MNON Deputy Secretary Addendum

As of 1500, June 24

Table of Contents

4. Pompeo seeks support from allies to monitor Persian Gulf region amid tensions with Iran

Washington Post Online, June 24 | Carol Morello

Secretary of State Mike Pompeo on Monday began recruiting allies to help outfit tankers and other ships in the Persian Gulf region with cameras that can monitor and corroborate threats from Iran.

5. Germany to ban exports of side-arms to non-allies

Reuters, June 24 | Tassilo Hummel and Andreas Rinke

Germany will ban exports of small side arms to most countries outside NATO and the European Union, government sources told Reuters on Monday, confirming an earlier report from the Funke media group.

6. China's race to 5G hampered by Huawei ban

Financial Times (UK) Online, June 24 | Louise Lucas and Yuan Yang

China's determination to be the first 5G superpower was on show again this month, as the government handed out commercial licences to its three telecoms carriers and a cable television network to roll out the next generation of mobile internet.

INDUSTRY

7. Raytheon chief stands by tie-up with UTC arm

Financial Times (UK), June 24, Pg. 10 | Sylvia Pfeifer

Raytheon, the US defence group, has defended its proposed merger with the aerospace arm of United Technologies, insisting it is not pursuing size for the sake of it. "This is not about just being bigger," Toby O'Brien, Raytheon chief financial officer, told the Financial Times.

8. Shipbuilding Industry Struggles to Recruit and Retain Workforce

U.S. Naval Institute News, June 21 | Otto Kreisher

The shipbuilding and repair industry is facing increasing challenges from an aging workforce, lack of stability in the contract workload and a problem convincing young Americans that shipyard work is essential and well-paying, industry officials said.

LOGISTICS/MAINTENANCE

9. Navy Refining How Data Analytics Could Predict Ship Maintenance Needs

U.S. Naval Institute News, June 24 | Ben Werner

Extending the lifespans of existing ships using data-driven maintenance efforts is the best strategy for achieving a 355- ship navy, said the Naval Sea Systems Command chief engineer.

PERSONNEL/READINESS

10. DoD changes name of security clearance agency, appoints new leadership

FederalNewsNetwork.com, June 24 | *Nicole Ogrysko*

The Defense Department's security clearance agency officially has a new name — and new acting leadership.

SECURITY ASSISTANCE

11. India, U.S. nearing industrial security pact for defense tech transfers

Reuters, June 24 | *Sanjeev Miglani*

India and the United States are closing in on an industrial security agreement that will allow the transfer of defense technology, sources said on Monday, ahead of U.S. Secretary of State Mike Pompeo's talks in New Delhi this week to promote strategic ties.

12. Indian MoD approves procurement of 10 more P-8I aircraft for Indian Navy

Jane's Defence Weekly, June 24 | *Rahul Bedi*

India's Ministry of Defence (MoD) has approved the procurement of 10 more Boeing P-8I Neptune long-range maritime multi-mission aircraft for the Indian Navy (IN) for a total of USD3 billion.

SPACE

13. SpaceX Attempts 'Big Bang' Military Mission With Massive Rocket

Bloomberg News, June 24 | *Dana Hull*

SpaceX's latest launch, billed by Elon Musk as the company's most difficult ever, has the potential to be extraordinary for a whole host of reasons. It's a fitting chapter in a remarkable story about a rocket maker that fought like mad to fly for the Air Force, and has made major business decisions since then on the basis of this relationship.

COMMENTARY

14. Huawei is national security issue, not trade football for our leaders

The Hill Online, June 24 | *Mike Rogers*

Put simply, Huawei is a national security and intelligence issue. It is not a football to be thrown around in trade discussions with China. However, there is a danger that this could become the narrative and undermine the progress made to date and weakening the arguments against Huawei.

15. Here's what an AI code of conduct for the Pentagon might look like

C4ISRNET Online, June 21 | Cortney Weinbaum

Have you ever witnessed two people talking past each other? They seem to be discussing the same topic using the same language, but you begin to wonder if they are actually talking about two different things. The public debate about the use of artificial intelligence in the Department of Defense is beginning to feel that way to me. Some technologists have called for DoD AI ethics, but in the next breath they call for an end to programs that have never been demonstrated to be unethical. What gives?

CYBER/IT

1. Virtually Defenseless

The national security establishment is woefully unprepared for the new era of cyber-warfare

CQ Magazine, June 24, Pg. 15 (Cover Story) | John M. Donnelly and Gopal Ratnam

Last fall, when the Navy was examining gaping holes in its cybersecurity, its outside consultant leading the project ordered his team to learn the ancient Chinese strategy game Go.

In that board game, two players place black and white discs one by one onto a grid. The players then slowly try to encircle each other until the victor completely envelops the loser's pieces.

The point, says Michael Bayer, the veteran Pentagon adviser who ran the Navy's review, was to show that China and other foes are encircling and exploiting America's weak flanks rather than directly challenging its conventional military strengths.

Meanwhile, he says, American policymakers tend to think in checkers or chess terms, directly attacking an opponent. The Chinese play both games, but westerners generally do not know Go.

"If you play checkers or chess you want to grab the data on weapons systems," Bayer says. "If you play Go, you want to grab the Office of Personnel Management background files on everybody," referring to a 2014 hack orchestrated by Beijing.

In the long game of information warfare, old strategies lose meaning. The battle is not in one region or another or over a particular time frame; it is everywhere and forever. The traditional distinctions between civilian and military lose meaning because defeat in one jeopardizes the other. The United States is, quite simply, playing the wrong game.

"I believe we are in a declared cyberwar," Bayer says. "It is aimed at the whole of society and the state. I believe we are losing that war."

China, Russia, North Korea, Iran and even terrorist groups have for years been waging — and, experts say, winning — conflicts in the so-called “gray zone” just below the threshold that would trigger a U.S. military response. A 2016 Pentagon report defined it as “not yet war but not quite peace.”

In the gray zone, two modes of fighting dominate. The first, information operations, constitutes everything from broadcasting propaganda to using social media for spreading information or misinformation. The second tool is cyber.

In these two realms, the U.S. military and civil society are virtually unprotected and will be for years, Pentagon experts have reported in the last two years.

Kenneth Rapuano, the Pentagon’s assistant secretary for homeland defense and global security, says the U.S. military is responding to the challenge in cyberspace.

But by most accounts, while America’s cyber warriors have stepped up their attacks in the last year, including in Russia, the ability to defend U.S. networks has not kept pace. Without a strong defense, offensive attacks can be invitations for disaster instead of deterrents.

And numerous experts say America’s ability to fight offensively or defensively in cyberspace is inadequate, with the required focus, leadership and strategic thinking all woefully wanting.

“While we have made progress, it would be fair to say we have a long way to go,” says Mike Rounds, the South Dakota Republican who chairs the Senate Armed Services Subcommittee on Cybersecurity.

The military’s torpid response has been caused by bureaucratic inertia, the political dominance of traditional weapons and military organizations, the distraction of the post-9/11 wars, and a failure to comprehend the cumulative damage that was occurring and how rapidly modes of warfare were changing.

“We need to have the bombers and planes and missiles to make sure we can defend the country in a conventional conflict, but we also need to face the reality, and gray zone conflict is happening now and will continue to go forward,” says Jim Langevin, the Rhode Island Democrat who chairs the House Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities.

The United States needs the kind of spur to action that came after Japan attacked Pearl Harbor in 1941; after Russia launched Sputnik, the world’s first artificial satellite, in 1957; or when al-Qaida attacked New York and Washington in 2001, several top analysts say.

But America's adversaries, mindful of this history, have stayed in the gray zone. Bayer compares this to a parasite that constantly saps its host — but not so much as to trigger a full-scale white-blood-cell counterattack.

Thomas Modly, the Navy undersecretary, thinks the Navy review got the cybersecurity problem right.

"Our vulnerabilities may make it so debilitating for us that we may not be able to get off the pier in San Diego if we had a major conflict," Modly says. "This is not just a Navy problem. This is a national problem."

Numerous experts — including Wisconsin Republican Rep. Mike Gallagher, co-chairman of the Cyberspace Solarium Commission, a bipartisan panel created in May to study competition in the infosphere — call for a nationwide public awareness campaign.

"Ultimately our success or failure in cyber will come down not to algorithms or technology but to human beings," says Gallagher, who noted that he was not speaking for the commission. "Everyone who has a cellphone in their pocket is in some ways on the front lines of a geopolitical competition."

The Gray Zone

America's reluctance to use force, especially against nuclear-armed foes, and the country's reticence to violate human rights, despite some exceptions, restrain it from reacting too strongly — and U.S. adversaries know it.

U.S. foes further reduce their chances of suffering retaliation by using proxies or otherwise disguising what is being done and by whom. The U.S. government also disguises its actions on many occasions.

The need to cover up identity is why Russia has covertly conducted assassinations in other countries and employed so-called "little green men" — paramilitary forces out of Russian uniform — as they fought in neighboring Crimea.

China, for its part, has used commercial fishing boats to overwhelm other countries' coast guards, among other guises.

Nowhere is gray zone activity more intense — and the perpetrators less identifiable — than in the ether, because the barriers to entry for cyber warriors are low and the possibility of acting undetected is higher.

"How can you effectively do deterrence by punishment or deterrence by denial if you can't attribute a cyberattack and clearly connect the dots to North Korea or Russia or China?" asks Gallagher.

