

Data ana...

APRIL 2023

Seven Critical Technologies for Winning the Next War

A REPORT OF THE CSIS INTERNATIONAL SECURITY PROGRAM

AUTHORS

Emily Harding
Harshana Ghoorhoo

CSIS

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

APRIL 2023

Seven Critical Technologies for Winning the Next War

A REPORT OF THE CSIS INTERNATIONAL SECURITY PROGRAM

AUTHORS

Emily Harding

Harshana Ghoorhoo

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.

Acknowledgments

The authors would like to thank Kari Bingen, Sue Gordon, Dr. Tara O’Toole, Tex Schenkkan, and Jacqueline Tame for their review of an initial draft and insightful feedback. Opinions and findings are solely those of the authors, and any errors or omissions are solely the responsibility of the authors. Analysis and graphs are based on collected data; the authors welcome recommendations of relevant data sets for future analysis on this subject.

This report is made possible through general support to CSIS.

For more information on how the U.S. government can effectively incorporate technology into national security efforts, see our new microsite, “Tech Recs,” at techrecs.csis.org.

Contents

Executive Summary	1
Introduction	2
<i>The Issue</i>	3
<i>Methodology</i>	3
Future Warfare	5
<i>What Will War, Peace, Competition, and Intelligence Look Like in 2030?</i>	6
<i>Smolder: Intelligence, Competition, and Hybrid War</i>	6
<i>The Hot Blast: Future War</i>	8
The Seven Technologies	9
<i>Foundational Technologies</i>	12
<i>Strategic Technologies</i>	13
<i>Tactical Technologies</i>	14
Recommendations: How to Get from Here to There	17
<i>Sprint Recommendations: Commit Resources and Senior-Level Focus</i>	18
<i>Follow Recommendations: Encourage and Manage Developments</i>	20
<i>Adapt Government Practices</i>	21
Conclusion	24
Appendix I: Below the Line: Technology That Almost Made the List	25
Appendix II: If I Had a Billion Dollars . . .	26
Appendix III: Mapping Technologies to Capabilities	27
Appendix IV: Contributing Experts	28
About the Authors	29
Endnotes	30


Executive Summary

After an in-depth review of dozens of important emerging technologies, researchers at CSIS identified the seven technologies that are most likely to make a significant difference in the success of the United States and its allies across the spectrum of conflict over the next decade.

The U.S. government should “sprint” on three critical technologies where current commercial developments are not fast enough or not tailored enough for U.S. government need: bioengineering technology; secure, redundant communications networks; and quantum technology. This sprint should include robust research in partnership with industry, investment, and innovative approaches to rapid adoption.

Further, the U.S. government should “follow” in four areas: space-based sensors; miniaturized, long-lasting batteries; robotics; and artificial intelligence/machine learning. In these sectors, private investment is robust, and encouraging offshoots of commercial technology will create effective dual-use products.

The U.S. government should pair these efforts with a critical self-evaluation of acquisition practices, in particular identifying how antiquated acquisition practices are getting in the way of mission and how to create a parallel pathway for software and other technologies. Meanwhile, the U.S. government should invest resources in building a tech-savvy workforce and fighting force over the next 10 years.

A photograph of two soldiers in camouflage uniforms and helmets. The soldier on the left is wearing glasses and looking at a rugged, green laptop. The soldier on the right is looking at the laptop and has a radio in his hand. The background is a blurred green field.

CHAPTER 1

Introduction

THE WORLD IS SPEEDING UP.

The Issue

The world is speeding up. Adversaries such as China are seeking to remake global power structures and compete with the United States for global influence. A race toward technological advancement underpins the competition over economic power, public health, influence over potential allies, intelligence work, hybrid conflict, and even military strength. The competitor who demonstrates a technological advantage on these fronts has an edge in global influence and an advantage across the spectrum of conflict, with corresponding deterrent effect.

This project seeks to draw a line from the capabilities the United States will need in this era of competition, to the technologies needed to secure those capabilities, and finally to a clear path for how to purchase, adapt, and incorporate those technologies into the national security apparatus.¹ Since competition is wide-ranging, this project could have explored a wide set of arenas. Instead, researchers focused on core national security functions and will leave discussions of economics, sustainability, and public health to other projects. Further, rather than identify which widget to purchase, the project defines critical technology areas. It is clear that the ideal piece of equipment has not yet been invented in many of these areas; this project encourages the government to prioritize these seven areas for facilitating innovation and thereby bring about the right, specific piece of technology.

U.S. government collaboration with industry—rather than demands on it—will be absolutely critical to success in these endeavors. This report’s recommendations section addresses how the U.S. government and industry must meet in the middle on requirements and contracts.

Efforts to change the government’s relationship with technology need urgency, prioritization, and focus. The challenge of the next decade will be maintaining peace while creating the urgency of a crisis. Preparing for competition—and perhaps conflict—with a committed adversary such as China will not happen overnight.

Methodology

This project was an iterative effort to construct—and then pare down—a list of technologies that will be critical to success across the spectrum of conflict. The research team reviewed the literature about the future of warfare to check assumptions and think critically about the needs of those on the front lines of competition and conflict. Researchers also reviewed previous efforts to construct lists of technologies for common threads and prioritizations, then interviewed a wide range of experts in government, industry, and venture capital to cast a wide net on emerging technologies. During those interviews, researchers pushed participants to go beyond the obvious, to try to look past the horizon, and to ruthlessly prioritize where to put the most effort.

Researchers used two techniques to force prioritization from a long list of technologies. First, participants in a roundtable brainstormed a list of nominated technologies. Then they were asked to spend a theoretical billion dollars on one project and explain their choice, leading to an eye-opening discussion about what basic elements underpin evolution and revolution in government practices. (See Appendix II for these billion-dollar votes.) In crafting the final list for this paper, researchers evaluated the list of technologies nominated by interviewees and those described in previous efforts against three criteria:

FIGURE 1: CRITERIA FOR INCLUSION



SOURCE: CSIS INTERNATIONAL SECURITY PROGRAM.

The final list comprises seven technologies that will be critical to the success of U.S. intelligence, military operations, and other defense enterprises in a conflict with a near-peer adversary or rival. While the list of technologies includes few surprises, this project strives to add value in four ways:

- » This list evaluates technologies alongside the needs of the United States and its allies across the spectrum of conflict. The next section is a discussion of the likely trajectory of the future of war; this analysis informed decisions about which technologies made the list.
- » Other lists included many technologies and lacked insight on precisely where effort should be focused. This project sought to create a short list, under the theory that a more targeted effort is more likely to lead to success.
- » This project included an assessment of what the U.S. national security community can and will actually use. While any technological advancement could be a game changer, if it sits on a shelf, it is irrelevant. Researchers looked at whether the technology was too alien to current practices and equipment for the Department of Defense (DOD) or intelligence community to reasonably incorporate into its tool kit.² While national security professionals can adapt extremely quickly in a crisis situation, short of that external urgency, researchers evaluated what was an achievable goal in the next 10 years.
- » Along these lines, conversations with experts universally turned to the challenges of developing, purchasing, and adopting technologies inside government structures. As a result, researchers devoted a chapter to specific, actionable recommendations for overcoming these obstacles.

—

While any technological advancement could be a game changer, if it sits on a shelf, it is irrelevant.

—



CHAPTER 2

Future Warfare

WAR IN THE FUTURE IS LIKELY TO BE A SLOW SMOLDER OR A HOT BLAST.

What Will War, Peace, Competition, and Intelligence Look Like in 2030?

War in the future is likely to be a slow smolder or a hot blast.³ In other words, conflicts either will look like measures far short of war that aim to shape the playing field or a blitz offensive designed to create a *fait accompli* before allies can mobilize to help. The critical capabilities the United States will need to compete are exquisite sensing capabilities, the ability to sort through more noise than ever before to find the signal, rapid decisionmaking, and communicating everything from strategic decisions to battlefield tactics reliably and securely. Further, should a near-peer conflict happen, the United States will need to be able to keep forces geographically scattered but tightly coordinated, and those forces will need the resilience to operate with limited resupply for unknown amounts of time.

The slow smolder is geared toward victory without firing a shot. Intelligence activities, competitive behaviors, and hybrid war result in a slow shift of the adversary's mindset until there is no will to fight. An example would be China attempting to take Taiwan not by force, but by slow coercion. China might undermine Taiwan's democratic institutions, support pro-reunification politicians, and drive a wedge between Taiwan and the United States to the point that Taipei assumes the United States will sit on the sidelines in a fight. For example, Beijing could then be well positioned to threaten Taiwan with economic ruin—or to promise economic prosperity—in exchange for reunification under “two systems, one China.”

The hot blast would be the opposite approach, incorporating lessons learned from the Russia-Ukraine war. Beijing could seek to achieve total victory on the battlefield extremely quickly—before the United States, Australia, or any other potential ally could come to the rescue. This form of war would involve overwhelming precision-strike capability, domination of communications, and a decapitation attempt, in addition to well-hidden preparations for war.

The contours of these two types of conflict are described below, and each description is paired with a capability required to succeed.

SMOLDER: INTELLIGENCE, COMPETITION, AND HYBRID WAR

Capability: Intelligence agencies will require the ability to securely transfer information to and from an asset.

- » The face of intelligence is changing. In a sense, that face is literal: facial recognition technology with artificial intelligence/machine learning (AI/ML) assistance is making traditional human intelligence (HUMINT) operations difficult, if not impossible. China has blanketed cities at home and abroad with CCTV and has stored years of footage, making it possible to trace the movements of suspected human assets over time.⁴ Communicating virtually with assets is an increasing challenge, and a post-quantum future could instantly decrypt decades of

previously secure communications. HUMINT will evolve into a high-risk activity only worth pursuing if the return is correspondingly high, for example, to gain exquisite insight into leadership decisionmaking. A form of low-end HUMINT may also evolve where relationships are temporary and transactional and directed at one-off transfers of specific pieces of information.

Capability: Intelligence organizations will add value by recognizing the potential of publicly available information, evaluating its authenticity, processing it, and combining it with exquisite, classified information to provide fast insights.

