



THE ETHICS OF ACQUIRING DISRUPTIVE MILITARY TECHNOLOGIES

C. Anthony Pfaff



Technological innovation is proceeding at a rapid pace and is having a dramatic effect on warfare. Not only do technologies such as artificial intelligence, human enhancement, and cyber reduce risk to soldiers and civilians alike, they also expand the kinds of actors who can pursue policy goals through military means. As a result, their development can make the use of force more likely even while reducing individual risk. Moreover, by changing how soldiers fight, they change who a soldier is, which has broad implications not just for military recruitment and training, but also the military's relationship with the society it defends.

Managing this change will require not only an understanding of disruptive technologies but also the establishment of norms to govern their development. Disruptive technologies change how actors compete in a given venue, whether in a market or on a battlefield. What makes such technologies disruptive is not their novelty or complexity, but rather how their particular attributes interact with a specific community of users in a particular environment. This interaction can raise moral concerns through its impact on human autonomy, justice, well-being, and social disruption. These categories thus offer a framework for assessing the moral effect, necessity, and proportionality of disruptive technologies to determine whether and how they should be developed.

*Any scientific advance is punished by the gods...*¹

— Boris Johnson

In his September 2019 United Nations General Assembly speech, British Prime Minister Boris Johnson warned of a dystopian future of digital authoritarianism, the practical elimination of privacy, and “terrifying limbless

chickens,” among other possible horrors.² Highlighting artificial intelligence, human enhancement, and cyber technologies, Johnson warned that “unintended consequences” of these technologies could have dire and global effects. While at times bizarre, Johnson’s speech aptly captured the *zeitgeist* of rapid technological change. Technological innovation is not just proceeding at a rapid pace. Civilian and military innovators are combining

1 “Boris Johnson Speech Transcript: Brexit, Chickens and AI — September 24, 2019,” *Rev*, Sept. 25, 2019, <https://www.rev.com/blog/boris-johnson-speech-transcript-brexit-chickens-and-ai-september-24-2019>.

2 Johnson, “Speech Transcript.” As a side note, “Terrifying Limbless Chickens” is a great name for a band.



these disruptive technologies in ways that are difficult even for them to control. From the outside, such loss of control can be unnerving; however, when applied to military technologies, it can also be downright frightening.

Aristotle famously pointed out that if machines could operate autonomously there would be no need for human labor, thus disrupting the social relationships of the time.

The resulting uncertainty has made enthusiasm for developing these technologies at best inconsistent, especially when they are being developed for military purposes. Despite artificial intelligence's (AI) potential for improved targeting to reduce collateral harm, Google, the European Union, and the 2019 winner of the Nobel Peace Prize, among many others, have called for a ban on research on machines that can decide to take a human life.³ A number of researchers have also raised concerns regarding the medical and social side effects of human enhancement technologies.⁴ While cyber technologies have been around a while, their dual-use nature raises concerns about the disruptive effect that an adversary's cyber operations can have on ci-

vilian life, something that could escalate into a very real war.⁵ In fact, whereas the previous U.S. administration was criticized for being ineffective regarding cyber operations, the current one is frequently criticized for being too aggressive.⁶ The confusion that disruptive technologies create suggests that the problem is not so much with the new capabilities themselves as with the norms that should govern their use, and by extension, their acquisition.

Because these technologies come with risk — at the very least, the risk of the unknown — a tension arises between limiting their development and employment and taking full advantage of what they can do. The problem, of course, is that there are competitors and adversaries willing to accept those risks, even if they entail unjust harms. One is therefore left with a choice: develop these technologies and risk inflicting such harm, or do not and risk being vulnerable and disadvantaged. For state actors who are bound by the social contract to see to the security and well-being of their citizens, allowing such vulnerabilities and disadvantages represents its own kind of moral failure. This does not mean that states are permitted to risk harm or violate international norms simply because adversaries do. However, it does mean that the morally correct answer is not to ignore disruptive technologies simply because such risks exist.

However, just because there may be times when states should develop disruptive technologies does not mean anything goes. When necessity is allowed to override moral commitments, the result is a normative incoherency that undermines the traditional rules of international behavior, thus increasing the likelihood of war and placing citizens' lives and well-being in jeopardy. To avoid this self-defeating dynamic, states are obligated, at a minimum, to take up the problem of disruptive technologies, even if, in the end, they determine that particular technologies are not worth the moral cost.

The question then is, under what conditions is one permitted to risk the harms that can result from disruptive technologies? Since the focus here is on military applications, it makes sense to start with norms that govern the use of military technologies. Military ethics requires one to fight for just

3 Scott Shane, Cade Metz, and Daisuke Wakabayashi, "How a Pentagon Contract Became an Identity Crisis for Google," *New York Times*, May 30, 2018, <https://www.nytimes.com/2018/05/30/technology/google-project-maven-pentagon.html>. See, "Thursday Briefing: EU Calls for Ban on Autonomous Weapons of War," *Wired*, Sept. 13, 2018, <https://www.wired.co.uk/article/wired-awake-130918>; Edith M. Lederer, "Nobel Laureate Jody Williams Campaigns Against Killer Robots," *Associated Press*, Oct. 21, 2019, <https://apnews.com/Oc99bd564d5f4cc585eb861adb20d28c>.

4 Thomas Douglas, "The Harms of Enhancement and the Conclusive Reasons View," *Cambridge Quarterly of Healthcare Ethics* 24, no. 1 (January 2015): 23–36, <https://doi.org/10.1017/S0963180114000218>, fn. 11. See also, Francis Fukuyama, "Transhumanism," *Foreign Policy*, Oct. 23, 2009, <https://foreignpolicy.com/2009/10/23/transhumanism/>.

5 John Arquilla, "Twenty Years of Cyberwar," *Journal of Military Ethics* 12, no. 1 (2013): 82, <https://doi.org/10.1080/15027570.2013.782632>.

6 Joseph Marks, "The Pluses and Perils of Trump's Cyber Strategy," *NextGov*, Nov. 29, 2017, <https://www.nextgov.com/cybersecurity/2017/11/pluses-and-perils-trumps-cyber-strategy/142831/>.

ends using just means. Disruptive technologies, even when developed with the best of intentions, risk the introduction of unjust means or at least their unjust application. Given the close link between ends and means, acquisition of these technologies risks putting one on the wrong side of one's moral commitments as well as undermining the cause for which one fights. Avoiding such an outcome requires not only establishing norms that govern the employment of each individual technology, but, at a deeper level, norms that govern the permissibility of risking the disruption their acquisition may result in.

Determining these norms requires an understanding of what disruption is, how technologies become disruptive, and why such disruption raises moral concerns. Disruptive technologies change how actors compete in a given venue, whether in a market or on a battlefield. What makes such technologies disruptive is not their novelty or complexity, but rather how their particular attributes interact with a specific community of users in a particular environment. To assess whether that interaction yields morally impermissible results, we must establish a basis for assessing the morality of certain outcomes. With the morality of such outcomes in mind, we can then establish the norms necessary to govern disruptive technology acquisition. In doing so, we may avoid, or at least mitigate, the "punishment of the gods" that Johnson warned about.

The Challenge of Disruptive Technologies

The idea of disruptive technology is not new. Aristotle famously pointed out that if machines could operate autonomously there would be no need for human labor, thus disrupting the social relationships of the time.⁷ In fact, the trajectory of technology development can largely be described as an effort to reduce human labor requirements, and, especially in the military context, the need for humans to take risk. There are plenty of examples, however, where such benign motivations have had disruptive, if not harmful, effects. Though funded

by the Department of Defense, the inventors of the Internet, for example, simply sought a way for researchers to collaborate.⁸ They did not anticipate the impact this technology would have on industries such as print media, whose profitability has significantly declined since the Internet's introduction.⁹ Nor did they fully anticipate the impact it would have on national security as increasing connectivity exposes military systems and information as well as critical civilian infrastructure to attack.¹⁰

Defining Technologies

For the purposes of this discussion, technology is broadly understood to include physical objects and activities and the practical knowledge about both, i.e., knowledge about the kinds of things one can do with those objects and activities.¹¹ Some technologies embody all three aspects. For example, a fully autonomous weapon system is a physical object. However, its associated targeting system, which includes things external to it such as communication systems and humans to provide instructions, is also an activity. Knowing how to conduct remote airstrikes is the practical knowledge without which the object and the activities would be useless. Any of these aspects of technology, separately or in combination, can be sources of disruption.

It is also important to specify what aspects of individual technologies are sources of moral concern. For example, not all autonomous systems are artificially intelligent and not all artificially intelligent systems are autonomous. In fact, as Wendell Wallach and Colin Allen point out, all technology fits on the dual spectrums of autonomy and ethical sensitivity. Some tools, like a hammer, have neither autonomy nor ethical sensitivity, while a rifle has no autonomy but can have some ethical sensitivity reflected in the attachment of a safety switch. A mechanical autopilot can be designed to take passenger comfort into account by limiting how steep it will climb, descend, or turn and thus has more autonomy and ethical sensitivity.¹²

While this discussion is not intended as a comprehensive survey of disruptive technology, it relies heavily on examples from AI, human enhancements,

7 Aristotle, *Politics, Book I, The Complete Works of Aristotle, Vol 2*, trans. Jonathan Barnes (Princeton, NJ: Princeton University Press, 1984), 1989.

8 P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (Oxford: Oxford University Press, 2014), 18.

9 Amy Watson, "U.S. Print Media Industry — Statistics and Facts," *Statista*, Aug. 27, 2019, <https://www.statista.com/topics/1052/print-media/>.

10 John M. Donnelly and Gopal Ratnam, "America Is Woefully Unprepared for Cyber-Warfare," *Roll Call*, July 11, 2019, <https://www.rollcall.com/news/u-s-is-woefully-unprepared-for-cyber-warfare>.

11 Wiebe E. Bijker, Thomas P. Hughes, and Trevor Pinch, eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: MIT Press, 2012), introduction.

12 Wallach and Allen, *Moral Machines*, 25.



and cyber technologies to illustrate key points. For the purposes of this discussion, artificially intelligent systems will refer to military systems that include both lethal autonomous weapons that can select and engage targets without human intervention and decision-support systems that facilitate complex decision-making processes, such as operational and logistics planning. What will not be discussed is the specific means — such as code or neural networks — these systems use to arrive at particular conclusions, but rather the extent to which that ability is able to replace human decision-making.

Human enhancements are any interventions to the body intended to improve a capability above normal human functioning or provide one that did not otherwise exist.¹³ As such, enhancements will refer to anything from pharmaceuticals to neural implants intended to enable human actors to control systems from a distance. They do not refer to treatments or other measures intended to restore normal functions or those that do improve or provide new capabilities but that do not involve a medical intervention, such as an exoskeleton, for example, that a soldier would simply put on.¹⁴

“Cyber” is a broad term that generally refers to technology that allows for and relies on the networking of computers and other information technology systems. This network creates an environment typically referred to as “cyberspace.” As the National Institute of Standards and Technology defines it, cyberspace refers to the “interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.”¹⁵

What is extraordinary about cyberspace is how this connectivity evolved into a domain of war, on par with air, land, sea, and space. However, it functions very differently from the physical world of the other four domains. Unlike in the physical realm, where an attack that constitutes an act of

war is violent, instrumental, and political, cyber attacks, which are directed at information, do not have to be. In fact, so far, no cyber attack has met all three of these criteria.¹⁶ However, subversion, espionage, or sabotage, which characterize a lot of cyber operations, are not adequate to describe the range of disruption such operations can create. It is in the range of cyber operations, though, to function coercively to achieve political objectives. As a result, many of these operations — and their associated effects — fall outside more traditional peacetime and wartime norms.