But attribution is a double-edge sword, says retired Army Gen. Keith Alexander, who headed the National Security Agency and the U.S. Cyber Command. If the U.S. government were to provide clear attribution in all cases, adversaries would use that knowledge to escape detection in the future, he says. “So you end up with that kind of Catch-22.”

Mounting Problem

Information operations and cyberattacks in the gray zone have grown in recent years — in number, sophistication and the damage they have wrought.

China’s 2018 attack on a Navy contractor gave that country access not just to details of a key new anti-ship missile known as Sea Dragon but also much of what the Navy knows about China’s maritime capabilities.

It was the latest in a long series of hacks by China, which has reportedly stolen data on F-35 fighter jets, Littoral Combat Ships, U.S. antimissile systems and drones operated by multiple U.S. military services.

The broader U.S. economy has lost $1.2 trillion in intellectual property pilfered in cyberspace, according to the National Bureau of Asian Research, a nonprofit group. The Navy’s review team assessed that figure to be an understatement. China has done most of the damage.

Russia has stolen and hacked in cyberspace, too, but it has specialized in a massive information warfare campaign to influence U.S. elections by sowing dissent and planting lies in U.S. social media circles.

In the most famous instance, Russian intelligence agents broke into the Democratic National Committee computers in 2016 and disseminated stolen information. They also attempted to break into election systems in 21 states, gaining entry to at least seven of them. Kremlin-backed operatives mounted a social-media influence campaign to confuse American voters, tactics they have perfected against former Soviet satellites such as Estonia, Georgia and Ukraine.

North Korea, meanwhile, famously hacked Sony Pictures in 2014 and stole company data, according to U.S. officials. Iran, meanwhile, is widely believed to have been behind a 2017 cyber assault on Aramco, Saudi Arabia’s national oil company, among other sophisticated hacks.

U.S. government computers aren’t immune to such attacks. Out of 330 confirmed data breaches in 2018 in U.S. federal, state and local governments, two-thirds were believed to be espionage by foreign governments, Verizon reported in May.

Even the Islamic State, or ISIS, has used hacking and social media to great effect in proselytizing for its so-called caliphate in Iraq and Syria.

Countries that have sophisticated offensive cyber tools often are not prepared to defend themselves in cyberspace, says Alexander, now CEO of cybersecurity firm IronNet.

In the case of the United States, “I think we are making gradual moves toward that, but I think there needs to be more,” he says. “I believe it’s the government’s responsibility under the Constitution for common defense. Period.”

The U.S. government shouldn’t distinguish between critical and non-critical sectors when it comes to defending against cyberattacks, he says.

To be sure, the United States is increasingly hitting back.

On June 11, National Security Adviser John Bolton publicly stated that the U.S. has stepped up its offensive cyber-assaults since last year, when President Donald Trump loosened restrictions on such campaigns. Bolton said they would keep up “in order to say to Russia, or anybody else that’s engaged in cyberoperations against us, ‘You will pay a price.’ ”

Four days after Bolton’s remarks, The New York Times reported that the United States, in a classified operation, had penetrated Russia’s energy grid not just with reconnaissance probes but with malware that, if triggered, could disrupt Russia’s electrical systems.

Yet without effective cyber-defenses, more aggressive overseas operations could come back to bite the United States, experts warn.

“Defense is a necessary foundation for offense,” the Defense Science Board, a Pentagon advisory panel, said in a report last summer. “Effective offensive cyber capability depends on defensive assurance and resilience of key military and homeland systems.”

Defenseless Defense

The Navy cybersecurity review, which was made public in March, was unsparing in its criticism of the Navy, but the dramatic critique applies to the entire national security establishment. Indeed, the report is a national call to cyber arms.

Protecting information systems is not just one of the Navy’s many challenges, the Navy review team said, it is the main challenge — an “existential threat.”

As the Navy prepares to win “some future kinetic battle,” the report said, it is “losing” the current one. Defense contractors continue to “hemorrhage critical data.” The Navy was No. 1 among 59 government departments in the amount of its information found on the so-called darknet, where criminals trade data.

The current situation is the result of a “national miscalculation” about the extent to which the cyber war is upon us, the report adds.

The threat, it says, is “long past the emergent or developing stage.” The current phase should be known as “the war before the war,” the report says. “This war is manifested in ways few appreciate, fewer understand, and even fewer know what to do about it.”

Notably, the review team found that the vaunted U.S. military’s systems for mobilizing, deploying and sustaining forces have been “compromised to such [an] extent that their reliability is questionable.”

The U.S. economy, too, will soon lose its status as the world’s strongest if trends do not change, the authors wrote.

The Army and Air Force did not do similarly sweeping reviews, but the Navy’s results are being applied across the Defense Department. Army and Air Force spokesmen stress that they take cybersecurity seriously by regular system evaluations, recruiting more cyber personnel and using emerging technology such as machine learning.

Military Within a Military?

Nonetheless, to put it bluntly, the U.S. military and civil society are all but completely vulnerable to a cyberattack — by China or Russia, in particular — so much so that the Defense Science Board recommended in 2017 that a second U.S. military that is truly cyber-secure be created as soon as possible, because the one America has will not necessarily work.

A cyberattack on the military, the science board said, “might result in U.S. guns, missiles, and bombs failing to fire or detonate or being directed against our own troops; or food, water, ammo, and fuel not arriving when or where needed; or the loss of position/navigation ability or other critical warfighter enablers.”

And if civilian and military attacks both occurred, the science board experts wrote, it could “severely undermine” the U.S. military’s role at home and abroad.

If cyber defenses are lacking, U.S. leaders not only will lack confidence in the reliability of their offensive weapons but will also worry that any U.S. offensive response could trigger a potentially debilitating cyber counterattack — one for which they have inadequate defenses.

The report chillingly warned that doubts about U.S. defense capabilities could cause a president to more quickly turn to nuclear weapons.

“If U.S. offensive cyber responses and U.S. non-nuclear strategic strike capabilities are not resilient to cyberattack, the President could face an unnecessarily early decision of nuclear use — assuming that U.S. nuclear capabilities are sufficiently resilient,” the report said.

James Gosler of Johns Hopkins Applied Physics Lab, an author of this and other cyber reports from the science board, says the conclusions still stand, though he notes progress in addressing the problem over the past two years.

“Across U.S. society, we have a way to go to get to where we have sufficient confidence — and the other guy does not have sufficient confidence — that their measures will work,” Gosler says, stressing that he is not speaking for Johns Hopkins or the science board.

Rapuano, the Pentagon assistant secretary who focuses most on cyber, says U.S. adversaries have “succeeded in waking up the giant” that is the United States.

The Pentagon, he says, is trying to implement “as a matter of top priority” the Defense Science Board recommendation to ensure that at least part of the military is at the highest level of cyber readiness, starting with nuclear weapons.

Moreover, top Pentagon officials convene weekly meetings to discuss progress at implementing cyber initiatives, Rapuano says.

“What you’re seeing is a consistent and continuous turning of the screws in terms of pressurizing cyberspace as one of the highest priorities of the department,” he says.

But Rapuano acknowledges there is much work to be done and says the Defense Department is in the middle of a transition that cannot occur overnight.

“It’s challenging to integrate a whole new domain of warfare,” he says. “It’s still very novel. We’re in the early days of understanding cyber doctrine and operations. Cyber and other advanced technologies are changing the character and composition of warfare.”

Rounds, of Senate Armed Services, says a recent presidential order and changes in the defense authorization law have made “a world of difference” in enabling U.S. cyber warriors to take the fight to the enemy overseas instead of merely blocking punches at home.

Still, Rounds says, among the military's domains — air, land, sea, space and cyberspace — the latter is "the weak point" and the one where the United States is "most challenged."

"Our adversaries are very, very good," Rounds says.

People Power

Power in cyberspace is a function not so much of hardware or software as of human beings, experts say. People can be either the ultimate weakness or the biggest strength.

If the Chinese want to find and exploit frailties in U.S. defenses, they can do it by "turning" just a handful of the millions of Americans who have contact with classified or sensitive data.

That is why China's two major 2014 hacks into the personal information of more than 22 million people — federal workers, contractors, family and friends in Office of Personnel Management databases — is worrisome.

People are also a weakness in that the lack of cyber hygiene by just one employee of the government — or even of a small subcontractor who has difficulty affording the most thorough cybersecurity — can be the entryway for a cyber break-in with strategic consequences.

Auditors have repeatedly found that major weapons such as antimissile systems have been exposed to cyberattacks because of a lack of simple computer hygiene: failure to use encryption or two-factor authentication or proper passwords or, in one instance, leaving a room full of servers unlocked.

There is no way to know with 100 percent certainty that one's defenses are working. The best way to test them is to have cyber "red teams" of qualified experts act as the adversary and attempt to penetrate and disable U.S. networks.

But the Defense Department also lacks a sufficient number of qualified "red teams" to test weapons. So each weapon is not tested long enough, and the threats they simulate are not realistic, the Pentagon's testing office says.

In fact, having an insufficient number of red teams, or teams lacking the right skills, may in some ways be worse than having none, because it can foster a false sense of security, the top tester has said.

However, it's not just that the Pentagon's cyber red teams are too few in number and less capable than they should be. More fundamentally, the entire enterprise is too "ad hoc," says William LaPlante, a former Air Force acquisition chief who has long advised the Defense Science Board.

What is needed is an institution that can regularly hold all programs to account on a regular basis and that is independent enough to unflinchingly deliver scathing assessments when necessary, says LaPlante, now a senior vice president at Mitre Corp., a federally funded research group.

