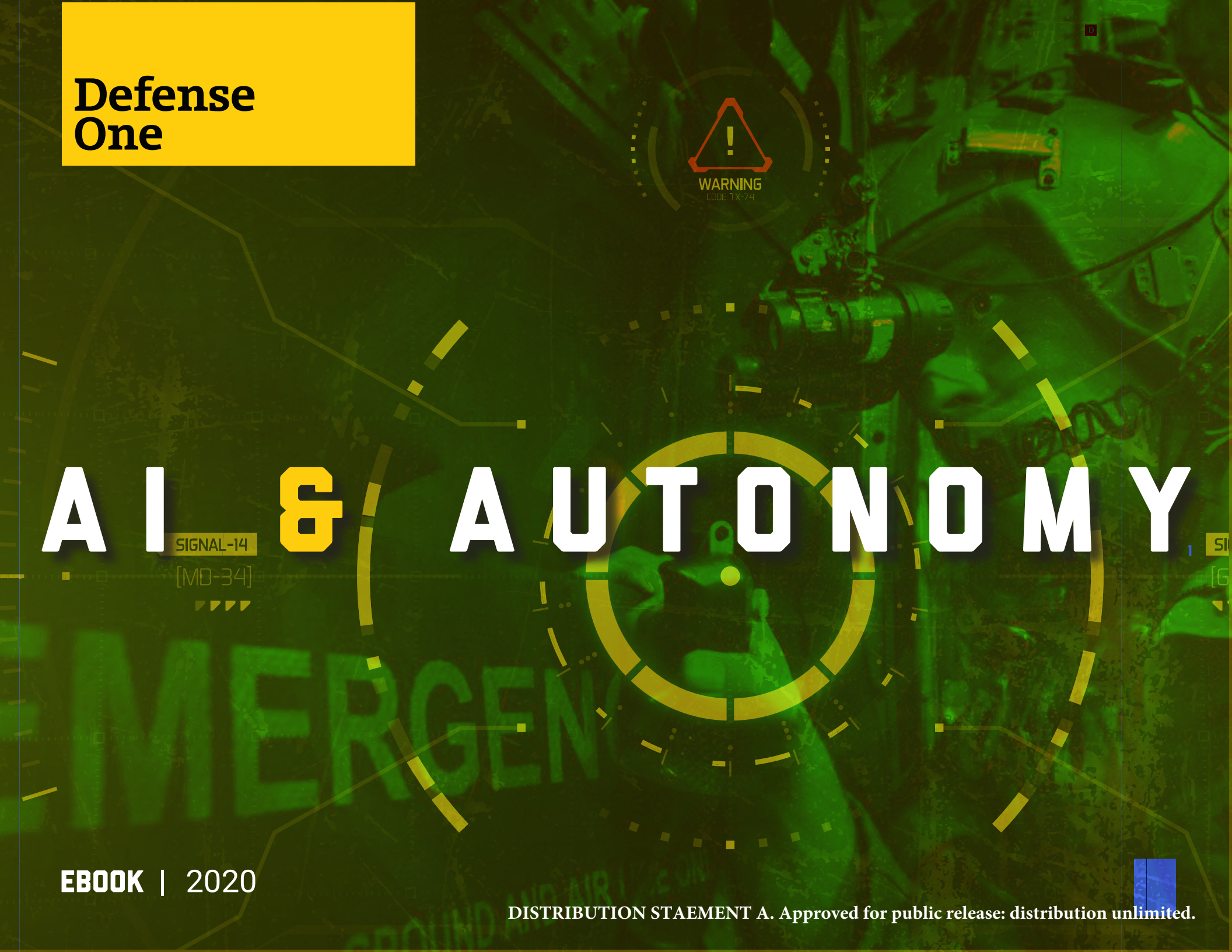
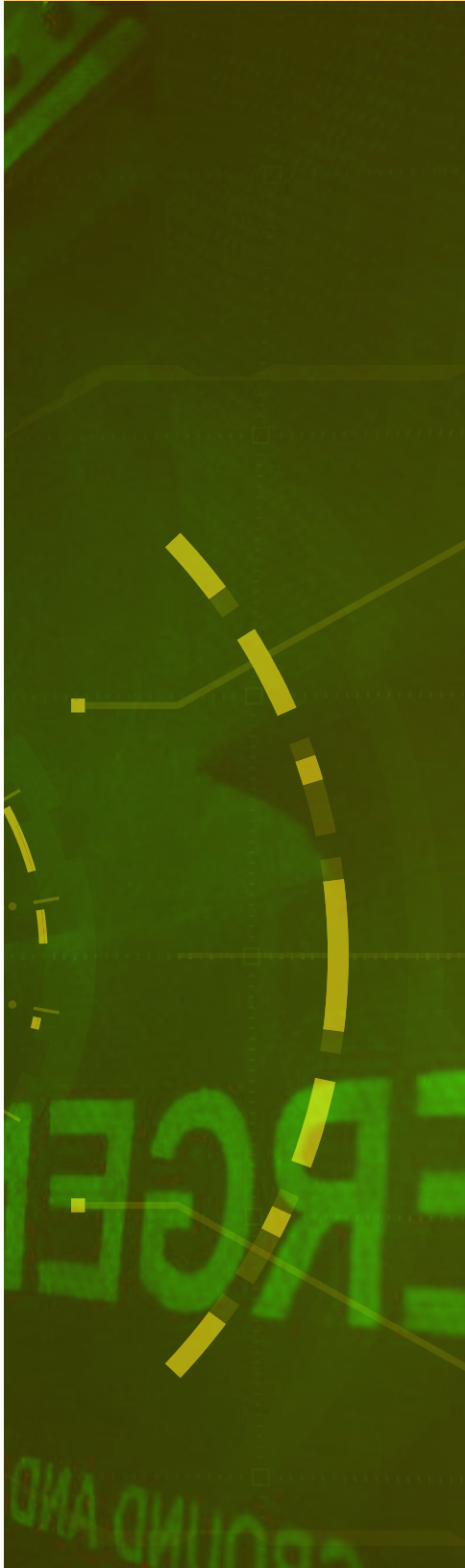
Defense One



