The US Army War College Quarterly: Parameters

Volume 50
Number 3 *Parameters Autumn 2020*

Article 8

8-14-2020

Technology and Strategic Surprise: Adapting to an Era of Open Innovation

Audrey Kurth Cronin

Technology and Strategic Surprise: Adapting to an Era of Open Innovation

Audrey Kurth Cronin

ABSTRACT: Technological revolutions affecting state power are either open or closed. The precursor to the digital age is not the twentieth century, with state-controlled programs yielding nuclear weapons, but the late nineteenth century, when tinkerers invented the radio, airplane, and high explosives—all crucial to subsequent wars. To avoid strategic surprise, the US government must take a broader view of how today's open innovation is changing society, and adapt.

The digital revolution is happening in an open technological context different from the period when the United States achieved global ascendancy, and US strategists cannot rely on twentieth-century frameworks if they want to avoid strategic surprise. Starting in 1993, the United States deliberately opened maturing information technologies to globalized commercial development, in effect giving American competitors and adversaries as much access to advanced technologies as the United States and its allies had.

The pace of technological development seemingly accelerated as a result, but this was untrue: it just seemed faster because technologies interacted in new ways and globally diffused, affecting more dimensions of human existence, including conflict. Further, this globalization of commercial development of information technologies happened outside the US military. The key to success in warfare now is not in direct technology development: the US military cannot innovate their way out of an open technological revolution. They must work with, draw from, and adapt to it.[1]

Open and Closed Technological Revolutions

Technological revolutions affecting military innovation and state power can be either open or closed.[2] In the twentieth century, military technological innovation was mainly closed. Crucial new systems such as nuclear weapons, battleships, jet fighters, or radar were expensive, rare, and difficult to build, usually supported by long-term government programs.

Dr. Audrey Kurth Cronin, professor of international security and founding director of the Center for Security, Innovation, and New Technology at American University, is widely published on strategy and nonstate actors. Her newest book, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (Oxford University Press, 2020), analyzes the risks and opportunities of emerging technologies.

1. For further information concerning this argument, see Audrey Kurth Cronin, *Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists* (New York: Oxford University Press, 2020).

2. James H. Moor, "Why We Need Better Ethics for Emerging Technologies," *Ethics and Information Technology* 7, no. 3 (2005): 111–19; and Henry Chesbrough, "Open Innovation: A New Paradigm for Understanding Industrial Innovation," in *Open Innovation: Researching a New Paradigm*, ed. Henry Chesbrough, Wim Vanhaverbeke, and Joel West (Oxford: Oxford University Press, 2006), 1.

Closed technological innovation requires high levels of specialized expertise. Military or scientific elites restrict access to advanced weapons systems through secret programs and security clearances, as well as copyrights or patents. Governments track the proliferation of high-level lethal technology and protect programs from each other, as well as from the broader public. In this context, military technology evolves by making incremental improvements on existing capabilities, such as precision-guided munitions, nuclear warhead configuration or size, or aircraft stealth capability, for example.

Closed innovation practices lead to slow, highly complex, and proprietary weapons development. The military sets requirements and drives the agenda, even as defense contractors chase hefty profits. Experts speak of dual-use capabilities, meaning parallel military and civilian applications. Over time costs climb, as major military systems—such as the F-22 Raptor, *Arleigh Burke* destroyer, or the Trident II intercontinental ballistic missile—are upgraded to reduce risk, meet demanding new standards, protect sunk costs, and maintain technological leadership in known capabilities.

By contrast, in the twenty-first century technological innovation is mainly open. Open innovation is driven by commercial processes, not by the military. Because there is popular access to potentially lethal technology, it affects everyone in society. There is no need to be a nuclear scientist or engineer to use emerging technologies or even any reason to fully understand them, because most digital platforms are cheap, user-friendly, and specifically designed to help people experiment. Companies such as Google, Facebook, and Microsoft are driving the development of these technologies and strive, above all, to expand global markets by drawing users in.

Not everyone who uses a smartphone to guide a simple unmanned aerial vehicle (UAV) or drive a robot, for example, understands how they work, nor do they need to. Personal phones are compact computers four times as powerful as the one the National Aeronautics and Space Administration (NASA) uses to drive the Curiosity rover, the car-sized robot that landed on Mars in 2012.[3] And yet smartphones are extremely easy to operate and experiment with. Via cheap, accessible software users can livestream events, send encrypted messages, steal valuable information, or identify targets with facial recognition technology.