- » Open-source intelligence (OSINT) will be a growing part of intelligence work. A sea of information is available to the public at large, and every cell phone in every pocket is a potential sensor. The combination of AI/ML, cloud capabilities, and this rich store of publicly available information can lead to a revolution in how the U.S. government thinks about intelligence and classification.⁵

Capability: This new world of intelligence will require tools that help sort through masses of information, process it efficiently, and flag the highest-interest items for human review.

- » Identifying small anomalies that unveil the “slow smolder” scenario will require smart processing of tiny indicators in the noise. Similarly, indications and warning of impending adversary hostility could provide crucial hours for avoiding catastrophe and averting the “hot blast” form of war. The required tools for success will be quantum sensing to collect the signals and minute signatures adversaries try to hide; AI/ML for tipping and cueing, perhaps paired with the power of quantum computing; and on-orbit processing of data to create efficiencies. The combination of these technologies will speed up sensor-to-decisionmaker time.

Capability: Offensive cyber operators will need a constant stream of vulnerabilities and access points and ways to obfuscate presence on a network; defenders will need instant awareness of unauthorized access and total visibility into their network and all endpoints.

- » Cyber offense and defense will continue to grow in sophistication in an ongoing cat and mouse game. A combination of cyber tools and AI/ML programs will be able to navigate around (or penetrate) defenses or, conversely, erect new defenses in the path of an exploitation effort. Intelligence agencies will work to develop disposable cyber

exploitation tools that can gain access and be discarded; persistence on a network will be rare and golden.

Capability: All sides will seek the capability to shock their adversary with a new technological success and to persuade allies that they are on the ascendant side.

- » In this era of competition, near-peer adversaries seek to shape the world to their preferences and establish a dominance that will deter others from challenging that dominance. Information warfare will be a core element of China and Russia’s shaping strategies. States will also demonstrate their capacity to dominate and deter with technology arms races. Announcements of breakthroughs will have the dual intent of making scientific progress while also bolstering deterrence.

Capability: The U.S. government will need sensing and processing capabilities that flag a potentially aggressive action or uncover a suite of incremental or clandestine actions that could outmaneuver an opponent.

- » Hybrid war—distinguished from competition—is an attempt to shape the global environment in a clandestine way with measures short of war. In these scenarios, an actor can assess that certain actions are beneath the threshold that might prompt a violent response. Information warfare features here as well, but in a more covert sense. Cyber activity for operational preparation of the environment will be a constant, as adversaries seek to hold at risk everything from command and control to civilian infrastructure to deter hostilities or as an early move in an emerging conflict. Hybrid war may be highly individualized, with AI/ML and OSINT making it possible to target particular people sitting behind keyboards or headed to the front lines; that targeting could range from psychological pressure up to biological warfare for targeted killings.⁶

THE HOT BLAST: FUTURE WAR

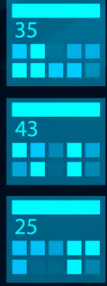
Capability: The United States will need a highly mobile and expeditionary military and a resilient communications system, using space-based, ground-based, and undersea assets to create a communications mesh network. Alternatives to GPS systems for long-range strike weapons likely will be necessary if the GPS system is disrupted. Functional autonomy will help with contested logistics, in particular if autonomous air- and sea-based assets can be used for supply delivery.⁷

- » The United States is shifting from a focus on a counterterrorism (CT) conflict against a mostly low-tech adversary to preparing for a high-end, high-intensity conflict against a sophisticated rival. This new world of warfare will likely see intense exchanges of precision weaponry, with rebuild and restock capability vital to success. In a fight in the Pacific, contested logistics will bedevil both sides, so the warfighters will need to be both highly networked and highly independent. Marshalling the right elements for a battle will require being able to communicate securely, and with low signatures, between a range of specialized units spread across a huge geographic area; contested logistics and likely disruptions to those communications mean that a fighting unit will also need to be temporarily self-sufficient. Just-in-time delivery of food, spare parts, and fuel will not be guaranteed. Planners must assume extensive loss of equipment. Disposable, or at least attritable, assets will be necessary, in particular uncrewed technology, from undersea resupply to sail drones for surveillance to airborne drone swarms used as loitering munitions. These systems will need sophisticated software and cheap hardware. On the other end, stealth technology empowering long-range strikes is also likely to be a critical asset. Submarines, long-range bombers, and hypersonics may prove the decisive edge in a high-end conflict. Secure communications will be at a high premium, with parties to the conflict likely succeeding in disrupting communications in the cyber and electromagnetic domain and with kinetic strikes. Undersea cables and space-based assets are all at risk.

66-1A 0000000000000000 025A1 83-6%
FULL 100% 7535-3525-2505-1105-0051
06 114 5D 0058875-12 /// 63K-185 ///
520390575 00 51-55% 1048 10000, 1.99
273959729A02 23415123 82-64% 1271 10000, 1.99

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer in leo nibh. In condimentum aliquam urna, et faucibus justo condimentum auctor. Morbi vel mattis quam, dignissim sodales

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Integer in leo nibh. In condimentum aliquam urna, et faucibus justo condimentum auctor.



Latitude - 40.97303563
Longitude - 73.71045369
Height - 23m



- List of routes
- Last route
- My location
- New route

Full Screen

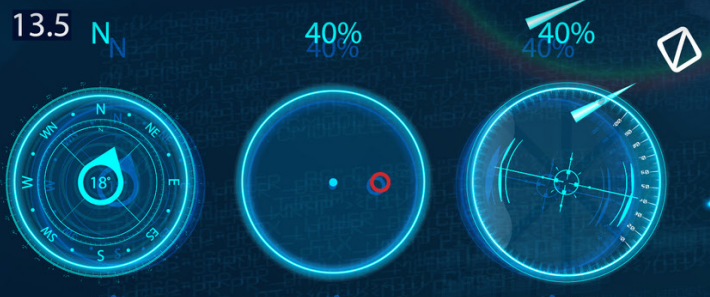
```
</style>  
<yt-d-app disable-upgrade="true">  
  <yt-d-masthead id="23.9" slot="masthead" class="shell  
  <div id="search-container" class="yt-d-search-box-spt">  
    <div id="search-input" class="yt-d-search-box-spt">  
      <input id="search" type="text" value="">  
    </div>  
  </div>  
</yt-d-app>
```



4 FN_1337 0.16 NY 114

CHAPTER 3

The Seven Technologies



LAT (N) 53°8'35' ING (E) 29°13'9'
LAT (N) 53°8'35' ING (E) 29°13'9'
LAT (N) 53°8'35' ING (E) 29°13'9'



PHOTO: SHUTTERSTOCK.COM

TO GET TO THESE CAPABILITIES, THE UNITED STATES WILL NEED MAJOR ADVANCES IN KEY TECHNOLOGIES.

To get to these capabilities, the United States will need major advances in key technologies. In discussions with national security professionals, researchers found that there was general consensus about needed advancements in a wide range of technologies—30 or more. However, when everything is a priority, nothing is. Controversy emerged in trimming that long list to a set of focused efforts.

Through interviews, research into the elements of competition, and the three-part test laid out above, researchers created the

following short list of seven priorities. While they are not in order of importance, the first three are “sprint” technologies, where the government should drive progress with intention and urgency. The remaining four are “follow” technologies, where the government can encourage and shape the private sector’s efforts.

These technologies will be critical to success across the spectrum of conflict:

FIGURE 2: THE SEVEN TECHNOLOGIES

SPRINT TECHNOLOGY	<p>Secure and Redundant Communications</p> <p>Tomorrow’s fight will depend heavily on communications. Jointness of forces, operations with allies, and even tactical coordination between dispersed units depend on secure and ever-present communications. Long-range engagements will make communications even more critical, from providing warning of incoming fire to coordinating with far-flung elements. High-end sensor suites and real-time targeting data are only as effective as the communications network used to transfer information from sensor to shooter.⁸</p>
	<p>Quantum Technology</p> <p>Quantum technologies will revolutionize computing power, encryption, and sensing. Current encryption is built to be so complex that a modern computer would take thousands of years to crack it by force. Quantum computers would be able to break asymmetric encryption in minutes.⁹ Quantum sensors, meanwhile, take advantage of the sensitivity of tiny particles to measure subtle changes in an environment, including rotation, electromagnetic signals of any frequency, and temperature.¹⁰ Quantum sensors could enable a navigating system that can operate even in GPS-denied environments.¹¹</p>

SPRINT TECHNOLOGY	<p>Bioengineering</p>	<p>Bioengineering applies engineering principles of design and analysis to biological systems and biomedical technologies. Bioengineering includes synthetic biotechnology, which is a subfield focused on creating biological processes or biological compounds not found in nature.¹² Bioengineering incorporates genetic engineering, modifying organisms in a way that produces a different behavior or outcome, and enhanced human biology.¹³ Bioengineering’s applications are hugely varied, from converting bacteria into fuel production factories to creating genetically modified pathogens for targeting a particular population.</p>
FOLLOW TECHNOLOGY	<p>Space-Based Technology</p>	<p>Tremendous advancements in on-orbit capabilities will create a definitive edge in the space domain, including on-orbit refueling, on-orbit data processing, and resilient space architecture. Hyperspectral and increasingly sensitive sensors mounted on clusters of small satellites and on-board processors equipped with tipping and cueing AI/ML algorithms could select data most likely to be important and downlink quickly to a ground-based mesh.</p>
	<p>High-Performance Batteries¹⁴</p>	<p>Modern militaries have tremendous demand for fuel and power, from vehicles to communications equipment to laptops that run backpack drones and other tactical surveillance. Power is also critical for intelligence—miniaturized batteries can fuel communications or collections devices concealed in unusual items. Further, a push toward unmanned systems with long dwell times will require long-lasting battery systems.</p>
	<p>AI/ML</p>	<p>With proper integration within DOD’s operations, AI/ML systems will accelerate—and complicate—most of the core functions of the U.S. national security community. The ability to process huge data sets and focus on the signal through the noise will help intelligence officers more effectively provide indications and warning, help policymakers understand complex trends, and help warfighters manage a multilayered battlefield, including autonomous vehicles and all-domain warfare.</p>
	<p>Robotics</p>	<p>Robotic advancements, combined with autonomous or semi-autonomous capabilities, will make it possible to minimize risk to human life in dangerous situations, on and off the battlefield, and perform tasks that are impossible or dangerous for people.</p>

SOURCE: CSIS INTERNATIONAL SECURITY PROGRAM.

