Defense One

CYBER

in the Era of Great Power Competition

November 2019

Time for a Zero Trust Check Up

Measure Your Cybersecurity Maturity with Okta's Zero Trust Identity Assessment Tool

Get your Zero Trust prescription

https://www.okta.com/zero-trust-whats-your-risk/ GO

The rise of cloud and mobile have served as a catalyst to rethink how organizations approach cybersecurity today. Today, people are the perimeter, and organizations need to ensure **the right people have access** to the right resources, and no more.

Organizations across all industries must adapt to this modern security landscape by employing the Zero Trust principle to "never trust, always verify". For that to work, identity has to be the foundation of any Zero Trust framework. **Do you know how your Zero Trust health measures up?** We do.

With our free **Zero Trust Identity Assessment Tool**, you can check where your organization succeeds and what it can do to improve on the path to enabling Zero Trust security. Regardless of where you are on your Zero Trust journey, **Okta has the right remedies to help you adapt to the ever-changing threat landscape and protect your organization.**

okta

Contents

Cover image / ISTOCK | KURMYSHOV

Foreword

Great power competition is both physical and digital, as much focused on innovation in information technology as the size of navies and the number of tanks.

The United States has long enjoyed supremacy in every warfare domain: on land, sea, air, and space. But the new domain of cyber is the one where the U.S. lead could erode the fastest. The barriers to entry are cheap and the rules for the use of new tools and weapons are few and difficult to enforce. Moreover, information technology now touches everything in modern life. So the digital battles of the future will play out in the robotic weapons and vehicles of the future as well as across the phones and internet-connected devices of individuals and businesses around the world. With very little cost, it's possible to have a huge and disturbing impact on a given nations physical and economic security.

With its allies, the United States is working to sustain and build on its current technological prowess in the cyber domain. Here's a look at the latest advances in that competition and a foreshadowing of where that contest is going next.

Patrick Tucker
Technology Editor
Defense One

NATO Getting More Aggressive on Offensive Cyber

By Patrick Tucker

NATO's Secretary General Jen Stoltenberg, right, with Secretary of State Mike Pompeo, left, at the Meeting of the North Atlantic Council in Foreign Ministers' Session 2 at the U.S. State Department in Washington, Thursday, April 4, 2019. AP PHOTO/PABLO MARTINEZ MONSIVAIS

Secretary General Stoltenberg says NATO pushes limits of what the alliance can do in cyberspace.

In the latest signal NATO is adopting a tougher posture against cyber and electronic attacks, Secretary General Jens Stoltenberg this week said that the defensive alliance will not remain purely defensive.

Stoltenberg told attendees at the Cyber Defence Pledge conference in London, "We are not limited to respond in cyberspace when we are attacked in cyberspace."

NATO members have already "agreed to integrate national cyber capabilities or offensive cyber into Alliance operations and missions," he said. But the parameters of a NATO response to cyber attacks remains undefined. In 2015, Stoltenberg said that a cyber attack against one member nation could trigger an Article 5 collective response by all members. Yet only once has a collective response ever been invoked, at the request of the United States following the attacks of September 11, 2001. NATO is a defensive organization, so what an offensive cyber posture looks like remains something of a mystery. An Article 5 response can take many different forms.

That's the strength of the article, according to NATO Deputy General Secretary Rose Gottemoeller. However, while an Article 5 response can be unpredictable, it must be coordinated, which can be tricky with many different partners in possession of many different capabilities.

At an event in May, Gottemoeller said NATO was in the processes of establishing a new innovation board to "bring together all of the parts of and pieces of NATO that have to wrestle with these new technologies to really try to get a flow of information. Many of you having served in any international institution or government, you know how things can get stove-piped. So we are resolved to break down those stove-pipes, particularly where

innovation is concerned," she said.

NATO is building a cyber command that is scheduled to be fully operational in 2023 and will coordinate and conduct all offensive cyber operations. Until then, whatever NATO does offensively, it will rely heavily on the United States and the discretion of U.S. commanders, according to Sophie Arts, program coordinator for security and defense at the German Marshall Fund, who explains in this December report.