Historical periods of open and closed technological innovation have different dynamics, and they require different strategic analyses, terms, and modes of practice to cope with their implications. Open technological periods encourage tinkerers. D*ual use* is replaced by *multiuse* to reflect a broader range of users developing and experimenting with emerging technologies—from professionals, to professional consumers

3. Sharon Gaudin, "Your Smartphone is as Smart as the Curiosity Rover," *Computer World*, August 8, 2012, https://www.computerworld.com/article/2505612/nasa--your-smartphone-is-as-smart-as-the-curiosity-rover.html; and Leslie Horn, "The iPhone Is Literally Four Times as Powerful as the Curiosity Rover," Gizmodo, August 6, 2012, https://gizmodo.com/the-iphone-is-literally-four-times-as-powerful-as-the-c-5932148.

(or "pro-sumers"), to hobbyists and consumers.[4] Instead of proliferating like nuclear, chemical, or biological weapons, these technologies diffuse, spreading globally as telegraphs, railroads, radios, or automobiles did.[5] The challenges presented by nuclear weapons and other high-end weapons are thus joined by the instability of lethal applications emerging from democratized technological innovation.

During open technological innovation, individuals and private groups buy, use, and distribute emerging technologies and in the process invent new purposes, new forms, and new surprise combinations of these technologies. They are deliberately designed to be fiddled with by ordinary people—tinkerers customizing their Apple I and II computers, college students building semiautonomous quadcopters, hackers accessing big databases, or hobbyists 3D printing firearms from online digital files. Sometimes new technologies are combined with older ones, such as the 2019 Hong Kong protestors using shortwave radios alongside smartphones. Open technologies facilitate widespread experimentation, enabling individuals with a wide range of proficiencies to combine clusters of technologies together and create new forms and uses, both good and bad—well beyond whatever their original inventors had in mind.

Open technological innovation has yielded clusters of technologies including smartphones, UAVs, robotics, CRISPR (clustered regularly interspaced short palindromic repeats) gene-editing tools, additive manufacturing, machine learning, and even simple forms of artificial intelligence accessible to all. The impact and consequences of these technologies are gradually coming into focus, but taken together they are just as important to the future of warfare as the 1945 nuclear explosion in Hiroshima was. The strategies, theories, and approaches developed during the twentieth century, a period of closed military technological innovation dominated by nuclear weapons, differ from those needed to adapt in today's era of open technological innovation.

War and Technology

Fortunately, we can learn a great deal from earlier periods of open technological innovation. A review of historical arguments about war and technology will distinguish those that apply from those no longer useful.

For about the past five centuries, the dominant historical narrative in the United States and Europe has been about major powers concentrating increasingly advanced, complex, and lethal systems under their control, culminating in the awesome destructiveness of nuclear weapons. Well-known books such as *From Crossbow to H-Bomb*, the 1962 history of the weapons and tactics of warfare by Fawn and Bernard Brodie, surveyed major technological developments like gunpowder, the

4. Alvin Toffler, *The Third Wave* (New York: William Morrow, 1980); and Eric Von Hippel, "Lead Users: A Source of Novel Product Concepts," *Management Science* 32, no. 7 (July 1986): 791–805.

5. Everett M. Rogers, *Diffusion of Innovations*, 5th ed. (New York: Free Press, 2003).

development of early artillery, the transition from wooden to iron ships, and the race between guns and armor.[6]

The Brodies argued that while the development of weaponry had been slow for most of history, it gathered momentum in the nineteenth century, accelerated further into the twentieth century, and culminated in 1945 with the use of nuclear weapons in Hiroshima and Nagasaki.[7] In subsequent years, if any proof of the importance of state-controlled military technology were needed, the US and Soviet capacity to wipe out millions of people instantly with nuclear weapons provided it.

