Foreign Policy at BROOKINGS

MILITARY INNOVATION AND TECHNOLOGICAL CHANGE: PREPARING FOR THE NEXT GENERATION OF CYBER THREATS

MICHAEL E. O'HANLON

JANUARY 2022

Editor's note: *This policy brief is largely drawn from the author's September 2018 Brookings report, "[Forecasting change in military technology, 2020-2040](#)"; analysis that also appears in his book* Defense 101: Understanding the Military of Today and Tomorrow *(Cornell University Press, 2021).*

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,

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.

COMMUNICATIONS

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.

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.

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.[1] 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.[2]

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).[3] 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.[4]

COMPUTERS

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.[5] Even 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 multi-core processers, 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.[6] These kinds of multi-platform networks can help mitigate the dangers associated with anti-satellite weapons attacking large, high-value military assets that previously had few if any backups.[7] The odds in favor of major breakthroughs in these technology areas are high for the next two decades.[8] 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.[9] 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.[10]

ROBOTICS

Largely as a result of the computer revolution, robotics will continue to improve dramatically.[11] 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.[12] Wingman is also being adapted to carry weapons at least for tests (albeit with real human soldiers in the decisionmaking loop).[13] Other countries such as Russia and Turkey are pushing the envelope in this realm of technology as well.[14] 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.[15] 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.[16] 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.[17] 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.[18] The Navy is increasingly thinking of how to deploy its littoral combat ships with families of unmanned ships and other robotics.[19] Some UUVs could have long persistence and low signature even within close proximity of an enemy's shores.[20]

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.

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.[31] 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.[32] 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.[33] 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."[34] 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.[35]

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.[36] 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.[37] 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.[38] 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.[39]

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 of 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.[40]

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.[41] 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

1 David W. Young, Hugh H. Hurt, Joseph E. Sluz, and Juan C. Juarez, “Development and Demonstration of Laser Communications Systems,” *Johns Hopkins APL Technical Digest* 33, no. 2 (2015), https://www.jhuapl.edu/content/techdigest/pdf/V33-N02/33-02-Young.pdf; George Leopold, “Laser Comms from Space Gets Another Test,” Defense Systems, February 17, 2017, https://defensesystems.com/articles/2017/02/17/spacelaser.aspx; and Sydney J. Freedberg, Jr., “Say It With Lasers: $45 Million DoD Prize for Optical Coms,” Breaking Defense, May 30, 2017, https://breakingdefense.com/2017/05/say-it-with-lasers-45m-dod-prize-for-optical-coms.

2 Seth Spoenlein, James Snodgrass, Michael Breckenridge, and Brian Rivera, “Path of Greatest Resilience,” *Army AL&T*, January-March 2018, 135-139, https://asc.army.mil/web/path-of-greatest-resilience/.

3 “Techniques for Tactical Radio Operations,” ATP 6-02.53, (Washington, DC: Headquarters, Department of the Army, February 2020), https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN20819_ATP_6-02x53_FINAL_WEB.pdf; David Axe, “Failure to Communicate: Inside the Army’s Doomed Quest for the ‘Perfect’ Radio,” Center for Public Integrity, Washington, D.C., May 19, 2014, https://www.publicintegrity.org/2012/01/10/7816/failure-communicate-inside-armys-doomed-quest-perfect-radio; and James Hasik, “‘The whole network needs to mesh in wartime,’” Atlantic Council, July 24, 2017, https://www.atlanticcouncil.org/content-series/defense-industrialist/the-whole-network-needs-to-mesh-in-wartime/.

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.

5 M. Mitchell Waldrop, “The chips are down for Moore’s law,” *Nature*, February 9, 2016, http://www.nature.com/news/the-chips-are-down-for-moore-s-law-1.19338; see also Rose Hansen, “A Center of Excellence Prepares for Sierra,” *Science and Technology Review* (March 2017), 5-11, https://str.llnl.gov/march-2017/neely; and Dave Vellante with David Floyer, “A new era of innovation: Moore’s Law is not dead and AI is ready to explode,” SiliconANGLE, April 10, 2021, https://siliconangle.com/2021/04/10/new-era-innovation-moores-law-not-dead-ai-ready-explode/.