"Yesterday's remarks indicate that NATO's leadership is thinking more seriously about buttressing the alliance's deterrence posture in cyberspace and address threats that fall under the threshold of an Article 5 violation," she told *Defense One*.

"This tracks recent shifts in strategy adopted by several NATO allies, including the United States, which integrate offensive cyber operations as an important tool to proactively address growing instances of cyber interference from hostile actors."

But Arts points out there is no field manual for coordinating cyber offensive operations among individual allies, including big players in cyber like Estonia, the U.K. and the United States, who keep command and control over their assets.

In 2017, Gregory Edwards, then director of infrastructure services at NATO's communication and information agency laid out what that might look like. "You could make a case-by-case decision" about responding to attacks, he said. "You need to have a policy that says, 'if our operation is disturbed, we will take a specific action.' The action will be listed. It will be listed what things the commander is allowed to do in that regard. It will be a specific action."

At an April meeting of NATO policy planners in Washington D.C., Kiron Kanina Skinner, director of Policy Planning at the U.S. State Department said that NATO policy planners had spent most of their time during the meeting discussing how to coordinate cyber effects and policy.

The issue was competing against traditional NATO concerns and even topics like the Russian military buildup on the border of Eastern Europe. "Today, we didn't talk about the Eastern flank; we talked about cybersecurity," she said. D

Russia Will Test Its Ability to Disconnect from the Internet

By Patrick Tucker

Demonstrators shout during the Free Internet rally in response to a bill making its way through parliament calling for all internet traffic to be routed through servers in Russia — making VPNs ineffective, March 10, Moscow. AP PHOTO/ALEXANDER ZEMLIANICHENKO

The nascent RuNet is meant to allow the country to survive an attack — and Putin to monitor and control the population.

Russia will test its internal RuNet network to see whether the country can function without the global internet, the Russian government announced Monday. The tests will begin after Nov. 1, recur at least annually, and possibly more frequently. It's the latest move in a series of technical and policy steps intended to allow the Russian government to cut its citizens off from the rest of the world.

"On Monday, the government approved the provision on conducting exercises to ensure the stable, safe and holistic functioning of the Internet and public communications networks in the Russian Federation," notes an article in D-Russia. (The original article is in Russian. We verified a translation with the help of a native Russian speaker.) "The exercises are held at the federal (in the territory of the Russian Federation) and regional (in the territory of one or more constituent entities of the Russian Federation) levels."

The word "holistic" shows that the exercises follow April's passage of the sovereign internet law that will require all internet traffic in Russia to pass through official chokepoints, allowing the government to shut down outside access, block websites that they don't like, and monitor traffic.

In 2016, Russia launched the Closed Data Transfer Segment: basically, a big military intranet for classified data, similar to the Pentagon's Joint Worldwide Intelligence Communications System. The following year, Russia announced that it intends to build its own domain name directory, which would allow it to re-route traffic intended for one website to another. And last year, Putin's top IT advisor Herman Klimenko and others suggested that the military intranet, properly expanded, might be able to carry the rest of the country's internet traffic.

Klimenko cautioned that moving to the new system would be painful — and as recently as March, Gen. Paul Nakasone, director of U.S. Cyber Command and the NSA, expressed skepticism that Russia would succeed.

Samuel Bendett, an adviser at the CNA Corporation and a fellow in Russia studies at the American Foreign Policy Council, said the announcement shows that the Russian government is eager to address what it sees as a strategic vulnerability: reliance on Western IT. "The larger context is Russia's dependence as a nation on imported/foreign hi-tech and the perceived vulnerabilities that Russia sees in such technology use. With so many government, public, and private-sector nodes using such foreign tech, the Russian government is seeking to impose a measure of control over how Internet communication over this technology is conducted," Bendett said. "In the event of what the government sees as outside influence affecting RuNet, the state can act — hence the annual exercise."