This centralization narrative was not watertight. European leaders outsourced their military power to private contractors during the seventeenth century.[8] And the Brodies did not explore instances in which new military technologies were counterproductive in warfare or periods when power became more widely distributed, such as in ninth- and tenth-century Europe. Their 1973 second edition, penned in the closing phase of the Vietnam War, expressed concern the conflict had "probably resulted in a net slowing down in technological development" and included an insightful discussion about the increasing costs of major weapons systems.[9]

But the view military technological innovation drove the evolution of warfare prevailed throughout the twentieth century.[10] In 1989, historian Martin Van Creveld opened *Technology and War: From 2000 B.C. to the Present* with: "The present volume rests on one very simple premise which serves as its starting point, argument and *raison d'être* rolled into one. It is that war is completely permeated by technology and governed by it."[11]

A focus on states gaining the technological edge vis-à-vis each other made sense—in many twentieth-century conflicts, advanced technology did indeed make the crucial difference. The history of the two world wars loomed large in most studies, as did careful analysis of innovation between the wars, because how major powers developed and employed military technology was important to the outcome.

Both academics and practitioners analyzed capital-intensive programs. Studying strategic bombing, amphibious warfare, aircraft carrier warfare, and submarines, for instance, they discovered key insights about why technologies may or may not be employed effectively for advantage in battle.[12] For example, the Germans were the most

6. Bernard Brodie and Fawn Brodie, *From Crossbow to H-Bomb: The Evolution of the Weapons and Tactics of Warfare*, 2nd ed. (Bloomington: Indiana University Press, 1973).

7. Brodie and Brodie, *Crossbow to H-Bomb*, 8.

8. David Parrott, *The Business of War: Military Enterprise and Military Revolution in Early Modern Europe* (Cambridge: Cambridge University Press, 2012).

9. Brodie and Brodie, *Crossbow to H-Bomb*, 280.

10. Alex Roland, *War and Technology: A Very Short Introduction* (Oxford: Oxford University Press, 2016), 1.

11. Martin Van Creveld, *Technology and War: From 2000 B.C. to the Present* (New York: Free Press, 1989), 1.

12. Williamson R. Murray and Allan R. Millett, eds., *Military Innovation in the Interwar Period* (Cambridge: Cambridge University Press, 1998).

technologically advanced of any of the combatants at the outset of the Second World War yet still failed to use radar effectively.

Interservice rivalry, resistance to radar in the Luftwaffe (World War I flying General Ernst Udet reportedly said, "if you introduce that thing you'll take all the fun out of flying!"), abandonment of shorter wavelength research, and failure to develop effective operational doctrine all contributed to Germany's defeat.[13] The British lagged behind the Germans technologically but more than compensated for the shortfall by the way they wove radar into every aspect of air defense, partly by necessity as they absorbed withering German air attacks during the 1940 Battle of Britain. According to Winston Churchill, "it was operational efficiency rather than novelty of equipment that was the British achievement."[14]

Other human factors also determined how effectively various state belligerents capitalized on technological advantages. Sometimes military training made the difference. When the Second World War started, for example, the United States already had a robust fleet of submarines capable of long-range cruising; but commanders had been peacetime-trained to attack well-escorted enemy warships and avoid exposure, training that emphasized stealth and the use of sonar. Consequently, commanders avoided risky actions that might have revealed their location such as surfacing to periscope depth where hostile destroyers or aircraft could detect them.

This training failed during the war, when the Allied mission changed to attacking fast-moving convoys of Japanese merchant ships who had to be espied at periscope depth. Harvard political scientist Stephen Rosen calculated only 31 of 4,873 known US submarine attacks were directed by sonar.[15] Yet most commanders hewed to their instinct to be invisible, missing target after target, a practice that changed only when more aggressive younger skippers took over during the war. Thirty percent of US submarine commanders were relieved for cause in 1942.[16]

The boom in twentieth-century studies of military innovation, doctrine, and training especially in the United States and United Kingdom produced important insights about how human elements influence military innovation and how new technologies are deployed. Nonetheless, despite limitations in high-end military innovations also revealed by these studies, the view that sophisticated military-controlled technologies were the lynchpin of strategic advantage for states prevailed.

The revolution in military affairs framework that emerged toward the end of the twentieth century followed this well-established tradition of favoring military-controlled technologies. It focused squarely on

13. David Pritchard, *The Radar War: Germany's Pioneering Achievement, 1904-45* (Wellingborough, UK: Patrick Stephens, 1989), 64.

14. Winston Churchill, *The Gathering Storm, The Second World War*, vol. I (New York: Houghton Mifflin Company, 1948), 140.

15. Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca, NY: Cornell University Press, 1991), 136.