AI & AUTONOMY

EBOOK | 2020

TABLE OF CONTENTS



CHAPTER 1

IN A POST-COVID WORLD, WE NEED AI MORE THAN EVER

ARTIFICIAL INTELLIGENCE TOOLS PROMISE, AMONG OTHER THINGS, TO MAKE THE PENTAGON MORE EFFICIENT.

BY ROBERT O. WORK & LISA DISBROW

The first annual report on artificial intelligence was released by the White House in February. This long-overdue document covers developments in the year since the American AI Initiative kicked off.

The report said that American research and development investments in AI "are measured not just by the specific dollar total of the financial investments, but also—and perhaps more importantly—in the quality and impact of those investments. These investments are now paying off in everyday lives, in applications from healthcare to financial services, from weather forecasting to transportation, and more."

YES MARKET MEDIA / SHUTTERSTOCK

The report is a welcome call to action. The U.S. approach to applying AI needs to be full-spectrum at full speed. We must use all applicable AI technologies, including computer vision, natural language processing, deep learning, and reinforcement learning, and apply these to all critical areas of national security, logistics, transportation, public services, and healthcare. We must also invest in developing secure, high-capacity architectures to enable AI technologies. Only with this focus will we begin to quickly gain experience in AI R&D, and in deployment of associated applications at scale. And it is only then that the benefits that accrue from AI, both to citizens and warfighters, will become manifest in a significant way.

There are a number of reasons why the U.S. government has lagged in adopting "exponential technologies." While the government has made plain it wishes to partner with the private sector, a variety of bureaucratic, regulatory and policy impediments have prevented this partnership from fully forming. This is especially true for smaller, innovative startup companies that are often the crucibles of innovation and out-of-the-box problem solving.

Despite some recent, innovative changes to acquisition processes, the usual bureaucratic minefields await bright-eyed innovators looking to contribute to the future of their country's defense. Complicated rules and slow processes mean that there is a mismatch

between the timelines of government-run projects and those of fast-moving, commercial organizations. Meanwhile, the lack of data standards within and across government agencies remains a problem. It's often exceedingly difficult for contracted companies to locate, access, and leverage pertinent data. Working with the government poses great challenges to many private companies, and the relationship between public and private sectors in the U.S. is difficult to develop and maintain. Private organizations are often disinclined or unable to attempt to bridge this gap.

This needs to change—and sooner rather than later. The sparing AI bets placed by some investors are now paying off, but the future of our country's technological investments still seems uncertain.

Federal AI research and development programs should not be viewed as zero-sum investments to be measured against other priorities. The country will need to deal with the budgetary implications of the $6 trillion we've spent to combat the pandemic. But exponential technologies are not a mere luxury in good times; they can provide critical efficiencies, global competitiveness, and cost-effective national security in the hardest of times.