RuNet isn't expected to improve the online experience for Russian people or companies. It's all about control, making the country more technologically independent, and reducing the Putin regime's vulnerability to popular uprising.

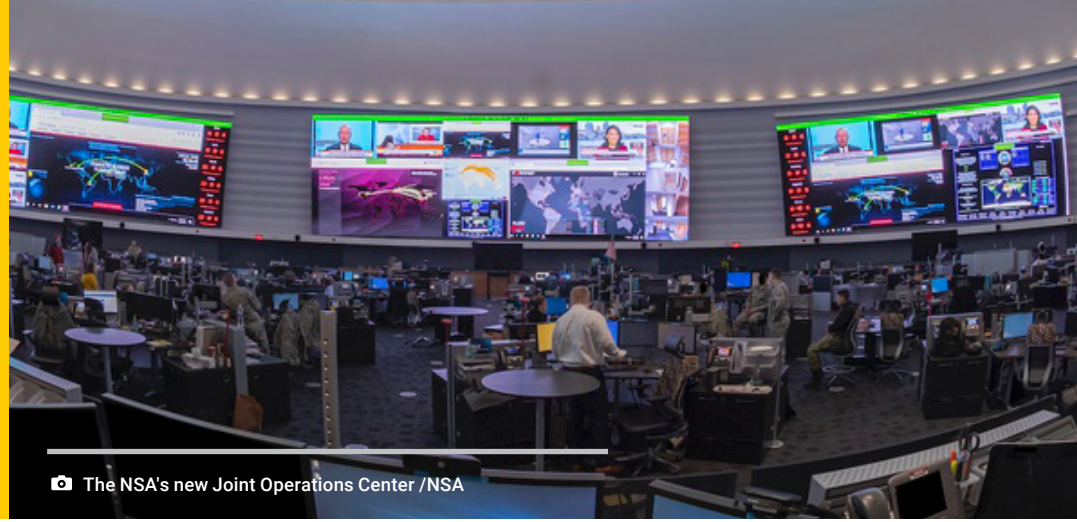
"The Russian government, particularly since seeing the role social media played in the Arab Spring, has wanted over the last decade to exert tight control over the online information space within Russia's borders," said Justin Sherman, a cybersecurity policy fellow at New America who studies internet governance and digital authoritarianism. "Free information flows are a threat to regime stability, and they need to be controlled, the narrative goes."

As the Russian government has built infrastructure that can disconnect Russia from the global internet, it has also worked to limit Russian citizens' access to sites and services that allow citizens to mobilize and protest. Access to services such as LinkedIn, Zello, and Telegram is limited by a 2006 Russian law (27.07.2006 number 149-FZ) that requires foreign companies to open their software to Russian security services and to hand user data to law enforcement agencies. Sherman said the passage of the sovereign internet law is one more item in this trend.

"When Russia passed its domestic internet bill into law, it wasn't clear how much the government would actually work to make it happen, but now it's clear they do intend to modify systems so the internet within Russian borders can be cut off from the global net at will," Sherman said. "These disconnection tests which Russia has planned for the near future—as well as, according to documents, annually going forward—are steps in the direction of making this so-called RuNet work. They also line up with a series of international pushes by authoritarian governments to make 'cyber sovereignty' of this kind more palatable to the global community." D

The NSA Wants To Help Design Safer Tech Products. Do You Trust Them?

By Patrick Tucker



The NSA's new Joint Operations Center /NSA

The leader of the agency's new public-facing group says she's all white hat.

The U.S. military's codemaking agency says it wants to help the tech industry make its products more secure, and better able to use emerging technologies like 5G networking. But the National Security Agency is also the military's codebreaking agency. Can it win over Silicon Valley types long suspicious of its help?

NSA aims to do this outreach with a new Standards and Futures group, part of the public-facing Cybersecurity Directorate that is set to reach full operational capability in January.

