: defending Defense Department networks, systems and information; defending against cyber attacks of what the department calls "signifi-

*See US CYBER, Page 6*


ROBYN BECK/ AFP/GETTY IMAGES

**Seeking the Experts:** The Pentagon wants to tap into Silicon Valley to help with cybersecurity challenges, but can the cultures merge?

# Poland Eyes Fund To Arm Eastern Europe

By JAROSLAW ADAMOWSKI

**WARSAW —** Poland plans to bolster armament efforts of neighboring countries through government, bank and export loans as a response to Russia's increased military presence in Ukraine.

Warsaw unveiled the plan shortly after announcing that it aims to award multibillion-zloty contracts to Airbus and Raytheon for helicopters and Patriot missiles, respectively.

"Poland aims to play the role of a regional leader, and rally other [Eastern European allies] behind the objective of intensifying regional cooperation in the field of defense and security," said professor Marek Jablonowski, a political scientist from the University of Warsaw.

The plan involves the Visegrad Group of countries — Poland, Czech Republic, Slovakia and Hungary — along with the Baltic states of Lithuania, Latvia and Estonia, in addition to Romania and Bulgaria, Col. Jacek Sonta, spokesperson for the Polish Defense Ministry, told local business daily Puls Biznesu.

*See E. EUROPE, Page 4*

JANEK SKARZYNSKI/AFP/GETTY IMAGES

**Air Defense:** US troops emplace a launching station of the Patriot air and missile defense system in Sochaczew, Poland, on March 21.

# Eastern Markets Drive Rise in Global Spending

By JOE GOULD

**WASHINGTON —** After three years in decline, global defense spending rebounded by 1.7 percent, driven by emerging markets in the East as the West largely continues with austerity, according to analysts with the International Institute for Strategic Studies (IISS).

US defense spending in 2014, at about $600 billion, still dwarfed its nearest rival, China, and the West still accounted for more than half of global defense outlays in 2014. However, this was down from two-thirds of global totals in 2010.

China spent some $112 billion, followed by Saudi Arabia at $81 billion and Russia at $70 billion, according to figures compiled in the recently released 2015 edition of "The Military Balance." The UK fell from third place to fifth, at $61 billion.

In contrast to Europe, overall defense spending has increased in Asia, growing to more than $340 billion in 2014 from $270 billion in 2010. China's spending outpaces its neighbors, accounting for about 38 percent of the Asian total in 2014. Japan, in contrast, fell from 20 percent in 2010 to just less than 14 percent in 2014.

Driven largely by the European economic crisis, countries there have together reduced defense spending by 2 percent every year since 2010, with the largest drop in the Balkans, Southern and Western Europe. The only increases are in the north and southeast.

"There is an emerging sub-regional difference within Europe," said James Hackett, editor of IISS' 2015 edition. "The eastern states

*See GLOBAL SPENDING, Page 7*


PERIODICALS-NEWSPAPER HANDLING

Vol. 30 No. 16 $4.50

# US CYBER

*From Page 1*

cant consequence;" and providing integrated cyber capabilities to military operations.

Defense Secretary Ash Carter officially launched the strategy with a speech at Stanford University. As part of his speech, Carter disclosed that hackers from Russia managed to access a Pentagon network.

Although the network was unclassified, and the issue was handled within 24 hours, Carter said the incident was "worrisome" and highlights the need for an updated cyber strategy.

Ben FitzGerald, of the Center for a New American Security, said the new strategy tries to encapsulate recent experiences of the Pentagon and the Obama administration.

"I think this strategy is trying to formalize some of the thinking and actions that have been taken over the last year or two," he said.

Jasper Graham, former technical director at the NSA and now a senior vice president with cyber intelligence firm Darktrace, said the updated strategy is "definitely something that was needed."

The latest strategy "assigns role and responsibilities, but also talks about understanding how they have to educate people and integrate across agencies," Graham said.

Both men were struck by the overall attitude of the strategy, one that openly discusses cyber deterrence and potential retaliation for digital attacks against the US.

That is a major change from how the Pentagon has discussed cyber attacks in the past, when using the term "offensive cyber" would provoke denials from military leaders that such a thing was on the table. That is a good thing, Graham said.

The Pentagon is "finally being a little more open about the fact it exists and there is a thing called 'offensive cyber' that is out there, and it's not just about playing defense," he said. "Other people are developing offensive cyber strategy, and if you have to protect yourself in the realm, you have to have both a defensive and offensive strategy."

ARMY SGT. 1ST CLASS CLYDELL KINCHEN

**Cyber Strategy Shift:** "Adversaries should know that our preference for deterrence and our defensive posture don't diminish our willingness to use cyber options if necessary," Defense Secretary Ash Carter said in an April 23 lecture at Stanford University. "And when we do take action — defensive or otherwise, conventionally or in cyberspace — we operate under rules of engagement that comply with domestic and international law."

### All In on Deterrence

Cyber deterrence has always been tricky. After all, it's not the same as nuclear deterrence. In the latter situation, the launch of a nuclear weapon would result in a counterlaunch — the infamous mutually assured destruction of the Cold War.

That situation doesn't exist with cyber, given the variety of digital attacks that can occur. Those range from a denial-of-service attack, to the stealing of a US company's intellectual property, to a full-on destructive virus such as the infamous Stuxnet worm that the US is alleged to have used against Iran's nuclear program.