Understanding Disruption

Of course, not all new technologies are disruptive. For example, stealth technology, at least in its current state, may now be required for advanced combat aircraft; however, it does not fundamentally change how aircraft fight. It simply improves on a quality all aircraft already have, at least to some degree.¹⁷ T.X. Hammes makes a similar point, especially when new or improved technologies are combined. He observes that “technological breakthroughs” such as “in metallurgy, explosives, steam turbines, internal combustion engines, radio, radar, and weapons” when applied, for example, to mature platforms like the battleship, certainly and significantly improved its capabilities. However, they did not change how the battleship fought. On the other hand, when these breakthroughs were combined with an immature technology, like aircraft, which in the beginning were slow, lightly armed, and limited in range, the combination revolutionized air and naval warfare.¹⁸ The effects of convergence, it seems, are difficult to anticipate and, as a consequence, control.

As Ron Adner and Peter Zemsky observe, what makes a technology — or combination of technologies — disruptive and not merely new are the attributes it introduces into a given market, or, for

13 Patrick Lin, Maxwell Mehlman, and Keith Abney, “Enhanced Warfighters: Risk, Ethics, Policy,” Case Western University, Case Research Paper Series in Legal Studies, Working Paper 2013-2, January 2013, 17.

14 Tony Pfaff, “Moral Autonomy and the Ethics of Soldier Enhancement,” *Pacem* 21, no. 1 (Oct. 29, 2018), 31, <http://pacem.no/2018/moral-autonomy-and-the-ethics-of-soldier-enhancement/>.

15 “Glossary,” Computer Security Resource Center, National Institute of Standards and Technology, <https://csrc.nist.gov/glossary/term/cyberspace>, accessed Dec. 23, 2019.

16 Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2013), 3.

17 Chester W. Richards, “Reforming the Marketplace: The Industrial Component of National Defense,” in *Spirit, Blood, and Treasure: The American Cost of Battle in the 21st Century*, ed. Donald Vandergriff (Novato, CA: Presidio Press, 2001), 307. See, Vivek Kapur, *Stealth Technology and Its Effect on Aerial Warfare* (New Delhi: Institute for Defense Studies and Analysis, 2014), 13. Kapur underscores the importance of stealth technology to an air force’s effectiveness. However, he also observes, “Stealth as a concept is not new to warfare.” I would also note that current stealth technology does not make an aircraft completely invisible to all radars. Also, aircraft do not come by whatever stealth capabilities they have all the same way. Helicopters, for example, are able to fly low and hover, which allows them to take advantage of natural cover to obscure them from radar or visual observation.

18 T.X. Hammes, “Cheap Technology Will Challenge U.S. Tactical Dominance,” *Joint Forces Quarterly* 81, no. 2, (April 2016): 76, <https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-81/Article/702039/cheap-technology-will-challenge-us-tactical-dominance/>.

the purposes of this discussion, a community of users within the larger national security enterprise. In fact, a new technology does not necessarily have to represent an improvement over the old. Rather, what is common to disruptive technologies is the novelty of the attributes they introduce and how useful those attributes are to at least a subset of the user community.¹⁹ To the extent they sufficiently meet user requirements *and* incorporate attributes a subset of those users find attractive, they could displace the older technology over time, even if they do not perform as well.

For example, Clayton M. Christensen, in one of the first studies on disruptive technologies, observed that smaller hard drives outsold better-performing larger ones despite the fact the smaller drives were less capable in terms of memory and speed. What they did have, however, was portability. That made smaller and cheaper computers possible, which opened up a much larger market than the corporate, government, and educational institutions that made up the established market. Thus, in the early market for hard drives, customers accepted reduced capacity in terms of memory and speed as well as higher costs per megabyte to get “lighter weight, greater ruggedness, and lower power consumption” than previous hard drive options provided.²⁰ Changing how actors compete in effect changes the game, which, in turn, changes the rules. In order to effectively compete in the new environment, actors then have to establish new rules. In the case of hard drives, companies that did not produce the smaller drives eventually went out of business. As Christensen observed regarding the market for hard drives,

Generally disruptive innovations were technologically straightforward, consisting of off-the-shelf components put together in a product architecture that was often simpler than prior approaches. They offered less of what customers in established markets wanted and so could rarely be initially employed there. They offered a different package of attributes valued only in emerging markets remote from, and unimportant to, the mainstream.²¹

Since its publication, critics have pointed out that Christensen’s theory of disruptive innovation frequently fails to be as prescriptive or predictive as he had intended. In fact, Christensen managed a fund that relied on his theory to identify opportunities for investment — within a year, it was liquidated.²² Subsequent analysis has attributed that failure in part to Christensen’s selectiveness regarding cases, with some accusing him of ignoring those that did not fit his theory. Others account for the predictive inadequacy of the theory by pointing out that other factors beyond those associated with the technology — including chance — can affect a technology’s disruptive effects.²³

The claim here is not that the conditions for disruptive effects dictate any particular outcome. Nor is the point, as Christensen claimed, that disruption should be pursued for its own sake. Rather, disruption is something to be managed and pursued only when certain conditions, which will be explored later, are met. Christensen’s concern was crafting a business strategy that would increase profits by harnessing disruption to increase market share or, preferably, create new markets. In the military context, the concern is not whether one can develop a theory that predicts the overall utility of a technology. Instead, it is to identify whether a technology is likely to have the kind of disruptive effects that ought to trigger ethical concerns that require employing additional measures to manage its acquisition. For that, Christensen’s understanding of the nature of disruptive technology is extremely useful.

Christensen’s focus on technology in competitive environments suggests his description of disruptive technologies applies in military contexts. Although business and national security arguably play by different rules, competing actors in both environments will generally seize on anything that offers an advantage. What Christensen gets right is that disruptive technologies do not have to be advanced to be disruptive. Instead, their disruptive qualities emerge from the interaction of the technology with a given community of users in a given environment. This interaction is often complex and difficult to predict, much less control. Therefore, it is no wonder that businesses that embrace dis-

19 Ron Adner and Peter Zemsky, “Disruptive Technologies and the Emergence of Competition,” *RAND Journal of Economics* 36, no. 2 (Summer 2005): 230, <https://www.jstor.org/stable/4135240>.

20 Clayton M. Christensen, *The Innovator’s Dilemma: When New Technologies Cause Great Firms to Fail* (Boston: Harvard Business Review Press, 2016), chap. 1, section title “Failure in the Face of Disruptive Technological Changes.”

21 Christensen, *The Innovator’s Dilemma*, chap. 1, “Failure in the Face of Disruptive Technological Changes.”

22 Jill Lepore, “The Disruption Machine: What the Gospel of Innovation Gets Wrong,” *New Yorker* 90, no. 15 (June 23, 2014), 6. Lepore argues that Christensen was too selective in his case selection and ignored cases that did not fit his model. I owe this point to an anonymous reviewer.

23 Andrew A. King and Baljir Baartartogtokh, “How Useful Is the Theory of Disruptive Innovation?” *MIT Sloan Management Review* (Fall 2015): 84–86, <https://sloanreview.mit.edu/article/how-useful-is-the-theory-of-disruptive-innovation/>. I owe this point to an anonymous reviewer.

ruption often fail. However, in the national security environment, when the conditions for disruption exist, the resulting potential for game-changing innovation forces state actors to grapple with how best to respond to that change.

Thus, the challenge for the United States in responding to the problem of disruptive technologies is best expressed this way: The U.S. way of war relies on technological superiority in order to overcome the strength of its adversaries or compensate for its own vulnerabilities. Yet, development of the technologies discussed here empowers smaller actors to develop “small, smart, and cheap” means to challenge larger, state actors — and win.²⁴ This dynamic simultaneously places a great deal of pressure on all actors to keep developing these and other technologies at an increasingly faster rate, creating ever more disruption. More disruption yields more confusion on how best to employ these technologies while maintaining moral commitments. Consider the following three examples.

First, in September 2019, Houthi rebels in Yemen claimed to have employed unmanned aerial vehicles and cruise missiles to launch a devastating attack on Saudi oil facilities, leading to an immediate 20 percent increase in global oil prices and prompting the United States to move additional military forces to the Middle East.²⁵ To make matters more complicated, there is evidence that the Houthis were not in fact responsible for the attacks, but that they were launched by Iranian proxies in Iraq. This use of autonomous technologies enabled the Iranians to obscure responsibility, which in turn constrained the political options the United States and its allies had to effectively respond.²⁶

Second, the Islamic State frequently provides its followers with Captagon, now known as the “Jihadist pill,” which is an amphetamine that keeps users awake, dulls pain, and creates a sense of euphoria. They do so in order to motivate fighters, in the words of one Islamic State member, to go to battle

“not caring whether you lived or died.”²⁷ It is this ability to enhance fighter capabilities that enabled the Islamic State to fight outnumbered and win against Iraqi, Syrian, and Kurdish forces, especially in 2014, when it rapidly expanded its presence in Iraq and Syria.

Third, in 2015, Iranian hackers introduced malware in a Turkish power station that created a massive power outage, leaving approximately 40 million people without power, reportedly as payback for its support for Saudi operations against Houthis.²⁸ While perhaps one of the more dramatic Iranian-sponsored attacks, there have been numerous others: Iran is suspected of conducting a number of directed, denial-of-service attacks as well as other attacks against Saudi Arabia, the United Arab Emirates, Jordan, and the United States.²⁹

None of the technologies in these examples is terribly advanced and most are available commercially in some form. Despite that fact, the targets of the attacks were caught by surprise. Moreover, even though the technologies described above have been around for several years, no one has developed an effective response yet. This suggests that as states and corporations continue to develop and promulgate these technologies, the potential for further disruptive effects will significantly increase. Furthermore, those effects will disrupt more than just the military. As Rudi Volti observes, “technological change is often a subversive process that results in the modification or destruction of established social roles, relationships, and values.”³⁰

Challenging the Norms of Warfighting

The question here is not *whether* such technologies as described above will challenge the norms of warfighting, but *how* they will. Take an example from the last century: the submarine. Its ability to move and shoot underwater introduced a novel attribute to naval combat operations. However, its

24 George M. Dougherty, “Promoting Disruptive Military Innovation: Best Practices for DOD Experimentation and Prototyping Programs,” *Defense Acquisition Research Journal* 25, no. 1 (January 2018): 4, <https://doi.org/10.22594/dau.17-782.25.01>. See, T.X. Hammes, “Melians’ Revenge: How Emerging Tech Can Fortify NATO’s Eastern Flank,” *Defense One*, June 28, 2019, <https://www.defenseone.com/ideas/2019/06/melians-revenge-how-emerging-tech-can-fortify-natos-eastern-flank/158083/>.