“This is going to be hard to put in place,” says LaPlante. “The system doesn’t like these things, because they are not the bearer of good news.”

Congress is starting to notice. When the Senate debates its fiscal 2020 defense authorization bill this month, it may consider an amendment by Kansas Republican Jerry Moran and others that would require the Pentagon to assess within six months its cyber red teams — including “permanent, high-end, dedicated” ones —and report back to Congress.

It is not just the Pentagon that is short on cyber-savvy personnel. As of April, America’s overall cyber workforce is short 314,000 workers, a House Armed Services subcommittee said in a report made public this month. Efforts are underway to deal with that problem as comprehensively as possible, but the country is starting from behind, and the government is especially hard-pressed to compete with high-paying Silicon Valley firms.

Leadership, Please

The main reason cyber is a people problem is that the human beings who are government leaders must step up their game, experts say. Without sustained, senior-level attention, the United States will not shore up its cyber vulnerabilities.

In the past two years, Trump and leaders in the Defense Department and Congress have begun to significantly increase their attention to the problem, even though many lawmakers contend that the administration has muddled the signal by getting rid of a White House cybersecurity coordinator’s position that they say is essential to getting all federal agencies working toward the same goal.

But their efforts are still dwarfed by the challenge, many observers believe.

This inadequate attention is manifest in how infrequently U.S. leaders talk about cyber issues. On congressional defense committees, cyber is essentially an afterthought compared to weapons hardware and military pay and benefits. In the Senate Armed Services press release last month on its fiscal 2020 authorization bill, cyber was barely mentioned at the end.

Likewise, Bayer and his team found a dearth of cyber references in Navy leaders’ speeches and a scarcity of cyber-related events on their calendars.

“You wouldn’t even know that cyber is a Top 20 problem,” he says.

Measured in dollars, cyber also does not stack up. Unclassified cyber spending across the federal government in fiscal 2020 budget request totals just over $17 billion, considerably more than it was a few short years ago, but that's only a bit more than 2 percent of the roughly $750 billion annual national defense budget.

Total security is unobtainable. But a higher degree of confidence in the safety of U.S. systems (military or electoral) and its offensive cyber tools can be achieved, experts say.

The way to get there is through a radical new commitment to cybersecurity driven by top political and corporate leaders.

For one thing, the government must demonstrate its resolve by holding more exercises to test cyber responses, according to lawmakers and analysts. The Government Accountability Office in 2016 urged U.S. military and civilian leaders to hold a so-called Tier One exercise with the private sector to gauge how to handle an attack on domestic infrastructure.

The exercise is set for later this year, but the House Armed Services Committee is tired of waiting. Its newly minted fiscal 2020 defense authorization bill (HR 2500) would withhold 10 percent of the fiscal 2020 money for Trump's communications office until the exercise occurs.

"Unless these actions are exercised, we won't be prepared to confront bad things," says Langevin, who began to focus on cyber over a decade ago. "We don't want to do this on the fly."

Other major changes in organizations and behaviors are also needed. For its part, the Pentagon needs chief information officers who are no longer operators of networks, but purely regulators of them, and who report directly to the leaders of their organizations, which is the best practice in industry, experts say.

The Navy has sought to create such an official — an assistant secretary for information management — but has run into congressional resistance.

Bombs in the Age of Bytes

Most analysts recognize that part of the reason U.S. enemies are fighting in the gray zone is because America's military has deterred those foes from fighting the United States on the sea, air or land. So maintaining a strong deterrent in traditional arms is not open to question, most experts say.

However, given that budgets will probably not grow considerably and may even come down, the military may have to cut into its spending for conventional weaponry to make room for more investment in offensive and defensive digital weapons.

It's becoming clearer that cyberattacks and disinformation campaigns are the domains where adversaries with fewer resources and smaller militaries will challenge American dominance, says Mark Warner of Virginia, the ranking Democrat on the Senate Intelligence Committee.

Continuing to spend at the same level on conventional military strengths while also boosting spending on the newer domains may not be possible without pushing defense spending to $1 trillion a year, and "further cutting out domestic discretionary spending," Warner says.

The Pentagon also needs to step up investment in and use of advanced technologies such as artificial intelligence because they offer multiplier effects, analysts say.

The Pentagon's 2020 budget proposal calls for spending about $1 billion on artificial intelligence programs, which "seems insufficient when considering that AI has more potential to change the way we fight wars than any other emerging technology," Susanna Blume, a senior fellow at the Center for New American Security, wrote in a paper published last month.

Policymakers in the Pentagon and other national security agencies also should step up use of artificial intelligence, says Mara Karlin, of Johns Hopkins University's School of Advanced International Studies and a former top Pentagon official.

Such applications, for example, could help policymakers understand "who the Syrian opposition is and think through the pathways on how they are likely to act and respond," she says.

Several issues arise as officials try to improve federal oversight of cybersecurity and information warfare. For one thing, there must be more public-private information sharing about threats and responses. That will probably require more declassification, but there are limits to that.

In the private sector, cyber defenses aren't cheap, and pose a burden for many smaller companies. And new government regulations requiring contractors to adhere to cybersecurity standards are so confusing that even larger companies are having trouble complying, surveys have shown.

In the Pentagon alone, the new rules are "not coordinated or deconflicted," the House Armed Services Committee's fiscal 2020 defense authorization report says.

Civilians Equally at Risk

Statutory limitations on the CIA and the National Security Agency, meanwhile, have barred the United States from responding comprehensively to the broad disinformation and influence operations mounted by Russia, China and Iran.

Say, for instance, U.S. intelligence agencies are monitoring a Kremlin operative preparing a disinformation campaign. Once the Russian agent launches the operation and Americans start to see it appear on their laptops and mobile devices “then it has to be handed over” to the FBI and the Homeland Security Department, Warner says.

Another reason for slow movement in the field of information operations is Americans’ understandable queasiness about engaging in propaganda, says retired Adm. James Stavridis, former commander of NATO forces and of U.S. Southern Command.

But “it’s not propaganda,” he says. “It’s critical to meet the adversary in that universe.”

U.S. adversaries see information and political warfare as key parts of their strategy, says Seth Jones, an expert with the Center for Strategic and International Studies who has advised military commanders in war zones. But the United States, he says, “is still focused heavily on the military, both conventional and nuclear, because that’s where the funding is.”

Domestically, the Homeland Security Department does not have enough power, some say.

C.A. Dutch Ruppersberger, formerly the top Democrat on the House Intelligence Committee, believes the NSA, which is based in his Maryland district, is doing well fighting information wars overseas.

But Ruppersberger believes the government needs to create a new agency focused exclusively on domestic cybersecurity.

“We have to keep continuing to make the issue of cybersecurity one of our highest priorities,” he says, citing China’s stated goal to be the world’s superpower by 2049.

Victory Is Possible

The last two years have shown hopeful signs of progress.

The congressionally created Cyberspace Solarium Commission, which is aimed at devising strategy, doctrine and policy, may be one such positive sign. The panel is named after former President Dwight D. Eisenhower’s Project Solarium, which came up with a national strategy for combating communism.

Most experts say that what’s needed now is just what was needed then.

In a sense, it's a geopolitical version of the Go board game — patient, encircling, steady. The United States and its allies went after the Soviet Union's weak spots, shining a light on its propaganda and falsehoods by using all means at the nation's command, short of war.

The good news is that the United States has the resources and creativity to soon gain the confidence it now lacks in its ability to hold its own in the ether. It is possible for the United States to get the upper hand, assuming changes are made.

That's what Bayer and his Navy cybersecurity review team found in interviewing government officials, defense contractors and executives from companies such as Goldman Sachs and Amazon.

But to be successful, people need to wake up every day and worry about the nation's cyber vulnerabilities.

"You win this not just by changing structures and moving money," Bayer says. "You win this by changing culture. That's easy to say and damn hard to do."

RETURN TO TOP

EXECUTIVE/LEGISLATIVE

2. POLITICO Pro Q&A: Rep. Ro Khanna
Politico Pro, June 24 | David Brown

Rep. Ro Khanna's congressional district may be in Silicon Valley, but his mind is all over the world.

The California Democrat has been one of the leading House critics of the U.S. involvement in Yemen and has worked to withdraw support for the Saudis amid accusations of widespread civilian deaths.

Khanna also wants to end the U.S. presence in Afghanistan and the Middle East and focus America's investments toward competing with the system of government in China, which he refers to as authoritarian capitalism.

Closer to Washington, Khanna, a lawyer, is pushing to decrease overall defense spending and reform Pentagon procurement practices. He was a leading critic of the defense firm TransDigm, which was accused of overcharging for aircraft spare parts and was forced to repay the government $16 million.

"We need to give contracting officers more discretion to be able to ask for cost information," he said in an interview. "If the contracting officers suspect they're being fleeced, they should have the discretion to request that."

A member of the House Armed Services Committee, Khanna discussed with POLITICO his views and priorities on a wide range of defense and foreign affairs issues.

This transcript has been edited for length and clarity.

***

What are lawmakers' next moves on the Yemen situation?

We're in discussions with [House Speaker Nancy Pelosi] to bring a lawsuit to vindicate Congress' authority over war and peace. There's a group of constitutional law scholars led by [Yale Law School's] Bruce Ackerman and some very respectable people on both the conservative and liberal side who believe that the Supreme Court needs to be the final voice when there is a conflict between the congressional branch and the president on whether we should be at war.

