Cyberattacks are the new reality and the U.S. is ill-prepared
From Top to Bottom, Cracks Are Showing in Our Defense

Mark Esper was President Donald Trump’s third pick for Army secretary. Now he’s suddenly the commander in chief’s second acting Defense secretary this year, and third Pentagon chief in Trump’s two and a half years in office.

The West Point grad and Gulf War veteran certainly checks all the traditional boxes for the top Pentagon job. He’s a former congressional aide, Pentagon official and defense industry executive. And by all accounts, he’s made a solid name for himself as the Army’s top civilian, impressing Democrats and Republicans alike on Capitol Hill.

But his rapid rise from third-choice service secretary to the very top of the massive defense bureaucracy underscores a bigger problem for an administration that has struggled to attract interested and willing candidates for the typically coveted Cabinet spot.

Patrick Shanahan, the department’s former deputy secretary who served as its acting chief for six months, wasn’t exactly a big name in defense circles prior to his appointment to the Pentagon. Trump ultimately announced his intent to nominate the former Boeing executive in May, after several other higher-profile (and arguably more qualified) candidates said they just weren’t interested.

That list reads like a Who’s Who of GOP hawks, the very people who would normally vie for the secretary’s Pentagon E-ring office. They include Sens. Lindsey Graham of South Carolina and Tom Cotton of Arkansas, both veterans; former Sen. Jon Kyl of Arizona, a leading voice on nuclear issues; and retired Gen. Jack Keane, a former Army vice chief who has become a fixture on Fox News, Trump’s favorite cable news network.

When Shanahan bowed out last week, Esper was the obvious — and perhaps only — choice.

Instability in Pentagon leadership is only the most visible challenge we face today

“I don’t know him well. I’m not surprised by that being the interim choice, I think it’s fine,” said Sen. Kevin Cramer, R-N.D., in what could hardly be described as a ringing endorsement. “But it remains to be seen whether he gets the nod, I guess, for the permanent position.”

None of this means Esper is a bad choice for the job. Indeed, House Armed Services Chairman Adam Smith — hardly a fan of the president’s — wasted no time praising Esper’s “track record of public service” and urging Trump to make the decision more permanent.

“Our national defense needs a confirmed Secretary of Defense as soon as possible,” Smith said in a statement last week. “We face a number of extremely complicated challenges around the globe and it is in our best interest as a country to have stable, predictable leadership at the Pentagon capable of withstanding internal political pressure.”

But it’s troubling that Trump’s short list for the job has become, well, so incredibly short at a particularly precarious time for the nation’s security.

Most imminently, war with Iran looms as a distinct possibility. But, as this week’s cover package illustrates, the threats go far beyond Tehran. And the United States, frankly, is woefully unprepared.

As John M. Donnelly and Gopal Ratnam write, China is playing a long strategic game of information warfare while the United States fumbles to come up with a cohesive cyber strategy to counter these digital threats.

And it’s not just China. Russia, North Korea, Iran and even terrorist groups have realized America’s weaknesses and are exploiting them. Information operations and cyberattacks have grown in recent years — in numbers, sophistication and the damage they have wrought, Donnelly and Ratnam write.

The United States, meanwhile, is stuck in its old habits. The slow churn of the Pentagon bureaucracy simply can’t keep up with our more nimble competitors, Andrew Clevenger writes. And the government, with its standardized pay and incentive system, is struggling to compete with the private sector for the best talent in this arena, Patrick Kelley writes, a worrisome fact that makes it even more difficult for the United States to compete.

A common phrase around the Pentagon is that you can’t turn an aircraft carrier around on a dime. Of course, the muscle of America’s military allows it to deter direct attacks and serve as the world’s policeman. But what good is it to simply outspend adversaries when they aren’t wedded to the old ways, tied to multibillion-dollar weapons systems with built-in political constituencies on both Capitol Hill and in the Pentagon?

Our adversaries have the luxury of thinking 10 steps ahead while the United States remains mired in an archaic planning system. In a rapidly changing age of bits and bytes, the expanse and expense of our gold-plated military — not to mention the burdensome bureaucracy that goes with it — can be more of a hindrance than a help.

That, perhaps more than anything, will be the biggest challenge for the next Defense secretary. Is Esper up for it? He very well may be. But it would certainly be nice to have more than one candidate for the job.
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 de-
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.

“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 — have been calling 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 United States needs the kind of spur to action that came after the attack on 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.