Combinations of these technologies are often more powerful than the sum of their parts. For example, AI/ML together with bioengineering could create radical breakthroughs, such as discovering new biological compounds, and combining space technology and quantum sensing could revolutionize intelligence work.

There is general consensus that the U.S. government needs these technologies, but making progress on the path to actual adoption has still been halting at best. The key to progress lies in ruthless prioritization to focus effort, identification

of specific use cases, and willingness to invest in risky applications that may not precisely answer the need, but could with iteration. The rest of this paper draws a line from the capabilities stated above, to the specific applications, to recommendations for investment.

The next section highlights the specific applications of each technology. To explain where each technology fits into the bigger defense and intelligence picture, researchers split the technologies’ use cases into three categories:

FIGURE 3: USE CASES



SOURCE: CSIS INTERNATIONAL SECURITY PROGRAM.

Foundational Technologies

AI/ML

AI/ML will accelerate most of the core functions of a national security apparatus and appears in all three categories. For the foundational technology category, the ability to process huge data sets and focus on the signal through the noise will help intelligence officers more effectively provide indications and warning, help policymakers understand complex trends, and support warfighters in managing an all-domain battlefield, including autonomous vehicles. DOD investing in a common data lake, and the manpower and compute power to curate it, will serve interests across the U.S. government.

AI/ML will be a force multiplier for several other technologies on the critical list:

- » **Robotics advances combined with AI/ML will create autonomous machines that can perform far more complex tasks**, perhaps reasoning their way through a battlefield or a set of collection targets.
- » **AI/ML could be applied to cyber offense and defense.** On offense, algorithms could study a network and “decide” the best path through the defenses. On defense, algorithms could rapidly discover a penetration and respond within seconds, without waiting for a human response, and potentially shut off access, preventing the opponent from establishing persistence on the network.¹⁵

- » **Combining the ability of AI/ML systems to analyze vast amounts of data with bioengineering concepts would rapidly accelerate advancements in the field.** AI/ML could work through thousands of combinations of molecules, identifying which ones can create viable products and potentially constructing new compounds that humans could not imagine, much like the “art” AI has created. Using quantum computing power to run AI/ML algorithms could someday accelerate all of these advances.

While AI/ML has the potential for astonishing advances, forward progress should be tempered with ethical checks and evaluations. Algorithms reflect the biases and issues contained in their training data, and the widespread beta testing of ChatGPT has shown that AI systems can invent information and present them as facts. Each use case for AI/ML mentioned in this paper should carry the caveat that extensive testing and evaluation of AI/ML systems is required before DOD or the intelligence community employ them for national security missions.

QUANTUM TECHNOLOGY

Quantum computing, once theoretical, now seems within reach. Quantum experts estimate—with low confidence—that a useful, utility-scale quantum computer, capable of far better computation than today’s supercomputers or high-performance computing, will be commercially in use within the next decade, and other uses of quantum technology are likely closer.¹⁶ Quantum sensing, in particular, would be foundational to intelligence work, allowing for sensing of small changes in an

environment.¹⁷ Next-generation sensors could detect slight underwater pressure changes and tiny atmospheric shifts and provide high-accuracy GPS and receiving signals for radar communication.¹⁸ When quantum computing comes online, it will make current encryption obsolete and allow the user to read old—but still potentially useful—messages. It will provide an open window into any nation that has neglected to update their encryption practices to a post-quantum environment. Conversely, quantum key distribution and quantum networking could provide additional security for communications.

There will be a significant first-mover advantage for whomever can achieve quantum decryption without the knowledge of the owner of the communications. The actor that achieves quantum sensing the fastest will also have an advantage in the hide-and-find of “smolder” activity.

BIOENGINEERING

Bioengineering will transform manufacturing, health, and probably weaponry. The capabilities of CRISPR Cas-9 brought new biological entities within reach of a wide range of actors, and the field has grown extensively.¹⁹ While scalability will be initially challenging, the ability to rapidly respond to need has been proven: the Defense Advanced Research Projects Agency (DARPA) asked the Foundry at the Broad Institute of MIT and Harvard University to create 10 specific molecules within 90 days; they succeeded in creating 6 out of 10.²⁰

Among other future applications, the following could provide disruptive capabilities to the military and intelligence community:

- » Bioengineering can be used to create energetic materials such as explosives, plasticizers, and binders.²¹
- » New synthetic biological compounds could invent stronger polymers for more effective protective gear, such as high-temperature composites, fire-resistant materials, coatings, fibers, fabrics, adhesives, and armor.
- » Editing bacterial genomes can transform them into microscopic factories that create medicines and fuel, perhaps alleviating supply chain demands for dispersed forces.²²
- » At its extreme end, bioengineering can create sophisticated weaponry, markers to track individuals, or detection devices for a range of substances.²³ Programmable vaccines could prove key to countering tailored and novel bioweapons, and new scientific approaches for tracing bioweapons back to their source will be important for effective policies around deterrence and attack response.²⁴

Editing bacterial genomes can transform them into microscopic factories that create medicines and fuel.

Strategic Technologies

AI/ML

Effective AI/ML will provide a strategic advantage by providing decisionmakers with better information more quickly and then implementing those decisions with greater efficiency. It will also revolutionize communications: AI translation and message crafting will give diplomats and officials the ability to communicate in any language with anyone in the world. One interviewee said it would change the communications game and forever alter public diplomacy.²⁵ Conversely, AI/ML could be used by a nefarious actor to create effective deepfakes that spread disinformation. ChatGPT’s immense and sudden popularity suggests people are eager to explore AI/ML; however, the problem of AI systems “hallucinating” answers to questions has not yet been solved.

Advances in natural language processing will accelerate intelligence work, helping analysts sort through reams of text and drawing connections a human brain might not notice. AI/ML will be able to review terabytes of data and tip and cue additional collection or human review. That pre-screening of data will speed the delivery of critical indications and warning to policymakers, who can then make decisions faster.

The tip and cue function of AI/ML will also help collectors make faster and more accurate decisions about directing further intelligence collection, helping to focus precious collection assets on the most fruitful targets. For example, a long-range surveillance drone attempting to enhance stealth by not communicating during flight could have a program on board that would instruct it to “recognize” a mobile missile and then follow that missile system and signal back home if it appears that the system is departing from “normal” movements or activities. In case of active hostilities, and if policy assessments found the program to be completely accurate, that drone could be programmed to act as a loitering munition or carry weaponry programmed to fire if final preparations for launch are underway.

SPACE-BASED SENSORS AND COMMUNICATIONS

Advances in sensitivity will allow placing suites of sensors on satellites. Sensors that now need to be mounted on air-breathing platforms in order to gain an image or other data with fidelity will become effective from increasing distance, in particular if on-orbit processing can reduce the quantity of data transmitted to ground stations. Some may be able to provide useful information with persistence mounted in a geo-synchronous orbit. Similarly, advances in space-based communications, including clusters of small satellites and widespread or mobile secure downlinks, will help create a resilient communications network.

The U.S. government is taking steps toward acquiring additional space-based sensors and data. The National Reconnaissance Office is investing in hyperspectral imagery from space, collected both by government and commercial assets. The agency granted a study contract to a company in 2019 to explore ways to collect detailed hyperspectral data from space, rather than from air-breathing assets. The company plans to launch its first satellite in 2023 and claims it will be able to collect hyperspectral data from 104 spectral bands.²⁶

Private entities are using space assets to provide communications capabilities, which brings both opportunity and potential challenges, should the industry partner disapprove of a government's actions. One company launching satellites in 2023 seeks to provide fast, affordable internet connectivity to underserved regions.²⁷ Another has announced plans for “a secured satellite network for government entities” focused on delivering processed earth observation data, securing global communications enabled by intersatellite laser links, and providing satellite buses that can support customer payload missions.²⁸ However, Ukrainian government officials have experienced the risks of depending on a company for critical communications—it can place national security at the whim of that company's leadership.²⁹

SECURE AND REDUNDANT COMMUNICATIONS

Secure communications will be essential to the way modern militaries fight. Jointness requires communication for coordination; capitals have come to depend on near-real-time visibility into the battlefield and up-to-the-second intelligence delivery. High-end sensor suites and real-time targeting data are only as effective as the communications network used to transfer information from sensor to shooter.³⁰ Ukraine's work

to hunt Russian command units by targeting communications signatures shows that fixed communications will be a tempting target.³¹ Low-signature communications capabilities will be critical to unit survivability. Next-generation networks will create resilience through a self-healing mesh. If one or more of the nodes is offline, signals will find a new way through the mesh.

Creating secure, redundant communications will involve layers of technologies, and those layers will vary based on the situation. Further, redundancy will be a combination of satellite and ground-based capabilities, and truly effective communications systems will be secure and seamless across services. That will require purchasing decisions that factor in encryption, resilience against cyberattacks and physical damage, and interoperability with allies.

Communications networks will be both essential to the fight and an early target of a sophisticated adversary, such as China. Beijing understands that the United States depends on being able to communicate to facilitate joint operations, and it will likely seek to disrupt that capability with kinetic attacks or cyber operations. Further, any infrastructure elements owned or manufactured by Chinese companies should be assumed to be compromised.

Tactical Technologies

AI/ML

AI/ML will serve an important tactical purpose. Anything that can be safely automated and take cognitive load off a commander will allow more time for tasks only a human can do. Further, AI/ML-enabled training and simulation models will help personnel anticipate the complexities of a battlefield.

AI/ML will have the following tactical applications in future conflict:

- » AI/ML-enabled systems will eventually be able to take much of the command-and-control burden off a battlefield commander—they can send a drone swarm to collect information, identify targets and “decide” whether those targets need more investigation, and flag items of highest concern, leaving the commander more time to focus on more pressing priorities.
- » With future advances in AI/ML, AI-embedded swarming drones could be programmed to identify approaching, potentially hostile targets and observe, and engage, if ordered. Drone swarms could obscure vision, disrupt

communications, and even cause physical damage. At a more advanced level, the swarm could learn how to prioritize targets or split to cover multiple targets.