This is under the Steel Seizure Case that the case law says the president's veto isn't the final word on the matter in a case of the War Powers Resolution. And so, there's group of us working with the Progressive Caucus to discuss with the speaker to bring a lawsuit on behalf of the entire House that would be expedited and go to the Supreme Court in challenging the president's veto.

What are some of your top concerns as the House debates the National Defense Authorization Act?

My biggest concern is the increase in defense spending. I believe we need, as a Democratic Party, to argue for smart cuts in defense that would fund infrastructure and college education and high-speed rail and health care in this country.

People say it's never been done. How do you run on strategic cuts in defense? President [Jimmy] Carter ran on 5-to-7 percent strategic cuts on defense in 1976 and won. So, it's certainly possible [following] this period of interventionism.

We need to reduce the topline in defense spending. I mean it's $100 billion more than where [President Barack] Obama left it. And this is from a president who wants to get us out of endless wars.

So, I'm going to insist and the Progressive Caucus is going to insist that we at least get an amendment on the floor in an up-or-down vote on lowering that topline number. I think that's going to be critical to

get progressive votes to pass the NDAA to have some up-or-down vote saying we can't have this kind of increase in defense spending.

Which topline are you referring to, $733 billion or the administration's $750 billion request?

733. I had introduced a resolution in the Budget Committee to freeze it at 2019 levels. That didn't pass. But I do think it needs to be a vote on the House floor putting people on record about whether they really are comfortable with these massive defense increases.

I don't think you can argue for greater restraint in our foreign policy or for ending these futile wars and then continue to fund many of these wars, especially increasing the overseas contingency fund. So, to me that's the biggest issue.

Where do you cut? Do have anything in particular in mind?

The overseas contingency fund. That and I would push for withdrawal in Afghanistan, and I would push for responsible withdrawal in Iraq.

What are we doing, given that ISIS has largely been handled, to remove ourselves from Iraq? ... At some point we need a president who’s going to extricate us from Afghanistan, extricate us from Syria, extricate us from Iraq.

I supported this president’s call for withdrawal in Afghanistan and withdrawal in Syria. I said we should do it responsibly, make sure we have an agreement with [Turkish President Recep Tayyip] Erdogan so that we have some protection for the Kurds.

I wrote an op-ed, it was one of my least popular op-eds because it said [President Donald] Trump is right. I was willing to go out on a limb to support this president on his instincts to withdraw. But he needs to follow through.

He ran on getting us out of Afghanistan. We’ve got more troops there than when he assumed office. He ran on getting us out of bad wars in the Middle East. Now, he’s sending an aircraft carrier to Iran.

One of the things — and no one really has covered this yet, but I think it’s so important to make this point: If we accept the administration’s strategic framework that China is going to be the largest competitor to the United States, which I actually agree with, then what follows is that this country, we’re going to have a competition between free enterprise democracy and what I would call authoritarian capitalism.

We know America can win and has won against fascism. We know it can win against communism. What we don't know is how difficult the competition is going to be against authoritarian capitalism with a country that has three times our population.

[China is] a very serious rival. If that's the rival and America right now is 24 percent of GDP and China is 15 percent of GDP, why in the world would we want to get bogged down in a place that's 3.5 percent of GDP, which is the Middle East? It makes no sense under the president's own National Security Strategy.

Oil no longer has the strategic value that it did in the 20th century, partly because of new industries and alternative energy. So, what our goal should be is to protect us from terrorism that has spread since some of our interventionism.

I was all for striking in Afghanistan. We should have gone after al-Qaida and we should make it very clear that we should obliterate any terrorist cell that in any way did harm to the United States. It's pretty obvious we would take decisive action, and I'd be the first to support it as would other people who are for restraint.

But being bogged down in these countries indefinitely is not a successful strategy against the threat of terrorism. It's not building the frameworks we need, and it's totally sucking our resources while China is out there with their Belt and Road initiative building alliances in Africa and other places.

I don't know why the president, given his own focus on China, hasn't been able to execute on a vision that frankly most Americans want.

What are your biggest concerns about our foreign policy?

The intellectual incoherence of the administration's National Security Strategy is at the core of my concern. If you really view China as a strategic competitor, what is our plan beyond slapping tariffs? What is our strategy?

It seems to me one coherent strategy would be restraining in interventions and a laser focus on a Sputnik-like response in developing our technology and industry and making sure that we're forming alliances with other parts of the world, whether it's India or South Korea or Japan to make sure that China doesn't have hegemonic power in East Asia.

It doesn't seem to me that this administration is following through on what would be the consequences of their own diagnosis of China as a world rival. And I think that that is one of the big missed opportunities of these years, that we don't have the coherent strategy for China, when we always did have a coherent strategy for the Soviets. Post-Sputnik, this country really went into high gear and had

a firmer vision of how we'd win the Cold War. I feel like we need that kind of strategy and I don't think that strategy has to be partisan.

Are you talking more about defense technology or other areas?

It's in all forms. So, I would say let's double the National Science Foundation budget, double the national health budget and win the green energy race.

The president should say 'by the end of my first term' or the next term if he wins, or our candidates should say, 'our country should be ahead of China when it comes to electric vehicles or alternative energy.'

We should have a posture in defense that's really building alliances with our allies in Asia, with India, with South Korea, with Japan. Strengthening alliances with NATO because of the risk that China is going around building their alliances, we should be making sure that more of the world is aligned with America and American values.

We should be focused on allowing the best and brightest to come here so that the innovation continues to be in the United States. I want the smartest Chinese students or Brazilian students doing their work in the United States, not in China.

It has to be a comprehensive national strategy about what it's going to take to stay ahead of a nation that has almost triple the population and at some point is going to have higher GDP.

Our advantage is we're going to have our GDP per capita probably higher for generations to come.

Americans' great skill is our paranoia. We never are complacent. We always fear — whether it's the Soviets or the Japanese — that someone's going to overtake us. ... I fear that there is a complacency right now and a lack of a coherent strategy about how we prepare for the 21st century.

My district needs to be consulted to make sure we're winning in artificial intelligence and synthetic biology and photonics and quantum computing and all the technology that's going to drive the 21st century.

RETURN TO TOP

F-35

3. Turkey stands by S-400s, says F-35 partners disapprove of U.S.
Reuters, June 24 | Ezgi Erkoyun

ISTANBUL -- Turkey has purchased Russian missile defenses and is discussing a delivery date irrespective of any U.S. sanctions, Foreign Minister Mevlut Cavusoglu said on Monday, adding the United States is isolated as it also squeezes Turkey on F-35 jets.

The Pentagon announced earlier this month that training by Turkish pilots on F-35 fighter jets had been halted at a U.S. air base in Arizona following Turkey's purchase of Russian S-400 defense systems.

The NATO allies have been at loggerheads over the issue for months. Washington says the S-400 is incompatible with NATO's defense network and could compromise its F-35 fighter jets, an aircraft Turkey is helping build and planning to buy.

Speaking at a news conference Ankara, Cavusoglu said partner nations in the F-35 jet program do not support the steps taken by the United States to halt pilot training.

"Whatever sanctions will be decided, whatever statement would come from the United States, we have purchased S-400s and right now we are talking about when they will be delivered," Cavusoglu said.

Buying military equipment from Russia leaves Turkey vulnerable to U.S. retribution under a 2017 law known as the Countering America's Adversaries Through Sanctions Act, or CAATSA.

Turkish President Tayyip Erdogan said on Thursday that he would discuss the issue with U.S. President Donald Trump at the G20 summit in Japan this week.

RETURN TO TOP

GLOBAL

4. Pompeo seeks support from allies to monitor Persian Gulf region amid tensions with Iran
Washington Post Online, June 24 | Carol Morello

ABU DHABI, United Arab Emirates — Secretary of State Mike Pompeo on Monday began recruiting allies to help outfit tankers and other ships in the Persian Gulf region with cameras that can monitor and corroborate threats from Iran.

A new program, called Sentinel, is being developed as a response to the dueling accounts that have arisen since Iran shot down a U.S. drone last week. Iran said the unmanned aircraft was in Iranian

airspace; the United States said it was in international airspace. Both countries provided coordinates to make their case and accused the other of lying.

Under the Sentinel program, ships traversing the Strait of Hormuz would be provided cameras and other monitoring devices. Some also would be escorted by other ships, both military and commercial.

"This is having eyes on," said a senior State Department official, briefing reporters flying with Pompeo after his meetings in Saudi Arabia with King Salman and his son, Crown Prince Mohammed bin Salman.

"So it's not about shooting at people," the official said, speaking on the condition of anonymity to describe private conversations. "It's about shooting pictures of Iranians. It's about proactive deterrents because Iranians just want to go out and do what they want to do and say, 'Hey, we didn't do it.' We know what they've done."

Saudi Arabia and the UAE are the first two stops on Pompeo's week-long trip to the Middle East and Asia. The Saudis are the first to sign on to the plan, and the United States intends to seek material and financial contributions from other allies in coming weeks.

Though the United States would lead the coalition, it is not clear whether it would provide escort ships, or how many.

President Trump weighed in on Twitter, lamenting that the United States was "protecting the shipping lanes" in the strait "for other countries . . . for zero compensation."

Later in the day, Pompeo met with Mohammed bin Zayed, the crown prince of Abu Dhabi and deputy supreme commander of the UAE's armed forces, and appealed for military help with maritime security.

"We'll need you all to participate, your military folks," Pompeo was heard telling him. "The president is keen on sharing that the United States doesn't bear the cost of this," he added, noting that the UAE, Saudi Arabia and "another 20 countries" would "need to help advance" the exercise.

