EXECUTIVE SUMMARY

Where are the greatest opportunities for the United States and its allies — as well as their authoritarian adversaries — in terms of military innovation in the cyber realm between now and 2040? And where can one expect the greatest vulnerabilities to develop or emerge? Both of these broad questions are at the heart of ensuring that the U.S. and other democracies are not surprised by an illiberal adversary which figures out big new ideas about military operations before we do — risking the failure of deterrence and defeat in any war that might occur.

My approach in this policy brief is to attempt look out roughly two decades into the future, extrapolating from today to gauge where technology may reach by that point. Such a time horizon allows opportunity for proper planning and innovation. Yet that time horizon is also short enough that existing trends in laboratory research can help us understand the future without indulging in rampant speculation. Since many defense systems take a couple decades to develop, it should not be an overly daunting task to gauge how the world might look, in terms of deployable military technology, two decades from now.

My overall prognostication is that technological change of relevance to military innovation may be faster and more consequential in the next 20 years than it has proven over the last 20 — and this sense of possibility is being driven mostly in the cyber realm. It is entirely possible that the ongoing rapid pace of computer innovation may make the next two decades more revolutionary than the last two. The dynamics in robotics and in cybersecurity discussed here may only accelerate. They may be more fully exploited by modern military organizations. They will likely extend in important ways into the artificial intelligence (AI) realm as well. At least, an examination of the last 20 years would seem to suggest the potential for such an acceleration. That is particularly true in light of the fact that multiple countries (most notably China, but also Russia) now have the resources to compete with Western nations in military innovation. Among other things, this confluence of factors and dynamics argues strongly for the United States and allies to redress major vulnerabilities in the cyber realm in anticipation of possible future attacks from Russia and/or China. It is, in my judgment, at least as much in the realm of vulnerability to paralyzing attacks,
Modern militaries, especially those of the United States and its key allies, have become extremely reliant on moving vast amounts of data around the battlefield as a normal part of operations. This has happened largely as the spread of computers, fiber optic cables, and other technologies has gone unchecked by adversaries like al-Qaida, the Islamic State group, and the Taliban. These enemies, whatever their considerable strengths in other domains, are not able to compete on the high-technology battlefield with the United States, or disrupt its use of advanced data and communications systems.

These happy trends will not continue in any future warfare the United States and its allies may conduct against more advanced militaries. To be sure, some new and exciting technologies may further aid tactical as well as theater-level and strategic communications. Laser communications systems, for example, could make an important difference, especially in space where clouds and other obstacles are not an impediment. Frequency-hopping radios with advanced computers coordinating the dance from one frequency to another are increasingly capable. Even if the radio technology per se is fairly mature, better computers allow levels of performance that were not previously possible.

And innovations from the commercial world of mobile communications and their advanced networks that allow for “network hopping” as well as other efficiencies will make the networks more robust and dependable against certain types of disruptions.

But the disruptions themselves will be much more threatening. Jamming, possible attacks on fiber optic undersea cables as well as satellites (discussed more below), and cyberattacks on the software of the radios and other systems used for communications are all serious worries, to say nothing of a high-altitude nuclear-induced electromagnetic pulse (EMP). Even when communications systems within a small unit survive enemy attack, or find themselves outside the targeted zone of intense jamming, communications with central authorities may suffer. It is because of such concerns, for example, that the U.S. Army’s Maneuver Center of Excellence at Fort Benning, Georgia is examining concepts of future operations in which a brigade might be cut off from divisional or corps headquarters for an extended period, and have to function entirely on its own during that time.

With regard to computers, rapid progress will likely continue. “Moore’s Law” — that the capacity and speed of computers doubles every 18 to 24 months — may not hold quite as it now has for several decades. But rapid progress seems likely to continue. Around 1970, several thousand transistors could be built onto a given chip; by 2000, the figure was roughly 10 million, and by 2015 or so it exceeded one billion. Even rather than opportunity for new and lethal methods of going on the offense, that an established superpower needs to focus its concerns and its efforts, lest it be surprised or overtaken by others. Allowing Achilles’ heels to develop in one’s military force planning, and national infrastructure, is among the most dangerous things a nation can do in regard to matters of war and peace.
if the pace of advance slows, it will not stop. And countless ways will continue to be invented to take advantage of all this computing capacity that is already available, with huge undeveloped potential in many areas. Notably, with the slowing of Moore’s Law, we can expect further developments in an accelerated shift to multicore processors, as well as some shifting of computing to more specialized chips.