“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 Langefin, 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 concludes it as “not yet war but not quite peace.”

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

Cyberattack definition:

**Cyberassault (n)**

A cyberattack comes in many forms, and the goals vary too.

**Attackers’ goals may comprise attempts to:**

- steal critical data and intellectual property;
- force a victim to pay ransom to recover data that is encrypted by hackers;
- enable undermining of critical infrastructure such as electrical grids or uranium-enrichment.
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.”

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.

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.
Progress Against Cyber Threats

In the last several years, Washington has begun to grapple with challenges in cyberspace. Numerous experts call the moves necessary but not sufficient. Without bipartisan support, positive steps will not gain traction, they say.

Recent defense authorization bills have required testing of weapons and crisis response scenarios, assessments of threats and responses, greater reporting to Congress on cyber-operations. The National Defense Authorization Act now includes cyber among the major domains of warfare.

The changes “have to survive administrations,” says James Gosler of the Johns Hopkins University Applied Physics Laboratory, a longtime cyber adviser to the Pentagon.

"Otherwise, every four years or so, you have to start over again. And if we do that, we’re probably losing ground at a rapid pace,”

SELECTED MILESTONES:

2018:
* U.S. director of national intelligence lists cyber threats for the first time as the top threat in annual congressional testimony on worldwide security perils.

2017:
* Senate Armed Services Committee creates Subcommittee on Cybersecurity.
* Defense Science Board warns United States “will not be able to prevent large-scale and potentially catastrophic” computer attacks by China or Russia and urges creation of a cyber-resilient military within the military.

2018:
* May: U.S. Cyber Command, which had been part of U.S. Strategic Command, becomes the 10th U.S. stand-alone combatant command.
* August: President Donald Trump issues executive order loosening rules for authorizing offensive cyberattacks overseas.
* September: White House and Pentagon both complete cyber-strategies, and Pentagon follows up with weekly meetings

2019:
* March: Fiscal 2020 federal budget proposal calls for hike in cyber spending (quantify?). Grown by how much over how many years???
* March: Navy’s cybersecurity readiness review says United States “is losing” the cyberwar and has made a “national miscalculation” in not dealing seriously enough with the threat.
* May: Administration unveils order aimed at strengthening the federal cyber-workforce.

May: Lawmakers create bipartisan Cyberspace Solarium Commission to explore policy solutions.

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 some instances, 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 “adhoc,” 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 scath- 
ing assessments when necessary, says 
LaPlante, now a senior vice president 
at Mitre Corp., a federally funded re-
search 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 de-
fense authorization bill this month, it 
may consider an amendment by Kan-
sas Republican Jerry Moran and oth-
ers 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 Ser-
ces 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 be-
hind, and the government is especially hard-
pressed to compete with high-paying Silicon 
Valley firms.

**Leadership, Please**

The main reason cyber is a people prob-
lem is that the human beings who are gov-
ernment 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 
had to significantly increase their atten-
tion to the problem, even though many law-
makers contend that the administration has 
muddied 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 com-
mittees, cyber is essentially an afterthought 
compared to weapons hardware and mili-
tary pay and benefits. In the Senate Armed

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

- Michael Bayer, 
Pentagon adviser

Services press release last month on its fis-
cal 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, consider-
ably 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 de-
fense budget.

Total security is unobtainable. But a higher 
degree of confidence in the safety of U.S. sys-
tems (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 demon-
strate 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 communica-
tions 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 organiza-
tions and behaviors are also needed. For 
its part, the Pentagon needs chief infor-
mation officers who are no longer oper-
ators 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 de-
terred 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 Intelli-
gencc 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 spend-
ing,” Warner says.

The Pentagon also needs to step up invest-
ment in and use of advanced technologies 
such as artificial intelligence because they of-
fer 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 combatting 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.”
The Price of Naïveté

U.S. security will continue to be threatened if we don’t counter disinformation

By GOPAL RATNAM
Stanislav Levchenko, a KGB agent turned defector, told a Paris weekly in 1987 that the Kremlin had been successfully tricking the West for 70 years because Americans and Europeans tended to be naïve.

Soviet leaders capitalized on the “factor of elementary naïveté” among westerners and “have used it for many years,” to spread disinformation, Levchenko said, in an eerie preview of the tactics used by Russian agents who created fake social media accounts and spread disinformation during the 2016 election.