The coalition envisioned by the State Department and Pentagon, which are developing Sentinel together, is made up of "all sorts of nations that want to preserve the freedom of navigation in what is the world's most important shipping way," the State Department official said.

Military officials said the Sentinel program was in the early planning stage. One official, who spoke on the condition of anonymity to discuss a program that has not been finalized, said that as envisioned now it would request foreign nations, particularly Asian or gulf countries, to provide financial assistance or ships to help monitor and protect maritime commerce in the Middle East. Countries that buy and sell

oil in the region would be asked in certain cases to escort ships, place ships at fixed positions in the region or provide maritime patrol aircraft.

According to a State Department account of Pompeo's talks in Jiddah, Saudi Arabia, the secretary talked with the Saudi king and the crown prince about the need for maritime security to ensure free navigation in the Strait of Hormuz. They also discussed ways to counter Iran's influence in the region and hold it accountable.

Pompeo was accompanied by several aides when he met with the king. But Pompeo and the prince had lunch together at a Jiddah restaurant with no aides joining them, so it was not immediately clear whether they discussed other issues.

Pompeo's visit to Saudi Arabia came one day after Houthi rebels allied with Iran fired a drone attack from Yemen on the Saudi airport in Abha. One person was reported killed, and 22 were wounded.

Pompeo cited the attack as a prime example of Iran's malign influence in the region.

"With every attack conducted by an Iranian proxy, the regime tacks another day onto its 40-year track record of spreading death and chaos in the region, and beyond," Pompeo said in a statement.

--Missy Ryan in Washington contributed to this report

RETURN TO TOP

5. Germany to ban exports of side-arms to non-allies
Reuters, June 24 | Tassilo Hummel and Andreas Rinke

BERLIN -- Germany will ban exports of small side arms to most countries outside NATO and the European Union, government sources told Reuters on Monday, confirming an earlier report from the Funke media group.

A small number of traditional allies - Australia, New Zealand, Japan and Switzerland - will be exempt from the ban, the government's latest attempt to implement the tightened arms export rules it promised in last year's coalition agreements.

Earlier restrictions on exporting weapons systems to countries involved in the Yemen war prompted howls of protest from Britain and France, since the presence of German components in many joint projects risked harming lucrative export deals with Saudi Arabia and the United Arab Emirates.

But this ban, which is much smaller in scale, is expected to have fewer international repercussions, since pistol, gun and rifle manufacture tends not to be transnational in nature.

While German side-arm manufacturers, including companies like Mauser and Walther, are major suppliers to armed forces and police around the world, the government expects the financial implications of the ban to be limited: export licenses were issued to a value of 39 million euros last year.

The Funke media group also reported that the government was also planning on introducing tougher rules on technology transfer, since small arms are often built under license in the country in which they are to be sold.

RETURN TO TOP

6. China's race to 5G hampered by Huawei ban

Beijing hopes to be mobile internet superpower after issuing commercial licences

Financial Times (UK) Online, June 24 | Louise Lucas and Yuan Yang

HONG KONG/BEIJING -- China's determination to be the first 5G superpower was on show again this month, as the government handed out commercial licences to its three telecoms carriers and a cable television network to roll out the next generation of mobile internet.

The race to 5G has become a focal point in US-China tensions, as China threatens to overtake its rival in building networks that will enable everything from instant film downloads to self-driving cars.

Michelle Wei, telecoms analyst at JPMorgan, said the decision to issue the licences was a show of bravado intended to "send a message to the world that China is capable of pushing forward 5G, and also to motivate domestic supply chain players".

But analysts and industry insiders warned that China's 5G rollout would be slower than the government might hope.

They said the development of 5G would be constrained by a US ban on Huawei, the country's largest telecoms equipment maker, as well as by the same issues dogging 5G elsewhere: a delay in agreeing standards, a lack of commercial applications, and the fracturing of the global supply chain.

Huawei is China's dominant 5G supplier, and Hosuk Lee-Makiyama, director of the European Centre for International Political Economy, a Brussels-based think-tank, estimated that it would win tenders for 37 out of the 40 cities in the first phase of China Mobile's 5G rollout.

Three-quarters of the cities were tendering for just one supplier, so Huawei had won a significant share of the tenders for China's biggest mobile carrier, he said. "Foreign vendors are likely to be excluded, or just given a symbolic share," he added.

But Huawei has been hit by a US ban on buying American parts and components — as well as from foreign companies reliant on US technology — which will severely stymie its ability to deliver 5G.

Analysts have estimated that the telecoms supplier has stockpiled enough parts and is sufficiently covered by licensing agreements to last through the end of the year.

But after that, it is likely to face difficulties obtaining power amplifiers — currently supplied by Skyworks and Qorvo of the US — and electronic design automation tools, made by the likes of Cadence, a US software and system design company.

China's other telecoms suppliers, ZTE and Datang, are much less advanced than their larger rival in 5G, despite having built a significant share of the 4G network.

Edison Lee, a telecoms analyst at Jefferies, said that Chinese telecoms companies were unlikely to switch vendors if Huawei was unable to deliver, suggesting that the rollout could be hampered.

"Chinese telecoms companies, if they cannot buy from Huawei and ZTE, will they just use Nokia and Ericsson? I don't think so, because one reason for 5G is to grow the domestic supply chain."

The European companies nevertheless remain hopeful of winning more business. "In China, the 4G market share of non-Chinese players is smaller than enjoyed in the rest of the world," said one executive familiar with the European vendors' thinking. "That's been something of a concern in the industry as to why that's the case."

Estimates of the duo's share of overall telecoms infrastructure kit in China vary at between 11 and 15 per cent, lower than their global shares. This partly reflects longstanding efforts to support national champions at home.

Analysts have warned that relying on Huawei may not necessarily be good for the Chinese telecoms carriers themselves as it could leave them scrabbling for equipment if Huawei is unable to deliver.

"Operators probably will be more conservative when it comes to network planning compared to what they would do had there been no ban on Huawei," said one Hong Kong-based telecoms analyst.

The analyst added that MIIT, the Chinese telecoms regulator, has left carriers that are reluctant to push ahead on 5G plenty of wriggle room by not defining "commercial" scale when granting the licences.

China Mobile and China Unicom, the two biggest mobile carriers, maintain that they will have some level of 5G service in 40 cities by the end of this year, but the spend and speed of the rollout may not be as fast as expected.

The number of signal-broadcasting base stations they have planned is small — in total, all three state carriers plan to deploy some 100,000 stations this year and the US defence department estimates that China currently has around 350,000 5G-operable base stations.

That compares with 1m stations carriers deployed every year during the 4G buildout, with capital expenditure of between Rmb150bn ($21.8bn) and Rmb190bn ($27.6bn) a year, according to JPMorgan estimates.

Telecoms carriers are also expected to spend less on 5G than they did on 4G rollout.

Market research firm IDC has projected that Chinese carriers' annual investment in 5G will reach between Rmb30bn and Rmb40bn this year, Rmb100bn in 2020 and Rmb150bn in 2021.

"We think the development of 5G networks will be much slower than 4G, it'll be a slope rather than a sudden hike," said Cui Kai, tech analyst at IDC. "Apart from geopolitical issues, the biggest challenge for 5G is the lack of a clear plan for profit," Mr Cui added. "The carriers are in a cautious position, trying to figure out the commercial value of 5G."

China Mobile saw its operating revenues dip last year while profit attributable to equity shareholders inched up 3 per cent, to Rmb117.8bn as government policies to cut data costs for consumers put further pressure on their revenues.

But the absence of a clear path to returns on 5G is not restricted to China.

"What is the business case for 5G?" asked one veteran telecoms consultant. "No one can answer that."

Those bullish on 5G say billions of connected devices on the roads, in our homes and in factories in the coming years will create demand for faster speeds and thus bigger revenues for carriers. But that leaves maybe five years before carriers can start reaping returns on their big investments.

Bin Liu, analyst at Citibank, said one possible solution would be a "4.5G level" that was faster than 4G and could be rolled out more quickly than 5G.

"My feedback from the China supply chain says that if [the Huawei export ban remains] China could reconsider its tech evolution path," he said.

RETURN TO TOP

INDUSTRY

7. Raytheon chief stands by tie-up with UTC arm

Financial Times (UK), June 24, Pg. 10 | Sylvia Pfeifer

Raytheon, the US defence group, has defended its proposed merger with the aerospace arm of United Technologies, insisting it is not pursuing size for the sake of it.

“This is not about just being bigger,” Toby O’Brien, Raytheon chief financial officer, told the Financial Times.

The deal to create a sprawling $120bn aerospace and defence group was unveiled two weeks ago but has come under fire from investors who have questioned the logic of the tie-up. There is just a 1 per cent overlap between the two companies in terms of revenues.

Activist investor Bill Ackman, whose hedge fund Pershing Square has a stake of more than $700m in UTC, came out against the deal arguing that the tie-up will lower the quality of its aerospace business.

US president Donald Trump has also waded into the merger, raising concerns that it could be bad for competition in a sector that is dominated by a small number of large participants.

Shares in the two companies initially fell as the market digested the news but have since recovered. Investors, said Mr O’Brien, were taken off-guard.

“The biggest thing for all investors, regardless of their initial reaction, this surprised them . . . [so] at the minimum I would have a lot of questions,” he said at the Paris air show last week.

“The sentiment today is much more positive than perhaps what the initial reaction was,” he added, but conceded that “you will always have outliers”.