STEVE SANCHEZ PHOTOS / SHUTTERSTOCK

If governmental AI investments can move beyond research prototypes to real, functional programs through a smarter acquisition strategy, these promising technologies could be used to alleviate many of our most difficult problems—even in the face of overall budget reductions. Spending smarter doesn't imply spending more overall.

DoD's Joint Artificial Intelligence Center organization can play a critical role in all this. There is a need for aggressive advocacy within the Pentagon to identify problems that can be paired with practical AI solutions in line with DoD's priorities of joint warfighting requirements, readiness, efficiency, and cost control. Investments in the JAIC should be increased and protected.

Civilian agencies face similar challenges with AI. Though less platform-centric than DoD, agencies like the Department of Energy or Health and Human Services must also hew to fiscal realities and become far more effi-

BUMBLE DEE / SHUTTERSTOCK

cient in how they manage and employ their personnel or prepare for future pandemics.

Even though scale and efficiency don't usually go hand in hand, given the budgetary pressures it is incumbent on agencies to reduce costs without harming performance. This is where AI has shown great promise in the commercial world. Natural language processing analyzes large amounts of text automatically and has made commercial call centers tremendously more efficient. The same systems could help cope with the unprecedented citizen demand for government assistance. Such capabilities are crucial to the next generation of AI-enabled public health initiatives, including global pandemic surveillance and emergency economic assistance that will reach federal, state, and local agencies.

To succeed, the U.S. government must redouble its efforts to cultivate real partnerships with private technology companies that understand both AI and governmental needs, and can provide an undiluted, full-spectrum focus. Granting key AI contracts to longtime prime contractors or consulting shops may be necessary, but it isn't sufficient. Acquisition professionals must go beyond their comfort zones to seek out expert AI partners committed to an across-the-board public sector transformation. To that end, AI companies are heavily focusing on government customers and the best ways to serve them.

This is a critical moment for the country—not only in its response to this pandemic, but for our future with AI. Navigating these tough times requires not just survival in the present, but a credible vision for a brighter future and a desire to engage with more action and less talk. D

Robert O. Work *is Chairman of the Board for SparkCognition Government Systems, and sits on the Board of Directors of Raytheon Technologies Corporation and several smaller defense-related firms. He is a Senior Fellow at the Johns Hopkins University Applied Physics Laboratory.*

Lisa Disbrow *sits on the Board of Directors for SGS, and on the Board of Directors of Mercury Systems, Perspecta, and BlackBerry, and several other defense-related companies. She is a Senior Fellow at the Johns Hopkins University Applied Physics Laboratory.*

CHAPTER 2

MORE COMPUTERS WOULD BRING MILITARY AI ALONG FASTER, NEW JAIC CHIEF SAYS

GROUNDBREAKING TOOLS ARE AROUND THE CORNER, 3-STAR GENERAL SAYS. THE LIMITING FACTOR IS LACK OF COMPUTING POWER TO GRIND THROUGH GIANT PENTAGON DATASETS.

BY PATRICK TUCKER

Many military applications for artificial intelligence — from grand strategy to supply-and-maintenance management to predicting incoming fire for platoon commanders — aren't far off, says the new director of the Pentagon's Joint Artificial Intelligence Center. But Marine Corps Lt. Gen. Michael Groen says AI still faces resource challenges and hopes that incoming defense leaders will continue to prioritize the fieldit as budgets face new headwinds.

Groen said AI will lead to a revolution in defense decision-making, particularly by combatant commanders.

LANCE CPL. DEVAN K. GOWANS / U.S. MARINE

"They're the people who are going to be awake at night when something weird is happening in Belarus," Groen said in his first one-on-one interview since becoming the JAIC's second commander in October. "There's a combatant commander who's on the hook for reacting to that. Shouldn't we enable those combatant commanders with data-driven, clear pictures of what's happening on the ground? "What's happening in the information space, tipping and queuing in an automated way, natural language processing and then being just as cognizant of 'What's blue doing? What tools do I have to react to that?'

"Today we do all of that, combatant commanders, great decision-makers all," Groen said — but too much remains "seat-of-your pants."

While seat-of-your-pants decision-making may sound rapid and agile, it can also mean delay and misuse of resource for the troops who are waiting for orders, Groen said.