Levchenko described the Kremlin’s Cold War-era effort as a “large machine,” with as many as 15,000 people working full time in Moscow alone in the “sphere of disinformation.” But, he said, the number of gullible westerners was likely declining because many of Moscow’s tactics had been exposed.

“In the past two years a fairly large number of Soviet forgeries have been caught,” Levchenko told the Paris émigré weekly Russkaya Mysl, according to a State Department report sent to Congress that cites the interview. “It has been known to everyone that these were done by the Soviet service for document disinformation and this, of course, reflects badly on the prestige of the Soviet Union.”

It wasn’t just forged documents. Moscow ran a fake news campaign claiming that the United States created the AIDS virus as a form of biological warfare and convinced an Indian newsletter called Patriot to publish it. The KGB also spread false news that the United States had developed an “ethnic bomb” that would only kill people of certain races and ethnicities.

Long before the advent of social media, these deceptions and many others had been a staple of Russian disinformation efforts and were meticulously tracked and exposed during the 1980s by the little-known U.S. Active Measures Group, a multi-agency effort led by the State Department.

“The group exposed Soviet disinformation at little cost to the United States, but negated much of the effort mounted by the large Soviet bureaucracy that produced the multibillion-dollar Soviet disinformation effort,” according to a case study by Fletcher Schoen and Christopher J. Lamb published by the National Defense University in 2012. The sustained exposure of the Kremlin’s disinformation helped convince Soviet leader Mikhail Gorbachev “that such operations against the United States were counterproductive.”

It’s time to revive such tactics for exposing today’s disinformation campaigns not only by the Kremlin but copycat attempts by China, Iran and others, says John Lenczowski, who served as President Ronald Reagan’s principal adviser on Soviet affairs, and one of the key players in the Active Measures Group.

Given the role of social media in disseminating information, the group should involve government agencies and technology companies, says Lenczowski, the founder and president of the Institute for World Politics.

“How else do you fight against propaganda, disinformation and active measures?” Lenczowski asks. “You have to collect intelligence and expose it because a lot of this happens in the darkness and that’s how criminals like to operate.”

While Russia, China, Iran and others have strengthened their information warfare playbooks in recent decades, the United States instead has dismantled its machinery for combating disinformation, Lenczowski says.

For about 20 years starting in 1954, the CIA’s legendary counterintelligence chief James Angleton focused on Soviet deception and disinformation, and zealously tracked down Russian moles he believed were providing Moscow with feedback on its campaigns.

That focus dissipated when news reports revealed that the CIA had been spying on Americans on the orders of President Lyndon B. Johnson to monitor anti-Vietnam War protests, in violation of the agency’s charter. The resulting congressional investigations and intelligence agency reforms led then-CIA Director William Colby to force Angleton’s retirement.

The Active Measures Group helped engineer the Soviet collapse, but fell victim to its own success during the Iran-Contra scandal, which led several top National Security Council officials to leave the White House.

The United States downgraded key tools it used in the fight against the Soviet Union, including Voice of America and Radio Free Europe that the Soviet dissident and writer Alexander Solzhenitsyn once called the “most powerful weapons we possessed during the Cold War,” Lenczowski says.

“Guns and rockets are more likely to be funded according to strategic needs, but we never fund diplomacy or information policy according to national strategic needs,” he says. “There’s a pandemic ignorance of the strategic importance” of information strategy.
The current U.S. efforts at combating disinformation are still sporadic and anemic.

In 2011, the Obama administration created the Center for Strategic Counterterrorism at the State Department with the goal of using Facebook and Twitter to push back against Islamic State propaganda.

In 2016, the administration renamed it the Global Engagement Center and expanded its mission to include countering Russian, Chinese and Iranian disinformation campaigns.

But the center’s efforts have been hobbled by poor management.

Rex Tillerson, then the secretary of State, refused in 2017 to take $60 million in funds Congress had redirected to the center from the Pentagon’s budget, and reluctantly accepted about $40 million after lawmakers complained for months.

In early June, the State Department suspended funding for a group called the Iranian Disinformation Project that was supposed to be targeting the Iranian government but was also aiming its fire against American journalists for being too soft on Tehran.

Despite these feeble attempts, the United States “as a society and its policymakers view conflict in binary terms as hot or cold, war or peace terms,” says David Glancy, a professor of strategy at the Institute for World Politics and a former adviser to the Pentagon and the State Department.