Mr O’Brien declined to comment on Mr Trump’s remarks but people familiar with the situation confirmed Greg Hayes, UTC’s chief executive, and Tom Kennedy, his counterpart at Raytheon, have since met with the president.

“It was a positive meeting,” said one person, adding that they discussed the deal’s impact on US manufacturing.

The merger will bring together Raytheon's military expertise and flagship products, such as its Patriot and Tomahawk missiles, with UTC's Collins Aerospace, a maker of cockpit avionics, and aero-engine group Pratt & Whitney.

While being billed as a "merger of equals", UTC shareholders would own approximately 57 per cent of the combined group and their Raytheon counterparts 43 per cent.

Mr O'Brien insisted that it was not a reverse takeover of Raytheon but a "nil premium merger", adding that the relative valuations as well as the governance structure around the deal were "fair".

The combined group, he said, would be "more resilient" and able to operate through all business cycles while returning $18bn-$20bn to shareholders in the first three years of the merger.

The groups have argued that the lack of overlap is a good thing and should help secure approval from regulators.

"This is all about the technologies," said Mr O'Brien, adding that the new group would be able to capture "a bigger part" of government programmes, as well as "at a higher probability".

RETURN TO TOP

8. Shipbuilding Industry Struggles to Recruit and Retain Workforce

U.S. Naval Institute News, June 21 | Otto Kreisher

WASHINGTON, D.C. -- The shipbuilding and repair industry is facing increasing challenges from an aging workforce, lack of stability in the contract workload and a problem convincing young Americans that shipyard work is essential and well-paying, industry officials said.

The search for new shipyard workers must overcome the constant pressure for high school graduates to go to college, as well as the lack of experience in today's youth in the kinds of skills the industry needs, a panel of shipyard officials and engineers told the American Society of Naval Engineers' annual Technology, Systems & Ship symposium on Thursday.

Todd Hooks, general manager of BAE Systems Ship Repair yard in Jacksonville, Fla., said the average age of his workers is 55 and that his skilled managers are retiring. Workflow fluctuations at the yard only aggravate his hiring and retention. In recent years, Hooks had 2,200 workers coming through the gates, then months later was down to 1,500 workers, and then staffing needs would go back up as demand from the Navy fluctuated.

“We can’t have that. … We need a stable workforce,” Hooks said. The challenge of getting and keeping trained workers will only get harder as future ships and their combat systems grow more advanced and therefore need different skills to maintain and modernize them, he added.

The policy of many high schools not welcoming industry recruiters hampers their ability to attract new workers, he said. High schools, he added, are more interested in getting every student into college, although less than one-third attend, Hooks said. The industry has the problem of getting the message out that the shipyards provide good-paying jobs. Then, when they get new workers, the industry has trouble keeping them because many do not come back after they are laid off during a drop in workload, he said.

William Crow, president of the Virginia Ship Repair Association, said the Norfolk-based institute is attacking the need for skilled workers with the support of its 286 member companies and financial support from the state of Virginia and the federal government. Illustrating the importance of the industry, Crow said there were 43,000 employees in the Norfolk shipyards, contributing $6.4 billion to the state’s economy and earning an average of $81,531 a year.

“The problem is lack of stability of the workload,” he said.

Extreme workload cycles at the yards don’t help with recruiting and retaining, said Crow, a retired surface warfare officer. He didn’t want “to throw rocks at the Navy,” but he noted the swings in Navy funding for repair and upgrades run counter to the Navy’s goal of expanding the fleet. Crow said he learned early in his career the Navy can’t build its way into a 355-ship fleet but must maintain the ships it has.

The association offers “a very wide range of training” in the classroom and online. In 2017, it trained 1,075 workers. With a grant from Newport News Shipbuilding, the area’s biggest employer, the association recently added a Marine Trade Training Program that is providing low-level skills that allow students to get entry-level jobs in the yards, he said.

Retired Vice Adm. David Architzel, chairman of the Maritime Industrial Base Ecosystem Institute, said his group formed to take a more in-depth look at the problem of getting workers into the shipyards and is evaluating the kind of workers needed in the future.

The industry needs more support nationally, similar to what is offered by Virginia and the Norfolk area, the panel members agreed. They want to see increased efforts to spread the message that ship repair is an essential and well-paying career.

RETURN TO TOP

LOGISTICS/MAINTENANCE

9. Navy Refining How Data Analytics Could Predict Ship Maintenance Needs

U.S. Naval Institute News, June 24 | Ben Werner

WASHINGTON, D.C. -- Extending the lifespans of existing ships using data-driven maintenance efforts is the best strategy for achieving a 355- ship navy, said the Naval Sea Systems Command chief engineer.

The key to maintaining ships and enabling the Navy to extend their lifespans is data analytics, Rear Adm. Lorin Selby, the chief engineer and deputy commander of ship design, integration and naval engineering at NAVSEA, said Thursday at the American Society of Naval Engineers' annual Technology, Systems & Ship symposium.

"I have ships with a number of sensors on them, measuring things like reduction gears, showering components, turbines, generators, water jets, air conditioning plants, high packs, a number of components, and we're actually pulling data off those ships, in data acquisition systems," Selby said.

At the Naval Surface Warfare Center Philadelphia Division, Selby's team is analyzing data gleaned from smaller ship component operations to determine how often such components need servicing, oil changes, filter changes, other maintenance actions and replacement. The process is called condition-based maintenance plus (CBM+), and Selby wants CBM to drive improvements in maintaining ships.

"That's one of the things we're doing to get after utilizing the technology we have today to operate the ships we have today more efficiently and more effectively," Selby said.

The Navy has dabbled with CBM for years. A 2008 Department of Defense Conditions Based Maintenance Plus guidebook mentions NAVSEA efforts. However, two years ago at the ASNE TSS symposium, NAVSEA Commander Vice Adm. Tom Moore told USNI News that the Navy's use of CBM had perhaps gone too far and was disrupting the shipyards' ability to plan for large maintenance jobs properly.

During previous attempts at incorporating CBM, there was a thought that, if major efforts like refurbishing tanks were only done when needed, rather than on a predetermined timetable, the Navy could avoid spending time and money on work ahead of need. However, that also meant that shipyards wouldn't have a clear work package before a ship showed up at the pier, adding uncertainty and, ultimately, more time and cost into the maintenance availability.

This time around, Selby sees condition-based maintenance as a way to address smaller maintenance items in such a way that data analysis points a ship crew to components that are experiencing minor performance issues or otherwise showing signs they are about to fail before the failure actually occurs.

This summer, a pilot program using enterprise remote monitoring will occur on an Arleigh Burke-class destroyer, he said. Data collected will be sent for analysis, and operators will learn how to use the data to understand how their systems are performing and if maintenance or repairs are needed.

Selby wants to have a system of apps the Navy can use to collect data from ship components, analyze the data, share it with operators and schedule work. He wants to hold a competition for app developers to create apps the Navy will test for use in the fleet.

Describing his vision, Selby said, “the systems that will be monitoring, say the turbine; it will tell the operators when a work procedure has to be performed and it will also then tap into the work package side of the house and generate a work package that gets sent to the ship, to the work center, to do the work. And if there’s a part involved, it will be able to pull a part from the supply system.”

Testing is occurring now, but Selby concedes there are some obstacles the Navy has to overcome before large-scale deployment. The Navy is struggling with how to transmit data securely, something Selby discussed during an earlier session at the symposium. The data also has to be secured.

“The performance of any given asset is something we want to hold close. So I think what you have to do is you have to architect this from kind of the get-go with that kind of security mindset in mind,” Selby said. “You can harvest that data and you could potentially discover vulnerabilities, so you have to protect that. That’s part of my project: as I do this, we’re bringing that security aspect into the program.”

Extending the lifespan of the Navy’s current fleet is essential if the Navy is going to grow to 355-ships, Moore said during his keynote address after Selby spoke Thursday. The Navy, military planners at the Pentagon, the White House and lawmakers are all anxious to reach 355 ships as soon as possible because Moore said current forces are stretched too thin.

“We in the Navy, we don’t have enough forces to go everywhere we need to go, and we have a pretty fragile mix of ships, so that when we miss an availability coming out on time, or we don’t build something to the schedule they’re supposed to build to, there are real-world consequences to that,” Moore said.

The true determining factor of whether a ship’s lifespan can be extended, Moore said, is the platform’s flexibility. The Arleigh Burke-class is the Navy’s workhorse today because, during the past 30 years, the Navy has successfully updated its operating systems. Moving forward, Moore said extending the life of the ships in this class means back-fitting many of the older Flight I and Flight II with a scaled-

back version of the AN/SPY-6(V) Air and Missile Defense Radar (AMDR) to keep these ships relevant to current and future mission needs.

“If you’re willing to do the maintenance on the ships, from a hull and mechanical perspective, you absolutely can keep them longer,” Moore said. “The issue is really not can you keep them 50 years; the issue is can they maintain combat relevance. If they can maintain combat relevance, we know we can keep them longer.”

RETURN TO TOP

PERSONNEL/READINESS

10. DoD changes name of security clearance agency, appoints new leadership
FederalNewsNetwork.com, June 24 | Nicole Ogrysko

The Defense Department’s security clearance agency officially has a new name — and new acting leadership.

The Defense Counterintelligence and Security Agency — formerly the Defense Security Service — will be led by Acting Director Charlie Phalen, currently director of the National Background Investigations Bureau, the NBIB confirmed to Federal News Network.