For example, improved computing power can allow a multitude of satellites and other sensors to have their data synthesized automatically through various algorithms and AI. In the United States, this kind of effort could be further accelerated if the Department of Defense (DOD) is successful in building up its relationships with Silicon Valley and other centers of computer excellence through innovations like the Defense Innovation Unit, or DIU. These kinds of multiplatform networks can help mitigate the dangers associated with anti-satellite weapons attacking large, high-value military assets that previously had few if any backups. The odds in favor of major breakthroughs in these technology areas are high for the next two decades. AI systems are basically computers that can “learn” how to do things through a process of trial and error with some mechanism for telling them when they are right and when they are wrong — such as picking out missiles in photographs, or people in crowds, as with the Pentagon’s “Project Maven” — and then applying what they have learned to diagnose future data. The House Armed Services Committee Future of Defense Task Force in 2020 as well as the National Security Commission on Artificial Intelligence in 2021 have made similar cases.

**ROBOTICS**

Largely as a result of the computer revolution, robotics will continue to improve dramatically. Already, of course, self-driving vehicles are possible. Soon, a number are likely to be built for specific military purposes like tactical resupply on the battlefield. The U.S. Army’s “Wingman” may be one example. Wingman is also being adapted to carry weapons at least for tests (albeit with real human soldiers in the decisionmaking loop). Other countries such as Russia and Turkey are pushing the envelope in this realm of technology as well. And of course, it may not end there. The former vice chairman of the joint chiefs of staff, General Paul Selva, argued half a decade ago that the United States could be about a decade away from having the capacity to build an autonomous robot that could decide when to shoot and whom to kill — though he also asserted that the United States had no plans actually to build such a creature. Indeed, it is likely still close to a decade away as of this writing in 2022.

Other robotics with more specific functions surely will be built. They will include advanced sensor systems, often acting as networks or “swarms.” In the air, they could also involve stealthier unmanned aerial vehicles (UAVs) with long range, usable as penetrating sensors, to give just one example. On the sea, future robotics could include unmanned surface vessels for intelligence gathering, mine clearing, and possible local point defense against threats like fast-attack craft. Underwater robotic devices (unmanned underwater vehicles or UUVs), like the Defense Advanced Research Projects Agency (DARPA)’s “Sea Hunter,” could for example perform search functions associated with anti-submarine warfare and mine warfare. It is already possible to talk somewhat precisely and realistically about how the U.S. Navy’s future fleet might include substantial numbers of unmanned surface and underwater vessels; a team of researchers including Bryan Clark and Bryan McGrath recommended a future fleet with 40 of each, for example. The Navy is increasingly thinking of how to deploy its littoral combat ships with families of unmanned ships and other robotics. Some UUVs could have long persistence and low signature even within close proximity of an enemy’s shores.
A $100,000 ocean glider recently crossed the Atlantic. Promising concepts could cut that cost for UUVs by a factor of 10.21

The speed at which military operations must occur will create incentives not to have a person in the decisionmaking loop in many tactical settings.22

Even if General Selva’s terminator is not built, robotics will in some cases likely be given the decisionmaking authority to decide when to use force. This highly fraught subject requires careful ethical and legal oversight, to be sure, and the associated risks are serious. Yet the speed at which military operations must occur will create incentives not to have a person in the decisionmaking loop in many tactical settings.22 Whatever the United States and other democratic militaries may prefer, restrictions on automated uses of violent force would also appear relatively difficult to negotiate (even if desirable), given likely opposition from Russia and quite possibly other nations.23 Moreover, given progress in Russia and China, it is far from clear that the United States will be the lead innovator in artificial intelligence in the years ahead, with some warning that one or both of these countries may soon set the pace in AI — and thus also warfighting robotics.24

For example, small robots that can operate as swarms on land, in the air, or in the water may be given certain leeway to decide when to operate their lethal capabilities. By communicating with each other, and processing information about the enemy in real time, they could concentrate attacks where defenses are weakest in a form of combat that John R. Allen and Amir Husain call “hyperwar” because of its speed and intensity.25 Other types of swarms could attack parked aircraft; even small explosives, precisely detonated, could disable wings or engines or produce secondary and much larger explosions.