“There’s a whole spectrum that goes between peace and war and a lot of our adversaries are engaged in that gray zone of conflict in a coordinated way,” Glancy says. “We are not very focused and are just waking up to it in light of the Russian actions in 2016.”

The United States has plenty of lessons to draw from on developing a coordinated approach, says Seth Jones, a senior adviser on international security at the Center for Strategic and International Studies who has advised military commanders in war zones.

The National Counterterrorism Center, established in the aftermath of the 9/11 attacks to share terror threat information and synchronize response, is an example of how a coordinated approach works, Jones says.

Another approach, Glancy says, could be an agency similar to the Office of the U.S. Trade Representative, an independent Cabinet entity with a small staff and officials drawn from different federal agencies to develop strategies not only to combat disinformation but apply other measures of U.S. power against adversaries that could be implemented across the government.

Unlike Russia, China and Iran, where the strategy flows from the country’s top leader, “there isn’t such a centralized approach in the United States,” Jones says. “We are very late to this game.”
Tech to Feds: ‘Be Cool’

Government cybersecurity teams can’t fill critical jobs without a new approach to recruiting

By PATRICK KELLEY
THE PENTAGON’S CYBERSECURITY
mission is facing a classic supply and demand problem: there’s a nationwide shortage of tech talent and an oversupply of jobs.

This leaves the Pentagon starved of the cyber-sentries needed to defend its digital networks as the nation’s top computer scientists and software engineers often choose careers in the private sector that offer fat salaries and generous benefits.

“They are so talented and in such high demand,” then-acting Defense Secretary Patrick Shanahan said of the Pentagon’s red team members, cybersecurity experts who test and defend Defense Department computer networks, at a Senate Defense Appropriations Subcommittee hearing in May. “We really get out-recruited.”

If there was ever a time the Pentagon would not want to lose the recruiting battle with the private sector, it’s now. The Chinese, Russians and Iranians have all hacked important aspects of American society since 2016. Moscow and Tehran targeted U.S. elections and Beijing has hacked U.S. defense contractors, highlighting the Pentagon’s need for cyber-defenders.

Offensively, the Pentagon will also increasingly need tech expertise. The military soon plans to integrate artificial intelligence technology into its weapons systems, an endeavor that would give war machines human abilities and rely on yet-to-be-implemented 5G wireless internet technology.

These tasks are monumental. Some of them may be done by entities on the Pentagon’s periphery, like defense contractors. Others, like those done by the red teams, must be carried out by the government.

Capitol Hill knows this, and is nudging the Defense Department to create a pipeline from top U.S. universities to the Pentagon.

But that pipeline will need to offer strong incentives to steer recruits with some of the highest-earning potential of all college students away from the private sector.

Many Opportunities
“Students have many choices these days,” Sally Luzader, manager of corporate relations at Purdue University’s Department of Computer Science, said in an email. “So the top candidates, especially, have the luxury of being very selective.”

Those graduates, sought by massive tech firms, startups and even Wall Street, often choose between multiple lucrative job offers at salary levels reserved for veteran government employees.

“It’s hard to beat the pay,” says Sibin Mohan, a computer science professor at the University of Illinois, whose 2018 computer engineering graduates — the talent the Pentagon struggles to recruit and retain — earned an average starting salary of $99,741. That salary level for 20-something computer nerd rivals the top level of what some government workers earn in the Washington metropolitan area.

The government pays its employees according to its “GS” salary table, a 15-tier pay scale with 10 different salaries at each grade. The average Illinois computer engineering graduate from 2018 earns $69 more per year than a GS-13 Step 1 employee in the Washington area, with the maximum amount a GS can make in the capital being $166,500 per year.

### Competitive Pay
The government struggles to compete for cyber and IT jobs.

<table>
<thead>
<tr>
<th>OCCUPATION</th>
<th>2018 MEDIAN PAY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer and information research scientist</td>
<td>$118,370</td>
</tr>
<tr>
<td>Computer network architect</td>
<td>$109,020</td>
</tr>
<tr>
<td>Software developer</td>
<td>$105,590</td>
</tr>
<tr>
<td>Information security analyst</td>
<td>$98,350</td>
</tr>
<tr>
<td>Database administrator</td>
<td>$90,070</td>
</tr>
<tr>
<td>Computer systems analyst</td>
<td>$88,740</td>
</tr>
<tr>
<td>Computer programmer</td>
<td>$84,280</td>
</tr>
<tr>
<td>Network and computer systems administrator</td>
<td>$82,050</td>
</tr>
<tr>
<td>Web developer</td>
<td>$69,430</td>
</tr>
<tr>
<td>Computer support specialist</td>
<td>$53,470</td>
</tr>
</tbody>
</table>

Source: Bureau of Labor Statistics
West Coast companies like Amazon, Microsoft and Uber are recruiting these students well before they graduate, and the local climate is part of the draw.