16. Rosen, *Winning the Next War*, 130–47.

high-end, large-scale capabilities, arguing future technology, specifically a system of US-dominated information age technologies—precision-guided munitions, surveillance satellites, battlefield command and communications, networked operations, and other computer-dependent systems—would virtually remove any guesswork from future conflicts.[17] And the overwhelming defeat of Iraq in the Persian Gulf War (1990–91) seemed to confirm it.

Some strategic thinkers even asserted information technologies had fundamentally transformed the nature of war by making the battlefield transparent and controllable. In the words of US Admiral and former Vice Chairman of the Joint Chiefs of Staff William Owens: "When technology is correctly applied to the traditional military functions—to see, to tell, and to act—a powerful synergy is created. . . . Together, these create the three conditions for combat victory: *dominant battlespace knowledge*, *near-perfect mission assignment*, and *immediate/complete battlespace assessment*."[18]

This line of argument was the logical culmination of theories gradually developed over decades of US-dominated, closed military technological innovation. Paradoxically, it was promulgated at the very time the US government was consciously opening key technologies to commercial development and global diffusion. In the 1990s, US military innovation practices began to diverge sharply from US commercial policy with respect to government-developed technology—a disconnect that only got worse as the years went by. This is why today's era of open technological innovation has matured some 30 years later, and the US military is neither driving it nor arguably keeping up.

Pandora's Box

The shift from closed development to open technological innovation began in 1993, spurred by deliberate US government policy in the post-Cold War euphoria about a US-dominated new world order.[19] Publicly financed, government-controlled basic and applied research from the 1960s, 1970s, and 1980s drove the technological boom of the 1990s, as research and development funds and tax incentives shifted from the defense to the civilian industry.[20] With federal government support, the Advanced Research Projects Agency Network (ARPANET) became the Internet. Tax dollars developed the Global Positioning System. The Google founders continued the development of their search engine

17. See Dima P. Adamsky, "Through the Looking Glass: The Soviet Military-Technical Revolution and the American Revolution in Military Affairs," *Journal of Strategic Studies* 31, no. 2 (April 2008): 257–94.

18. Bill Owens with Ed Offley, *Lifting the Fog of War* (Baltimore, MD: Johns Hopkins University Press, 2000), 100 (emphasis in the original).

19. William J. Broad, "Clinton to Promote High Technology with Gore in Charge," *New York Times*, November 10, 1992, https://www.nytimes.com/1992/11/10/science/clinton-to-promote-high-technology-with-gore-in-charge.html.

20. William J. Clinton and Albert Gore Jr., *Technology for America's Economic Growth: A New Direction to Build Economic Strength*, (Washington, DC: Executive Office of the President, February 22, 1993), https://eric.ed.gov/?id=ED355929.

with funding from a National Science Foundation grant. All of the major components of smartphones were derived from US government programs, including microchips, touchscreens, and natural language voice activation, such as Apple's Siri system.[21]

The contrast may be most starkly illustrated by comparing the management of the highly secret Manhattan Project, which resulted in the nuclear bomb in 1945, to the current development of machine learning artificial intelligence (AI) technology. Private companies, foremost Microsoft, IBM, Facebook, Amazon, Apple, and Alphabet (Google's parent), now drive AI research. Worldwide spending on AI research is projected to reach $35.8 billion in 2019, a 44 percent increase over what was spent in 2018, and is expected to double by 2022.[22]

The Pentagon has recently established and funded its Joint Artificial Intelligence Center, but commercial actors like Microsoft, with state-of-the-art computing power, immense cloud storage and massive data sets that power new forms of deep learning, have a 10-year lead.[23] Meanwhile technology companies have entirely globalized their operations. In December 2017, for example, Google announced a new AI institute in Beijing, stating, "the science of AI has no borders."[24]

As the Information Age barrels along, we are embarking on an era of full automation, autonomy, narrow artificial intelligence and, perhaps ultimately, artificial general intelligence. Yet most analyses of current and future threats apply concepts such as deterrence and compellence, developed during the nuclear revolution. History is indeed relevant, and the nuclear threat remains; but the scope of strategic and historical analyses must be further widened, not only beyond formal military organizations but also to periods predating the current disruptive moment. The next "big thing" in warfare may well be a bunch of little things used by ordinary people in new ways.

Lessons from the Nineteenth Century

The last comparable period of open technological innovation occurred during the second half of the nineteenth century when globalized industrialization matured in ways that mirror today's ripening information age. When innovation processes are open and there is rapid change, not just war is permeated by technology; all of society is.