25 Shawn Snow, “Drone and Missile Attacks Against Saudi Arabia Underscore Need for More Robust Air Defense Measures,” *Military Times*, Oct. 25, 2019, <https://www.militarytimes.com/flashpoints/2019/10/25/drone-and-missile-attacks-against-saudi-arabia-underscore-need-for-more-robust-air-defenses/>.

26 C. Anthony Pfaff, “The Saudi-Oil Attacks Aren’t Game-Changing. They Show How the Game Has Changed,” *Defense One*, Sept. 17, 2019, <https://www.defenseone.com/ideas/2019/09/saudi-oil-attacks-arent-game-changing-they-show-how-game-has-changed/159947/>.

27 Mirren Gidda, “Drugs in War: What Is Captagon, the ‘Jihad Pill’ Used by the Islamic State Militants,” *Newsweek*, May 12, 2017, <http://www.newsweek.com/drugs-captagon-islamic-state-jihad-war-amphetamines-saudi-arabia-608233>.

28 Micah Halpern, “Iran Flexes Its Power by Transporting Turkey to the Stone Age,” *Observer*, April 22, 2015, <http://observer.com/2015/04/iran-flexes-its-power-by-transporting-turkey-to-the-stone-ages/>.

29 Masood Farivar, “U.S. Charges 9 Iranians with Massive Cyber Attack,” *Voice of America*, March 23, 2018, <https://www.voanews.com/a/us-charges-iranians-for-global-cyber-attacks-on-behalf-of-iran/4313154.html>.

30 Rudi Volti, *Society and Technological Change* (New York: Worth Publishers, 2006), 18.

slow speed and light armor made it vulnerable and ineffective against the large surface warfare ships of the day.³¹ As a result, it was initially used against unarmed merchant ships, which, even at the time, was in violation of international law.³²

What is ironic about the introduction of the submarine is that its disruptive effects were foreseen. In fact, the anti-submarine measures developed by Britain's first sea lord, Sir John Jellicoe, were so successful that the British lost no dreadnoughts to German submarines during World War I. Nonetheless, the attacks against British merchant vessels were so devastating he was forced to resign.³³ In fact, unrestricted submarine warfare traumatized Britain such that after the war it tried to build an international consensus to ban submarine warfare altogether.³⁴ When that failed, Britain and the United States backed another effort to prohibit unrestricted submarine warfare and in 1936 signed a "procès-verbal" to the 1930 London Naval Treaty, which required naval vessels, whether surface or submarine, to ensure the safety of merchant ship crews and passengers before sinking them.³⁵ Later, to encourage more states to sign onto the ban, that prohibition was modified to permit the sinking of a merchant ship if it was "in a convoy, defended itself, or was a troop transport."³⁶

Despite this agreement, both Germany and the United States engaged in unrestricted submarine warfare again in World War II. German Adm. Karl Donitz was tried and convicted at Nuremberg for his role in the unrestricted use of German submarines, among other things. His sentence, however, did not take that conviction into account given that Adm. Chester W. Nimitz admitted to the court that the United States had largely done the same in the Pacific.³⁷ So while certainly a case of mitigated victor's justice, this muddled example also illustrates two things: the normative incoherency that arises with the introduction of new technologies as well as the pressure of necessity to override established norms.

The subsequent evolution of submarine warfare also illustrates how norms and technology can interact. First, as noted above, state actors tried to impose the existing norm, though with little meaningful effect. Later, to accommodate at least some of the advantages the submarine provided, they modified the norm by assimilating noncombatant merchant seamen into the class of combatants by providing them with some kind of defense.³⁸ In doing so, they accepted that the submarine placed an obligation on them to defend merchant vessels rather than maintain a prohibition against attacking them, at least under certain conditions.

Eventually, however, submarine technology improved to the point it could more effectively compete in more established naval roles and challenge surface warfare ships, which, along with naval aviation and missile technologies, not only helped make the battleship obsolete, it brought the submarine's use more in line with established norms. Thus, in this case, while the technology eventually caught up to the norms, it also forced the norms to accommodate the innovation that it represented, even if in a restricted way. In fact, submarine use continues to evolve, challenging surface ships for their role in launching strikes on land.³⁹

Of course, disruption, by itself, is not necessarily a bad thing. Thus, even on utilitarian grounds, there will typically be a moral case for acquiring disruptive technologies. However, utility is seldom the final word in ethics. As Melvin Kranzberg wrote in 1986, "Technology is neither good nor bad; nor is it neutral."⁴⁰ Kranzberg's point is not simply that technologies can have unexpected and negative second- and third-order effects. Rather, it is that the introduction of new technologies changes the "social ecology" in ways that have a cost. For example, advances in medical science and improved water and sewer services have increased the average human life span. While these developments were welcome, over time they contributed to population increases

31 Gautam Mukunda, "We Cannot Go On: Disruptive Innovation and the First World War Royal Navy," *Security Studies* 19, no. 1 (2010): 125, <https://doi.org/10.1080/09636410903546731>.

32 Adam Roberts and Richard Guelff, eds., *Documents on the Laws of War*, 2nd ed. (Oxford: Clarendon Press, 1989), 147.

33 Mukunda, "We Cannot Go On," 125.

34 Nachman Ben-Yehuda, *Atrocity, Deviance, and Submarine Warfare: Norms and Practices During the World Wars* (Ann Arbor: The University of Michigan Press, 2013), 84.

35 Roberts and Guelff, *Documents on the Laws of War*, 147. Ben-Yehuda, *Atrocity, Deviance, and Submarine Warfare*, 86.

36 Ben-Yehuda, *Atrocity, Deviance, and Submarine Warfare*, 86.

37 Roberts and Guelff, *Documents on the Laws of War*, 148. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 2nd ed. (New York: Basic Books, 1992), 150.

38 Walzer, *Just and Unjust Wars*, 150.

39 David B. Larter, "Submarines Are Poised to Take on a Major Role in Strike Warfare, but Is that a Good Idea?" *Defense News*, Oct. 28, 2019, <https://www.defensenews.com/naval/2019/10/28/submarines-are-poised-to-take-on-a-major-role-in-strike-warfare-but-is-that-a-good-idea/>.

40 Melvin Kranzberg, "Technology and History: 'Kranzberg's Laws,'" *Technology and Culture* 27, no. 3 (July 1986): 545, <https://www.jstor.org/stable/3105385>. I owe this point to an anonymous reviewer.



that strain the economy and lead to overcrowding.⁴¹ This dynamic is especially true for disruptive technologies whose attributes often interact with their environment in ways their designers may not have anticipated, but which users find beneficial.

cerns that motivated the just war tradition.⁴³

In the military context, norms for warfighting are more broadly captured in what Michael Walzer refers to as the “war convention,” which is “the set of articulated norms, customs, professional codes,

Acknowledging the importance of consent in determining specific moral obligations does not mean treating others in the way they would prefer.

However, this dynamic invites a “give and take” of reasons and interests regarding both which technologies to develop as well as the rules to govern their use that is not unlike John Rawls’ conception of reflective equilibrium, where, in the narrow version, one revises one’s moral beliefs until arriving at a level of coherency where not only are all beliefs compatible, but in some cases, they explain other beliefs.⁴² While likely a good descriptive account of what happens in the formation of moral beliefs, such a process will not necessarily give an account of what those beliefs *should* be. For that, we need an assessment of what should be of moral concern — in this case, regarding disruptive technologies.

Assessing Disruption

So far, I have described disruption in terms of its effect on competition and the norms that govern it. However, simply challenging traditional norms is not by itself unethical. For example, the introduction of long-range weaponry eventually displaced chivalric norms of warfighting, which were really more about personal honor than the kinds of humanitarian con-

legal precepts, religious and philosophical principles, and reciprocal arrangements that shape our judgments of military conduct,” which includes choices regarding how to fight

wars and with what means.⁴⁴ The war convention includes the just war tradition, which evolved to govern when states are permitted to go to war and how they can fight in them. In general, the purpose of the just war tradition is to prevent war and, should that fail, limit the harms caused by war. Many theories fall under this tradition, some more restrictive than others. For the purposes of this discussion, it makes sense to set a reasonably high standard, which, if met, should provide a sense of confidence that developing certain technologies is permissible, if not obligated. Thus, I employ an understanding of just war that draws largely on Walzer’s work, *Just and Unjust Wars*, except where otherwise noted.

Walzer’s conception of *jus ad bellum* demands wars only be fought by a legitimate authority for a just cause and even then only if it can be done so proportionally, with a reasonable chance for success, and only as a last resort.⁴⁵ When it comes to fighting wars, *jus in bello* further requires force be used discriminately to avoid harm to noncombatants and in proportion to the value of the military objective.⁴⁶ These conditions suggest that any technology that makes war more likely, less discrimi-

41 Kranzberg, “Technology and History,” 547.

42 John Rawls, *A Theory of Justice* (Cambridge, MA: Belknap Press, 1971), 48–51. Employing reflective equilibrium in this context does not require one to accept the entirety of Rawls’ political theories. However, in the context of policymaking, this process requires one to account for how all of one’s moral beliefs and commitments fit together and then how that fit relates to others’ beliefs and commitments. Thus, it is more a strategy of giving and taking of reasons with the point of developing a stable consensus regarding what, in any given context, counts as morally good.

43 Peter Olsthoorn, *Military Ethics and Virtues: An Interdisciplinary Approach for the 21st Century* (London: Routledge, 2011), 19–20.

44 Walzer, *Just and Unjust Wars*, 44.

45 Walzer, *Just and Unjust Wars*, 51–124. See, Eric Patterson, *Just War Thinking: Morality and Pragmatism in the Struggle Against Contemporary Threats* (Lanham, MD: Lexington Books, 2007), 22–23. Patterson provides a more concise list of *jus ad bellum* conditions that is largely in line with Walzer’s view but that draws on ancient, medieval, as well as contemporary sources. He lists just cause, comparative justice, legitimate authority, right intention, probability of success, proportionality, and last resort as conditions for a just war. It is the case that there is some variation on the conditions of just war among different theories and approaches. The ones listed in the text, however, are generally common to most theories, most of which address the same categories as Walzer, if not also with the same conclusions.

46 Walzer, *Just and Unjust Wars*, 127–59. See also, Patterson, *Just War Thinking*, 23.

nate, or less proportional is going to be problematic, if not prohibited.

These norms only govern the initiation and conduct of war. The acquisition of technology, however, impacts much more than just how wars are fought. It also impacts soldiers and the societies they serve in ways that Walzer's war convention does not address. To assess those impacts requires a broader framework to fully account for the range of moral commitments that these technologies challenge. Establishing such a framework naturally requires a review of those commitments.