6 Jacquelyn Schneider, “Swiping Left on Silicon Valley: New Commercial Analogies for Defense Innovation,” War on the Rocks, May 16, 2017, https://warontherocks.com/2017/05/swiping-left-on-silicon-valley-new-commercial-analogies-for-defense-innovation/.

7 Todd Harrison, Kaitlyn Johnson, and Makena Young, “Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons,” (Washington, DC: Center for Strategic and International Studies, February 25, 2021), https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons.

8 James Somers, “Is AI Riding a One-Trick Pony?” *MIT Technology Review*, September 29, 2017, www.technologyreview.com/s/608911/is-ai-riding-a-one-trick-pony.

9 Gregory C. Allen, "Project Maven Brings AI to the Fight against ISIS," *Bulletin of the Atomic Scientists*, December 21, 2017, https://thebulletin.org/project-maven-brings-ai-fight-against-isis11374; Phil Stewart, "Deep in the Pentagon, a secret AI program to find hidden nuclear missiles," Reuters, June 5, 2018, https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J.

10 Seth Moulton, Jim Banks, Susan Davis, Scott Desjarlais, Chrissy Houlihan, Paul Mitchell, Elissa Slotkin, and Michael Waltz, "Future of Defense Task Force Report 2020," (Washington, DC: House Armed Services Committee, September 2020), https://armedservices.house.gov/_cache/files/2/6/26129500-d208-47ba-a9f7-25a8f82828b0/424EB2008281A3C79BA8C7EA71890AE9.future-of-defense-task-force-report.pdf; Eric Schmidt, Robert Work, Safra Catz, Steve Chien, Mignon Clyburn, Chris Darby, Kenneth Ford, José-Marie Griffiths, Eric Horvitz, Andrew Jassy, Gilman Louie, William Mark, Jason Matheny, Katharina McFarland, Andrew Moore, "Final Report," (Washington, DC: National Security Commission on Artificial Intelligence, 2021), https://www.nscai.gov/2021-final-report/.

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).

12 Thomas B. Udvare, "Wingman is the First Step toward Weaponized Robotics," *Army AT&L*, January-March 2018, 86-89, https://asc.army.mil/web/news-alt-jfm18-wingman-is-first-step-toward-weaponized-robotics/; Hector Montes, Lisbeth Mena, Roemi Fernández, and Manuel Armada, "Energy-efficiency hexapod walking robot for humanitarian demining," *Industrial Robot* 44, no. 4 (2017): 457-466, https://doi.org/10.1108/IR-11-2016-0281; Robert Wall, "Armies Race to Deploy Drone, Self-Driving Tech on the Battlefield," *The Wall Street Journal*, October 29, 2017, www.wsj.com/articles/armies-race-to-deploy-drone-self-driving-tech-on-the-battlefield-1509274803; and Scott Savitz, "Rethink Mine Countermeasures," *Proceedings* 143, no. 7 (July 2017), https://www.usni.org/magazines/proceedings/2017/july/rethink-mine-countermeasures.

13 Thomas B. Udvare, "Wingman Is First Step toward Weaponized Robotics."

14 Jeffrey Edmonds, Samuel Bendett, Anya Fink, Mary Chesnut, Dmitry Gorenburg, Michael Kofman, Kasey Stricklin, and Julian Waller, "Artificial Intelligence and Autonomy in Russia," (Arlington, VA: CNA, May 2021), https://www.cna.org/centers/cna/sppp/rsp/russia-ai; Sinan Tavsan, "Turkish defense company says drone unable to go rogue in Libya," Nikkei Asia, June 20, 2021, https://asia.nikkei.com/Business/Aerospace-Defense/Turkish-defense-company-says-drone-unable-to-go-rogue-in-Libya.

15 Matthew Rosenberg and John Markoff, "The Pentagon's 'Terminator Conundrum': Robots that Could Kill on Their Own," *The New York Times*, October 25, 2016, https://www.nytimes.com/2016/10/26/us/pentagon-artificial-intelligence-terminator.html.

16 Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, nos. 1-2 (2015): 38-73, https://doi.org/10.1080/01402390.2014.958150.