- » For intelligence work, AI/ML could help with the ubiquitous technical surveillance that makes modern HUMINT operations challenging. Algorithms could develop tricky surveillance detection routes based on what the service knows about patterns of life for counterintelligence officers, CCTV cameras, and traffic. AI could also use deepfake technology to create a robust cover identity for officers, complete with social media profiles, photos and videos, and call histories.

ROBOTICS

Military personnel often put their lives on the line when securing perimeters, disposing of improvised explosive devices (IEDs), delivering fuel, and conducting reconnaissance missions. Robots and autonomous ground, subsea, or aerial vehicles can eventually replace or assist them in these operations, reducing casualties.

Military robots are already in use. The Multi-Utility Tactical Transport is a semi-autonomous Army unmanned ground vehicle (UGV). It is capable of transporting 1,200 pounds and providing 3,000 watts of power with low thermal and noise signatures.³² In 2021, the Israel Defense Forces revealed Jaguar, a six-wheeled, semi-autonomous UGV armed with a 7.62 mm MAG machine gun that can self-destruct if it falls into enemy hands.³³ Robotics will play an important role in future conflict in two ways.

- » Military robots can provide support to logistics and sustainment operations from the service to the squad level. They can carry heavy burdens, such as powerful batteries, retrieve and extract wounded soldiers from the front lines, clear mines, explore disaster sites, and conduct battle damage assessments. Any job too strenuous or too dangerous for a soldier could become the responsibility of robots.
- » Robotics can also play a role in ramping up industrial-scale production of munitions and other equipment. A great



Army personnel handling a Mark II Talon explosive ordnance robot during employment training on August 2, 2018, in Camp Hansen, Japan.

SOURCE: SMITH COLLECTION/GADO/GETTY IMAGES

power conflict in the future is likely to burn through huge stores of precision weapons, putting a heavy burden on the industrial base to replenish stocks quickly.³⁴ Robots could assist with fabrication, testing, and warehouse management, for example. Several companies are proving the value of cloud-connected, AI/ML-enhanced robots, and MIT is working at the cutting edge of robotic dexterity.³⁵

BIOENGINEERING

Bioengineering can play a critical role in keeping soldiers healthy, but it could also be used to conduct surveillance, micro-target individuals or populations, and create advanced weaponry.

Among other use cases, bioengineering will have the following applications:

- » Biomedicine, including bioengineering, will be increasingly capable of enhancing soldiers' performance and enabling them to stay active, for example, by maximizing health and alertness in high-stress environments, creating bridges for wearable technology and human-machine teaming, and even creating field dressings and bandages that can seal a wound.³⁶ The private sector's efforts to perform brain manipulation for enhanced cognitive clarity and lowered sleep requirements will have direct offensive and defensive military applications.³⁷
- » Biosensors could be a game changer for surveillance, either at the individual or population levels. DNA markers can track a person, while governments can track the health of a population through biosensing.³⁸ Similarly, biosensors could be tailored to flag certain chemicals and other types of contamination as well as complex signatures such as radiation, acoustics, and electromagnetism.³⁹ Biological compounds could be used to tag specific items or individuals and track their progress or verify their identity.
- » The dark side of bioengineering could lead to sophisticated and deadly bioweaponry, including genetically modified pathogens to which humans have no natural immunity and that are resistant to vaccines.⁴⁰ Scientists could also create specialized toxins that disrupt water or food supplies. Understanding the possibilities—and what an adversary with little regard for human life could do with them—will be critical to defense, including detection and antidotes.

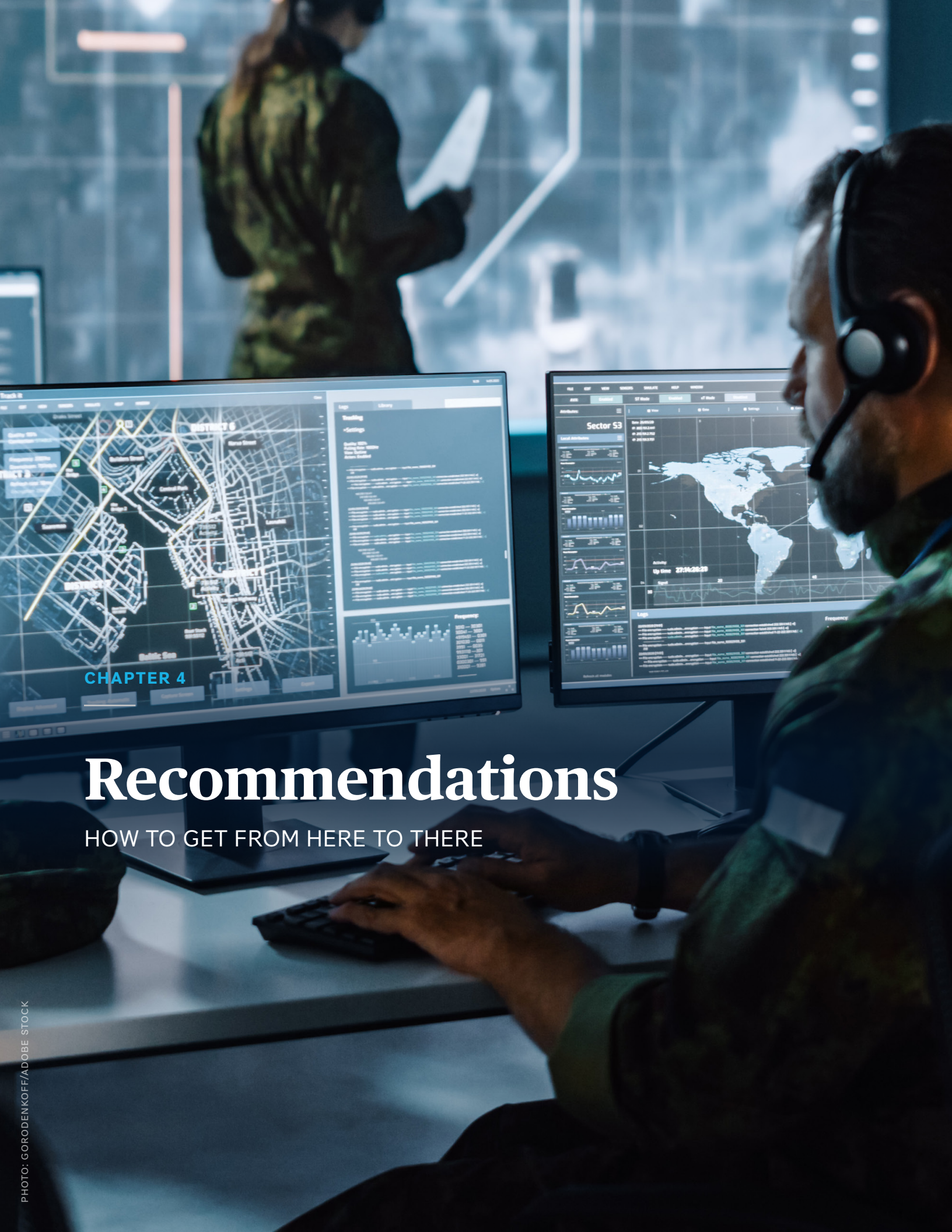
HIGH-PERFORMANCE BATTERIES

The tactical applications of batteries are as varied as commercial applications, but swapping today's heavy, bulky batteries for long-lasting, light, and reusable ones could yield a critical edge in intelligence and war. Vikram Mittal wrote in *Forbes*: “And just as King Richard III lost a battle because of a horse, future armies can lose a battle because of a dead battery.”⁴¹ Today's military cannot fight without power, and the fights of the future could be far from fuel sources.

Among other applications, high-performance batteries will have two important use cases:

- » Long-lasting batteries will power everything from an individual soldier's communications package to battlefield drones to long-dwell undersea vehicles; those batteries could recharge through the motion of the waves or occasional surfacing for solar power. Long-lasting batteries will help power miniaturized satellite space technology as well.
- » Miniaturized batteries will be essential for covert and clandestine surveillance and communications devices, which are sometimes crafted to look like an everyday object. Insect-sized microbots could infiltrate a hostile area unnoticed or facilitate search and rescue.⁴²

According to an article by Nadia Schadow and Arthur Herman in the *Wall Street Journal*, “During one five-year period at the height of the wars in Iraq and Afghanistan, more than 3,000 American soldiers and contractors were killed in fuel-supply convoys.”⁴³ In the intervening years, the need for fuel has only grown, with soldiers running miniaturized surveillance drones out of backpacks and operating weapons systems off laptops. Expeditionary forces must carry their own fuel and power with them, leading to an estimated 30 to 50 pounds of batteries for a three-day mission.⁴⁴ A conflict in the Pacific is likely to be spread over huge distances and to require long logistics tails, risking far more lives than in Iraq and Afghanistan.



Recommendations

HOW TO GET FROM HERE TO THERE

“HAVING A GRAND VISION IS GREAT, BUT WHO DO I EMAIL ON MONDAY MORNING TO CHANGE THE WORLD?”

—Leading UK defense official⁴⁵

While earlier sections of this paper described needed capabilities and their requisite technologies, this section recommends ways for the U.S. government to find, nurture, and procure those technologies in conjunction with industry partners.

First, this section will further discuss the three technologies that require a sprint. These technologies are classified as “sprint” because they fit one or more of three criteria: the need is urgent; lead times for research and development (R&D) are long; or first-mover advantage will be significant, and the United States is in danger of falling behind. Next, it will discuss the other four technologies—which this report classifies as follow technologies—where the U.S. government can encourage, nurture, and signal demand while largely following the lead of industry’s innovations.⁴⁶ Third, this section will cover the role of industry and government and how the two must collaborate. Finally, the section closes by providing recommendations for government to improve acquisition and develop a capable workforce, which were constant themes in the project’s discussions with industry and government officials alike.

Sprint Recommendations: Commit Resources and Senior-Level Focus

The following three technology areas require a sprint. The U.S. government should give a high priority to nurturing private sector research, conducting in-house R&D for military-specific functions, and funding these areas as if the United States were in a conflict.