Many countries will have the capacity to do such things in the coming 20 years.26 Even if the United States tries to avoid using such swarms for lethal and offensive purposes, it may elect to employ them as defensive shields (say, against North Korean artillery attack against Seoul) or as jamming aids to accompany penetrating aircraft. With UAVs that can fly 10 hours and 100 kilometers now costing only in the hundreds of thousands of dollars, and quadcopters with ranges of a kilometer more or less costing in the hundreds of dollars, the trendlines are clear — and the affordability of using many drones in an organized way is evident.27 Although defenses against such robotics will surely be built, too, at present they are underdeveloped against possible small UAV swarms.28 And unless area defense allows for a certain part of the sky, or sea, or land effectively to be swept clear of any robotics within a certain zone, it seems statistically likely that some offensive UAVs will survive a defense’s efforts to neutralize them — meaning that their capabilities to act as a swarm, even if perhaps a weakened one, will probably remain.

Robotics with artificial intelligence may also deploy on the battlefield in close partnership with real humans. These robotics could be paired one for one, or in larger numbers, under the control and for the purposes of a single soldier or unit.29 The Israeli operation, using a robotic vehicle and gun, to kill an Iranian nuclear weapons scientist in 2020 stands out as a potential harbinger in this domain.30

**CYBER VULNERABILITY**

With the progress in computers has, as noted, come far greater cyber vulnerability. By effectively building Achilles’ heels into everything they operate, modern militaries — and modern societies writ large — have created huge opportunities for their potential enemies. The fact that everyone is vulnerable, in some sense, is no guarantee of protection. Deterrence
of some actions is not impossible in cyberspace, but it is surely difficult, and likely to fail in many important situations. Vulnerabilities may vary across countries based on different types of software employed in their military systems and different relative abilities of their respective offensive hacking units.

The United States undoubtedly possesses among the best, and probably the very top, offensive cyber capabilities on the planet... Distressingly, however, the U.S. may also be among the most vulnerable.

The United States undoubtedly possesses among the best, and probably the very top, offensive cyber capabilities on the planet. These could be used against the computer and networking capabilities of the militaries as well as the broader economies and national infrastructural capabilities of other countries. Distressingly, however, the U.S. may also be among the most vulnerable, given how much it has computerized in modern times, often somewhat carelessly and often with software of questionable resilience. A country figuring out how to integrate cyberattack plans that are temporarily crippling into an integrated operational concept may, even if still vulnerable to reprisal itself, be able to achieve dramatic success in the opening (and perhaps decisive) phases of a war. A military and a national infrastructure with key systems plugged into the internet, running on flawed software, and often employing a simple password system for user access rather than a two-factor authentication system is inherently vulnerable. That is especially true when, as in the recent debacle in the United States that saw thousands of businesses suffer compromises to their cyberservices due to breaches at the software company SolarWinds, a key password was mindlessly set to something as easily guessable as “solarwinds123.” This is precisely the situation the U.S. and most of its major allies face today. Faced with such a situation, in a future conflict, an enemy is likely to roll the dice and attempt large-scale cyberattacks — even if, in crossing such a threshold, it opens itself up to inevitable retaliation in kind.