On Thursday, NSA officials took the highly unusual step of inviting more than a dozen reporters to their new Integrated Cyber Center. It's built around the Joint Operations Center, a giant room resembling the fictional NORAD command center in the movie *War Games*. Three 47-by-20-foot screens tower over the agency operators below, displaying real-time data about U.S. operations and threats. Some 200 NSA and U.S. Cyber Commander operators will handle cyberdefense and foreign-intelligence collection, and coordinate with representatives of the Department of Homeland Security and other U.S. agencies.

NSA officials said having a big space to collaborate would help coordinate U.S. operations and responses to cyber incidents.

But the new Futures and Standards group will be less focused on the tactical back and forth of cyber defense and offense and more on predicting and spotting bugs and vulnerabilities in commercial products — and even helping businesses and consumers use good products safely.

To do that, the agency will have to overcome the false perception that it would rather hold onto vulnerabilities for its own use than disclose them to manufacturers for fixing. Agency leaders say that they need to speak out more — a rather big culture change at the "No Such Agency" — to rebut that notion, get bugs fixed, and keep the public safe.

Anne Neuberger, the director of the new Directorate, said that the NSA now believes its mission includes

spreading the word about small problems before they become huge ones. “Our role is taking the insights we have…whether it’s 5G, whether it’s quantum system crypto, whether it’s distributed ledger, and trying to work to ensure those products are built more secure. And we give advice to users who need different levels of security.”

"A big part of standing up a separate cybersecurity directorate was to convey the message that NSA has long had two missions: our cybersecurity mission and our foreign intelligence mission."

Anne Neuberger
Director, Cybersecurity Directorate, NSA

Neal Ziring, the directorate’s technical director, said the new group aims to inoculate the public by reaching out to the tech industry before bad products gain wide adoption. “Futures and Standards is going to look out a little ahead of today’s threats…look what’s coming down the pike, what sort of risks [a new technology or architecture] might engender, what sort of security improvements might be made to it, and then work with entities that might help effect those changes, usually industry, but sometimes standards bodies, to try and make sure that some of those security improvements are in there before that technology becomes widespread.”

Ziring said the NSA would offer recommendations to help businesses use some products and emerging technologies as safely as possible.

Chinese-produced 5G telecom equipment has become an issue of disagreement between the U.S. and some in Europe. But many institutions, businesses, some governments have quietly acquiesced to the fact that Chinese 5G equipment from makers like Huawei, will be in a lot of places in the future, despite the fact that Huawei’s products are highly vulnerable to attack from Chinese intelligence services (among other actors.)

Europe, which has declined to ban Huawei products, is moving toward a method of what might be called quarantined architectures. As senior vice president at the Center for Strategic and International Studies James Lewis explained in April, “They don’t let Huawei near their sensitive intelligence facilities, their sensitive military facilities.”

Ziring said the new group would look at Huawei and other 5G equipment, asking, “How can it be used most safely? When can it be used for national security purposes and when might it not be so suitable? Understanding that stuff takes time. And experimentation…And collaboration with the folks who are developing or deploying the

technologies, that's where our Futures and Standards" group will come in.

Of course, the NSA still has a longstanding mission of breaking into and spying on computers, phones, and networks. Should device makers, network administrators, and userstrust NSA to for advice on setting up a 5G network? The answer from Neuberger is: Yes. Really.

She says her directorate will speak out only "in the white-hat mission," meaning to help friendly organizations stiffen their defenses. "Those who break things know best how to secure them."

She said the Cybersecurity Directorate will run entirely separately from, say, the Tailored Access Operations office.

"A big part of standing up a separate cybersecurity directorate was to convey the message that NSA has long had two missions: our cybersecurity mission and our foreign intelligence mission. I think that, in the past, when the Information Assurance Directorate came [into being], I don't think that there was ever a question that that was a pure 'white-hat mission,'" she said.