During much of the nineteenth century, amateur and professional scientific communities had no clear dividing line between them. Just

21. Lewis M. Branscomb et al., *Beyond Spinoff: Military and Commercial Technologies in a Changing World* (Boston: Harvard Business School Press, 1992); David Hambling, *Weapons Grade: How Modern Warfare Gave Birth to Our High-Tech World* (New York: Carroll & Graf, 2005); and Mariana Mazzucato, *The Entrepreneurial State: Debunking Public vs. Private Sector Myths* (New York: Public Affairs, 2015).

22. "Worldwide Spending on Artificial Intelligence Systems Will Grow to Nearly $35.8 Billion in 2019, According to New IDC Spending Guide," International Data Corporation, March 11, 2019, https://www.idc.com/getdoc.jsp?containerId=prUS44911419.

23. Brad Smith and Carol Ann Browne, *Tools and Weapons: The Promise of the Digital Age* (New York: Penguin Press, 2019), 195–7.

24. Fei-Fei Li, "Opening the Google AI China Center," Google in Asia (blog), December 13, 2017, https://www.blog.google/around-the-globe/google-asia/google-ai-china-center/.

as today members of the public are free to purchase quadcopters, build robots, experiment with simple gene-splicing kits, or download instructions for building 3D printed weapons, 150 years ago the public could buy wiring kits, chemicals, and explosives at the local hardware store or through the mail.[25] The changes underway then were even more sweeping than they are today, affecting patterns of human habitation, transportation, energy consumption, food production, sanitation, and medicine, and people wanted to understand and participate in them.[26]

Especially in Europe and the United States, new periodicals began to appear that explained science in nontechnical terms to a newly literate public excited about the potential of new technologies. *Popular Science Review* (founded 1862) and *Nature* (1869) emerged out of Britain, for example, while *Scientific American* (1845) and *Popular Science Monthly* (1872, now called *Popular Science*) began in the United States, all designed to serve the enthusiastic layman.

The result was a burst of popular creativity by pro-sumers, hobbyists, and consumers. For example, in 1867 Alfred Nobel patented the first stable and safely detonatable high explosive—dynamite—after first experimenting with nitroglycerin in a backyard shed behind the family home in Stockholm, Sweden. Italian electrician and physicist Guglielmo Marconi invented the radio using homemade equipment in the attic of his Bologna home and patented it in 1896.[27] Orville and Wilbur Wright, bicycle manufacturers operating out of a home workshop in Dayton, Ohio, designed and built the Wright Flyer, which made the first sustained, powered flight in Kitty Hawk, North Carolina in 1903.

Alfred Nobel's most critical invention, the blasting cap, used one explosive (mercury fulminate) to detonate another (nitroglycerine), thus solving a key problem in the evolution of explosives and introducing a method of detonation ultimately used in everything from artillery to atom bombs. He also invented ballistite, a more controlled yet powerful explosive that launched an entire class of munitions and enabled rapid-fire artillery. Thus high explosives, radios, and airplanes all resulted from open technological innovation achieved by and for civilians, at less than $1,000 each. All were crucial to future military operations, yet none originated in government-sponsored programs—or arguably could have done so.

Some inventions also dramatically affected global patterns of nonstate violence. Nobel's dynamite set off the first global wave of modern terrorism, the so-called anarchist wave, which spread to every continent (except Antarctica), killing or injuring thousands of civilians.[28]

---

25. W. W. Huntley and F. M. Robinson, *Catalogue of Standard List-Price of Material Used by Railroads 1900* (Richmond, VA: I.N. Jones, 1900), 35.

26. Martin Wolf, "Same as It Ever Was: Why the Techno-Optimists Are Wrong," *Foreign Affairs*, July–August 2015, https://www.foreignaffairs.com/articles/same-it-ever-was.

27. C. Mackechnie Jarvis, "The Distribution and Utilization of Electricity," in *A History of Technology, Vol. V: The Late Nineteenth Century, 1850-1900*, ed. Charles Singer, E.J. Holmyard, Ar. G. Hall, and Trevor I. Williams (New York: Oxford University Press, 1958), 227–8.