"That's how you wind up with a lance corporal sitting in the middle of nowhere going 'ok what idiot told us to go here and why?'" he said. "That's the result of seat-of-the-pants decision-making based on imperfect information."

The cure for that is for military leaders to get "much better at using data to drive the decisions that we actually have data on." This kind of data already exists — and if it could be collected, structured, and presented more coherently, Groen said, it might answer questions such as "'What is the status of your unit? What is the status

PANCHENKO VLADIMIR / SHUTTERSTOCK

of your reserve? Is that unit really ready to go or not? What's the status of your logistics? What's the status of your medical [evacuation] capability; can you meet the Golden Hour?" he asked, referring to the best window of time to get an injured operator to medical care.

Groen sees military AI as little more than the wise application of well-known and common machine learning and methodologies to vast stores of Department data. This means, he believes, that AI can begin to change planning, strategies, and operations today.

AI tools aren't just for combatant commanders. Groen thinks it's long past time to give platoon and squad leaders battlefield options and services that they enjoy in civilian life in apps like ride-sharing app Uber or navigation app Waze. "Shouldn't I be able to pull up…map data the way I'm riding home in my car? Shouldn't I be able to do automated navigation or assisted navigation? Shouldn't I be able to click on things that [are] 'artifacts of the battlefield?" he said. "So if you're doing a [helicopter] linkup…want to make sure you have resupply because you've been in a place for a long time. That kind of stuff can be data-driven so you don't even have to ask. You report and things happen. The logistics start flowing to you."

And even before AI changes soldiering, Groen expects it to change less glamorous Defense Department activities. "The business case stuff, it's not as compelling as the warfighting stuff but it's closer and it's easier. The data is more available." Activities away from combat are also the sort of thing that a wider variety of companies, like Google, may want to help with.

Getting the military to where it needs to be to fully use the data it has as part of an AI-first enterprise won't be cheap, he says. And the JAIC, just like every data-based enterprise, is constrained by the amount of sheer computing power it has to throw at problems.

"Training an algorithm is not that expensive," but it's not free, Groen said. JAIC could move faster to exploit the Pentagon's large datasets if it had access to more computers, and particularly graphical processing units. "The cost is a limiting factor, certainly a limiting factor for the JAIC. And we don't have that big of a budget," he said. "We have a capacity issue, like how fast can we get to all of the people who need AI across the Department? We were going to run as fast as we can but our duty cycle is going to be… we're going to be working out butts off."

Groen hopes future Defense Department leaders appreciate how AI could change much of what they do. There's some indication that will be the case. Michelle Flournoy, widely regarded as president-elect Joe Biden's likely Defense Secretary pick, has been a vocal supporter of robust investment in AI.

"I think with leadership from the top within the Department that's really focused on: 'Okay, we agree that artificial intelligence and information-age decision-making can really facilitate our transformation and it's necessary.' With leadership that's focused like that, we'll get to where we want to go," he said. D

CHAPTER 3

PENTAGON'S 'AI FACTORY' LOOKS TO DISTRIBUTE TOOLS ACROSS DOD

THE JOINT ARTIFICIAL INTELLIGENCE CENTER WILL BEGIN ROLLING OUT ITS JOINT COMMON FOUNDATION NEXT YEAR, ITS NEW DIRECTOR SAYS.

BY MILA JASPER

The Joint Artificial Intelligence Center is looking to become an AI service hub for the Defense Department rather than a product building unit, according to the JAIC's new director.

Lt. Gen. Michael Groen assumed JAIC leadership last month, taking over from acting director Nand Mulchandani. Groen outlined his priorities for the JAIC during a Friday webinar with the center for Strategic and International Studies. He said he's moving JAIC beyond building products that demonstrate the possibilities of AI applications to a "JAIC 2.0," working on the broader enablement of AI across DOD.

"The instantiation of AI across the department is very uneven," Groen said. "Some places are very robust, some places haven't even thought it through yet. So we will continue to adapt our organization to meet that demand signal wherever that is and as the department matures and as AI integration we'll continue to move up the value chain."

One key program coming online that will enable the "JAIC 2.0" vision is the Joint Common Foundation, or JCF. Groen said during the webinar he anticipates JCF will start offering simple services in 2021, and then begin growing in complexity to scale the project.

Deloitte Consulting was awarded a $106 million contract in August to design and build the JCF. The JCF will operate as a kind of factory providing DOD with "an AI development environment to test, validate and field AI capabilities," according to a statement from the Defense Information Systems Agency released when the contract was awarded.