What's changed? The widespread adoption of IT and other new technologies have made the U.S. more vulnerable. "There are two lessons that our defensive mission needs to learn. One is they [adversaries] will take the easiest way in. And, if they are given national security intelligence leads, it's their mission to achieve those," she said. "We have some critical government networks, critical military networks, where a foreign adversary has been given direction to get and gain access and we want to ensure that the security advice that we're giving is as sophisticated and as persistent as those kind of actors."

That says a lot about how the NSA has changed, at least in terms of public outreach, since the days of Edward Snowden. But it also says something about how cybersecurity has evolved.

The NSA has recently become more public in how it handles its foreign intelligence collection mission and the way it uses cyber effects to disrupt malicious behavior out of places like Russia. They've discussed how the NSA's Russia Small Group intervened against Russian cyber efforts to disrupt the 2018 election and how the Cyber Command infiltrated ISIS communication networks to help bring about the terror group's territorial loss. They've also been more public on their defensive mission and have shifted to offering more detail and context in the official NSA communications about threats.

In the future, there may well be some friction between the team that breaks things and the one that fixes. But right now, everyone is in the same room, watching the same threatening reality play out on the 47-foot screens. D

The US Army Is Struggling to Staff Its Cyber Units: GAO

By Jack Corrigan

Members of the Illinois National Guard practice digital forensic skillsets during a Cyber Shield 19 training week class at Camp Atterbury, Ind. April 7, 2019. U.S. ARMY NATIONAL GUARD / STAFF SGT. GEORGE B. DAVIS

Congress' watchdog concluded that the Army launched its new cyber units before trying to determine whether the concept is affordable, supportable, and sustainable.

The U.S. Army is struggling to staff, train, and equip its new cyber and electronic warfare units, and officials haven't assessed how those challenges will affect the Pentagon's digital capabilities, according to a congressional watchdog.

In recent years, the Army has been rapidly expanding its cyber capabilities to stay ahead of the growing digital threats posed by adversaries like Russia and China, but the Government Accountability Office found the service is having a tough time keeping up with its ambitious plans. The Army activated two digital warfare units last year despite personnel shortages, auditors said, and officials are struggling to update the equipment and doctrine used to train soldiers.

Furthermore, the Army hasn't conducted thorough risk assessments for its new units, which could make it harder for top brass to keep the forces running at full capacity in the long term, GAO said in a report published Thursday.

While Army officials said the digital threats posed by Russia and other adversaries justify the accelerated deployment process, auditors said the hasty plan could leave the Army "fielding units that are not capable of providing the needed capabilities."

Army officials told GAO they're struggling to recruit personnel to fill their new cyber units, particularly for high-level positions. Last year, officials stood up two cyber units with numerous vacancies—one unit had only 55% of its posts filled as of March, while the other was operating with less than 20% of its required personnel. According to auditors, the Army is considering increasing pay and offering retention bonuses to make the positions more attractive.

The accelerated activation process has also left the Army scrambling to equip its cyber forces, auditors said. The problem is even more prevalent in the Army Cyber School because officials are diverting resources away from trainees toward its operational units.

"If the Army does not acquire new equipment quickly enough, the result could be that soldiers in the Army Cyber School will be trained on outdated equipment, which they will not use when they get to the

field," GAO said. And because the Army is still finalizing its doctrine for cyber units, instructors said they may soon have "difficulty designing training for the new units, and soldiers will not have a clear understanding of their tasks and missions."

Army officials are also required to conduct a risk assessment whenever they activate a new unit, but GAO found the branch hasn't completed those evaluations for its new cyber squads. Such assessments inform the Army's future readiness planning, and without them, "leaders may be left with an incomplete picture of the challenges in affording, supporting, and sustaining these units over the long term," auditors said.

GAO recommended the Army complete risk assessments for the two cyber units it activated last year—the Intelligence, Cyber, Electronic Warfare, and Space unit and the 915th Cyber Warfare Support Battalion—and examine the risk of its accelerated activation strategy. D

US Air Force to Shift Billions of Dollars to Network Its Weapons

By Marcus Weisgerber

Gen. David Goldfein, the U.S. Air Force chief of staff, speaks at the Air Force Association's Air, Space, Cyber conference. WAYNE CLARK/USAF

The clock is ticking on Gen. David Goldfein's signature project.