From a Kantian perspective, moral commitment begins with moral autonomy, as it is the ability to make moral choices that allows for morality in the first place.⁴⁷ Thus, anything that undermines moral autonomy will either be prohibited or there will have to be some account given why compromises to it should be permitted. Concerns regarding moral autonomy in turn give rise to concerns regarding fairness. As Rawls observed, people act autonomously when they choose the principles of their action as "the most adequate possible expression" of their nature as "free and equal" rational beings.⁴⁸ Because people are free and equal in this way, they are entitled to equal treatment by others. This requirement of fairness, which Rawls saw as synonymous with justice, is reflected in the universality of moral principles: They apply to all, regardless of contingencies such as desire and interest.⁴⁹

Any discussion of fairness, of course, will require answering the question, "Fairness about what?" For Rawls, it is fairness over the distribution of a broad range of social goods. However, in a military context, one can narrow those goods down to reward and risk. When it comes to warfighting, soldiers in general seek victory while minimizing the cost, both in terms of personnel, equipment, and other resources associated with achieving that victory.

As with the concept of reflective equilibrium, it is not necessary to ignore the critiques and limitations of Rawls' broader political theories in order to accept a commitment to moral and legal universalism that upholds the equality and dignity of persons.⁵⁰ At a minimum, that commitment means

treating others in a manner to which they have consented. Acknowledging the importance of consent in determining specific moral obligations does not mean treating others in the way they would prefer. Kant acknowledged that people consent to treatment by virtue of their actions, not their desires. In this way, consent enables imprisoning thieves, killing enemies, and ordering soldiers to take risks.

Of course some sentences, killings, and risks are not acceptable even if they are fairly distributed. Human life and well-being has its own intrinsic value. As Kant also argued, the fact that people can exercise moral autonomy gives them an inherent dignity that entitles them to be treated as ends and not merely as means to some other end.⁵¹ As a result, all people have a duty "to promote according to one's means the happiness of others in need, without hoping for something in return."⁵² A consequence of that duty is to care not just for the lives of others but for the quality of that life as well. In the military context, this duty extends to both soldiers and civilians who may be affected by the acquisition of a new technology.

Disruptive technologies do not just impact individuals, but also have an effect on the groups to which individuals belong. Thus, it is necessary to take into account the effect these technologies have on the military profession as well as the society a military serves. To the extent these technologies change the way soldiers experience reward and risk, they change how the profession serves its role and in so doing changes soldiers' professional identity. Moreover, these technologies can also change how members of the military profession hold themselves accountable. Reliance on autonomous systems, for example, may mitigate human responsibility in ways that lead to impermissible acts for which no one is accountable. Similarly, enhancements could impair cognitive functioning in ways that make it impossible to attribute praise or blame to individuals.⁵³ Together, these developments could change the professional identity of the military, which in turn will change the way society views and values the service the profession provides.

47 Immanuel Kant, *Foundations of the Metaphysics of Morals*, trans. Lewis White Beck (Indianapolis, IN: Bobbs-Merrill Educational Publishing, 1983), 9.

48 Rawls, *A Theory of Justice*, 252.

49 Rawls, *A Theory of Justice*, 253.

50 Seyla Benhabib, "High Liberalism: John Rawls and the Crisis of Liberal Democracy," *The Nation*, Oct. 29, 2019, <https://www.thenation.com/article/john-rawls-liberal-philosophy-review/>. Benhabib provides an excellent and accessible critique of Rawls' theory that correctly points out not just its limitations, but how it can be misapplied.

51 Immanuel Kant, *The Metaphysics of Morals* (Cambridge, UK: Cambridge University Press, 1991), 49.

52 Kant, *The Metaphysics of Morals*, 247.

53 I owe this point to an anonymous reviewer, Dec. 11, 2019.



Society's relationship to the military profession is, of course, complex. In general, society values the profession not just in terms of the service it provides, but also because of the risks required to provide that service. The unmanned aerial vehicle operator may provide as good a service as the infantry soldier on the ground. However, their service is valued differently, as evidenced by the controversy over awarding unmanned aerial vehicle operators a medal superior to the Bronze Star, which is normally reserved for those serving in combat zones.⁵⁴ While such reevaluation may not affect the relationship between political and military leaders, it can change how military service is regarded, how it is rewarded, and perhaps most importantly, who joins. Army Cyber Command is already discussing ways to alter physical requirements in order to get individuals with cyber skills into the service.⁵⁵

Society can also be affected more directly by the kinds of technology the military acquires. Aircraft technology, for example, benefited from military investment, which paved the way for today's mass airline travel. The technologies under discussion here could have a similar impact. For example, human enhancements could result in enhanced veterans entering the civilian workforce, possibly putting unenhanced civilians at a disadvantage. This could then force society to accept enhancements for civilians it might not have otherwise, so that civilians can remain competitive. This last point is speculative, but it does suggest that the disruptive effects of military technologies are not confined to the military.

The above analysis establishes the following categories with which to make a moral assessment of the disruptive effects of technology: autonomy, justice, well-being, and social disruption. In what follows, I will describe in more detail how disruptive technologies challenge moral commitments within each category. The point here is not that these concerns cannot be addressed but rather to highlight the need to do so.

Moral Autonomy

Moral autonomy is required for moral accountability. The reason is fairly straightforward: If one's choices are determined by factors independent of one's will, then one cannot be fully responsible for the choices one makes. Exercising that will requires a certain cognitive capacity to appropriately collect and assess information that is relevant to moral choices and act on that information.⁵⁶ It is not hard to see how new technologies could impact those abilities.

Take, for example, artificial intelligence, which can displace humans in the decision-making process, thus removing moral agency from life and death decisions. With conventional systems, when something goes wrong, accountability, in principle at least, can be assigned to the operator, the manufacturer, the designer, or another human involved in the design, acquisition, and employment process. AI-systems, on the other hand, can be a "black box," where it is not always clear why or even how the machine decides on a particular outcome or behavior. Because of this, it is impossible not only to determine who may have erred, but whether there was an error in the first place. As Hin-Yan Liu points out regarding lethal uses of artificial intelligence, unjust harms can arise not just from bad intent and negligence, but from everyone doing a "job well done."⁵⁷

This point is more intuitive than it sounds. Take, for example, noncombatant deaths. If soldiers intentionally kill noncombatants, they have committed a war crime. Others, like their commanders, who may have ordered or encouraged them to do so, would thus share responsibility. Even without such malicious intent, weapon systems can be used improperly or malfunction, also leading to noncombatant deaths. For example, the 2016 airstrike against a Doctors Without Borders hospital in Afghanistan that killed 42 people was the result of multiple human errors. While no one involved intended to strike a hospital, bad instructions, poor procedures, communication and targeting-system malfunctions, and possibly some recklessness all

54 Andrew Tilghman, "DOD Rejects 'Nintendo Medal' for Drone Pilots and Cyber Warriors," *Military Times*, Jan. 6, 2016, <https://www.military-times.com/2016/01/06/dod-rejects-nintendo-medal-for-drone-pilots-and-cyber-warriors/>.

55 Crispin Burke, "The Pentagon Should Adjust Standards for Cyber Soldiers — As It Has Always Done," *War on the Rocks*, Jan. 24, 2018, <https://warontherocks.com/2018/01/pentagon-adjust-standards-cyber-soldiers-always-done/>. Army Cyber Command currently offers the possibility of a direct commission for STEM-educated persons to join the command, something previously reserved for medical, legal, and religious fields. See, "Cyber Direct Commissioning Program," Department of the Army, Army Cyber, accessed Oct. 29, 2019, <https://www.goarmy.com/army-cyber/cyber-direct-commissioning-program.html>.

56 Wallach and Allen, *Moral Machines*, 16.

57 Hin-Yan Liu, "Refining Responsibility: Differentiating Two Types of Responsibility Issues Raised by Autonomous Weapons Systems," in *Autonomous Weapon Systems: Law, Ethics, Policy*, ed. Nehal Bhuta et al. (Cambridge, UK: Cambridge University Press, 2016), 340.

contributed to the incident. Whether one agrees with the severity of the punishment or not, those individuals were held accountable.⁵⁸

With AI, such tragedies can occur without their being a function of chance or human error and thus no one can be held accountable. For example, AI systems associated with hiring, security, and the criminal justice system have demonstrated biases that have led to unjust outcomes independent of any biases developers or users might have.⁵⁹ It is not hard to imagine similar biases creeping in to AI-driven targeting systems. Of course, developers, commanders, and operators can make mistakes in the development and employment of AI technology for which they *can* be held responsible. However, there is little precedent for holding persons, including commanders, responsible for legal or moral violations when there is no action or failure to act that contributed to the violation.⁶⁰

For example, despite Staff Sgt. Robert Bales' being found guilty of murdering 16 Afghan civilians in 2016, no one in the chain of command was held accountable for those murders.⁶¹ This is, in part, because, even under the idea of command responsibility, there has to be some wrongful act or negligence for which to hold the commander responsible.⁶² It also arises because one *can* hold Bales' responsible. With AI, there may be no mediating morally autonomous agent between commanders, operators, or developers and the violation. Thus, an "accountability gap" arises from there being no one to whom one can assign moral fault when moral harm has been done.⁶³

Such a gap threatens to undermine the application of the war convention. Norms are the means by which people hold each other accountable. However, when norms are not upheld, they die.⁶⁴ It is not hard to understand how: If one person violates a norm without being held accountable, others will be incentivized to do so as well. Over time, with

enough violations, everyone feels free to violate the norm and it ceases to exist. That is not necessarily a bad thing. The civil rights movement, for example, succeeded by violating segregationist norms to the point that those who tried to impose them were themselves sanctioned. However, if violations of the war conventions committed by machines are attributed as mere accidents, soldiers may be incentivized to use them even when not entirely necessary. Over time, holding humans accountable would seem pointless, if not impossible.⁶⁵

One could just restrict the use of AI systems but that ignores the problem of disruptive technologies and exacerbates the tension between effectively using a technology, which can have its own moral force, and risking moral harm. On the other hand, one could just adopt a policy whereby commanders and operators are held accountable for violations committed by autonomous machines under their supervision or control, whether there is any wrongful act or negligence on their part or not. Doing so, however, will disincentivize their use, defeating the purpose of introducing them in the first place. Thus, such policies, rather than resolving concerns regarding accountability, simply are alternate means to banning autonomous machines. As a result, they do not solve the problem, they merely ignore it.

Certainly, there are remedies to the accountability gap. Nevertheless, when acquiring technologies where this gap — or others like it — exists, one has a moral obligation to seek such remedies or restrict their use, a point I will return to later. Otherwise, to the extent these technologies can absolve humans of accountability for at least some violations, it will establish an incentive to employ them more often and find ways to blame them when something goes wrong, even when a human is actually responsible. It is not hard to imagine that, over time, there would be enough unaccountable violations that the rules themselves would be rarely applied, even to humans.

58 Matthew Rosenberg, "Pentagon Details Chain of Errors in Strike on Afghan Hospital," *New York Times*, April 29, 2016, <https://www.nytimes.com/2016/04/30/world/asia/afghanistan-doctors-without-borders-hospital-strike.html>. According to CENTCOM, all punishments were administrative as opposed to criminal *because* there was no intent to commit a war crime by anyone involved.