SECURE AND REDUNDANT COMMUNICATIONS

Creating redundant and secure communications networks should be a top priority for the U.S. government. Today, setting up that communications capability in the field is challenging at best. According to a U.S. Army study, tent-based command posts require “hours of setup, including thousands of feet of copper wiring, which delays network availability and results in a dangerous lack of situational awareness for commanders. . . . Entering a dynamic tactical environment ‘blind’ puts warfighters at a significant disadvantage, which can lead to loss of life and mission failure.”⁴⁷ While allies are building to match the United States’ highly networked approach, space has become a contested domain, concern has grown around the vulnerability of undersea cables, and Huawei’s global expansion has called into question which information and communications technology (ICT) networks are secure.

The goal should be self-healing mesh networks, such that an adversary would need to take out several communications nodes to impinge on an ally’s ability to function. Creating secure, redundant communications will involve layers of technologies, and those layers will vary based on the situation. Redundancy will be a combination of satellite and ground-based capabilities, and truly effective communications systems will be secure and seamless across services. As a CSIS report on communications networks noted:

Dissimilar platforms can be integrated to share data by using common communication links or connecting through communication hubs. For example, NATO uses Link 16 for tactical data links, and more than 5,000 different platform types across the alliance incorporate Link 16 into their communications capabilities. . . . It also may not be cost feasible to upgrade some legacy platforms to include common data links such as Link 16. In these instances, the best alternative may be to create communications hubs or teleports that house a variety of different communications systems and can connect across any number of them. These communications hubs can be at fixed ground sites, on airborne platforms, or in space.⁴⁸

Getting to a seamlessly connected fighting force will require coordinated purchasing decisions that factor in encryption, resilience against cyberattacks and physical damage, and interoperability. Services will need to adopt a mindset of jointness first and specific needs second to make this mesh network a reality. Further, contracts should require interoperability with existing systems and the capability to work with NATO and other allied communications systems. A cross-service, civilian-led study group should establish a path from current capability to an ideal capability and budgets for getting from here to there in two, five, and ten years, to be submitted to the secretary of defense and Congress.

QUANTUM TECHNOLOGY

As one interviewee put it, “Where we believe there is a strong first-mover advantage of the tech, we need to sprint. With quantum, the real advantage is being first.”⁴⁹ Government investment will be necessary in a range of areas, including researching quantum networking and implementing quantum-resistant encryption standards across the government. Quantum research is expensive and long term; to drive progress, DOD needs to signal government demand for quantum over the long run. One approach would be to contract for a series of small milestones, rather than a finished product, or to signal an intent to purchase precursor equipment, perhaps even buying equipment and leasing it back to scientists to signal commitment to the field.

A quantum sprint will require encouraging bright scientific minds to turn their sights on quantum advances. According to McKinsey, there is only one qualified candidate for every three quantum jobs, and by 2025, less than 50 percent of quantum computing jobs will be filled.⁵⁰ DOD, in partnership with universities, can launch summer fellowships for high school students to foster intellectual interest in quantum

science and encourage young people to build quantum-relevant knowledge and skill sets. The intelligence community can build on the Intelligence Community Centers of Academic Excellence Program by adding a quantum track of study.⁵¹ Both DOD and the intelligence community can sponsor data scientists to spend a two-year tour with industry partners working on quantum science, which would create awareness and information exchange on both sides.

By 2025, less than 50 percent of quantum computing jobs will be filled.

BIOENGINEERING

Much of the energy behind bioengineering is in the medical industry, which could serve a dual-use function with some military requirements. However, applications such as self-healing textiles, high-temperature compounds, and emergency field medicine are likely to get less attention without the U.S. government signaling strong demand.

Research into defensive applications is also essential and urgent. The U.S. government must assume that U.S. adversaries are likely exploring weapons applications for bioengineering and should devote extensive resources to understanding the potential uses well enough to create both norms and effective defense. That will likely take the form of highly classified and restricted R&D, diplomatic efforts to describe the threat and the need for international rules, and collaboration with industry to ensure that potentially harmful applications are effectively controlled. Computer scientists and ethicists recognize the perils of an AI system with no moral compass creating new biological and chemical compounds and functions, making the establishment of norms and rules for this combination of technologies urgent.⁵² Creating effective defense will require a close collaboration between cutting-edge researchers in government and industry.

A large, heterogenous collection of well-sequenced and well-curated genomes will be necessary to many bioengineering

advancements.⁵³ This collection will supply the necessary genes or combinations that would enable biomedical interventions.⁵⁴ However, the U.S. government will need to build in stringent privacy protections, likely partnering with private entities, in order to access the information needed while gaining public trust.

Follow Recommendations: Encourage and Manage Developments

With the following four technologies, the U.S. government can encourage industry down the path they are currently pursuing and make minor changes to commercial-off-the-shelf (COTS) products to accomplish the government's needs. These technologies are ordered from areas where the government needs to be most involved to least involved in order to develop the capabilities the government most needs.

SPACE-BASED SENSORS

Industry has a robust capability for launch and for building satellites, from CubeSats to sophisticated communications networks. The government can go along for that ride and also encourage the creation of sensitive sensor packages and on-orbit processing of data. This industry is well funded, so the government could hold competitions to signal demand, for example, for the most effective on-orbit deployment of AI/ML-enabled computing power to tip and cue off satellite images, or a sophisticated hide-and-seek competition where industry must use automation to find an object the U.S. military or intelligence community has hidden somewhere in the world. That competition could also find signals, such as a beacon, or a chemical signal, to encourage development of a variety of sensors.

HIGH-PERFORMANCE BATTERIES

The commercial sector has a huge financial incentive to create long-lasting and sustainable miniaturized batteries. From screens that fold to devices connected to the internet of things (IoT), the demand for commercial battery solutions is rising.⁵⁵ For example, the medical industry is driving extreme miniaturization in order to create wearable diagnostics and implantable medical devices.

Military demand will share some overlap, but high-end military requirements will be for longer-lasting, more stable, and heat-free solutions, particularly batteries that do not degrade when exposed to water or in extreme heat or cold. Military acquisition experts should look for the 80 percent solution and the 100 percent solution as two different requirements:

COTS products will do 80 percent of the job providing power for military needs, but in a small percentage of use cases, such as stealthy special forces missions or underwater use, only the 100 percent solution will do. Those small-percentage use cases should be built and bought separately.

Military acquisition experts should look for the 80 percent solution and the 100 percent solution as two different requirements.

Most likely, the demand created by the U.S. government will translate into unforeseen commercial applications. The U.S. government should purchase, or pledge to purchase, a small number of products from a handful of innovative battery companies that are currently producing batteries in the 80 percent solution category but seem capable of meeting the high-end need in the near future. That U.S. government signaling will lead to additional private investment. For example, NSIC funded a battery start-up that created highly flexible, non-flammable batteries. NSIC's early funding helped the company achieve key technical milestones, and private venture capital funds followed with additional investment.⁵⁶

AI/ML

AI/ML development is robust in the commercial sector, and many companies are pursuing a dual-use strategy. DOD has a role to play in driving innovation in specific use cases of the technology as well as in establishing high standards for integrity and security of AI/ML systems. It should further establish robust protocols around data integrity throughout the AI/ML adoption cycle, from acquisition to integration.

The following recommendations can support DOD in advancing AI/ML development and acquisition:

- 1 As an interviewee noted, AI is ready for data analysis but not ready to be fielded yet due to its lack of advanced reasoning capabilities.⁵⁷ In its quest to achieve advances in AI capabilities, DOD should establish and fund research

programs that explore complex algorithms, new learning methods, and hybrid techniques, such as neuro-symbolic AI.⁵⁸ Neuro-symbolic AI research, in a shift away from purely data-centric approaches, meshes the properties of symbolic logic and deep learning to achieve systems that excel at both pattern recognition and causal structure comprehension.⁵⁹ DOD is already thinking about what kinds of AI/ML capabilities could assist in specific problem sets.⁶⁰ In considering those use cases, the department must align its acquisition and adoption practices to meet the necessary capabilities. DOD should first identify a clear set of AI/ML use cases for each agency and clearly communicate those needs with start-ups and industries looking to enter the defense market. Each agency should have a plan for AI/ML adoption, a person or group of people responsible for implementing that plan, and accountability mechanisms to agency leadership for managing the incorporation of AI/ML technology. The intelligence community can begin by updating Intelligence Community Directive 203 to begin to describe analytic standards for use of AI/ML.

- 2 DOD and the intelligence community must urgently find a middle ground between security of data and systems and allowing private entities access to U.S. government data for training AI/ML systems and testing government applications. The government should create two tiers: (1) a sanitized, likely public data set that researchers can use to train and develop AI/ML, and (2) a restricted sandbox where vetted industry partners can work and demonstrate capability. For the latter, the default should be access for U.S. companies, with security officers needing to show security concerns rather than the applicant needing to prove a lack of vulnerabilities. Further, DOD and the intelligence community should have appeal mechanisms for decisions by a security officer, likely ending with the deputy secretary or deputy director of the agency in question.⁶¹

ROBOTICS

Industry is witnessing a growing shift to modular industrial and collaborative robots that are smaller, more agile, and designed to facilitate human-machine teaming. Large companies and small start-ups are loading robotic systems with cloud-enhanced capabilities and AI/ML software to add autonomous features.⁶² MIT is using AI/ML to teach robotic arms how to manipulate and reorient objects in various holding positions.⁶³ According to an interviewee, the robotics industry will trend toward intelligent robots integrated with AI/ML and open-source software.⁶⁴

Generally, what the military needs will be readily transferable from COTS products. Ruggedness and dependability will be the main additional requirements. Once again, the kind of advancements

the military needs can be encouraged by competitions for robots to accomplish tasks in harsh environments, with minimal fuel usage, and to act predictably when they lose connection, such as using a “home base” functionality. The U.S. government should explore collaboration with industry partners who have solved complex logistical problems with the help of robotics and explore options for incorporating those solutions into DOD practices.

Adapt Government Practices

The government was once the only player with the capital and demand to drive innovation at scale, but now private sector entities have the cash, talent, and incentives—and lack the restrictions and rules that bind the federal government. Further, universities and others outside DOD’s traditional orbit are leading innovation in key areas.⁶⁵ The government’s acquisition processes largely focus on requests for proposals (RFPs) asking for bespoke products on long time horizons—a structure that makes government contracts risky for small and medium-sized companies. As a result, the government finds itself simultaneously celebrating private sector innovation and struggling to take advantage of new technological advances.