"What we're talking about is enabling sort of all the disadvantaged users across the department, those warfighting functions, those enterprises that see artificial intelligence use cases in their workflow, in their process, in their mission, but they really don't know what to do," Groen said.

Groen said the JCF will have a technical aspect, meaning a platform based in the cloud for users across DOD to work on AI projects, as well as what Groen called a soft services component.

The technical aspect will help with things like taking advantage of data services, and the JCF may eventually store and catalogue algorithms that entities across the department can reuse for various functions, Groen said.

The services side will promulgate best practices around areas like testing, evaluation, verification and validation, Groen said. It may also help components figure out how to contract for various AI use cases and build contract vehicles for other users to take advantage of. JAIC is also looking at certification—using the JCF platform to create educational opportunities—he added.

"We're eager to make progress," Groen said. "We're cranking it out."

CHAPTER 4

WANT REAL SECURITY? CREATE BETTER GLOBAL DIGITAL RULES AND NORMS

THE LONGER THE U.S. WAITS TO THROW ITS WEIGHT BEHIND EFFORTS TO CREATE RULES FOR TODAY'S DIGITAL COMPETITION, THE LESS HOPE IT HAS OF RETAINING ADVANTAGE.

BY C. ANTHONY PFAFF & PATRICK GRANFIELD

There will be no effective Third Offset reasserting American leadership in emerging technologies such as artificial intelligence until there is simultaneous effort on a — well, call it a Fourth Offset, to revitalize global norms and rules of the road.

Advances in autonomous systems, information warfare, and material sciences are well on their way to transforming national security. Not only have these technologies helped the United States' authoritarian adversaries to solidify control over their own populations, they have also expanded the ways and means through which states and non-state actors compete, blurring the lines between war and peace. Thus, any normative offset must not just address the technologies themselves, but also the competitive environment they help create.

THEN-DEPUTY SECRETARY OF DEFENSE BOB WORK SPEARHEADED THE PENTAGON'S THIRD OFFSET STRATEGY. | NAVY PETTY OFFICER 1ST CLASS TIM D. GODBEE / DOD

We already see how repressive states are taking advantage of technology. New tools for mass surveillance are helping China, Russia, and Iran — not to mention U.S. partners — to track and invasively monitor their population. Advances in autonomous and semi-autonomous weapons give a wide range of actors the means to strike in more precise, prolific, and deniable ways. Cyber attacks hold critical infrastructure and services at risk. Advances in other spheres allow friendly and unfriendly actors to shape global narratives — even to undermine the legitimacy of governments and institutions necessary for a successful defense.

As a result, U.S. planners are rethinking the roles the military should play in competition below the threshold of war. What is striking about the nature of this competition is not so much the sophistication of these new challenges, but rather the primitive state to which they reduces competition. By undermining and eroding the complex norms currently in place to manage conflict and escalation, the use of these technologies force actors to rely on blunter instruments, such as proxies and reprisals, to shape adversary behavior. Proxies are under-regulated, allowing actors to avoid cost and accountability. To deter future attacks, aggrieved parties have little choice but

SGT. KYLE C. TALBOT / U.S. MARINE CORPS

to engage in reprisals, which are illegal in peacetime and which tend to lead to escalation. For example, Washington's maximum pressure campaign against Iran has led to violent exchanges between U.S. forces and Iran and its proxies.

Another under-regulated area is automation in the military sphere. Human control is being supplemented or replaced by machine learning based on data sets that can be manipulated and polluted. Moreover, as competitors work to outdo one another, rapidly developing and deploying capabilities that depend on artificial intelligence, it is less likely they will account for their unintended consequences and safeguard against accidents.

Cyber operations, and society's growing dependence on technologies that use artificial intelligence to regulate their operations, present another danger. The line between civilian and military targets is less clear online, making it more difficult to protect innocent civilians from potential conflicts. We must draw clear boundaries with our partners and hold ourselves and others accountable it.

Leaders across the Pentagon have grappled with the convergence of technology and the international order across administrations. They have promoted closer collaboration between national security efforts and the private sector to ensure U.S. technical parity, if not superiority, to make the most of the United States' nimble and innovative economy. This same emphasis is also reflected in defense budgets, which have

increased spending on research and development for the purpose of national security.