The DCSA will subsume NBIB and will serve as the governmentwide security clearance provider. Phalen’s appointment begins July 1 and he will lead both NBIB and the DCSA until the two agencies merge by Oct. 1.

DoD will make the official announcement at a press conference later this morning.

“Mr. Phalen has the full support and confidence of the acting Secretary of Defense, the acting director of the Office of Personnel Management and myself,” Joseph Kernan, undersecretary of defense for intelligence, wrote Monday in a memo to Defense Security Service and NBIB employees. “His current position, background and experience in both government and industry make him well qualified to serve as the acting director of DCSA. He will provide the steady leadership, continuity, and depth of knowledge necessary to successfully transfer the background investigation mission to DoD and to integrate the workforces into a cohesive team.”

Patrick Shanahan, in one of his last acts as acting Defense secretary, made the name change official in a June 20 memo.

Kernan said the new name reflects both the DSS and NBIB’s missions.

“We are at a key moment in time and have a unique opportunity ahead of us, as we bring together the missions and workforces of NBIB and DSS,” he wrote. “Foreign threats to our personnel, technology, information and facilities are pervasive and growing. They demand that we elevate our focus on security, modernize our processes and capabilities and better integrate our efforts to allow trusted people and technology in, while keeping adversaries out. This combined team is well positioned to bring greater focus and alignment to U.S. government-wide efforts to strengthen our trusted workforce, mitigate supply chain threats, protect sensitive information, and bolster counterintelligence capabilities.”

Monday’s announcement comes as the Trump administration officially recognized DoD as having primary responsibility for security clearances across much of government.

A long-awaited executive order, which President Donald Trump signed back in April, made this move official and set two major timelines. It gave both DoD and OPM until June 24 to finalize the details of the security clearance transfer and sign an agreement that codifies how NBIB and OPM authorities, resources and personnel will move to the Pentagon’s newly rebranded security clearance agency.

The transfer itself won’t be final until Oct. 1, the start of the new fiscal year.

Kernan, as the undersecretary of defense for intelligence, will oversee the DCSA and the transfer of governmentwide security clearance portfolio from OPM to DoD. In addition, the undersecretary will oversee the development of updated security vetting procedures and strengthen the DCSA’s abilities to protect technology within the defense industrial base, according to Shanahan’s June 20 memo.

The DCSA director will “program and budget for the emerging resource requirements necessary for the successful reorganization of the DSS to the DSCA and is authorized from fiscal year 2019 to fiscal year 2021 to increase civilian manpower, acquire facility space and enter contractual agreements within the agency’s budget authority,” the June 20 memo reads.

Dan Payne, the current director of the Defense Security Service, will retire in the coming months, Kernan said. Phalen’s appointment as acting DCSA director gives both DSS and NBIB, which will continue their efforts to merge as one entity, some consistency as they prepare for the security clearance transfer by Oct. 1.

“This also provides us the preamble to start fresh, to shape an integrated, responsive organization, and to foster a culture that reflects the best of both NBIB and DSS,” Kernan said.

RETURN TO TOP

SECURITY ASSISTANCE

11. India, U.S. nearing industrial security pact for defense tech transfers
Reuters, June 24 | Sanjeev Miglani

NEW DELHI -- India and the United States are closing in on an industrial security agreement that will allow the transfer of defense technology, sources said on Monday, ahead of U.S. Secretary of State Mike Pompeo's talks in New Delhi this week to promote strategic ties.

Disputes over trade and protectionist moves have escalated between the two countries in recent months, but defense ties remain strong with Washington seeking to build Indian capabilities as a counterweight to China.

India has bought weapons worth more than $15 billion from the United States over the past decade as it seeks to replace its Russian-origin military and is in talks for helicopters, armed drones and a bigger Indian plan for local production of combat planes together worth billions of dollars.

To allow for transfer of technology for building combat jets locally and other joint ventures, the United States had sought guarantees for the protection of classified information and technology.

A draft of the agreement called Industrial Security Annex is now ready and will go up before the Indian cabinet for approval in the next few weeks, sources aware of the India-U.S. defense negotiations said.

It would be the first time New Delhi has entered into such a pact with any country, although the United States has such agreements in place with several countries, one of the sources said.

Lockheed Martin and Boeing are both in the race for a deal estimated at over $15 billion to supply the Indian air force with 114 fighter planes to replace its aging fleet of MIG 21 jets.

The planes have to be built in the country as part of Prime Minister Narendra Modi's Make-in-India drive to cut expensive imports and build a domestic industry.

Pompeo will arrive in New Delhi on Tuesday and will hold talks with Modi and his Indian counterpart Subrahmanyan Jaishankar the following day.

After years of hesitation, India signed an agreement in 2016 to allow both countries to access each other's military bases and a second one last year on secure military communications.

A third accord on sharing geospatial information is still in the early stages, the source said. These are all foundational agreements designed for closer military cooperation, the source said.

RETURN TO TOP

12. Indian MoD approves procurement of 10 more P-8I aircraft for Indian Navy
Jane's Defence Weekly, June 24 | Rahul Bedi

India's Ministry of Defence (MoD) has approved the procurement of 10 more Boeing P-8I Neptune long-range maritime multi-mission aircraft for the Indian Navy (IN) for a total of USD3 billion.

Official sources told Jane's on Monday that the MoD's Services Capital Acquisition Plan Categorisation Higher Committee endorsed in mid-June the import of the additional platforms via a direct commercial sale with Boeing, while the related weaponry, radar, and associated equipment are set to be acquired via the US Foreign Military Sales (FMS) programme.

The sources said that over the next few weeks the MoD's Defence Acquisition Council (DAC), which is headed by Defence Minister Rajnath Singh, would grant 'acceptance of necessity' (AoN) to fast-track the procurement of the aircraft and related equipment. This will then be followed by a final approval from India's Cabinet Committee on Security once various FMS-related formalities have been completed.

The actual contract is likely to be signed in early 2020, said officials.

The 10 proposed P-8Is are expected to supplement 12 similar platforms, eight of which were ordered in 2009 for USD2.1 billion and delivered by 2015. The other four were ordered in 2016 for USD1.1 billion and are scheduled for delivery from 2021.

The eight P-8Is currently operated by the IN feature anti-submarine, anti-surface warfare as well as intelligence, surveillance, and reconnaissance (ISR) capabilities. The same is expected to be the case for the four ordered in 2016 and for the 10 proposed additional platforms.

The aircraft is armed with Harpoon Block II anti-ship missiles and Raytheon Integrated Defense Systems Mk 54 Mod 0 lightweight anti-submarine warfare torpedoes capable of being released from a height of about 6 km.

That said, the four newly ordered will be equipped with Raytheon Space and Airborne Systems' newly designed AN/APY-10 multi-mission maritime, littoral, and overland surveillance radar capable of providing high-resolution images in land and sea modes.

Moreover, these four platforms are likely to be fitted with encrypted US-sourced communication suites and electronic warfare (EW) systems as a result of New Delhi signing the Communications Compatibility and Security Agreement (COMCASA) with Washington in September 2018, which allows the US to offer these additional force multipliers to the IN.

IN sources said that the 10 proposed P-8Is are likely to be similarly equipped.

Comment

The MoD's approval to procure 10 more Boeing P-8I maritime multimission aircraft is another step in meeting the IN's long-pending demand for such platforms to enhance its anti-submarine and anti-surface and ISR capabilities in the turbulent Indian Ocean Region.

The acquisition of such platforms would also increase interoperability between the IN and the US Navy, especially after overcoming the outstanding hurdle posed by COMCASA, in a bid to counter growing Chinese presence in the IOR, senior naval officials said.

RETURN TO TOP

SPACE

13. SpaceX Attempts 'Big Bang' Military Mission With Massive Rocket

Bloomberg News, June 24 | Dana Hull

SAN FRANCISCO -- SpaceX's latest launch, billed by Elon Musk as the company's most difficult ever, has the potential to be extraordinary for a whole host of reasons. It's a fitting chapter in a remarkable story about a rocket maker that fought like mad to fly for the Air Force, and has made major business decisions since then on the basis of this relationship.

Late Monday night, SpaceX will fly its massive Falcon Heavy rocket for just the third time ever. The mission for the branch of the U.S. military is to deliver 24 satellites to space on boosters that are being reused after having flown in the past. The payloads are assembled from several partners, including the National Oceanic and Atmospheric Administration, NASA, Department of Defense Research labs and university research projects.

The mission will take part over the course of more than six hours after liftoff, which is slated for 11:30 p.m. local time from Kennedy Space Center in Florida. The Falcon Heavy, which SpaceX bills as the most powerful operational rocket in the world by a factor of two, will carry the two dozen spacecraft into three distinct orbits. The company also will attempt to land the Falcon Heavy's two boosters back on

earth simultaneously, then land the first stage of the rocket on a drone ship in the ocean about 770 miles away from where it initially takes off.

“This is like the modern Big Bang,” said Luigi Peluso, an aerospace and defense consultant at AlixPartners. “The Air Force is a hugely important customer, and there are multiple stakeholders. It’s like UberPool for space, which increases the complexity. SpaceX has a technology roadmap that they are executing, and this is a big milestone.”

SpaceX first demonstrated the 230-foot-tall (70-meter) Falcon Heavy in February 2018, with Musk famously making his cherry red Tesla Roadster and a dummy driver called Starman the payload. The launch generated enormous buzz, with millions of viewers tuning in to watch the rocket’s 27 engines send the vehicle rumbling aloft. In April, SpaceX launched Falcon Heavy for its first paying customer, Saudi Arabia’s commercial satellite operator Arabsat. Monday’s launch will be another spectacle for space fans who are expected to crowd the area west of Orlando.