Still, the mission focus of the government means that where there is a will, there is a waiver. During a crisis, committed patriots in the government find ways to speed up processes and find ways through or around the maze of restrictions. The Ukraine conflict has been a prime example of this mindset, from the rapid delivery of advanced systems and training to bolting HARMs missiles on a MiG-29.⁶⁶ Conflicts of the future will require similar urgency, inventiveness, and “why not” thinking. The government needs a shift in the understanding of risk and a preemptive urgency that will accelerate the progress already underway.

**The mission focus of the
government means that
where there is a will, there
is a waiver.**

Those who argue against preemptive urgency and against committing the needed resources cite two arguments: First, they point to the United States' industrial prowess during World War II and assume that a similar outcome would materialize should a conflict erupt tomorrow. This argument often ignores that the United States began creating the industrial capacity to accomplish technological dominance years before entering the war, allowing a significant ramp up to a wartime footing, and that supply chains are far more globalized today.⁶⁷ Second, critics argue that accelerating toward a wartime footing will provoke the very outcome the country seeks to avoid. The flaw in that argument is that deterrence is impossible without a credible ability to respond to a threat, and that credibility will come from demonstrating that the United States can compete today and is committed to winning a fight in the future.⁶⁸ The real risk comes from doing nothing. As one interviewee put it: "People don't understand risk. By saying they won't do risky projects, they are transferring risk to the warfighter. [A] Congress not willing to take risks . . . could endanger soldiers by giving them bad software and tech. We need a new way of thinking about this."⁶⁹

ACQUISITION

"Government should just buy what they say they want. If they really believe 'AI is the future,' then buy some AI. Only 0.4 percent of the budget is going to AI. If it's so important, why not invest 1 percent or more? Congress and senior leadership say it's important. So, move to a wartime footing by buying what they want."⁷⁰

- Interviewee

While this quote captures the correct sentiment, just buying what the government says it wants is not that easy. One major problem is that the government's descriptions of what it wants are overly detailed and focus on requirements, not capabilities.⁷¹ That practice takes a COTS solution that meets 80 percent of the need out of contention for winning a contract; the alternative is to rework the product, potentially spending millions, in the hopes of recouping that money by winning the contract. Further, a maze of regulations dictates who can even compete for contracts, creating a barrier to entry for small firms that do not have an army of lawyers to navigate those requirements.

The U.S. government should consider these recommendations:

- 1 DOD and the intelligence community should create alternative acquisition processes for purchases that do not buy a complete capability but rather signal government demand to the markets. These purchases might include a limited

run of equipment, an initial proof of concept, or even a briefing of a capability. A new DOD initiative called National Security Innovation Capital, part of the Defense Innovation Unit, is operating along these lines, helping hardware startups accelerate the development of products with small investments.⁷² The Office of Strategic Capital is also attempting a new model for DOD acquisition: providing "patient capital" to companies.⁷³ Congress should lean forward on multiyear funding for technology projects, particularly for those with long lead times, like quantum computing.

- 2 DOD and the intelligence community should also begin to create a test and evaluation strategy for each of the seven technologies, perhaps most urgently for AI-embedded technology. In that area the U.S. government and vetted partners should create context-specific test data sets for training the eventual algorithms.⁷⁴
- 3 The government should also retrain a portion of the acquisition workforce—including the lawyers who oversee it—specifically on technology acquisition practices, emphasizing quick turnarounds and how to creatively work within existing regulations, like making use of flexible indefinite delivery, indefinite quantity (IDIQ) contracts. Retraining should include incentives for accepting risk and creating efficiencies to support the mission.
- 4 Contracting officers having personal liability for contracts is also a huge obstacle to greater risk acceptance; DOD lawyers should find ways to guard against corruption that are less of a deterrent to taking calculated risks. In the longer term, a zero-based review of software acquisition should evaluate why each step in the process is necessary and brainstorm how to cut the number of steps by 75 percent.⁷⁵ The Commission on Planning, Programming, Budgeting, and Execution (PPBE) Reform is working on critical reforms, including considering potential alternatives to current practices, and researchers look forward to their findings.⁷⁶

WORKFORCE

Interviewees for this project unanimously agreed that creating a tech-savvy workforce would be necessary to implementing any of these technologies. As one interviewee put it, "you need to think about capabilities that the U.S. government will require to develop and use these technologies. It includes talent, public-private relationships, education, and agility in the government's ability to assess and support these techs."⁷⁷ Kenneth Werrell, in an Air University report, stated it simply: "High-technology weapons demand high-quality personnel."⁷⁸

DOD and Congress should consider the following recommendations:

- 1 Military services should create technology-focused career paths for uniformed personnel. Fully incorporating technological advancements will require personnel who are curious and open to trying new approaches and have a solid grounding in the possibilities associated with new technologies.⁷⁹ Part of their training could be “externships” in industry. To pay it forward, the military could incentivize retiring veterans to get teaching certificates, especially in science and technology. Since many military recruits are from military families, Congress should create grant programs for schools on and around military bases that will create an elite-caliber science, technology, engineering, and medicine (STEM) curriculum, starting in elementary school and providing military technology apprenticeships in high school.
- 2 In addition to uniformed and civilian personnel in the executive branch being tech savvy, Congress needs a solid knowledge base on how these technologies can make or break a modern military. The Congressional Research Service should significantly bolster its cadre of technologists, and Congress should undertake a briefing program for members and staff on its appropriations, armed services, and intelligence committees, along with the personal office staffs of those who serve on those committees. Several universities like MIT and Stanford conduct immersion programs for members and staff, and research institutions in D.C. also have executive education programs that can provide a short course in technology policy.

Part of bolstering workforce competencies in emerging technologies will be training personnel in human-machine teaming. These trainings must create trust and help personnel understand the limitations of these technologies.

Conclusion

The adversary also gets a vote, and Beijing and Moscow are surely eyeing U.S. technological prowess with concern. As CSIS's Jim Lewis put it, "The Russians and Chinese worry about American space and anti-satellite attack, cyberattack, hypersonic strike, precision-guided munitions, electronic warfare, autonomous weapons and vehicles, and robots linked to AI. They worry that these technologies give the United States a strategic edge."⁸⁰ They need to stay concerned. In order to maintain a deterrent, the U.S. national security apparatus needs vision and humility—vision to see the capabilities needed to prevail in competition and humility to let industry partners provide solutions off the shelf that achieve most of the U.S. government's needs. Where the requirements really must be bespoke and nonnegotiable, the partnership between industry and government will be able to create that game-changing technology.

As one interviewee who works in venture capital said: "We have a window into the future now. The private sector has it, not the military."⁸¹ A collaborative group of industry, capital investors, government, and scientists will create that future if given a chance. ■

Below the Line: Technology That Almost Made the List

This project aimed to create ruthless prioritization for DOD and the intelligence community, and that meant leaving some technologies that are still quite important to national security below the line. These were left out because the technology was more evolutionary than revolutionary, the commercial market was robust, the applications would be important but not critical in the spectrum of conflict, or they were more relevant to economic prowess than national security. Some are a subcomponent of the listed technologies above. These technologies are listed below in a rough order of importance:

FINTECH

Financial technologies, such as electronic payment systems and digital assets, have growing power in the global economy.⁸² WeChat Pay has an extensive global reach, handing China the ability to affect financial transactions or collect information.⁸³ The cryptocurrency markets have been a roller coaster of late, but the promise of a secure, globally relevant currency that sidesteps the influence of the dollar must be tantalizing to sanctioned regimes.

ADDITIVE AND SMART MANUFACTURING

Far-flung units will likely need to be self-sufficient not only in fuel but also in spare parts. Contested logistics chains will make it difficult to rebuild broken equipment, and the United States and its allies will not be able to afford losing key units to broken communications or a failed engine in a conflict. Intelligence work often requires highly specialized parts, and “printing” one can be both more cost effective and less vulnerable to exposure.

REDUCED CARBON FOOTPRINT OF THE MILITARY

Green technology could create innovative ways to power a modern military with less impact on the environment and, by extension, lower costs. The military can signal demand in this area, but it is highly likely to be following commercial applications.

AUTOMATED REASONING

Automated reasoning attempts to answer questions about a program (or a logic formula) by using known techniques from mathematics. Using logic, rather than computing direct

answers, can shortcut thousands of hours of computations and streamline programming.⁸⁴ It could underpin advancements in a wide range of computer science applications.

MICROELECTRONICS AND NANOMANUFACTURING

Also a foundational technology, microelectronics and nanomanufacturing will enable the miniaturized devices discussed above and will pack more computing power into a small, light, and portable piece of kit. Commercial applications of nanomanufacturing are vast and are opening the door to potential military and intelligence uses. Because these commercial efforts are so robust, and the transfer into national security applications is relatively straightforward, this technology just missed the top seven.

SYNTHETIC TRAINING ENVIRONMENTS AND SIMULATION

AI/ML systems need copious amounts of data to “learn” the world. Finding enough real-world data to train these systems can be challenging, in particular if the AI/ML is looking for an uncommon object, such as a submarine. Synthetic data is generated artificially but mimics the real world and can be used to increase the volume of training data introduced to an AI/ML program. As an interviewee said, “If you can mathematically emulate a phenomenon or system and simulate it, digitally perfecting it, you can build it for a lot cheaper in the real world.”⁸⁵

If I Had a Billion Dollars . . .

Participants in the roundtable and interviewees were given a theoretical billion dollars to spend on one technology initiative; researchers took this approach to push participants to prioritize their own lists of important technologies. Some of the answers aligned with the technology list above; others were surprising. A comprehensive list of their choices is below:

- 1 Develop AI/ML, especially for autonomy. (This answer received a plurality of votes.)
- 2 Develop self-healing and redundant communications. (This was a favorite among uniformed military participants.)
- 3 Leverage quantum sensing in space.
- 4 Create a commission that will rebuild acquisition practices from the ground up. (This answer received laughs and knowing nods of approval.)
- 5 Fix the supply chain.
- 6 Create nationwide electric vehicle infrastructure.
- 7 Bolster the defense of Taiwan. (As one participant explained, “All we are currently doing for Ukraine, we should also do for Taiwan.”)
- 8 Support candidates for office who are willing to invest in technology and take risk in government contracts.
- 9 Invest in K-12 STEM education. (This answer also received support from the room.)