Wait till next year! The Brooklyn Dodgers' classic rallying cry might well belong to the U.S. Air Force these days.

Last year, service leaders showed up to the annual Air, Space & Cyber conference near Washington with a big message: they need 386 squadrons — one-quarter more than currently funded — to fight and win wars against China and Russia, as prescribed in the National Defense Strategy. Asked for details — How many planes? What kinds of planes? — the leaders responded: wait till next year.

Now it's next year, and the Air Force Association's giant conference is once again underway. So about those answers? Service officials say they're coming — yes — next year, in the Pentagon's 2021 budget proposal to Congress.

But for Gen. David Goldfein, there is no next year, at least not as the Air Force chief of staff. Now in the last of four as the top Air Force general, Goldfein is hustling to cement his legacy. Speaking at the conference, he promised "radical changes" in coming years.

The Air Force is talking about creating a new battle network, fielding a new series of fighter jets every five years, and modifying existing weapons to make them more lethal and survivable. Goldfein also said the 2021 budget would contain "significant investment" in weapons that can strike heavily defended enemy targets.

Much of the money will be redirected from existing projects — echoing the Army's year-old "night court" effort that is shifting $25 billion over five years into higher-priority programs. At the conference, Acting Air Force Secretary Matt Donovan said his service was planning to shift tens of billions of dollars as well — in the same "ballpark" as the Army.

The Air Force calls its "night court" a "zero-based review." It was used for the 2019 and 2020 budgets and now again for the 2021 budget plan, which is typically sent to Congress in February.

"We wire-brushed every program in the United States Air Force and we graded that against the National Defense Strategy," Goldfein said in a Tuesday speech. "As a result, you're going to see some of the largest movement of resources" in the 2021 budget "in probably the last two to three decades."

That money, Goldfein said, will build "the Air Force we need to do multi-domain operations."

The general called the 2020 budget, which Congress still hasn't approved, "the first budget which has complete National Defense Strategy alignment."

Throughout his tenure as the Air Force's 21st chief of staff, Goldfein's top priority has remained the same: pushing his service to ensure that all of its weapons can connect with each other, and with those of the Army, Navy, Marine Corps and allies. He calls the concept multi-domain operations.

"This is going to be as hard for us culturally as it is technically to shift from a platform-centric orientation that we all grew up with to a network-centric orientation," Goldfein said. "The question for us is: Can we look beyond the devices? Can we look beyond the trucks? Can we look beyond the platforms and actually focus on the highway we need to build for the future?"

He'll need the support of lawmakers who tend to fund hardware projects — and constituents' employers — before software and networking visions. And he seems to have made a good start: many lawmakers and staffers have expressed support for the initiative.

Explained Goldfein: "I've not yet met a highway-man who is on the Hill lobbying, but I sure have met a lot of truckers."

Right now, the Air Force is trying to figure out how to build that highway.

"This is the challenge I face: I don't know how to make through contract what I'm asking for truly profitable, which will then drive the incentives for industry to move out on what I'm asking [for] because the big money is actually in proprietary data, ... [and] long-term sustainment contracts," he said. "The big money is for us to buy weapon systems at a lethargic rate over long periods of time and the adversary and the threat is not going to allow us to stay in that environment.

"If we can figure out how to make this profitable, it will take off"

Gen. David Goldfein
Chief of Staff, United States Air Force

"If we can figure out how to make this profitable, it will take off," he added.

Goldfein believes he is making decisions that will shape the Air Force a decade from now.

"I spent a lot of time thinking about Chief 24," he said. "Chief 24 is going to go to war in 2030 with the force that Goldfein built."