59 Karen Hao, "This Is How AI Bias Really Happens — and Why It's So Hard to Fix," *MIT Technology Review*, Feb. 4, 2019, <https://www.technologyreview.com/s/612876/this-is-how-ai-bias-really-happens-and-why-its-so-hard-to-fix/>. Often, the bias is introduced because of the nature of the data collected, though that bias is not apparent at the time of its collection.

60 For a more complete discussion of AI and its implications for moral autonomy, see, C. Anthony Pfaff, "The Ethics of Acquiring Disruptive Technologies: Artificial Intelligence, Autonomous Weapons, and Decision Support Systems," in *Special Report: Ethical Implications of Large Scale Combat Operations* (Leavenworth, KS: Simons Center, 2019), 140–41, <http://thesimonscenter.org/special-report-ethical-implications-of-lsco/>.

61 Richard Sisk, "US Army Leaders Cleared of Wrongdoing in Soldier's Killing Spree," *Military.com*, Aug. 18, 2015, <https://www.military.com/daily-news/2015/08/18/us-army-leaders-cleared-of-wrongdoing-in-soldiers-killing-spree.html>.

62 Sanford Levinson, "Responsibility for Crimes of War," in *War and Moral Responsibility*, ed. Marshall Cohen, Thomas Nagel, and Thomas Scanlon (Princeton, NJ: Princeton University Press, 1974), 117–18.

63 Heather M. Roff, "Killing in War: Responsibility, Liability, and Lethal Autonomous Robots," in *The Routledge Handbook of Ethics in War: Just War Theory in the Twenty-First Century*, ed. Fritz Allhoff, Nicholas G. Evans, and Adam Henschke (New York: Routledge, 2013), 355.

64 Geoffrey Brennan et al., *Explaining Norms* (Oxford: Oxford University Press, 2013), 35–39.

65 Pfaff, "The Ethics of Acquiring Disruptive Technologies," 133–34.



Moreover, AI systems are not the only technologies that threaten moral autonomy. To the extent that enhancements or other medical interventions suppress fear or enhance aggression they mitigate the responsibility of an agent under their influence.

Human enhancements can also pose a challenge to the exercise of moral autonomy in terms of the role that consent, which is an expression of moral autonomy, should play when authorizing medical interventions intended to improve soldier resilience or lethality. One could simply adopt a policy requiring consent. However, necessity will impose a great deal of pressure to override that requirement not only in cases where consent is not possible to obtain, but when it simply is not likely to be forthcoming. The U.S. military, for example, sought and received a consent waiver to provide pyridostigmine bromide to counteract the effects of nerve agent by arguing a combination of military necessity, benefit to soldiers, inability to obtain informed consent, and lack of effective alternatives that did not require informed consent.⁶⁶

Faced with a choice of risking some negative side effects to soldiers or significant casualties and possible mission failure, the Department of Defense conformed to Rawls' condition that goods — in this case the right to consent — should only be sacrificed to obtain more of the same good. Assuming the vaccine was effective, had the Iraqis used nerve agent arguably more soldiers' lives would have been spared than those affected by symptoms later on.

I will say more regarding whether the Defense Department's decision was justified later. For now, it is important to note that part of the department's justification was that there was not sufficient time to test the safety of the drug. While it had been shown to be safe for patients with a certain autoimmune disease, there was insufficient testing on healthy populations to understand the range of effects the drug could have. However, the Defense Department had been stockpiling pyridostigmine bromide for use as a nerve agent vaccine since 1986, but had not taken any steps to collect the data necessary to determine the safety of the drug.⁶⁷ Thus, as Ross M. Boyce points out, the department's claim that obtaining consent was not feasible was really "code" for "non-consent is not acceptable."⁶⁸

This point simply underscores the importance of addressing one's moral commitments regarding new technology early in the development and acquisition process.

Enhancements also have a coercive side that can render consent pointless. To the extent an enhancement improves soldiers' short-term survivability, there can be significant pressure to accept the enhancement despite the possibility of long-term side effects. Depending on the severity and likelihood of the side effects and the degree to which the enhancement improves chances of survivability, accepting the enhancement and risking the side effects will typically make sense. Placing persons in such a situation, where they must choose between undesirable options, is a form of coercion.⁶⁹

Justice

In the context of military ethics, most concerns of justice are captured in the just war tradition, which, as described above, is a subset of the war convention. The principles associated with both the ends of war (*jus ad bellum*) and the means of war (*jus in bello*) in the war convention are intended to apply universally, regardless of which side one is on. Embedded in the tradition is a conception of human dignity that allows for holding others accountable for their actions, but not using them as mere means. One is permitted to kill an enemy, for example, because the enemy is a threat. When an enemy is no longer a threat, either due to surrender or injuries, that permission goes away. In this way, the just war tradition recognizes the equality of all the actors without having to recognize the moral equality of their respective causes.

Technology can impact justice at both these levels. Any technology that distances soldiers from the violence they do or decreases harm to civilians will lower the political risks associated with using that technology.⁷⁰ The ethical concern here is to ensure that decreased risk does not result in increased willingness to use force. By decreasing risk, these technologies can incentivize disregarding costlier, but nonviolent, alternatives, possibly violating the condition of last resort. Thus, one risks offsetting the moral advantage gained from

66 Patrick Lin, Maxwell Mehlman, and Keith Abney, *Enhanced Warfighters: Risk, Ethics, Policy* (Cleveland, OH: Case Western University, 2013), 47; and Efthimos Parasidis, "Human Enhancement and Experimental Research in the Military," *Connecticut Law Review* 44 no. 4 (April 2012): 1125, in Pfaff, "Moral Autonomy and the Ethics of Soldier Enhancement," 31.

67 Boyce, "Waiver of Consent," 14.

68 Boyce, "Waiver of Consent," 10.

69 Pfaff, "Moral Autonomy and the Ethics of Soldier Enhancement," 33–34.

70 Of course, decreasing risk to soldiers often comes at the expense of increasing risk to civilians and vice versa. The point here is that committing to one over the other does not necessarily bring about better moral outcomes.

greater precision and distance.

The question of adhering to just war norms, however, does not exhaust the justice concerns associated with disruptive technologies in the military context. The accountability gap also raises such issues. One could, for example, adopt a general policy holding operators and commanders responsible for the actions of the machines they employ. However, as noted above, those operators and commanders could do everything right *and* their machines could be functioning appropriately and moral harm could still be done. It seems unjust to place soldiers in such a position.

Human enhancement technologies similarly raise fairness concerns. It might seem unfair to provide some soldiers enhancements while denying it to others. However, one can always compensate non-enhanced soldiers by reducing their risk. But to the extent those enhancements make the soldier more lethal, they also make it more likely enhanced soldiers will see combat and thus be exposed to more risk. Thus, in the military context, inequality can accrue to the enhanced rather than the non-enhanced. What may matter more is not who *gets* to receive an enhancement as much as it is who *must* receive one.

Cyber technologies also raise concerns regarding justice, most notably when it comes to privacy. Edward Snowden's revelations that the U.S. government collected information on its citizens' private communications elicited protests as well as legal challenges about the constitutionality of the data collection.⁷¹ While these revelations mostly raised civil rights concerns, the fact that other state and nonstate actors can conduct similar data collection also raises national security concerns. Maj. Gen. Charles Dunlap observed back in 2014 that U.S. adversaries, both state and nonstate, could identify, target, and threaten family members of servicemembers in combat overseas, in a way that could violate international law.⁷²

In what Dunlap refers to as the "hyper-personalization" of war, adversaries could use cyber technologies to threaten or facilitate acts of violence against

combatants' family members unless the combatant ceases to participate in hostilities.⁷³ Adversaries could also disrupt family members' access to banking, financial, government, or social services in ways that significantly disrupt their life. Such operations would violate the principle of discrimination as well as expand the kinds of intentional and collateral harm civilians can suffer in wartime.

Well-Being

Well-being takes into account not only physical safety and health, but also mental health and quality of life. So far, this discussion has provided numerous examples where disruptive technologies have placed all those concerns at risk. Pervitin, for example, caused circulatory and cognitive disorders.⁷⁴ Pyridostigmine bromide use is also closely associated with a number of long-term side effects including "fatigue, headaches, cognitive dysfunction, musculoskeletal pain, and respiratory, gastrointestinal and dermatologic complaints."⁷⁵ As noted above, the likelihood of these side effects was not fully taken into account due to inadequate testing at the time.

Human enhancement technologies are not the only technologies that pose a risk to the well-being of soldiers. Risk-reducing technologies, such as autonomous weapon systems or cyber operations conducted from positions of relative safety, have been associated with both desensitization and trauma on the part of operators. In fact, use of these technologies has resulted in a complex variety of mental injuries among soldiers who employ remote systems. For example, a 2017 study catalogued a number of mental trauma, including moral disengagement as well as intensified feelings of guilt resulting from riskless killing among drone operators.⁷⁶ Making matters even more complex, a 2019 study of British drone operators suggested that environmental factors, such as work hours and shift patterns, contributed as much, if not more so, to the experience of men-

71 Patrick Toomey, "The NSA Continues to Violate Americans' Internet Privacy Rights," The American Civil Liberties Union, Aug. 22, 2018, <https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy>.

72 Charles J. Dunlap Jr., "The Hyper-Personalization of War: Cyber, Big Data, and the Changing Face of Conflict," *Georgetown Journal of International Affairs* (2014): 115, https://scholarship.law.duke.edu/faculty_scholarship/3381/.

73 Dunlap, "The Hyper-Personalization of War," 115.

74 Norman Ohler, *Blitzed: Drugs in Nazi Germany* (London: Allen Lane, 2016). See also, Andreas Ulrich, "The Nazi Death Machine: Hitler's Drugged Soldiers," *Der Spiegel*, May 6, 2005, <http://www.spiegel.de/international/the-nazi-death-machine-hitler-s-drugged-soldiers-a-354606.html>.

75 Roberta F. White, et al., "Recent Research on Gulf War Illness and Other Health Problems in Veterans of the 1991 Gulf War: Effects of Toxicant Exposures During Deployment," *Cortex*, no. 74, (January 2016): 456, <https://doi.org/10.1016/j.cortex.2015.08.022>.

76 Alaa Hijazi et al., "Psychological Dimensions of Drone Warfare," *Current Psychology* 38, no. 5, (October 2019): 1285–96, <http://dx.doi.org/10.1007/s12144-017-9684-7>.



tal injury as visually traumatic events associated with the strikes themselves.⁷⁷

Social Disruption

Social disruption in this context has two components. The first is the civilian-military relationship, which is expressed not only in terms of control, but also in terms of how that relationship reflects how a military organizes for war and performs in combat.⁷⁸ Risk-reducing technologies, for example, not only alter how society rewards military service, it can alter who serves. As P.W. Singer observed a decade ago, multiple technologies are driving the military demographic toward being both older and smarter — the average age of the soldier in Vietnam was 22, whereas in Iraq it was 27.⁷⁹ Further complicating the picture is the fact that those younger soldiers may be better suited to using emerging military technologies than those who are older and in charge.⁸⁰

Not only could this pressure the military to reconsider how it distributes command responsibilities, it also pressures it to reconsider whom it recruits, as mentioned above.