Mapping Technologies to Capabilities

CAPABILITY: EXQUISITE SENSING

- AI/ML
- Quantum Sensing
- Space-Based Sensors
- Bioengineering

CAPABILITY: ASSET COMMUNICATIONS

- High-Performance Batteries
- Quantum Computing
- Redundant Communications
- AI/ML

CAPABILITY: RAPID DECISIONMAKING

- AI/ML
- Robotics

CAPABILITY: SHOCK WITH TECH PROWESS

- All Play

CAPABILITY: SIGNAL FROM NOISE (TIP AND CUE)

- AI/ML
- Quantum Sensing
- Quantum Computing
- Space-Based Sensors

CAPABILITY: MOBILE, SELF-SUFFICIENT EXPEDITIONARY UNIT

- Bioengineering
- High-Performance Batteries
- Robotics
- Redundant Communications

CAPABILITY: AUTONOMY TO PENETRATE CONTESTED LOGISTICS

- Robotics
- AI/ML
- Redundant Communications

Contributing Experts

The authors would like to extend their gratitude for the insights and feedback provided by the experts who took part in the “Critical Technologies for National Security” roundtable or participated in expert interviews. The authors interviewed a wide range of experts in government, industry, and venture capital, including those listed below. Since the interviews and roundtable were conducted under Chatham House Rule, only experts who agreed to be included are listed. The listed experts participated in their individual capacities and neither their comments, nor this report’s findings and recommendations, reflect the positions of their respective organizations, departments, or agencies. The authors would also like to thank government officials who contributed their time to this project in their personal capacity. While these experts provided insights that informed the report, the conclusions and recommendations are those of the authors.

BILAL ZUBERI

General Partner, Lux Capital

BIZ PEABODY

Director of Defense Policy and Business Development, Shield AI

CHRIS BROSE

Chief Strategy Officer, Anduril Industries

JACQUELINE S. TAME

Director of Government Affairs, PsiQuantum

JAMES LEWIS

Senior Vice President, Pritzker Chair, and Director of the Strategic Technologies Program, CSIS

JENNIFER M. STEWART

Executive Vice President for Strategy and Policy, National Defense Industrial Association

JOSEPH IMWALLE (RET. COL)

Senior Director of Space & C2 Systems, Raytheon Intelligence & Space, Raytheon Technologies

KARI BINGEN

Senior Fellow and Director of the Aerospace Security Program, CSIS

KATHRYN WHEELBARGER

Vice President, Global Program Support, Lockheed Martin Corporation

DR. PAUL KILLWORTH

Deputy Chief Scientific Advisor for National Security, UK GCHQ

RAJ SHAH

Managing Partner, Shield Capital

DR. STEFANIE TOMPKINS

Director, Defense Advanced Research Projects Agency

HON. SUE GORDON

Board Member, Defense Innovation Board; Former Principal Deputy Director of National Intelligence

DR. TARA O'TOOLE

Executive Vice President and Senior Fellow, In-Q-Tel

TEX SCHENKKAN

Director, National Security Innovation Capital

About the Authors

Emily Harding is deputy director and senior fellow with the International Security Program at the Center for Strategic and International Studies (CSIS). She joined CSIS from the Senate Select Committee on Intelligence (SSCI), where she was deputy staff director. In her nearly 20 years of government service, she has served in a series of high-profile national security positions at critical moments. While working for SSCI, she led the committee's multiyear investigation into Russian interference in the 2016 elections. The five-volume, 1,300-page report reshaped the way the United States defends itself against foreign adversaries seeking to manipulate elections, and it was lauded for its rigor, its thoroughness, and as the only bipartisan effort on election interference. During her tenure on the committee, she also served as the subject matter expert on election security, counterintelligence and associated cybersecurity issues, and the Middle East. She oversaw the activities of 18 intelligence agencies and led SSCI staff in drafting legislation, conducting oversight of the intelligence community and developing their expertise in intelligence community matters.

Harshana Ghoorhoo is a research assistant with the International Security Program at CSIS. Prior to joining CSIS, she interned with the Modern War Institute at West Point Academy where she researched urban warfare and military strategy during the Revolutionary War. Her current research focuses on artificial intelligence, emerging technology and sustainability, and Indian technology innovation. She holds a bachelor of science in international relations and a bachelor of arts in philosophy and modern languages from Seton Hall University.

Endnotes

- 1 Interviewee #13. Note: All interviews were conducted under Chatham House Rule, hence interviewees are cited anonymously, with the exception of interviewees who agreed to be quoted and cited by name or affiliation.
- 2 Interviewee #11.
- 3 That said, predicting the future of warfare is notoriously difficult. As then-defense secretary Bob Gates said in 2011 during a speech at West Point Academy, “When it comes to predicting the nature and location of our next military engagements, since Vietnam, our record has been perfect. We have never once gotten it right.” (See Robert Gates, “Final Address to U.S. Military Academy Cadets,” speech delivered February 25, 2011, West Point, NY, <https://www.americanrhetoric.com/speeches/robertgateswestpointspeech.htm>.) Given this difficulty, the United States should attempt to minimize uncertainty at the high end of a conflict, so that a potentially existential fight is winnable, while capitalizing on opportunities to position well for an era of global competition.
- 4 Paul Mozur and Aaron Krolik, “A Surveillance Net Blankets China’s Cities, Giving Police Vast Powers,” *New York Times*, December 17, 2019, <https://www.nytimes.com/2019/12/17/technology/china-surveillance.html>; and Catarina Demony and Pedro Nunes, “Chinese embassy in Lisbon removes CCTV camera after residents’ concern,” Reuters, January 19, 2023, <https://www.reuters.com/world/chinese-embassy-lisbon-faces-scrutiny-over-surveillance-cameras-2023-01-19/>.
- 5 Emily Harding, *Move Over Jarvis, Meet OSCAR: Open-Source, Cloud-Based, AI-Enabled Reporting for the Intelligence Community* (Washington, DC: CSIS, January 2022), <https://www.csis.org/analysis/move-over-jarvis-meet-oscar>.
- 6 Special Competitive Studies Project (SCSP), *The Future of Conflict and the New Requirements of Defense*, Defense Panel Interim Panel Report (Washington, DC: SCSP, October 2022), <https://www.scsp.ai/2022/10/scsp-defense-panel-releases-interim-panel-report/>.
- 7 Interviewee #7.
- 8 Mauro Gilli, “Beware of Wrong Lessons from Unsophisticated Russia,” *Foreign Policy*, January 5, 2023, <https://foreignpolicy.com/2023/01/05/russia-ukraine-next-war-lessons-china-taiwan-strategy-technology-deterrence/>.
- 9 World Economic Forum, *State of Quantum Computing: Building a Quantum Economy* (Geneva: World Economic Forum, 2022), https://www3.weforum.org/docs/WEF_State_of_Quantum_Computing_2022.pdf; “What is asymmetric encryption?,” Cloudflare, <https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/>.

- 10 David L. Chandler, “Quantum sensor can detect electromagnetic signals of any frequency,” MIT News, June 21, 2022, <https://news.mit.edu/2022/quantum-sensor-frequency-0621>.
- 11 Rajesh Uppal, “Quantum navigation is emerging technology for GPS-denied and deep space environments,” International Defense, Security & Technology, October 20, 2020, <https://idstch.com/technology/quantum/quantum-navigation-emerging-technology-for-gps-denied-and-deep-space-environments/>.
- 12 “Synthetic Biology Explained,” Biotechnology Innovation Organization, n.d., <https://archive.bio.org/articles/synthetic-biology-explained>.
- 13 Steven A. Benner and A. Michael Sismour defined synthetic biology as having two subfields: “One uses unnatural molecules to reproduce emergent behaviors from natural biology, with the goal of creating artificial life. The other seeks interchangeable parts from natural biology to assemble into systems that act unnaturally.” In other words, synthetic biology seeks to adjust—or even construct—core components that will perform in certain ways, then assemble those parts into larger, engineered systems. Steven Benner and Michael Sismour, “Synthetic Biology,” *Nature Reviews Genetics* 6 (2005): 533-543, <https://www.nature.com/articles/nrg1637>. See also “What is Bioengineering?,” Berkeley Bioengineering, n.d., <https://bioeng.berkeley.edu/about-us/what-is-bioengineering>.
- 14 The authors discuss batteries specifically in this paper, but power generation and storage will likely go beyond traditional batteries. For example, an interviewee pointed out the potential of betavoltaics and fuel cells for expeditionary energy.
- 15 Interviewee #7.
- 16 Interviewee #12; Interviewee #15.
- 17 “What is Quantum Sensing?,” BAE Systems, n.d., <https://www.baesystems.com/en-us/definition/what-is-quantum-sensing>.
- 18 Gaura Batra et al., “Shaping the long race in quantum communication and quantum sensing,” McKinsey & Company, December 21, 2021, <https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/shaping-the-long-race-in-quantum-communication-and-quantum-sensing>.
- 19 Melody Redman et al., “What is CRISPR/Cas9?,” *Disease in Childhood - Education and Practice* 101, no. 4 (2016): 213-215, doi:10.1136/archdischild-2016-310459.<http://dx.doi.org/10.1136/archdischild-2016-310459>
- 20 Meriem El Karoui, Monica Hoyos-Flight, and Liz Fletcher, “Future Trends in Synthetic Biology,” *Frontiers* 7 (August 2019), doi:10.3389/fbioe.2019.00175.
- 21 Daniel Pereira, “Bio-Futures 2050: Defense Impacts and Opportunities for Advantage,” OODA Loop, August 16, 2022, <https://www.oodaloop.com/archive/2022/08/16/bio-futures-2050-defense-impacts-and-opportunities-for-advantage/>.
- 22 Diane DiEuliis, Peter Emanuel, and Brian Feeney, “Study Predicts Bio-Tech’s Long Impact on Defense,” *National Defense Magazine*, August 1, 2022, <https://www.nationaldefensemagazine.org/articles/2022/8/1/study-predicts-biotechs-long-term-impact-on-defense>.