But the clock is ticking. Goldfein's term ends in July, and for the 21st chief of staff, there is no next year. D

Weapons Makers Unveil A Herd of Robotanks — As the Army Worries about Battlefield Bandwidth

By Patrick Tucker

Ripsaw, a 10-ton, 20-foot electrically-powered treaded minitank, on display at AUSA /PATRICK TUCKER

The U.S. Army is determined to field a mid-sized combat robot vehicle, but the prototypes are outstripping the datalinks that would connect them.

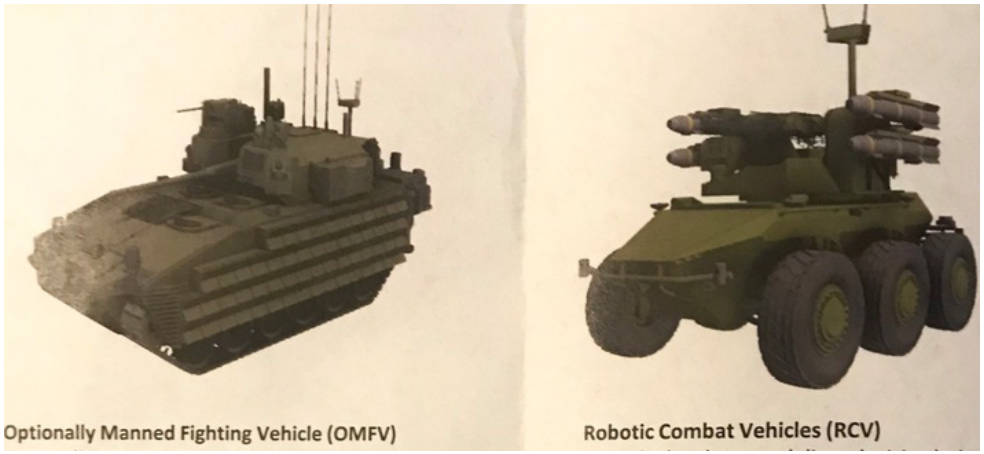
The show floor of the country's biggest land-warfare convention was crowded with robot tanks this week, roughly two years after the U.S. Army's declaration that its core 5-year priorities include a new combat vehicle. Among them, and with the greatest fanfare, Textron unveiled its Ripsaw, a 10-ton, 20-foot electrically-powered treaded minitank that can carry a small aerial drone on its back and can pop a smaller ground robot out of a front compartment. But companies from South Korea and Germany brought their own robo-battle machines to flaunt. Army leaders say that they've also been experimenting with battle concepts that combine soldiers, unmanned tanks, and small UAVs.

They're also worried about getting all of those systems to link up and share massive amounts of data.

"The thing that keeps me up at night — well, nothing keeps me up at night, but the thing I think about often is the network," Gen. John "Mike" Murray, the commanding general of the Army Futures Command, told reporters on Monday. "It's not problems within the network, it's that we're relying on the network for so much"

Jeff Langhout, who runs the Army Combat Capabilities Development Command's Ground Vehicles Systems Center, said that the Army recently ran an experiment in which two Bradley Fighting Vehicles were outfitted to command four roboticized M113 armored personnel carriers. While these are experiments show how far the Army and technology has come, he, too, has real worries about the network.

"There are some huge autonomy challenges," Langhout said, "but I still think one of the greatest challenges we're going to have is the network. On the



An illustration from a U.S. Army document showing a robotic combat vehicle.

ground, when you have robots wanting to talk to other robots, wanting to talk to ground vehicles and you go behind the hill, you go behind the rock, you go down in the gully; you're in a city and you go around the corner of the building… Hey, we're right here in Washington, D.C., how well does your cell phone work 100 percent of the time?" he asked.

The Army has had bad luck trying to institute large-scale data standards. Case in point: the Joint Tactical Radio System program spent $6 billion in a fruitless attempt to buy a single radio to serve all of its communications needs. In 2013, the U.S. military mandated the Commercial Mobile Device (CMD) Implementation Plan — essentially an effort to lower its data-transfer costs by using commercial networks for unclassified data. But as the current debate over 5G networking shows, even commercial cellular providers are having trouble getting ahead of what they see as future demand.