17 Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton, 2018); Anika Torruella, "USN Seeks to Fill SSN Shortfalls with Unmanned Capabilities," *Jane's Defence Weekly*, July 5, 2017, 11; and Scott Savitz, Irv Blickstein, Peter Buryk, Robert W. Button, Paul DeLuca, James Dryden, Jason Mastbaum, Jan Osburg, Philip Padilla, Amy Potter, Carter C. Price, Lloyd Thrall, Susan K. Woodward, Roland J. Yardley, and John M. Yurchak, *U.S. Navy Employment Options for Unmanned Surface Vehicles* (Santa Monica, CA: RAND Corporation, 2013), xiv-xxv, https://www.rand.org/pubs/research_reports/RR384.html.

18 Bryan Clark and Bryan McGrath, "A Guide to the Fleet the United States Needs," War on the Rocks, February 10, 2017, https://warontherocks.com/2017/02/a-guide-to-the-fleet-the-united-states-needs/.

19 Kris Osborn, "Navy Littoral Combat Ship to Operate Swarms of Attack Drone Ships," Warrior Maven, March 28, 2018, https://warriormaven.com/sea/navy-littoral-combat-ship-to-operate-swarms-of-attack-drone-ships.

20 Shawn Brimley, "While We Can: Arresting the Erosion of America's Military Edge," (Washington, DC: Center for a New American Security, December 2015), 17, https://www.cnas.org/publications/reports/while-we-can-arresting-the-erosion-of-americas-military-edge.

21 T.X. Hammes, "The Future of Conflict," in *Charting a Course: Strategic Choices for a New Administration*, ed. R. D. Hooker, Jr. (Washington, DC: National Defense University Press, 2016): 25-27, https://ndupress.ndu.edu/Publications/Books/charting-a-course/.

22 Matthew Rosenberg and John Markoff, "The Pentagon's 'Terminator Conundrum.'"

23 Patrick Tucker, "Russia to the United Nations: Don't Try to Stop Us from Building Killer Robots," Defense One, November 21, 2017, www.defenseone.com/technology/2017/11/russia-united-nations-dont-try-stop-us-buying-killer-robots/142734; "Special report: The future of war," *The Economist*, January 27, 2018, 4, https://www.economist.com/special-report/2018/01/25/the-future-of-war.

24 Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power," (Washington, DC: Center for a New American Security, November 28, 2017), https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power.

25 John R. Allen and Amir Husain, "On Hyperwar," *Proceedings* 143, no. 7 (July 2017), https://www.usni.org/magazines/proceedings/2017/july/hyperwar; Jules Hurst, "Robotic Swarms in Offensive Maneuver," *Joint Forces Quarterly* 87, no. 4 (2017): 105-111, https://ndupress.ndu.edu/Publications/Article/1326017/robotic-swarms-in-offensive-maneuver/; Graham Warwick, "Powerful Pairing," *Aviation Week and Space Technology*, November 27-December 10, 2017, 35-36, https://archive.aviationweek.com/issue/20171127/; and Graham Warwick, "Swarm Enabler," *Aviation Week and Space Technology*, April 3-16, 2017, 31-32, https://archive.aviationweek.com/issue/20170403.

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

27 Ben Knight, "A guide to military drones," Deutsche Welle, June 30, 2017, http://www.dw.com/en/a-guide-to-military-drones/a-39441185.

28 Kelsey Atherton, "As Counter-UAS Gains Ground, Swarm Threat Looms," *Aviation Week and Space Technology*, March 26-April 8, 2018, 36-37, https://archive.aviationweek.com/issue/20180326.

29 Alexander Kott, "The Artificial Becomes Real," *Army AT&L*, January-March 2018, 90-95, https://asc.army.mil/web/news-alt-jfm18-the-artificial-becomes-real/.

30 Ronen Bergman and Farnaz Fassihi, "The Scientist and the A.I.-Assisted, Remote Control Killing Machine," *The New York Times*, September 24, 2021, https://www.nytimes.com/2021/09/18/world/middleeast/iran-nuclear-fakhrizadeh-assassination-israel.html; see also Sarah Kreps, "Democratizing harm: Artificial intelligence in the hands of nonstate actors," (Washington, DC: The Brookings Institution, November 2021), https://www.brookings.edu/research/democratizing-harm-artificial-intelligence-in-the-hands-of-non-state-actors/.