While this focus may be necessary, it is clearly insufficient. It does little good to develop and field superior technology in a space where technologically inferior actors can still exploit vulnerabilities to cause harm and disrupt civil life. What is needed is a new international order that gives states better alternatives to force.

In this regard, America's greatest advantage is not the example of its power, demonstrated here in a well-funded military at the bleeding edge of technology. Rather, it is the power of its example that has allowed the United States to underwrite global security for the past seven decades and that example is needed now more than ever as global competition takes a potentially chaotic turn. The ability of the United States to continue that legacy today depends on how effectively we convene our Allies and partners in developing a framework that governs the use of emerging technologies. Without one, technological competition with our adversaries will become a race to the bottom, leading to greater instability and the erosion of democratic norms at home and across the world.

SO, WHAT CAN WE DO?

• Address the proliferation of technologies that allow for deniability, lower the physical cost of employing violent means, and that exploit vulnerabilities that disrupt civil life.

• Strengthen laws and institutions to hold actors who employ proxies responsible for crimes those proxies commit.

• Address the role of peacetime reprisals as a form of international law enforcement. Decrease the likelihood of their necessity by strengthening international institutions and other measures to hold violators accountable. Given that there will also be some gap between violations and accountability, establish norms that expand on non-lethal means of reprisals while limiting their scope to avoid harms to innocents.

• Prioritize non-lethal over lethal alternatives to shaping adversary behavior and where lethal force is used, demand a higher standard for success and a much lower tolerance for civilian harm. What justifies the resort to these measures is that they represent an alternative to war; therefore, actors will be morally required to take measures to avoid escalation.

While these times are different, the United States has faced crossroads before. The country's relative global power is less than it was in the 1950s or even the 1990s, but American leadership remains a potent, essential force. Though there is less tolerance overseas for talk of American exceptionalism and dictates from Washington, there is a case to be made for democratic exceptionalism and for convening partners and allies around shared democratic values that inform the development and application of technological systems.

The world watches us; however, it will not wait for us. If the United States does not focus on defining the terms for the ethical use of emerging technologies as well as the environment they give rise to, then the world we live in will be defined by these technologies and their unscrupulous use by autocratic governments. D

CHAPTER 5

66 WAYS TO BEAT CHINA IN AI: REPORT

THE NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE SUGGESTS A CTO FOR THE INTELLIGENCE COMMUNITY; A WHITE HOUSE AI COUNCIL, LIKE THE NATIONAL. SPACE COUNCIL; AND MORE.

BY MILA JASPER

The National Security Commission on Artificial Intelligence submitted its interim report and third-quarter recommendations to the president and Congress Tuesday.

The commission, composed largely of private-sector tech experts from companies such as Google and Oracle, submitted 66 recommendations across six lines of effort, including workforce, education and research and development. Commissioners voted on recommendations last week during a virtual public plenary meeting.

The far-reaching recommendations pointed to a theme that has increasingly gripped the minds of policymakers: the return of great power competition. Commission co-chairs Robert Work, former deputy secretary of Defense, and Eric Schmidt, former CEO of Google, told reporters during a press call Tuesday that artificial intelligence is an essential component of competition with nations like China.

"It's become very clear that we are in an innovation competition unlike anything we've ever faced before," Work said.

One of the most significant recommendations targeted at this competition calls for the creation of a technology council chaired by the vice president and tasked with the development of a national technology strategy.

This council could live within existing White House entities such as the National Security Council or the Office of Science and Technology Policy, according to the report. The report also recommends the council include an assistant to the president to run day-to-day activities. NSCAI specifically states this assistant should be someone who not only understands the workings of government, but who also has "strong ties to the private sector technology community."

Both the Trump and Obama administrations have received criticism regarding revolving-door relationships with Silicon Valley, though. Lately, President Trump's relationship with Oracle's Larry Ellison has raised eyebrows, particularly after Trump approved a deal that anointed Oracle as TikTok's "trusted tech partner" in the U.S. Similarly, the Obama administration was criticized for its close ties to Google.

Schmidt said the commission had in a mind a model for the technology council similar to the National Space Council, which is currently headed by Vice President Mike Pence.

"What I've learned as an amateur in government bureaucracy is that it really matters how high you are in the organization and so we think, collectively, that this set of issues around competitiveness are so defining that it needs to be at the vice president or presidential level, and not as part of some bureaucratic process," Schmidt said.