"This is commercial technology that everyone uses and relies on and so we are trying to take some of that and pass full-motion video in some cases. This is a big technological challenge and everyone is going to say, 'I've got a radio that will do it.' Fine, as long you're 100 feet apart and can see each other. So that's going to continue to be our biggest challenge because we just haven't fixed the physics yet," Langhout said.

Beyond its quest for semi-autonomous ground robots, the Army is looking into more and more data-intensive gear, such as the Integrated Visual Augmentation System, or IVAS, a set of augmented-reality goggles intended to give soldiers a lot of visual real time data to help with tasks like targeting during operations, and also with training and simulation during downtime. That's also supposed to hook up with data feeds from tanks or other robots. But the rush to develop and field the newest tech concepts, and to integrate heavy amounts of data into all facets of operation, have driven the Army's data needs skyward.

"Sensor to shooter? It's the network. The synthetic training environment? It's the network. IVAS is the network. If there's one thing that's cross cutting everything we're working on, it's the network," said Murray. "The bandwidth requirements, the latency we can't have, there's a lot of technical hurdles to overcome with that."

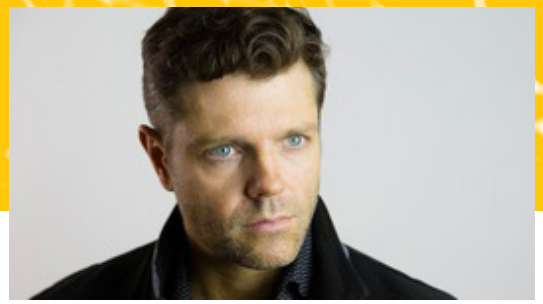
In a call with reporters, Textron officials said the Ripshaw's open architecture would allow the Army to upgrade its communications and data networking as needed, as well as to incorporate higher levels of autonomy, as those capabilities emerged. They said that they had experimented with integrating ground and aerial robots with the Ripsaw, but not yet in a communications-denied environment, in part because the Army has not yet published their specific needs for future mid-sized robot combat vehicles.

Brig. Gen. Richard Coffman, director of the Army's Next-Generation Combat Vehicle cross-functional team,

said that robots may help extend solid data connectivity further afield, serving as flying or rolling cellular towers in a moving mesh network. “We’re also looking at unmanned vehicles to expand the network, to expand the line of sight so we can push these robots out as far as possible. So that they get in the riskiest places on earth and the soldier,” Coffman said.

In the meantime, the Army will work with the network it has until more capability comes online at a price it can afford. Said Murray, “You can’t just walk away from what you had because we invested a lot of money into the network. And so thickening, augmenting, improving the network with commercial solutions, and in two-year increments so you can capture the very best technology you possibly can.”

About the Authors



Patrick Tucker

Patrick Tucker is technology editor for Defense One. He's also the author of *The Naked Future: What Happens in a World That Anticipates Your Every Move?* (Current, 2014). Previously, Tucker was deputy editor for *The Futurist* for nine years. Tucker has written about emerging technology in *Slate, The Sun, MIT Technology Review, Wilson Quarterly, The American Legion Magazine, BBC News Magazine, Utne Reader*, and elsewhere.

Jack Corrigan

Jack Corrigan reports on cyber and national security issues. Before joining *Nextgov* in 2017, he wrote for multiple publications around his hometown of Chicago. Jack graduated from Northwestern University with degrees in journalism and economics.

Marcus Weisgerber

Marcus Weisgerber is the global business editor for *Defense One*, where he writes about the intersection of business and national security. He has been covering defense and national security issues for more than a decade, previously as Pentagon correspondent for *Defense News* and chief editor of *Inside the Air Force*. He has reported from Afghanistan, the Middle East, Europe, and Asia, and often travels with the defense secretary and other senior military officials.