Singer also notes, however, that contractors and civilians, who are not subject to physical or other requirements associated with active military service, may be better positioned to use these autonomous and semi-autonomous technologies.⁸¹ Doing so, especially in the case of contractors, could allow the military to engage in armed conflict while displacing health care and other costs to the private sector. If, as discussed above, remote warfare comes with its own harms, or if operators in the future require enhancements to operate the equipment, there could be a significant population of physically and mentally injured people who do

not have adequate health care. Consider: 80 percent of contractors who deployed to Iraq reported having health insurance for the time they were deployed, but that insurance was not available if they experienced symptoms after their return.⁸²

In addition, these trends could affect the professional status of the military. If the expert knowledge required to defend the nation is predominantly employed by civilians, it is possible that the military will not retain its professional status. Instead, it could devolve into a technocratic bureaucracy that manages civilian skills and capabilities, while relatively few soldiers bear the burden of risk.⁸³ Such a bureaucracy will not be up to the task of the ethical management of disruptive technologies.

It is this reduction of risk, which is arguably the point of military innovation in general, that will have the most disruptive impact on the civilian-military relationship. Society rewards soldiers precisely because they expose themselves to risks and hardships on society's behalf. If soldiers experience neither risk nor sacrifice, they are not really soldiers as currently conceived and are likely better thought of as technicians than warriors. While enhancing soldier survivability and lethality always makes moral sense, enhancing it to the point of near-invulnerability (or even the perception of invulnerability) will profoundly alter the warrior identity. This is not necessarily a bad thing, but militaries need to be prepared for such disruptive effects.⁸⁴

The second concern, of course, is the transfer of technology — or its effects — to civil society. Of course, such a transfer is not always a bad thing. Perhaps the most beneficial technology of all, duct tape, was developed by Johnson and Johnson to seal ammunition boxes so they could be opened quickly.⁸⁵ Missile technologies for military use, another example, paved the way for space explo-

77 A. Phillips, D. Sherwood, N. Greenberg, and N. Jones, "Occupational Stress in Remotely Piloted Aircraft System Operators," *Occupational Medicine* 69, no. 4 (June 2019): 244–50, <http://dx.doi.org/10.1093/occmed/kqz054>.

78 Martin Shaw, *The New Western Way of War* (Cambridge, UK: Polity Press, 2005), 42. Martin Shaw describes a way of war as a "particular way of organizing for war adopted by an actor or group of actors."

79 Kim Parker, Anthony Cilluffo, and Renee Stepler, "6 facts About the U.S. Military and Its Changing Demographics," *Pew Research Center*, April 13, 2017, <https://www.pewresearch.org/fact-tank/2017/04/13/6-facts-about-the-u-s-military-and-its-changing-demographics/>. According to this report, in 2017, the average age of enlisted soldiers was 27 years old. The survey also notes that 92 percent of enlisted have completed high school or some college, compared to 60 percent for civilians of similar ages. However, 19 percent of civilians in the same age range have bachelor's degrees compared to 7 percent of enlisted.

80 P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (London: Penguin Books, 2009), 368–71.

81 Singer, *Wired for War*, 372.

82 Molly Dunigan et al., *Out of the Shadows: The Health and Well-Being of Private Contractors Working in Conflict Environments* (Santa Monica, CA: Rand Corp., 2013), xvii–xviii.

83 Don M. Snider, "The U.S. Army as Profession," in *The Future of the Army Profession*, ed. Lloyd J. Matthews (Boston: McGraw Hill, 2005), 13.

84 Pfaff, "Moral Autonomy and the Ethics of Soldier Enhancement," 32–33. See also, Nick Bostrom, "Dignity and Enhancement," in *Human Dignity and Bioethics: Essays Commissioned by the President's Council on Bioethics* (Washington, DC: Georgetown University, March 2008), https://bioethicsarchive.georgetown.edu/pcbe/reports/human_dignity/chapter8.html. Bostrom writes more generally on how enhancements impact human dignity and affect how humans assess the value of the actions of others.

85 "The Long History of Duct Tape," PPM Industries, Feb. 14, 2017, <https://www.ppmindustries.com/en/news/long-history-duct-tape>.

ration. However, not all transfers of military innovation are as helpful as these. Cocaine use, for example, became widespread in Europe during and after World War I as addicted troops returned home.⁸⁶ Of course, military technologies would not transfer to civilian use unless there is a perceived benefit. However, even when there is such a benefit, there can also be a downside to those transfers. One major concern is the way military research often can distort research priorities and direct technology development in a way that reduces the efficiency of civilian applications. For example, the U.S. Navy's dominant role in the development of nuclear reactors led to design choices that were less efficient and came with greater risk than alternative designs.⁸⁷

There is, of course, a lot more one can say regarding the potential disruptive effects of these technologies. Perhaps more to the point, there is not much more to say regarding whether the United States should develop these technologies for military purposes. As long as adversaries are willing to do so, as noted earlier, the pressure to develop such technologies will be overwhelming. What we now need is an ethic governing that development.

Permissibility and Disruptive Technologies

Military ethics employs a certain logic. This logic begins with a just cause, understood as a response to an act of aggression. In response to that aggression, soldiers will seek means that maximize the harm done to the enemy while minimizing risk to themselves. Such means are justified by virtue of the fact that if one is fighting for a just cause, one maximizes the good by winning. While such justification does preclude gratuitous acts of violence, it precludes little else. Military necessity will justify

whatever means are more likely to lead to victory with the least expenditure of time, resources, and human lives. Since enemy lives — both combatant and noncombatant — stand in the way of that victory, they are discounted relative to those defending against an aggression. Thus, if one left the justification for military measures to utilitarian calculations, then no technologies — including weapons of mass destruction — would be prohib-

If soldiers experience neither risk nor sacrifice, they are not really soldiers as currently conceived and are likely better thought of as technicians than warriors.

ited as long as one could make a reasonable case that harm to the enemy was maximized and risk to one's own soldiers minimized.

However, as Walzer notes, while “the limits of utility and proportionality are very important, they do not exhaust the war convention.”⁸⁸ That is because, even in war, people have rights, and those who do not pose a threat, whatever side of the conflict they are on, have a right not to be intentionally killed.⁸⁹ As Arthur Isak Applbaum puts it, utility theory “fails to recognize that how you treat people, and not merely how people are treated, morally matters.”⁹⁰

Thus, while aggression permits a response, it does not permit any response. Just as an act of aggression represents a violation of rights, any response should respect rights, which is to say it should be discriminate, necessary, and proportional. To be morally permissible, the effect of the means used has to not only conform to *jus in bello* norms associated with international humanitarian law and, more broadly, the just war tradition, but also to the obligations one owes members of one's community — both soldiers and civilians alike. To be necessary, there must not be any effective alternative that results in less harm. To be proportional, the good achieved must outweigh

86 Lukasz Kamienski, *Shooting Up: A Short History of Drugs and War* (Oxford: Oxford University Press, 2016), 96–97.

87 Mario Pianta, *New Technologies Across the Atlantic: US Leadership or European Autonomy?* (Tokyo: The United Nations University Press, 1988), section 4.3, <https://unu.edu/publications/books/new-technologies-across-the-atlantic-us-leadership-or-european-autonomy.html>.

88 Walzer, *Just and Unjust Wars*, 130.

89 Thomas Nagel, “War and Massacre,” *Philosophy and Public Affairs* 1, no. 2 (Winter 1972): 123–44, <http://www.jstor.org/stable/2264967>.

90 Arthur Isak Applbaum, *Ethics for Adversaries: The Morality of Roles in Public and Professional Life* (Princeton, NJ: Princeton University Press, 1999), 173.



the harm. These conditions apply not just to the technologies themselves, but to the disruption they cause.

In what follows, I will discuss each of these conditions and how they apply to disruptive technologies to arrive at a general framework for their acquisition.

Moral Effect

Moral effect refers to the potential that employing a weapon, or any means of warfare, has for conforming to or violating moral norms. Conforming to these norms is one of the conditions required to determine the moral permissibility of developing a disruptive technology. Moral effect not only concerns a technology's effect on noncombatants or other prohibited targets but also on the soldiers who would employ them and the society they defend. There are, of course, already rules in place governing the acquisition of new military technology. International law prohibits the development and acquisition of weapons that intentionally cause unnecessary suffering, are indiscriminate in nature, or cause widespread, long-term and severe

damage to the natural environment or entail a modification to the natural environment that results in consequences prohibited by the war convention.⁹¹ It goes without saying that these rules would apply to disruptive technologies.

To the extent new technologies would violate these rules, they would be characterized *mala in se*, or "evil in themselves." Acquiring such technologies would be prohibited. In fact, Article 36 of the Geneva Conventions' Additional Protocol I specifically states,

In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.⁹²

The protocol, like the rest of the war convention, only addresses obligations to adversaries. Unsurprisingly, it says little about what one owes one's own citizens and soldiers. Here, Kant's imperative

91 William H. Boothby, ed., *New Technologies and the Law in War and Peace* (Cambridge, UK: Cambridge University Press, 2019), 37.

92 Yoram Dinstein, *The Conduct of Hostilities Under the Law of International Armed Conflict* (Cambridge, UK: Cambridge University Press, 2010), 87.

to avoid treating people as mere means applies. In general, complying with this imperative means governments and military commanders should avoid deceptive and coercive policies when it comes to new technology acquisition and employment. Having said that, respecting someone as an end does not always entail taking into account individual preference. By taking on their particular role, soldiers have agreed to take on certain risks and make certain sacrifices in service to their country. These risks and sacrifices require, sometimes at least, subordinating their autonomy to military necessity. While I will discuss necessity in more detail later, the question here is, when is such subordination permissible?

Boyce, in his discussion regarding the use of pyridostigmine bromide in the Gulf War, acknowledges the government's claim that soldiers may be subjected to some risk of harm if it "promotes protection of the overall force and the accomplishment of the mission."⁹³ As noted above, such a utilitarian limit is helpful, in that it does restrict what counts as permissible by aligning it with the needs of other soldiers and citizens. As is true regarding most utilitarian constraints, however, this limit still seems to permit too much. In this case, it allowed the government to force soldiers to take a drug that had not been adequately tested and which caused subsequent harm.

The problem with following a general policy that soldier autonomy should be subordinated to the greater good is that such calculations pit individual interests against often ill-defined conceptions of the good or insufficient understandings of how a particular act works to realize the good. The fact that no soldiers were exposed to nerve agent in the Gulf War underscores this point. The difficulty here is that these calculations are typically plagued by uncertainty and imprecision not only in causes and effects but also in weighing a particular good against a particular harm, points I will return to later in the discussion on proportionality. More importantly, as noted above, they also place few limits on the kinds of harm soldiers must endure as long as the government can make a plausible case that enough others benefit. So, just as moral effect places additional limits on how one treats an enemy, it should place similar limits on how one treats one's own citizens, including those who agreed to serve.