Or as Alec Ross, a senior fellow at Columbia University's School of International and Public Affairs put it in an emailed statement, ""Cyber conflict is a domain with no widely accepted rules. There are not treaties to keep countries in check.

"The weaponization of code is the most significant development in warfare since the weaponization of fissile material," wrote Ross, who served as senior adviser on innovation to then-Secretary of State Hillary Clinton. "Cyber offense is easier than cyber defense. A reasonably small number of hackers can develop weaponized code that requires a massive amount of defense."

The formal language included in the strategy goes like this: "Deterrence is partially a function of perception. It works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed.

"The United States must be able to declare or display effective response capabilities to deter an adversary from initiating an attack; develop effective defensive capabilities to deny a potential attack from succeeding; and strengthen the overall resilience of US systems to withstand a potential attack if it penetrates the United States' defenses."

In his speech, Carter said the goal is to "deter malicious action before it happens," but warned that retaliation is on the table.

"Adversaries should know that our preference for deterrence and our defensive posture don't diminish our willingness to use cyber options if necessary," Carter said. "And when we do take action — defensive or otherwise, conventionally or in cyberspace — we operate under rules of engagement that comply with domestic and international law."

FitzGerald noted that the strategy smartly leaves open multiple options for how the US can respond to a cyber threat.

"It doesn't say 'if you hack us, we hack you,'" he said. "We may use a legal response. We may use a diplomatic solution. We may use sanctions. We've seen all of that in the past 24 months."

That language shows an "understanding that cyber is kind of an asymmetrical platform," Graham said.

"We do have the ability within the cyber realm to push if we're pushed back," he added. "And I think that's OK to say that, [so] folks understand that there will be repercussions for their actions."

Given the Pentagon's renewed focus on cyber, FitzGerald argues it should "absolutely elevate" US Cyber Command to a combatant command.

"The primary reason for that should be to improve command and control," he said. "Regardless of offense or defense, DoD will need to increase its ability to coordinate cyber actions internally and with its partners, as Carter discussed [in his speech]. Removing the additional layer of C2 that USSTRATCOM brings would help do that."

### Help From California

It was no surprise that Carter picked Stanford to make his big announcement. Throughout his time at the Pentagon, Carter has established a reputation as a technocrat, someone who appreciates the rapid growth of technological development that comes out of Silicon Valley.

Carter used the Russian incident to drive home his message that government and industry need to work more closely on cyber issues.

"One way we're responding is by being more transparent, to raise awareness in both the public and private sector," Carter said. "Indeed, shining a bright light on such intrusions can eventually benefit us all — governments and businesses alike — by spurring us to better work together."

Attempts over the last 15 years to bridge relations between Silicon Valley and the Pentagon have failed, largely due to a culture shock between the two sides. That culture shock was exacerbated by the revelations of Edward Snowden about government intrusion of private data, which still resonates in the tech industry.

"I think there are some fairly rational business concerns for a number of Silicon Valley tech companies," FitzGerald said of the post-Snowden world. "It's not just an outrage issue. It hurts their business if they're seen to be collaborating too closely with the Department of Defense. If they're a global business, they can't necessarily afford to have global revenues impacted for smaller dollar opportunities with the DoD."

FitzGerald acknowledged that the "jury is absolutely out" on whether this latest attempt to tap the tech industry will work, but held out some optimism, in particular because of Carter's plan to establish the Defense Innovation Unit Experimental, a permanent DoD office housed just minutes from the heart of the valley.

"DoD has been talking up Silicon Valley engagement, but it's usually just shuttle diplomacy," FitzGerald said. "This is a good way to have an ongoing relationship."

Steve Grundman, principal of Grundman Advisory and Lund Fellow at the Atlantic Council, also sees reason for optimism.

He sees important symbolism in Carter coming to California and in creating the permanent office there. "If we could not get Silicon Valley to come to the Pentagon, we're going to bring the Pentagon to Silicon Valley," Grundman said. And that symbolism will resonate not just with industry, but with a Pentagon bureaucracy known for grinding outside thinkers down to a fine powder.

"Carter is signaling to the Pentagon itself that 'I, the new secretary of all defense, care about this. I know some things about it, and I know some people out here, and it matters to me,'" Grundman said. "The symbolism has some substance to it."

Graham said the department will probably find more success going for smaller start-ups in need of cash first, rather than targeting the Googles of the world.

"As smaller companies interact with DoD, there will be really good ideas that start to get implemented, some of the bigger players will notice and they'll want to get involved," he said. "I don't think it will be an instantaneous reward."

One positive sign for Carter's hopes? A warm reception from the National Defense Industrial Association (NDIA), which represents the traditional defense players.

In a statement, NDIA Board Chair Arnold Punaro called Carter's speech and cyber strategy release "a game-changer towards harnessing the entrepreneurial genius of American industry and providing a realistic and achievable strategy in the incredibly complex cyber world."

"We welcome Secretary Carter's approach with open arms, but we also recognize that significant institutional and cultural barriers remain — in Congress, in the department, and in industry, both traditional and non-traditional suppliers," the statement reads. "We commit to breaking down our own barriers and look forward to working with Congress and the department to breaking down theirs." □

Email: amehta@defensenews.com