31 Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyberspace," *International Security* 41, no. 3 (Winter 2016/2017): 44-71, https://doi.org/10.1162/ISEC_a_00266.

32 David E. Sanger and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," *The New York Times*, June 15, 2019, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html; Nigel Inkster, "Measuring Military Cyber Power," *Survival* 59, no. 4 (August-September 2017): 32, https://doi.org/10.1080/00396338.2017.1349770; and Damien Dodge, "We Need Cyberspace Damage Control," *Proceedings* 143, no. 11 (November 2017), 61-65, https://www.usni.org/magazines/proceedings/2017/november/we-need-cyberspace-damage-control.

33 Tunku Varadarajan, "Report from the Cyberwar Front Lines," *The Wall Street Journal*, December 29, 2017, https://www.wsj.com/articles/report-from-the-cyberwar-front-lines-1514586268.

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.

35 Erica D. Borghard and Shawn W. Lonergan, "The Logic of Coercion in Cyberspace," *Security Studies* 26, no. 3 (2017): 452-481, https://doi.org/10.1080/09636412.2017.1306396; Travis Sharp, "Theorizing cyber coercion: The 2014 North Korean operation against Sony," *Journal of Strategic Studies* 40, no. 7 (2017): 898-926, https://doi.org/10.1080/01402390.2017.1307741; David D. Kirkpatrick, "British Cybersecurity Chief Warns of Russian Hacking," *The New York Times*, November 14, 2017, https://www.nytimes.com/2017/11/14/world/europe/britain-russia-cybersecurity-hacking.html; and Nicole Perlroth, " Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say," *The New York Times*, July 6, 2017, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html.

36 Richard A. Clarke and Robert K. Knake, *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats* (New York: Penguin Press, 2019); Ellen Nakashima, "At nations' request, U.S. Cyber Command probes foreign networks to hunt election security threats," *The Washington Post*, May 7, 2019, https://www.washingtonpost.com/world/national-security/at-nations-request-us-cyber-command-probes-foreign-networks-to-hunt-election-security-threats/2019/05/07/376a16c8-70f6-11e9-8be0-ca575670e91c_story.html.

37 David E. Sanger and Nicole Perlroth, "Pipeline Attack Yields Urgent Lessons about U.S. Cybersecurity," *The New York Times*, May 14, 2021, https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.

38 Edd Gent, "US Air Force is guarding against electromagnetic pulse attacks. Should we worry?," Live Science, March 11, 2021, https://www.livescience.com/air-force-emp-attacks-protection.html; Michael Frankel, James Scouras, and Antonio De Simone, "Assessing the Risk of Catastrophic Cyber Attack: Lessons from the Electromagnetic Pulse Commission," (Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2015), https://www.jhuapl.edu/Content/documents/AssessingtheRiskofCatastrophicCyberAttack.pdf; Robert McMillan, "Cyber Experts Identify Malware that Could Disrupt U.S. Power Grid," *The Wall Street Journal*, June 12, 2017, https://www.wsj.com/articles/cyber-experts-identify-malware-that-could-disrupt-u-s-power-grid-1497271444; and Richard A. Clarke and Robert K. Knake, *The Fifth Domain*, 159-161, 187-196.

39 "Task Force on Cyber Deterrence," (Washington, DC: Defense Science Board, Department of Defense, February 2017), https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf.

40 For a good overview of the EMP threat, see Sukeyuki Ichimasa, "Threat of Cascading 'Permanent Blackout' Effects and High Altitude Electromagnetic Pulse (HEMP)," NIDS *Journal of Defense and Security* 17 (December 2016): 3-20, http://www.nids.mod.go.jp/english/publication/kiyo/pdf/2016/bulletin_e2016_2.pdf.

41 Michael E. O'Hanlon, *Defense 101: Understanding the Military of Today and Tomorrow* (Ithaca, NY: Cornell University Press, 2021), 134-61.

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.