28. Cronin, *Power to the People*, chaps. 3 and 4.

The resulting violence included dozens of politically destabilizing assassinations of presidents, prime ministers, and monarchs, from Russia, across Europe, to the United States. Newly laid underwater telegraph cables then spread news of what were called "dynamitings" throughout the world, in stories packed with graphic details that helped build the Joseph Pulitzer and William Randolph Hearst mass-market print empires in the United States. This wave of violence was propagated by the worldwide publication of anarchist newspapers and pamphlets. At the same time, individuals could easily buy dynamite, selling in Oregon at the time for thirty-six cents per pound, for example.[29]

By the time Archduke Franz Ferdinand was shot on June 28, 1914, a global trifecta of openly accessible lethal technology, new communications vectors, and the diffusion of individual or small-group violence was solidly in place—a situation that in some ways resembles what we face today.

Contemporary Parallels

Innovation with twenty-first-century information age technologies is driven as much by widespread popular experimentation and tinkering as by secret development projects and elites holding high-level clearances. In the same way that the key to understanding innovation in the years before World War I was not just the 1897–1914 *Dreadnought* competition between Germany and the United Kingdom, the key to understanding innovation today is not just the well-publicized US-Chinese artificial intelligence arms race.

The bigger picture before World War I included global power politics between states such as Austria-Hungary, Germany, Russia, France, and Britain, but also open technological innovations such as the civilian use of the telegraph, the invention of steel, the development of fine machine tooling, the transition from coal to petroleum, and the creation of stable high explosives. Together these commercial innovations spawned vast killing machines for which the European powers were unprepared and had no effective military responses. Rapid military innovation then happened during the war through a bloody process of trial and error, but none of the belligerents had accurately assessed the implications of a preexisting open technological context, and the cost of learning on the job was cataclysmic.

Likewise, today's digital revolution includes a global story regarding the evolution of future war, centered on changes happening outside the military. Commercial-sector-driven technology clusters such as globalized social media, additive manufacturing, widespread robotics, driverless vehicles, Internet-connected devices, machine learning, and evolving artificial intelligence are altering how force can and will be used. Most obviously, popular mobilization and

29. Finn J. D. John, "Dynamite Used to Be a Regular Part of Oregon Life," Offbeat Oregon, January 11, 2015.

psychological operations have profoundly changed through digital profiling and the weaponization of social media. But avenues of physical attack are shifting too, as cheap facial recognition tools democratize assassination and the "Internet of Things" makes everyone vulnerable to assault. Functions that for centuries required a well-funded and well-trained army are accessible now to private actors and individuals—not at the same level of competency, but good enough to kill and to have widespread political impact.

To adapt, the military must pay closer attention to accessible open technologies, especially who is using them. Violence is taking new forms, not just in the hands of authoritarian powers but also from below, degrading the future effectiveness of the US military in both state and nonstate contests. Initiatives such as the Third Offset Strategy, a well-funded, admirable effort to develop capabilities such as military robotics and human-machine teaming, actually employ the wrong historical analogy.

Unlike the Cold War period when the United States employed US technology—nuclear weapons and precision-guided munitions—to offset Soviet geographic and numerical advantages, today the United States must respond in a technological context where threats and opportunities arise from surprise commercial advances not developed for the military and not under centralized state control.

Monitoring accessible open technologies, however, does not mean ignoring the actions of potential state adversaries. In the past 20 years, Chinese technological espionage alone has been harmful to American interests and those of Allies and partners. "In effect, by stealing and exploiting U.S. and Western technical secrets, they have been able to level the technological playing field with the U.S. Joint Force, in some key military capabilities, in little less than two decades—a relative blink of an eye in a peacetime, long-term strategic competition," former Deputy Secretary of Defense Robert O. Work and defense analyst Greg Grant rightly observed.[30]

But it is also worth noting deliberate US decisions about privatizing and sharing digital technologies during the techno-utopian 1990s leveled the playing field by making Internet-assisted economic espionage *possible* for China. China and other countries are stealing American and allied secrets because years ago we made it extremely easy for them to do so. From the vantage point of the 1990s, one person's espionage is another person's open access to information.

The question, now that we have opened this Pandora's Box, shared basic technologies, and fostered a dynamic era of open innovation, is how can the US military better adapt to the consequences and come out ahead?

30. Robert O. Work and Greg Grant, *Beating the Americans at Their Own Game: An Offset Strategy with Chinese Characteristics* (Washington, DC: Center for a New American Security, June 2019), 7.