A lot of people want to live in California, “as opposed to say living in D.C.,” Mohan says.

But it is smaller tech firms that are escalating the bidding war.

“Startups are ready to pay extra money just to attract students away from some of these big names,” Mohan says.

And back on the East Coast, Wall Street quantitative trading firms are showering computer geniuses with cash to help shave lucrative nanoseconds off transaction times.

In recruiting tech talent, the government simply can’t outbid the private sector. Luckily for the Pentagon, some of the country’s brightest college graduates aren’t solely motivated by money.

“I know students who’ve had offers from the Wall Street firms, a decent amount of money, and turned it down because they were not excited about it,” Mohan says. “If the government agencies show them the cool work that can be done, then some students might be attracted to it.”

So-called “cool” work for recent grads could very well be their deciding factor between jobs. Those jobs could include the short-staffed red teams at the Pentagon and other cybersecurity roles across the government.

“Students often want to work on ‘cool’ projects,” Luzader says.

William Crumpler, a research assistant at the Center for Strategic and International Studies who has studied the federal cyber workforce gap, says government cyber programs need to “focus on the coolness factor.”

By this logic, the Pentagon would do well to shed its stiff, top-down image, which some veterans say is a myth.

“I’ve been lots of places that are not the military that were way more rigid than my experience both at the [U.S. Naval Academy] and onboard a submarine,” J.P. Mellor, a Naval Academy graduate and head of the computer science and software engineering program at the Rose Hulman Institute of Technology, says. “There was plenty of room [in the military] for my creativity.”

Mellor left the Navy decades ago, but sees ample room for innovation on the Pentagon’s red teams.

“That’s a super-creative activity,” Mellor says. “You have to try figure out what could go wrong here or how can I turn it on its head?”

Mohan agrees, saying working on teams tasked with testing network security — hacking, essentially — “becomes a bit of an art and not completely a science.”

More Savvy Needed

One reason — perhaps the main reason — the Pentagon has trouble filling these jobs is its sales pitch, or lack of one.

Mellor couldn’t recall the Defense Department recruiting on Rose-Hulman’s Terre Haute, Ind., campus, but said his students often intern and later start careers at the companies with structured internship programs that recruit the students in person.

A provision in the House version of the fiscal 2020 defense spending bill would direct the Pentagon to hire like private companies, saying the Pentagon should work with universities to recruit cyber-skilled students during their junior and senior years, giving them time to complete the requisite security clearance.

“That would totally do it,” Mellor says. “I think that’s a great strategy.”

But Mellor would advise the Pentagon not to wait until the students’ junior years.

Many Rose-Hulman students, like those at other universities, often start internships after their freshman year, return to school and spread the word about their apprenticeships, sometimes recruiting classmates to apply to the company where they worked.

The result is job security before graduation, with more than 90 percent of Rose-Hulman students accepting full-time job offers before their senior year final exams, Mellor says.

So for the military to win the future wars in ethereal digital conflict zones, they must first win on an equally competitive battlefield: the college career fair.
Old Habits, Old Gear

Reliance on 20th century weapons handicaps the military in the 21st

By ANDREW CLEVENGER

IF A WAR BROKE OUT tomorrow with China or Russia, the U.S. would enter the fray with an aged military — many of the ships, tanks and planes have been in service since the Cold War.

The reasons are numerous: the decades it often takes to develop new equipment, long periods of insufficient investment and a reluctance to abandon familiar weapons.

Two years into the Trump administration, the Pentagon’s budget decisions have not fully aligned with its rhetoric about retooling and boosting its military edge over China and Russia. And that raises questions about how the Pentagon is preparing for its next conflict.

“Does technology drive strategy or does strategy drive technology?” wonders Richard Aboulafia, vice president of analysis at Teal Group. “I’m not really convinced that we have a strategy that drives technology.”

American ingenuity helped produce two great technological advances that extended the United States’ run as the world’s pre-eminent military power, even as potential adversaries amassed larger armies and stores of conventional weapons.