Thus, when questions of utility arise, we need a

way to ensure that whatever one does, one takes into account the interests of all the individuals affected by that decision. Sven Ove Hansson argues that permissions to expose others to risk should be based on one of the following justifications: self-interest, desert, compensation, and reciprocity.⁹⁴ Since the concern here is coercively assigning risk, self-interest and reciprocity do not really apply, though, as the discussion on autonomy showed, the conditions governing self and mutual interest can shape interests in a way that is essentially coercive. This does not mean that one should never permit individuals to take on such risks. It does, however, require considering the conditions under which such decisions are made and removing any unjust coercive elements.

Desert refers to the extent someone has done something to warrant involuntary exposure to risk. This category also does not apply to soldiers. Desert used in this sense is a function of justice: One's virtuous actions can entitle one to some benefit while one's vicious actions can entitle one to some punishment.⁹⁵ Becoming a soldier, by itself, is neither virtuous nor vicious. Individual motivations for joining the military range from the admirable, to the self-interested, to the pathological. One might admire the individual who foregoes a more lucrative civilian career to take on the burden of soldiering. But in such cases what one admires is the sacrifice more than the particular choice. One might also condemn the individual who joins because he or she enjoys the prospect of killing. But again, in general, it is the motivation we condemn, not the activity of soldiering. Since soldiering does not really factor into what one thinks either individual deserves, it cannot be the basis for coercively assigning risk based on desert.

A better basis for assigning risk that accounts for fairness is compensation. There are two forms of compensating for risk: One in which an individual accepts risk but is not harmed, and the other in which an individual is actually harmed.⁹⁶ In the former, one is compensated simply for taking risk and in the latter one is compensated only if harm occurs.

In general, society confers benefits on individuals who accept the risks associated with soldiering. In addition to pay and benefits, soldiers have opportunities for education and social recognition not available to civilians. To the extent soldiers are harmed while serving, they may accrue additional benefits

93 Boyce, "Waiver of Consent," 2.

94 Sven Ove Hansson, "Ethical Risk Analysis," in *The Ethics of Technology: Methods and Approaches*, ed. Sven Ove Hansson (London: Rowman and Littlefield, 2017), 162.

95 Rawls, *A Theory of Justice*, 314–15.

96 Hansson, "Ethical Risk Analysis," 163.



Thus, acting on the principle that it is fair to override consent in cases where no one is worse off and at least someone is better off seems a plausible justification for coercively assigning risk.

such as pensions and long-term medical care. Because soldiers consent to receive such benefits in exchange for their willingness to take risks, they may be ordered by their commanders into harm's way, even though there is the possibility they will die. More to the point, they may be ordered to do so despite their immediate preference otherwise.

There is, of course, an asymmetry in risk and compensation that suggests any compensation that the service or society offers is not going to be entirely commensurate with the sacrifices some soldiers will make. Soldiers take on an unlimited liability to harm because they have answered the call to serve and that is what service demands. However, there are limits on the sources of harm to which soldiers may be exposed. Soldiers are expected to risk being killed by the enemy. They are not expected to risk being killed by their leadership. That fact places a limit on the kinds of risks leaders can require soldiers to accept when assimilating new technologies, especially when the risks associated with those technologies are neither well understood nor thoroughly researched.

The role leadership plays, of course, obligates leaders to take extra measures to ensure soldier safety and well-being. It also obligates them to ensure that other less risky alternatives are taken into consideration. However, the uncertainty associated with these technologies means that such measures cannot fully guarantee that safety and well-being. The question then arises, should soldier consent be required when employing new technologies or are there conditions where it may be overridden?

As Applbaum also argues, in general, it is "fair" to act without someone's consent when it results in no one being worse off and at least some being better off. As he notes, "If a general principle sometimes is to a person's advantage and never is to that person's disadvantage (at least relative to the alternatives available), then actors who are guided by that principle can be understood to act for the sake of that person."⁹⁷ To illustrate, Applbaum draws on Bernard Williams' thought experiment where an evil army officer who has taken 20 pris-

oners offers a visitor named "Jim" the choice of killing one person in order to save the remaining 19 or killing no one, which will result in the evil actor killing all 20.⁹⁸

From the perspective of individual rights, Jim should not kill anyone. However, in this case, not violating one person's rights does not prevent the right from being violated. It just prevents additional violations. To the extent Jim presents each prisoner with an equal chance of being killed, the prisoners can understand that he is giving them a chance for survival and that he is doing so for their own sake, even though one person will be killed.⁹⁹ Thus, acting on the principle that it is fair to override consent in cases where no one is worse off and at least someone is better off seems a plausible justification for coercively assigning risk.¹⁰⁰

This rationale, in fact, was a factor in the Federal Drug Administration's (FDA) decision to grant the Department of Defense the pyridostigmine bromide waiver.¹⁰¹ Given equal chances of exposure to a nerve agent, everyone was in a better position to survive and since the expected side effects were not lethal, no one was in a worse position. Of course, given those side effects, granting the waiver is not a perfect application of this principle. Since there was no use of nerve agent, some were, in fact, worse off than if they had not taken the drug. However, what matters here is what soldiers would have chosen not knowing in advance what their individual chances were. Given the severe effects of the nerve agent and the relatively less severe possible side effects, it would be rational to take the drug. It is worth noting that the Defense Department agreed to follow up with those who took the drug to address any adverse effects.¹⁰² To date, these requirements have not been completely fulfilled.¹⁰³ That failure, however, does not undermine the principle. It does suggest an obligation to further minimize risk and harm even if the principle is fulfilled, but that is more a matter regarding appropriate compensation to soldiers exposed to the drug.

The remaining question is how to respond when adversaries persist in developing technologies

97 Applbaum, *Ethics for Adversaries*, 151.

98 Applbaum, *Ethics for Adversaries*, 150–51. For the original discussion of "Jim's Scenario," see, J.J.C. Smart and Bernard Williams, *Utilitarianism: For and Against* (Cambridge, UK: Cambridge University Press, 1973), 98–100. I discuss this scenario in Pfaff, "Moral Autonomy and the Ethics of Soldier Enhancement," 39–40.

99 Applbaum, *Ethics for Adversaries*, 151.

100 Of course, if Jim did not kill any of the civilians, it does not follow that their deaths are his fault. However, the point here is not to establish that killing the one individual is the best response to Williams' dilemma. It is just to highlight that utilitarian calculations are not the only justifications for shooting the one person. Rather one can choose to kill the one individual in a manner that maintains respect for people in a way that utilitarianism does not.

101 Lin, Mehlman, and Abney, *Enhanced Warfighters*, 37.

102 Pfaff, "Moral Autonomy and the Ethics of Soldier Enhancement," 39–40.

103 Parasidis, "Human Enhancement and Experimental Research in the Military," 1125–26.

that would otherwise be prohibited. Would that fact justify developing such technologies as well? The rationale behind the 1868 Declaration of St. Petersburg serves as a possible justification for doing so. In the mid-1860s, the Russian Imperial Army acquired exploding bullets that shattered on contact with soft surfaces and whose intended use was to blow up ammunition wagons. Even at the time, the imperial war minister considered it improper to use these bullets against troops because it caused suffering that was unnecessary to the purpose of military force, which is destroying enemy combat capability. In 1868, Russia convened a conference in St. Petersburg with 16 states, which resulted in an agreement to ban exploding projectiles under 400 grams, due to the unnecessary suffering they cause. At the conference, Prussia requested that the scope be broadened to deal with any scientific discoveries that had military applications, but Britain and France opposed and the request was not adopted.¹⁰⁴

The Russians did not develop exploding bullets with the intent to ban them. However, once the technology found an application that would have rendered them *mala in se*, they used the bullets as leverage to put a ban in place. This point suggests that there may be conditions where developing a prohibited technology — even if one does not field it — for its deterrent or counter-proliferation effect makes sense. Of course, pursuing a general policy that permits such development comes with a great deal of risk. Once technologies are developed, their use and proliferation can be difficult to control. For example, while bans on chemical weapons held in Europe during World War II, they have been used extensively in other conflicts, such as the Iran-Iraq War, where thousands were killed.

Therefore, there need to be conditions for when deterrence and counter-proliferation can justify the development and use of prohibited technologies. Since the point of developing prohibited technologies is to control such technologies, establishing control measures should occur concurrently. Moreover, there is a difference between developing a technology and fielding it. Either should only be pursued to the extent it offers the necessary leverage to get the relevant bans or control measures put in place. Finally, even if

these conditions were met, a further condition of last resort would also have to apply. If there were alternate means to prevent or counter the development of prohibited technology, they should be considered first.

Necessity

Albert Einstein reportedly said, “I made one great mistake in my life — when I signed the letter to President Roosevelt recommending that atom bombs be made; but there was some justification — the danger that the Germans would make them.”¹⁰⁵ Einstein conditioned his support for the bomb not by the fact that it conferred a military advantage or that it could hasten an end to the war, but rather by the concern that the Germans might build one as well. The atomic bomb was not simply destructive. It was *inherently* indiscriminate. As such, its development — much less its use — violated the war convention.

However, Einstein’s other concern, that the Germans would develop it first, carried greater weight for him. A German bomb would very likely ensure a German victory. That fact does not change the moral permissibility of its use by any side. However, it does entail the *necessity* of developing the bomb first or finding some other means to neutralize the advantage the Germans would gain. It is worth noting that the fact that the bomb did not turn out to be necessary to defeating the Germans was a cause for Einstein’s regret.

Einstein’s experience underscores the important role necessity plays in assessing the permissibility of developing disruptive technologies. However, as his experience also suggests, what counts as necessary can be a little difficult to nail down. In the military context, Walzer describes necessity in terms of not only a capability’s efficacy in achieving military objectives, but also in terms of the expenditure of time, life, and money. Thus, something can only be necessary in relation to the available alternatives, including the alternative to do nothing.¹⁰⁶ It is not enough that something works — it must work at the lowest cost.¹⁰⁷ Under this view, any technology could be necessary as long as it provided some military advantage *and* there was no less costly means to obtain that advantage. For example, alertness-enhancing amphetamines would be considered necessary as long as other means to achieve that alertness,

104 Roberts and Guelff, *Documents on the Laws of War*, 29–30.

105 Alice Calaprice, *The Ultimate Quotable Einstein* (Princeton, NJ: Princeton University Press, 2011), 284.

106 Christine Gray, *International Law and the Use of Force*, 3rd ed. (Oxford: Oxford University Press, 2008), 150.

107 Walzer, *Just and Unjust Wars*, 144.

such as adequate rest, were not available.¹⁰⁸

Conceived this way, necessity is more a reason for violating norms rather than a norm itself.¹⁰⁹ Invoking it when it comes to a disruptive technology gives permission to set aside concerns regarding moral permissibility and proceed with the technology's introduction and use. Take, for example, two alternatives that both achieve the same legitimate military purpose, but one does it with less cost and risk while violating a norm while the other entails slightly higher but bearable costs and risks while not violating any norms.¹¹⁰ Returning to the amphetamine example above, if it were possible to achieve the same number of sorties by training more aircrews or placing bases closer to targets, then on what basis would drugging pilots be *necessary*? Clearly it would not be. Depending on what the violation entails and what the costs actually are, one could find oneself invoking necessity *unnecessarily*.