Musk waged an intense battle years ago for the right to compete for U.S. military launches against United Launch Alliance, the joint venture between Boeing Co. and Lockheed Martin Corp. ULA is building a new rocket, called Vulcan, that will compete with Falcon Heavy. The Vulcan's BE-4 engine is built by Jeff Bezos's Blue Origin.

After all that effort, Musk came close to canceling Falcon Heavy as the business case for the rocket waxed and waned and the company continually improved the capability of its workhorse vehicle, the Falcon 9. In an interview with Bloomberg Businessweek last year, SpaceX President and COO Gwynne Shotwell said she convinced Musk to reconsider by refreshing his memory about a Falcon Heavy mission that the Air Force had paid for.

“I reminded him that we had customers that had purchased it, and this is a good rocket,” Shotwell said. “That’s a case where I think he would say I was right.”

SpaceX’s valuation has climbed to about $34 billion as it has racked up successful missions and lucrative government contracts, making it among the most valuable venture-backed companies in the U.S. Last month, it disclosed raising more than $1 billion in equity offerings a day after launching the first satellites for its Starlink project, a broadband service network that Musk is counting on becoming a major revenue source.

RETURN TO TOP

COMMENTARY

14. Huawei is national security issue, not trade football for our leaders
The Hill Online, June 24 | Mike Rogers

Put simply, Huawei is a national security and intelligence issue. It is not a football to be thrown around in trade discussions with China. However, there is a danger that this could become the narrative and undermine the progress made to date and weakening the arguments against Huawei.

President Trump recently said, “If we made a deal, I could imagine Huawei being possibly included in some form or some part of it.” This is precisely the wrong message and represents a gross misunderstanding of the real threat that Huawei poses to the United States and our European allies.

Over the last 18 months, we have seen significant progress, albeit with fits and starts, on educating Congress, the public, and our partners and allies of just how significant a threat Huawei is to our collective security. It is, for all intents and purposes, an arm of the Chinese Ministry of State Security. It is a tool of the stated goal of Beijing to achieve “digital dominance” by 2025 and aims to control the flow of data worldwide to benefit China.

As a company, Huawei acts much less like a global business and far more like a nation state intelligence apparatus of a criminal syndicate. If you are still not convinced, read the federal indictment of Huawei from the Justice Department. Huawei conducts corporate and industrial espionage, usurps national laws, pays bribes, and violates sanctions. We have finally seen the fruits of our campaign to shed light on all this.

This year, the United States government added Huawei to a Commerce Department “entity list” necessitating special approval to do business. ZTE, another Chinese telecommunications company, was added to this list and subsequently removed last year. President Trump has also signed an executive order creating a process that could lead to banning the use of communications equipment from companies deemed a national security risk. While it did not identify expressly Huawei, the effect is all the same.

Internationally, our partners and allies are waking up to the risk posed by Huawei and similar companies. Japan, Australia, and New Zealand, among other countries, have all taken steps to prevent Huawei from accessing their communications networks. These efforts are to be applauded. The problem is, however, that the remarks of President Trump and inclusion of Huawei in trade negotiations or discussions undermines the real national security rationale and provides further unnecessary fodder for those who say this is purely protectionist policy or just part of a broader trade war.

To be clear, I along with Representative Dutch Ruppersberger raised the alarm in Congress in 2012, well before this latest trade war erupted and well before President Trump entered office. Then, as now, our biggest fears were about national security and intelligence. They were not about trade or commerce.

The behavior of Huawei, its sheer efforts to penetrate national communications networks, and its ties to the Chinese communist government truly represent a clear and present national security threat.

To arbitrarily connect Huawei to ongoing trade discussions fundamentally undermines and weakens the potency of that argument. Our European allies will simply point to the words of President Trump and say that they "knew it was a trade issue" all along. Beijing could also point and say that it is merely protectionism disguised in national security dressing. Huawei is a security national threat, full stop, and it needs to be treated as such.

--Mike Rogers is a former member of Congress from Michigan who served as the chairman of the House Intelligence Committee. Today he is the David Abshire Chair at the Center for the Study of the Presidency and Congress and founder of the Mike Rogers Center for Intelligence and Global Affairs

RETURN TO TOP

15. Here's what an AI code of conduct for the Pentagon might look like
C4ISRNET Online, June 21 | Cortney Weinbaum

Have you ever witnessed two people talking past each other? They seem to be discussing the same topic using the same language, but you begin to wonder if they are actually talking about two different things. The public debate about the use of artificial intelligence in the Department of Defense is beginning to feel that way to me.

Some technologists have called for DoD AI ethics, but in the next breath they call for an end to programs that have never been demonstrated to be unethical. What gives?

I recently completed a study examining ethics across all scientific disciplines, and my team identified 10 ethical principles that span disciplines and international borders. With this foundation, I believe what advocates want from DoD is actually a code of conduct for how DoD will use AI: a set of rules and guidelines that the government will hold itself accountable to adhering to and that would allow technology developers and researchers to know how their work will be operationalized.

Since 1948, all members of the United Nations have been expected to uphold the Universal Declaration of Human Rights, which protects individual privacy (article 12), prohibits discrimination (articles 7 and 23), and provides other protections that could broadly be referred to as civil liberties. Then, in 1949, the Geneva Convention was ratified, and it created a legal framework for military activities and operations. It says that weapons and methods of warfare must not "cause superfluous injury or unnecessary suffering" (article 35), and "in the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects" (article 57).

Therefore, if someone's particular concern with DoD is its ethics of AI — such as in the imagery-analysis program Project Maven — then this person can feel confident that ethical principles already exist. If instead this person is concerned about whether he or she can trust that DoD will adhere to ethics, then creating new ethics on paper will hardly help. And those who demand the prohibition of AI in autonomous weapons altogether might see their goal realized too, since this topic seems unlikely to disappear from international debate.

So here we are, stuck in the middle of a discussion in which both sides may not actually be talking about creating new ethics, but rather discussing a code of conduct — a set of rules and guidelines for how AI will be used and monitoring and oversight mechanisms to ensure it is being adhered to.

Here is one path for how developing a code of conduct might begin:

DoD could identify areas where it may use AI in the foreseeable future and begin with three categories for such uses, shown in the figure below. The bottom-most foundational layer is for all applications of AI (including business functions that would be found in any large organization); the next layer is for non-lethal military applications (such as intelligence systems, like Project Maven); and the top layer, with the greatest number of rules and oversight, is for applications that result in lethality (either directly or indirectly). Each layer would have its own rules and guidelines for AI, and the activities in each layer would have to adhere to the rules and guidelines of every layer below it in the pyramid.

To pursue this idea, DoD could bring together internal experts who know the department's missions, programs and processes alongside external experts who advocate for vulnerable populations and oversight to develop a code of conduct for each layer.

Such a working group could be responsible for creating guidelines for the bottom-most, foundational layer that would apply to all AI uses across DoD. These applications could include IT systems that monitor for cyber intrusion or insider threat; human capital systems that assist with recruitment or reviewing resumes and job applications; and financial systems that conduct autonomous financial accounting or transactions. The working group could address topics that apply broadly across all uses of AI, such as how to mitigate bias in training data or how to ensure that training data is itself ethical.

This working group — or perhaps a second group working in parallel — could address the middle layer of specialized, nonlethal, military uses of AI and develop policies or guidelines for their use. These applications of AI could include intelligence collection and analysis systems; systems that conduct force protection around military bases and installations; systems that manage detention facilities for enemy combatants; and so on. Such uses for AI would need all of the same guidelines established in the foundational layer, but they might also need additional guidelines or policies for issues such as whether "black-box" systems will be allowed or whether explainable AI will be required; how to value "human-

in-the-loop" versus "human-on-the-loop"; and how these systems will be audited to ensure they are meeting expectations.

Lastly, any use of AI that might lead to a lethal result would require the greatest level of oversight of all DoD's AI systems. This top layer could include systems that are weaponized (even if the weapon itself is not initiated by AI) and systems that may have lethal outcomes (such as cyber tools that may result in lethal effects). One of the goals of a working group overseeing this top layer may be the creation of an oversight body that includes members from outside of the executive branch, including from the legislative branch and from nongovernmental organizations (such as civil liberties advocates and experts from academia). The working group could create policies to dictate how often programs are reviewed by this oversight body, which milestones trigger a review, and so on.

This proposal is intended to motivate further discussion. Many questions would need to be answered. Is supply chain management a foundational layer business function, or do threats from counterintelligence and foreign interference elevate it to the intermediate layer? Do existing combat rules of engagement need to change for AI, or are current oversight mechanisms for the lethal layer already sufficient? Would any rules or guidelines that are created for DoD apply to the CIA, the State Department, the FBI and other departments and agencies?

For as long as society has achieved technology advancements, people have sought ways to weaponize or militarize them. Democratic societies can make decisions that are representative of their citizens' values and stand up to public scrutiny. It is these values that distinguish the U.S. from its adversaries. The Defense Innovation Board's public listening sessions is an example of the department demonstrating these values, and the National Security Commission on Artificial Intelligence has an opportunity to create whole of government leadership across departments. In order to advance these discussions effectively, the U.S. government must frame the militarization of AI in a manner that reflects the values of its stakeholders and of American society.

--Cortney Weinbaum is a management scientist specializing in intelligence topics at the nonprofit, nonpartisan RAND Corporation

RETURN TO TOP