The first was the development and deployment of tactical nuclear weapons, which helped counteract the Soviet Union advantage in conventional forces that threatened to overrun Eastern Europe. The second was the maturity of U.S. surveillance and reconnaissance capabilities, coupled with new stealth technology and precision-guided weapons that could strike targets with relative impunity.

For Elbridge Colby, who served as deputy assistant Defense secretary for strategy and force development early in the Trump administration, the 1970s and ‘80s offer a useful model of success.

That second major advance “is considered the gold standard for successfully dealing with great power competition,” says Colby, who now directs the defense program at the Center for a New American Security.

A self-described optimist who spearheaded the Pentagon’s National Defense Strategy in 2018, Colby believes the U.S. is better positioned to maintain its warfighting edge now than it was in the 1970s.

“We’re not going to be able to march on Beijing, but that’s not what we’re thinking about,” says Colby. “We’re thinking about how we help Taiwan defend itself.”

If that’s the case, some ask, why put priorities on making incremental advances to last century’s military, like a new armed scout helicopter?

“Are you really going to do an air assault into Shanghai?” asks Byron Callan, an analyst with Capital Alpha Partners.

Part of the Pentagon’s reliance on older systems comes from practical necessity. To paraphrase former Defense Secretary Donald Rumsfeld, you go to war with the equipment you have, not the equipment you would like to have.

Another hurdle: defense contractors shrewdly spread the work of developing, manufacturing and assembling major weapons programs across multiple states and districts, making it less palatable for Congress to pull the plug on older programs and risk losing those jobs.

“Inevitably, you’re going to have the congressional support come down on the side of existing platforms and associated jobs rather than the side of a handful of engineers working on transformational technology,” Aboulafia says.

Army Undersecretary Ryan McCarthy, who is responsible for devising a more modern approach, acknowledges that these forces can be hard to overcome.

“It’s very difficult to step away from legacy systems,” he says. “There’s obviously the congressional interest, but also institutionally, these are systems that many of the officers and noncommissioned officers have grown up on. They’re comfortable with them. They’ve fought with them in combat.”
To convince decision-makers in the Pentagon and Congress to approve a new concept, he says, “you have to be relentless in explaining in why you’re doing it, and you need to be really ruthless with the prioritization of those requirements.”

The Pentagon’s budgets do contain crucial seed money for new technologies like hypersonic missiles and artificial intelligence. The plans also contain massive investments in a new stealth bomber, the next generation of aircraft carrier and ballistic missile submarines, and updates to Bradley Fighting Vehicles and Stryker combat vehicles.

Dov Zakheim, who served as the Pentagon’s comptroller during the George W. Bush administration, notes that House appropriators cut back fiscal 2020 funds in several critical areas, including artificial intelligence, and the Defense Innovation Unit, the Pentagon’s outreach effort to Silicon Valley.

“There are the kind of things you need if you are thinking ahead instead of looking backward. It’s an indication of very, very short-term perspective,” he says. “As long as appropriators focus so heavily on the upcoming year, they tend not to have a strategic view.”

It’s an uphill push to overcome the risk-averse culture on the Hill and in the Pentagon, he says, but Congress needs to take the lead in demanding a coherent approach.

Zakheim notes that the Pentagon has pushed for 21st century warfare technology, such as systems for cyberspace conflicts, which go beyond shooting wars.

“The question then is, when does Congress really take charge and move ahead?” he asks.

CNAS’ Colby agrees that Congress could force the issue.

“My hope is that it will become increasingly embarrassing for Congress to do logrolling in defense rather than supporting and demanding strategically sound policy and programming,” he says.

But the Pentagon is falling well short of full-throated support for that approach, Callan notes. As appropriators angle to cut funds for forward-looking technologies, the Defense Department has barely pushed back.

“Where’s the hue and cry about, ‘No! No! No! These are priorities!’” Callan says.

Some key lawmakers want more details about how the Pentagon intends to use new tech for national security. House Armed Services Chairman Adam Smith says he wants to see strategic plans before he can wholeheartedly embrace the Pentagon’s approach.

“What are they hoping to use these technologies for, how do they help them accomplish their goals, what’s the application of the technology, instead of just saying, ‘Hey, this would be neat,’” the Washington Democrat said at the Center for Strategic and International Studies June 10. “My overall concern is that we are embracing more projects than we’re ultimately going to have money to fund.”

ANCIENT WARRIOR:
A B-52 bomber flies over Osan Air Base in Pyeongtaek, South Korea.