How to Succeed

The United States is still the world's leader in the most important technologies for civilian and military purposes, including robotics and artificial intelligence. Maintaining this leadership position involves reversing the disastrous 1990s divergence between US commercial policy and US government innovation policy.[31]

First, we must reconceptualize our understanding of military technological innovation to reflect the reality of the commercially driven, open technological context. Second, we must reorganize around new strategic concepts, models that adopt a whole-of-society approach and jettison neat, state-on-state frameworks. Commercial tech companies are now much more wealthy and powerful than many states. Finally, we must work with, educate, train, and reward the personnel necessary for winning the wars of the Fourth Industrial Revolution, when surprise destabilizing threats are as likely to emerge from small groups and individuals or even private commercial entities, as they are directly from major powers—who already use them as proxies.

Technology is no longer supporting the centralization-of-force narrative that defined the Western nation-state.[32] At the moment, the entities centralizing technology and power are the tech companies, and authoritarian actors such as China and Russia. Enhanced government surveillance during the COVID-19 pandemic further strengthens authoritarian state power. The United States and some of its adversaries still have massive nuclear capabilities, but these arsenals are joined by diffuse, digital-based technologies many people can access. Nuclear deterrence remains crucial for managing nuclear weapons but insufficient to counter the threat posed by the panoply of twenty-first-century technologies changing our societies.

The US military must prepare for an era where professional armies are indistinguishable from proxies, and nonstate actors develop unanticipated lethal capabilities. Cyber contests, economic espionage, Internet device hacking, and theft of intelligence happen below the level of interstate war yet pose an ongoing cumulative threat. And our domestic political polarization offers weaknesses for adversaries to exploit.

Democratized technologies favor contests of harassment, disruption, and attrition that erode our strength. Building smart regulations that minimize the risks of popular emerging technologies such as shoring up security standards for Internet-connected devices, increasing resiliency to online psychological operations, improving

31. Ash Carter, "Technology and Public Purpose: Reflections on the Dilemmas of Tech and Possible Solutions," (annual Ernest May Memorial Lecture, "Technology and National Security: Maintaining America's Edge," Aspen Strategy Group Summer Workshop 2018, Aspen, Colorado, August 3, 2018).

32. Michael Howard, *War in European History* (Oxford: Oxford University Press, 1976); and Charles Tilly, *Coercion, Capital, and European States: AD 990–1992* (Oxford: Blackwell, 1990).

privacy standards, building a legal structure for personal data rights, and preventing wholesale hacking of databases, is as much a national security imperative as a law enforcement challenge.

Second, thriving in an era of open technological innovation demands working with and encouraging tinkerers and pro-sumers, those driven by curiosity and technological creativity both in and out of the military. In the nineteenth century, Orville and Wilbur Wright did not want to join the military, nor did Alfred Nobel or Guglielmo Marconi. They wanted to invent, create, and innovate independently. Alternately, when government-sponsored programs were driving cutting-edge research, people like J. Robert Oppenheimer, Edward Teller, and Enrico Fermi left academe and went to the Manhattan Project to invent, create, and innovate.

They wanted to make a difference in the war effort, but they also knew Los Alamos was a center of pioneering nuclear research. Throughout much of the twentieth century, all of the services, along with government-funded think tanks like RAND Corporation, drew many of the best scientists because the most advanced research, especially in physics and engineering, was government funded and led.[33] This is not the situation now.

It is too late to recapture cutting-edge digital innovation in traditional military or government organizations on any large scale. Innovation within the military or even defense innovation is the wrong way to think about it. It is also inherently impossible, as well as undesirable, to try to coerce commercial companies to serve national military aims, as they do in authoritarian countries like Russia and China. But we have time to adapt. Innovation actually happens pretty slowly: the military can gain advantages by appealing to the ideals of tech innovators and offsetting their economic risk. Most tech company employees and independent entrepreneurs sincerely want to serve the public good.

Commercial tech companies such as Microsoft, Google, or Facebook should remember the long history of how paradigm-shifting, brilliant innovations are used—often regardless of inventors' intent. In July 2019 Microsoft invested $1 billion in OpenAI, which seeks to create artificial general intelligence rivaling the human brain.[34] Amazon and Google are also avidly competing in this area: AI is integral to Amazon's e-commerce and Google owns DeepMind. Absent clear ethical principles and restraints and a deep understanding of history, the US commercial sector is just as likely as the US military to inadvertently set off an arms race where humanity loses.