NSCAI in quarter three is recommending other administrative changes to orient the bureaucracy toward

AIRMAN 1ST CLASS COREY HOOK / U.S. AIR FORCE

emerging technologies as well. The report calls for the creation of a chief technology officer for the intelligence community along with greater empowerment of the Defense Department's CTO.

One recommendation meant to help elevate the DOD CTO, also known as the undersecretary of Defense for research and engineering, calls for a dedicated fund for the CTO to use to integrate promising artificial intelligence technologies. The goal of the fund would be to support emerging AI technologies beyond initial research and development so that these technologies can become operational faster even when planned program funds aren't yet available.

The new intelligence community CTO position should be an evolution of the director of science and technology role within the Office of the Director of National Intelligence, according to the report. NSCAI also wants the new CTO to have a dedicated fund for AI investments.

"With this type of high-level oversight, we think we can really start to organize ourselves for the competition," Work said.

A significant portion of the recommendations are dedicated to workforce and talent initiatives. Work said the commission feels the only way to win the AI competition is by developing the best talent. Some of NSCAI's workforce and talent measures, especially from previous NSCAI reports, have made their way into versions of the 2021 National Defense Authorization Act. Schmidt said the commission has made a targeted effort in 2020 to work with Congress on implementing its recommendations in the NDAA.

Now that the quarter three report and recommendations are out, NSCAI will turn its attention to the development of its final report, which is due in March. Schmidt said the commission has released its work to "both political camps" so that it will be ready to collaborate with either a second-term Trump administration or a new Biden administration depending on the result of the election. D

CHAPTER 6

WILL COMMANDERS TRUST THEIR NEW AI WEAPONS AND TOOLS?

A STUDY OF DOD'S ARTIFICIAL-INTELLIGENCE EFFORTS REVEALS A KEY GAP.

BY MARGARITA KONAEV

As the Department of Defense races to develop AI-enabled tools and systems, there are outstanding questions about exactly where their investments are going, and what benefits and risks might result. One key unknown: will commanders and troops trust their new tools enough to make them worth the effort?

Drawing on publicly available budgetary data about the DOD science and technology program, the Center for Security and Emerging Technology, or CSET, examined the range of autonomy and AI-related research and development efforts advanced by the U.S. Army, Navy, Marines, Air Force, and DARPA. Among the main research lines are programs dedicated to increasing automation, autonomy, and AI capabilities in air, ground, surface, and undersea unmanned vehicles and systems; increasing the speed and accuracy of information processing and decision making; and increasing precision and lethality throughout the targeting processes. We recently released a two-part analysis of the scope and implications of these efforts. One of the most consistent themes is an emphasis on human-machine collaboration and teaming.

SGT. HENRY VILLARAMA / SGT. JOSH LECAPPELAIN

Indeed, while in the public imagination the integration of AI into military systems foretells a future where machines replace humans on the battlefield and wartime decisions are made without human input or control, in our assessment of U.S. military research on emerging technologies, humans remain very much in the loop.

The U.S. Army's flagship Next Generation Combat Vehicle research program is a good example of human-machine teaming cutting across different use cases and applications of autonomy and AI. One of its research activities develops AI and ML software and algorithms to "team with soldiers in support fully autonomous maneuver of NGCV and other autonomous systems, both physical and non-embodied." This effort is meant to develop capabilities for NGCV that will "increase autonomy, unburdening the soldier operator, with a high degree of survivability and lethality in a highly contested environment." Another applied NGCV research initiative

looks to new "ML and reinforcement learning methods" to enable "joint human-intelligent agent decision making, optimizing the strengths of each in the decision process and creating an adaptive, agile team." In other words, this research envisions intelligent technologies that interact, collaborate, and integrate with soldiers, optimizing performance for both humans and human-machine teams in different environments and missions.

DARPA's applied research on "Artificial Intelligence and Human Machine Symbiosis," however, takes the human-machine teaming concept a step further, aiming to develop technologies that "enable machines to function not only as tools that facilitate human action but as trusted partners to human operators."

Trust is central to human-machine teaming because it affects the willingness of humans to use autonomous and AI-enabled systems and accept their recommendations. CSET research, however, identifies important gaps in U.S. military research on the role of trust in human-machine teams and gaps in investment toward building trustworthy AI systems. In fact, the 'Budgetary Assessment' report which analyzes the 2020 U.S. military science and technology programs finds that only 18 out of the 789 research components related to autonomy and 11 out of the 287 research components related to AI mention the word "trust."