Uncertainty abounds in the cyber domain. Software vulnerabilities that might exist at one time could be patched up subsequently. Indeed, methods for detecting and responding to intrusion proactively and quickly have improved dramatically in recent years; one example was Cyber Command’s success in thwarting Russian attempts to interfere in the 2018 midterm elections in the United States. But other vulnerabilities can and will continue to emerge, as shown by the 2021 Colonial Pipeline ransomware attack that compromised movement of fuel and created shortages for an extensive period in the United States, to name just one. Firewalls are often breachable; passwords are guessable; lack of two-factor identification compounds many vulnerabilities, as does sloppiness on the part of many human operators. Moreover, cyber vulnerabilities are not static. They are always evolving in a game of measures and countermeasures, even faster than in other areas of military operations characterized by these kinds of dynamics, such as electronic warfare. In addition, the ripple effects of any cyberattack often cannot be easily foreseen even when specific vulnerabilities are understood. There may also be important path dependencies about how different types of failures might collectively affect a larger system. It is difficult to evaluate these possibilities by examining individual vulnerabilities alone. The overall situation today though is, on balance, very worrisome, in regard to the cyber systems of the private sector, the national civilian infrastructure (on which the DOD depends in many ways), and the armed forces themselves. A recent Defense Science Board study asserted that virtually no major U.S. weapon system had cybersystems that could be confidently viewed as resilient in the face of enemy attack.
A separate type of problem related to the same basic phenomenon of ongoing progress in computers and electronics is the vulnerability of domestic infrastructure and military weaponry to electromagnetic pulse from a high-altitude nuclear explosion. (U.S. systems could also be vulnerable to severe solar storms of a type that can typically occur once a century or so.) These vulnerabilities may be growing because smaller and smaller electronics are progressively more vulnerable to a given electric insult, and because as the Cold War recedes in time, the perceived likelihood of an EMP attack may decline. American strategists, military services, and weapons manufacturers may delude themselves into a false sense of perceived invulnerability, believing that an EMP attack would be seen as tantamount to a direct nuclear attack against populations and hence too risky. It is debatable whether all adversaries would in fact make such a calculation; as such, U.S. vulnerabilities in this area could easily grow further.

Communications systems are also highly vulnerable to jamming from sophisticated electronic-warfare technologies. Digital electronics are amplifying and accelerating these challenges, to the point where in recent years some DOD research and development documents have prioritized electronic warfare as among the most rapidly changing and threatening of technological developments.

**CONCLUSION**

This survey of trends in digital technologies, and associated systems including robotics and modern military communications, suggests that much is happening at a rapid pace. By contrast, my surveys of various kinds of vehicles, ships, planes, and even rockets suggests much less rapid change. If a military revolution is to happen between 2022 and 2040, I would submit it will be driven in the digital realm. If we in the United States and other democracies are to avoid losing the resulting competition, it is not crucial that we always be the first to deploy every possible offensive technology. But it is essential that we not leave ourselves vulnerable to a disabling first blow that could provide an aggressor enough time to achieve its goals overseas before America and allies can get back on their feet, rebuild, and respond.
REFERENCES


4 Briefing at the U.S. Army’s Maneuver Center of Excellence, Fort Benning, Georgia, December 13, 2017. It is not clear that the Army has continued to prioritize training in environments of extremely contested command and control, however; see *Field Manual 7-0: Training* (Washington, DC: Headquarters, Department of the Army, June 2021), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN32648-FM_7-0-000-WEB-1.pdf.


11 For a good general overview of this subject and related matters that goes beyond the military sphere, see Darrell M. West, The Future of Work: Robots, AI, and Automation (Washington, DC: Brookings Institution Press, 2019).


22 Matthew Rosenberg and John Markoff, “The Pentagon’s ‘Terminator Conundrum.’”


26 T.X. Hammes, "The Future of Conflict.”


34 Debate continues over whether that password was the cause of the breach, but such practices remain unfortunately common; see Keumars Afifi-Sabet, “Solar Winds Blames Intern for Weak ‘solarwinds123’ Password,” IT Pro, March 1, 2021, https://www.itpro.com/security/cyber-attacks/358738/intern-blamed-for-weak-password-that-may-have-sparked-solarwinds.


ABOUT THE AUTHOR

Michael E. O’Hanlon holds the Philip H. Knight Chair in Defense and Strategy in the Foreign Policy program at the Brookings Institution, where he is director of research and director of the Strobe Talbott Center on Security, Strategy, and Technology. He is the author, recently, of Defense 101: Understanding the Military of Today and Tomorrow (Cornell University Press, 2021), and The Art of War in an Age of Peace: U.S. Grand Strategy and Resolute Restraint (Yale University Press, 2021). In addition to a Ph.D. in public and international affairs, he earned bachelor’s and master’s degrees in the physical sciences, all from Princeton.

ACKNOWLEDGEMENTS

Ted Reinert edited this policy brief and Rachel Slattery provided layout.