---

33. Richard Rhodes, *The Making of the Atomic Bomb* (New York: Simon & Schuster, 1986); and Fred Kaplan, *The Wizards of Armageddon* (1983; repr., Stanford, CA: Stanford University Press, 1991).

34. Taylor Telford, "Microsoft Invests $1 Billion in OpenAI to Pursue Artificial Intelligence That's Smarter Than We Are," *Washington Post*, July 22, 2019.

Finally, in this period of open technological innovation, we must move beyond the military-civilian firewall in our defense institutions. For example, we must find a way to permit unorthodox talent to move horizontally in and out of US military service without penalty. The current career path of selecting and promoting officers is anachronistic and fails to provide the range of experience our military leaders need. If Army Futures Command, for example, is staffed strictly by lifelong government servants and Army officers who never experience working at a start-up, developing a cutting-edge technology, or engaging in entrepreneurial risk-taking (and even failure), it will lack the skills to work effectively with the tech sector. That will make it impossible to identify the most promising commercially driven technologies, build forward-leaning operational doctrine, and capitalize upon evolving military capabilities in military contests.[35]

From the commercial side, notwithstanding Google employees' 2018 protests against the Department of Defense's Project Maven, the problem is not inherently cultural. A Ronald Reagan Institute survey indicates 53 percent of those under 29 still have "great confidence" in the military, and more Americans have confidence in military officers (59 percent) than in doctors (54 percent), teachers (52 percent) or clergymen (25 percent).[36] Young people seem as favorably disposed toward intelligence and national security as they ever were, and they have tremendous confidence in the military as the most trusted and effective American institution.

But those who are trained and driven to innovate in cutting-edge twenty-first-century technologies fear industrial-era bureaucracies, and there is little evidence to convince them otherwise.[37] Furloughs of highly trained government professionals only make things worse. Obtaining a US government contract is difficult, risky, expensive, and time-consuming, and the system is heavily weighted toward existing players who know how to access and navigate this byzantine system. Most tech start-ups cannot survive the process. For people with

35. Daisuke Wakabayashi and Shane Scott, "Google Will Not Renew Pentagon Contract That Upset Employees," *New York Times*, June 1, 2018; and Damon V. Coletta, "Navigating the Third Offset Strategy," *Parameters* 47, no. 4 (Winter 2017–18): 60.

36. Ronald Reagan Presidential Foundation and Institute, *2018 National Defense Survey* (Boston: Anderson Robbins Research, and Austin, TX: Shaw & Company Research, November 2018), Questions 8, 11–18, https://www.reaganfoundation.org/media/299217/reagan-survey-full-charts-112918.pdf.

37. Jiwon Jung, Barry Bozeman, and Monica Gaughan, "Fear in Bureaucracy: Comparing Public and Private Sector Workers' Expectations of Punishment," *Administration & Society* 52, no. 2 (February 2020): 233–64.

creative new ideas, commercial markets offer better opportunities for developing and implementing them at scale and speed.[38]

Periods of open technological innovation contain exciting potential, but also widespread societal instability, and military organizations have and will continue to be forced to respond. To understand how best to engage opportunities and minimize risks, we cannot merely consider how new technologies might be employed on the battlefield; they affect societies in uncontested environments first. Failing to appreciate the broader social context of technological innovation by private and public actors and across a broad swathe of political and economic sectors leaves us unprepared for how the next war will actually unfold. And relying on the wrong models of innovation, developed for a different technological context, yields outmoded strategy and doctrine. Technological surprise is inevitable now; it must be built into US planning. Rather than try to wrest control of the chaotic process of open technological innovation, the US government should better inspire and incentivize today's whiz kids—the Nobels, Marconis, and Wright Brothers of the twenty-first century—to channel their creative energies to serve American interests.

38. Artificial Intelligence Initiatives within the Defense Innovation Unit: Hearings before the Senate Armed Services Committee, Subcommittee on Emerging Threats and Capabilities, 116th Cong. (2019) (statement of Michael Brown, Director of the Defense Innovation Unit), https://www.armed-services.senate.gov/imo/media/doc/Brown_03-12-19.pdf; and Rachel Olney, "The Rift between Silicon Valley and the Pentagon is Economic, Not Moral," War on the Rocks, January 28, 2019, https://warontherocks.com/2019/01/the-rift-between-silicon-valley-and-the-pentagon-is-economic-not-moral/.