- 23 Ibid.
- 24 Interviewee #13.
- 25 Interviewee #5.
- 26 Debra Werner, “HyspecIQ Selects Advisers, Offering Clues to Early Applications,” *SpaceNews* (blog), December 14, 2021, <https://spacenews.com/hyspeciq-selects-advisers/>.
- 27 Tomas Kellner, “How Amazon’s Project Kuiper Is Building Satellites to Survive Extreme Conditions in Space,” Amazon News, October 27, 2022, <https://www.aboutamazon.com/news/innovation-at-amazon/how-amazons-project-kuiper-is-building-satellites-to-survive-extreme-conditions-in-space>; Amazon Staff, “Amazon’s Project Kuiper Satellites Will Fly on the New Vulcan Centaur Rocket in Early 2023,” Amazon News, October 12, 2022, <https://www.aboutamazon.com/news/innovation-at-amazon/amazons-project-kuiper-satellites-will-fly-on-the-new-vulcan-centaur-rocket-in-early-2023>.
- 28 Mike Wall, “SpaceX reveals ‘Starshield’ satellite project for national security use,” *Space.com*, December 6, 2022, <https://www.space.com/spacex-starshield-satellite-internet-military-starlink>.
- 29 Micah Maidenberg, “SpaceX Limits Ukraine’s Military Use of Starlink Satellite Business,” *Wall Street Journal*, February 8, 2023, <https://www.wsj.com/articles/spacex-to-limit-ukraines-military-use-of-starlink-satellite-business-11675894401>.
- 30 Gilli, “Beware of Wrong Lessons from Unsophisticated Russia.”
- 31 Interviewee #8.
- 32 “Multi-Utility Tactical Transport (MUTT) UGV,” *Army Technology*, July 8, 2020, <https://www.army-technology.com/projects/multi-utility-tactical-transport-mutt-ugv/>.
- 33 Eyal Boguslavsky, “IDF unveils the Jaguar, its new revolutionary unmanned ground vehicle,” *Israel Defense*, May 6, 2021, <https://www.israeldefense.co.il/en/node/49744>.
- 34 Seth G. Jones, *Empty Bins in a Wartime Environment: The Challenge to the U.S. Defense Industrial Base* (Washington, DC: CSIS, January 2023), <https://www.csis.org/analysis/empty-bins-wartime-environment-challenge-us-defense-industrial-base>.
- 35 Evan Ackerman, “Q&A: Marc Raibert on the Boston Dynamics AI Institute> Boston Dynamics’ founder thinks creatively with \$400 million AI institute,” *IEEE Spectrum*, August 17, 2022, <https://spectrum.ieee.org/marc-raibert-boston-dynamics-institute>; “10 years of Amazon Robotics,” June 21, 2022, <https://www.aboutamazon.com/news/operations/10-years-of-amazon-robotics-how-robots-help-sort-packages-move-product-and-improve-safety>; and Rachael Gordon, “Dexterous robotic hands manipulate thousands of objects with ease,” *MIT News*, November 12, 2021, <https://news.mit.edu/2021/dexterous-robotic-hands-manipulate-thousands-objects-1112>.
- 36 Pereira, “Bio-Futures 2050.”
- 37 Interviewee #13.
- 38 Interviewee #5.

- 39 Pereira, “Bio-Futures 2050.”
- 40 “What is Bioengineering?,” Berkeley Bioengineering.
- 41 Vikram Mittal, “U.S. Soldiers’ Burden of Power: More Electronics Mean Lugging More Batteries,” *Forbes*, October 26, 2020, <https://www.forbes.com/sites/vikrammittal/2020/10/26/energy-management-a-deciding-factor-of-future-battles/?sh=272213942b1a>.
- 42 Amber Rose, “Novel designs help develop powerful microbatteries,” University of Illinois Urbana-Champaign: Materials Research Laboratory, January 12, 2023, <https://mrl.illinois.edu/news/novel-design-helps-develop-powerful-microbatteries>.
- 43 Arthur Herman and Nadia Schadlow, “A Good Battery Is the Best Defense Against a Military Assault,” *Wall Street Journal*, March 30, 2021, <https://www.wsj.com/articles/a-good-battery-is-the-best-defense-against-a-military-assault-11617136935>.
- 44 Todd South, “Can Soldiers Use Their Own Movement, Marching to Charge the Batteries They Carry? The Army’s Working on It,” *Army Times*, September 6, 2018, <https://www.armytimes.com/news/your-army/2018/09/06/can-soldiers-use-their-own-movement-marching-to-charge-the-batteries-they-carry-the-armys-working-on-it/>.
- 45 Conversation with a UK defense official.
- 46 Interviewee #14.
- 47 Charlie Kawasaki, “Four Future Trends in Tactical Network Modernization,” U.S. Army, January 14, 2019, https://www.army.mil/article/216031/four_future_trends_in_tactical_network_modernization.
- 48 Todd Harrison and Christopher Reid, *Battle Networks and the Future Force: Part 3* (Washington, DC: CSIS, March 2022), <https://aerospace.csis.org/battle-networks-and-the-future-force-part-3/>.
- 49 Interviewee #5.
- 50 Mateusz Masiowski et al., “Quantum computing funding remains strong, but talent gap raises concern,” McKinsey Digital, June 15, 2022, <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-computing-funding-remains-strong-but-talent-gap-raises-concern>.
- 51 Interviewee #15.
- 52 Justine Calma, “AI suggested 40,000 new possible chemical weapons in just six hours,” *The Verge*, March 17, 2022, <https://www.theverge.com/2022/3/17/22983197/ai-new-possible-chemical-weapons-generative-models-vx>.
- 53 Interviewee #13.
- 54 Ibid.
- 55 Haje Jan Kamps, “A Big CES 2023 Trend: All Battery Power, Everywhere, All the Time,” *TechCrunch*, January 7, 2023, <https://techcrunch.com/2023/01/07/batteries-batteries-everywhere/>.

- 56 Interviewee #16.
- 57 Interviewee #10.
- 58 Nathan Strout, Jen Judson, and Mark Pomerleau, “The Army sees a future of robots and AI. But what if budget cuts and leadership changes get in the way?,” *Defense News*, January 10, 2022, <https://www.defensenews.com/land/2022/01/10/the-us-army-put-experimentation-and-prototyping-at-the-core-of-its-modernization-initiative-is-it-working/>; and Jing Pei et al., “Toward artificial general intelligence with hybrid Tianjic chip architecture,” *Nature* 572 (August 2019): 106-111, <https://www.nature.com/articles/s41586-019-1424-8>.
- 59 Don Monroe, “Neurosymbolic AI,” *Communications of the ACM* 65 (October 2022), 10-11, <https://cacm.acm.org/magazines/2022/10/264844-neurosymbolic-ai/fulltext>; and Srishti Deoras, “What is Neuro-Symbolic AI and Why are Researchers Gushing Over It,” *Analytics India Mag*, May 1, 2020, <https://analyticsindiamag.com/what-is-neuro-symbolic-ai-and-why-are-researchers-gushing-over-it/>.
- 60 Dave Vergun, “Digital Transformation, AI Important in Keeping Battlefield Edge, Leaders Say,” Department of Defense, June 9, 2022, <https://www.defense.gov/News/News-Stories/Article/Article/3058028/digital-transformation-ai-important-in-keeping-battlefield-edge-leaders-say/>.
- 61 Interviewee #9.
- 62 Those companies include Amazon, Boston Dynamics, Waymo, Cruze, and Skydio. See Marcus Law, “Amazon warehouse robot uses AI to handle millions of items,” *Technology Magazine*, November 15, 2022, <https://technologymagazine.com/articles/amazon-warehouse-robot-uses-ai-to-handle-millions-of-items>.
- 63 Gordon, “Dexterous robotic hands manipulate thousands of objects with ease.”
- 64 Interviewee #2.
- 65 Interviewee #13.
- 66 Kyle Mizokami, “Somehow Ukraine Slapped U.S. Anti-Radar Missiles onto MiG-29 Fighter Jets,” *Popular Mechanics*, September 1, 2022, <https://www.popularmechanics.com/military/aviation/a41033452/ukraine-puts-harm-missiles-on-mig-29-fighter-jets/>.
- 67 See Arthur Herman, *Freedom’s Forge: How American Businesses Produced Victory in World War II* (New York: Random House, 2012).
- 68 Carol Kuntz, *Genomes: The Era of Purposeful Manipulation Begins* (Washington, DC: CSIS, July 2022), <https://www.csis.org/analysis/genomes-era-purposeful-manipulation-begins>.
- 69 Interviewee #7.
- 70 Interviewee #7.
- 71 Ibid.
- 72 “National Security Innovation Capital,” Defense Innovation Unit, <https://www.nsic.mil/>.

- 73 “Office of Strategic Capital (OSC),” Office of the Undersecretary of Defense, <https://www.cto.mil/osc/>.
- 74 Interviewee #13.
- 75 Harding, *Move Over Jarvis, Meet OSCAR*.
- 76 “Section 1004 FY22 NDAA,” Commission on PPBE Reform, U.S. Senate, <https://ppbereform.senate.gov/section1004-fy22-ndaa/>.
- 77 Interviewee #3.
- 78 Kenneth Werrell, *Archie to SAM: A Short Operational History of Ground-based Air Defense* (Alabama: Air University Press, 2005), 174, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0028_WERRELL_ARCHIE_TO_SAM.pdf.
- 79 Kuntz, *Genomes*.
- 80 Interview with Jim Lewis, Senior Vice President, Pritzker Chair, and Director, Strategic Technologies Program at CSIS. Note: Although this interview was conducted under Chatham House Rule, the interviewee agreed to cited by name and affiliation.
- 81 Interviewee #7.
- 82 Interviewee #9.
- 83 Interviewee #7.
- 84 Byron Cook, “A gentle introduction to automated reasoning,” Amazon Science, December 1, 2021, <https://www.amazon.science/blog/a-gentle-introduction-to-automated-reasoning>.
- 85 Interviewee #17.

COVER PHOTO SERGEYBITOS/ADOBE STOCK

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | www.csis.org