SGT. CHRISTOPHER HUBENTHAL / U.S. AIR FORCE

As the Department of Defense AI ethics principles dictate, humans are ultimately responsible for the development, use, and outcomes of AI systems in both combat and non-combat situations. If left unaddressed, gaps in research on the role of trust in human-machine teams could hinder the development and fielding of AI systems in operational environments.

For instance, AI-enabled decision support technologies in particular are meant to help commanders process and assess more options for action and make better and faster decisions in complex and time-sensitive situations. Advances in real-time analytics and recommender systems technologies could help warfighters adapt and gain the initiative in dynamic operational settings. But if human operators don't trust the system, they would be reluctant to follow

MASS COMMUNICATION SPECIALIST 3RD CLASS SEAN ELLIOT / U.S. NAVY

its recommendations. Thus, without trust in human-machine teams, the U.S. military may not be able to capitalize on the advantages in speed and precision AI promises to deliver.

Understanding the role of trust in human-machine teams is also important for effective collaboration with allies. Some research suggests that trust in AI varies by country of origin. If commanders from some allied countries are less willing to trust and use AI-enabled systems during multinational operations, such divergence could undermine coordination, interoperability, and overall effectiveness.

Finally, in addition to research into human attitudes toward technology, progress toward advanced human-machine teaming will also depend on making the AI systems themselves trustworthy, in part by making them more transparent, explainable, auditable, reliable and resilient.

The U.S. military has several S&T programs focused explicitly on increasing AI system robustness and resilience, strengthening security against deceptive and adversarial attacks, and developing systems that behave reliably in operational settings. DARPA's "AI Next Campaign" is a prominent effort. Yet as previously noted, in our assessment, most of the research programs related to autonomy and AI don't mention those safety and security attributes that are so pertinent to trustworthiness. Now, beyond hampering progress toward advanced human-machine teaming, our "Strategic Assessment" report also finds that failing to consistently invest in reliable, trustworthy, and resilient AI systems could increase the risk from miscalculations, misuse, and unintended escalation, especially in contested environments such as the South China Sea.

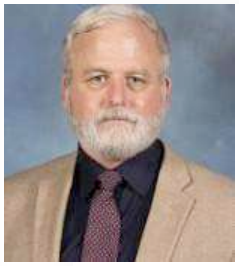
Today's research and development investments will set the course for the future of AI in national security. By directing more attention to understanding the role of trust in human-machine teams, the U.S. military could accelerate the development and fielding of intelligent agents and systems as trusted partners to human operators across different missions and environments. Furthermore, by prioritizing reliable and secure AI systems, the United States will be able to ensure long-term military, technological, and strategic advantages. D

CONTRIBUTORS

LISA DISBROW

FORMER ACTING SECRETARY,
U.S. AIR FORCE

Lisa Disbrow is a member of the Board of Directors for SGS, and of the Board of Directors of Mercury Systems, Perspecta, and BlackBerry, and several other defense-related companies.



C. ANTHONY PFAFF

ARMY WAR COLLEGE

Dr. C. Anthony Pfaff is the Research Professor for Strategy, the Military Profession and Ethics at the Strategic Studies Institute at the U.S. Army War College and a Senior Non-resident Fellow at the Atlantic Council.

PATRICK GRANFIELD

SPEECHWRITER FOR DEFENSE
SECRETARY ASH CARTER AND
SECRETARY OF STATE JOHN KERRY

Patrick Granfield, who directed strategic communications for Army Secretary Eric Fanning, is a former speechwriter for Defense Secretary Ash Carter and Secretary of State John Kerry.

PATRICK TUCKER

TECHNOLOGY EDITOR

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.

MILA JASPER

EDITORIAL FELLOW

Mila Jasper is an editorial fellow at Nextgov. She is interested in covering national security, defense and technology issues. A DMV native, Mila has returned to the area to report after graduating from Northwestern University.

ROBERT O. WORK

CHAIRMAN, SPARKCOGNITION
GOVERNMENT SYSTEMS

Robert O. Work is Chairman of the Board for SparkCognition Government Systems, and sits on the Board of Directors of Raytheon Technologies Corporation and several smaller defense-related firms.

MARGARITA KONAEV

RESEARCH FELLOW, CSET

Dr. Margarita Konaev is a Research Fellow at the Center for Security and Emerging Technology, specializing in military applications of AI and Russian military innovation. CSET is a policy research organization within Georgetown University's Walsh School of Foreign Service.

Defense One