This view of necessity conflates effectiveness and efficiency, making efficiency the criterion that really determines what counts as necessary. When considering alternatives, one would only consider those of equal effectiveness. If a more effective option were available, it would be the one under consideration and the less effective ones would be disregarded. If the options under consideration are all equally effective, efficiency is the only way to distinguish between them. The problem with efficiency, however, is that it discounts the costs of violating the norm. Put simply, to the extent a norm reflects the values one holds, violating it risks those values.

Of course, it is not possible, except in the simplest of cases, to effectively weigh the value of a norm against expenditures in funds, material, and lives. How would one assess what level of risk to pilots is worth how many additional pilots, aircraft, or bases that would offset those risks? Fortunately, doing so is not really necessary. What matters is how the norm is accounted for in the conception of necessity itself. This is done by determining which less effective but norm-conforming actions should be considered alongside the more efficient action. Considering all possible actions would be self-defeating because it would include actions whose costs may be difficult to sustain. This would elim-

inate efficiency as a condition of necessity, leaving only efficacy, which, as discussed above, could justify too much by reducing the moral component of decision-making to an "ends-means" calculation.

By considering options that are sustainable, even if less effective, one can both account for the norm in question as well as preserve the value of efficiency in determining necessity. Here, sustainability refers to the adequacy of the technology to offset an adversary's advantage, though it might not be the "best" option for doing so. Thus, when determining necessity, one should consider the sustainable options. When deciding between an efficient, norm-violating option and a less efficient but sustainable and non-norm-violating option, one should consider the latter as "necessary" instead of the former since it better accounts for the moral costs the option entails.

Doing so, of course, will not solve all of the problems associated with establishing the necessity of a given technology. There will still be cases, especially when it comes to technology acquisition, where there are no sustainable, non-norm-violating options. Yet, necessity will nevertheless place pressure on those who govern to act. As Walzer observes in his discussion on "dirty hands," great goods are often accompanied by great harms. In fact, he argues, to govern is to give up one's innocence since governing innocently is not just impossible, it is *irresponsible*.¹¹¹ This demand for "great goods" is acutely felt regarding matters of war. As David Luban notes, "if it is technically impossible to win the war under a given prohibition, the prohibition has no force."¹¹²

The point is *not* that the ends of warfighting justify the means, but that the imperative of defense and avoiding moral harm are in tension. That tension, however, does not mean both choices are equally valid. Instead, it means one must find a way to preserve both norms. As noted earlier, frequent disregard of a norm, for whatever reason, is a good way to kill it. However, that fact does not necessitate absolutism. Sometimes, there are grounds for violating a moral commitment. The measure of the norm, then, is found in the other moral concerns those grounds represent.

For example, Walzer argues that when defeat is

108 Lin, Mehlman, and Abney, *Enhanced Warfighters*, 67.

109 Robert D. Sloane, "On the Use and Abuse of Necessity in the Law of State Responsibility," *American Journal of International Law* 106, no. 3 (July 2012): 452, <https://doi.org/10.5305/amerjintlaw.106.3.0447>.

110 David Luban, "Military Necessity and the Cultures of Military Law," *Leiden Journal of International Law* 26, no. 2 (June 2013): 341–45, <https://doi.org/10.1017/S092215651300006X>.

111 Michael Walzer, "Political Action: The Problem of Dirty Hands," in *War and Moral Responsibility*, ed. Marshall Cohen, Thomas Nagel, and Thomas Scanlon (Princeton, NJ: Princeton University Press, 1974), 63.

112 Luban, "Military Necessity and the Cultures of Military Law," 341.



not only imminent, but represents a grave harm — such as the enslavement of a people that would have resulted from a Nazi victory in World War II — then one is justified in setting aside *jus in bello* norms if there is no other way to carry on a defense. This is known as “supreme emergency.” Once defeat is no longer imminent, the permission to violate those norms would no longer apply.¹¹³ Of course, supreme emergency cannot be used as a justification in the context of disruptive technologies. Decisions about technology acquisition often take place long before wars start. So, while a future threat may be grave, it is not imminent. Nevertheless, one can construct a similar kind of threshold for disruptive technologies.

This is where Einstein’s condition regarding atomic weapons offers a helpful insight. Atomic weapons may have been the most efficient way to defeat Germany, but they were clearly norm-violating. Moreover, there were equally effective, if more costly, ways of winning. Had the Germans obtained atomic weapons before the Allies, however, those alternatives would have lost their effectiveness. This suggests another condition on necessity: It is not enough that an option provide an advantage — it must also prevent a disadvantage. Otherwise, it is difficult to make moral sense of the potential suffering such technologies can produce.

Einstein was right: The development of the atomic bomb, and I would argue any disruptive technology, should be conditioned on whether it avoids a disadvantage for one’s side that an adversary would likely be able to exploit. In this context, it is worth asking if it matters whether that disadvantage arises because of the adversary’s pursuit of the same technology or from some other capability. For example, would the pursuit of a disruptive technology be permissible to offset an adversary’s conventional advantage, such as superior numbers and equipment?

Answering that question would, naturally, depend on the alternatives available. For example, the United States deployed nuclear weapons in Europe as a way of compensating for the Soviet Union’s superiority in terms of personnel and equipment.¹¹⁴ In doing so, it threatened what would arguably be an immoral, if not also unlawful, means to counter an enemy advantage as a result of a lawful military capability. That would only be permissible if there were no other permissible options available, such

as matching Soviet forces conventionally. Even then, the use of nuclear weapons, if they could be justified at all, could only be justified in terms of a supreme emergency, which requires that a threat be grave and imminent.¹¹⁵

Arguably, the Soviet conquest of Western Europe would have met such a threshold, though in retrospect it is worth asking how likely it was that the Soviets would have attempted it. Nonetheless, threatening the use of these weapons had some deterrent value and to the extent there was no other equally effective but permissible option, it would have been acceptable to possess them for their deterrent effect, even if their actual employment would only have been permitted under very extreme circumstances.

Of course, the disruptive technologies considered here do not have an inherently impermissible effect. Still, because of concern over their potential disruptive effects, it is still the case that there would have to be some disadvantage that is being avoided as well as no reasonable, non-disruptive alternative in order to permit their use. However, having a moral effect and avoiding a disadvantage are not sufficient to assure the moral permissibility of a particular technology. As discussed, disruptive military technologies risk some harm and thus raise the question whether such harms, even if morally permissible themselves, are worth it.

Proportionality

The fact that a new technology may have a positive moral effect and also be necessary does not imply that its introduction is morally worth the cost. For example, the NATO allies could have chosen to initiate a draft and increase defense spending, rather than rely on nuclear weapons to achieve parity with Soviet forces. However, the cost not just in terms of resources, but also in social disruption, likely made that option, while possible, too costly to be worthwhile. Such situations suggest another criterion for determining whether it is worth pursuing a disruptive technology: proportionality.

In general, proportionality is a utilitarian constraint that requires an actor to compare the goods and harms associated with an act and ensure that the harm done does not exceed the good.¹¹⁶ In this way, proportionality is closely connected with necessity: For something to be necessary, it must al-

113 Walzer, *Just and Unjust Wars*, 251–68.

114 Donald A. Wells, ed., *An Encyclopedia of War and Ethics* (Westport, CT: Greenwood Press, 1996), 337.

115 Walzer, *Just and Unjust Wars*, 259–60.

116 Thomas Hurka, “Proportionality in the Morality of War,” *Philosophy & Public Affairs* 33, no. 1 (Winter 2005), 37, <https://www.jstor.org/stable/3557942>.

ready represent the most effective choice for pursuing the good in question. If there were a more effective option, then, as already mentioned, the less effective ones would no longer be necessary, unless they were sustainable and more humane.

This does not mean that proportionality and necessity are indistinguishable. Necessity refers to the alternatives available while proportionality refers to the scope of the response.¹¹⁷ This link between proportionality and necessity applies to the acquisition of new technologies. There has to be a reason to risk the possible disruption of a new technology, which is typically expressed in terms of the benefit it is expected to bring. Whatever that reason, part of what will make it a *good* reason is that, on balance, it represents more benefit and less harm than any alternative.

Though simple in form, applying the principle of proportionality can be difficult in practice. To do so, one needs to determine what goods and harms count as relevant and then determine how they weigh against each other.¹¹⁸ In the context of national security, necessity defines a good as deterrence, and failing that, victory, while it defines a harm as aggression or defeat. The pursuit of deterrence and victory in turn points to additional goods and harms, which include human lives and the environment. Technology acquisition would specifically include autonomy, justice, well-being, and social stability as goods. This list is not exhaustive of course. However, anything that promotes or strengthens these goods would count positively toward the proportionality of introducing a new technology. Anything that leads to a loss or degradation of these goods would count as a harm.

It should be clear however, that such a comparison is hardly straightforward. A technology that results in fewer deaths, both combatant and non-combatant, would be more proportionate than a technology that does not. However, as Walzer notes, “proportionality turns out to be a hard criterion to apply, for there is no ready way to establish an independent or stable view of the values against which the destruction of war is to be measured.”¹¹⁹ Even in conventional situations, it is not clear how many noncombatant lives are worth any particular military objective. The decision to conduct air at-

tacks against civilian population centers like Dresden was typically justified by the belief that doing so would incite terror and break German morale, ending the war sooner and saving more lives than the attack cost. That conclusion, as it turned out, was false. While morale may have suffered, German resolve did not.¹²⁰ But even if it had hastened an end to the war, one still has to consider how many civilian lives that is worth. That is not a question anyone can really answer.

Fortunately, one does not have to answer that question, or questions like it, in order to apply proportionality to moral decision-making. If proportionality is conceived of as a limit on action rather than a permission, then what matters is not whether an act is proportionate but rather whether an act is disproportionate. For example, one does not need a precise quantification to know that threatening divorce over a disagreement about what to have for dinner is disproportionate. Moreover, assessing the disproportionality of such an act does not require committing to what would be a proportionate response.¹²¹ But it does mean that after all disproportionate actions are rejected, then whatever ones are leftover are permissible, even if there is some uncertainty regarding the balance of the cost and benefit of implementing them.

Nor does assessing disproportionality mean that assessment is hopeless in more marginal cases. Take, for example, when Iran shut down electricity for approximately 40 million Turks because the Turkish government criticized its support for Houthi rebels in Yemen. Since the Turkish government’s criticism did not have a similar effect on Iranian civilians and civil life, imposing a massive blackout would count as disproportionate, even if there were no equally effective and less disruptive alternatives.

And yet, it would be extremely unsatisfying to leave it to intuition to determine disproportionality: One still has to determine how to weigh alternatives, even if one cannot precisely weigh specific goods against specific harms. The use of atomic weapons against Japan provides a useful illustration. Though clearly indiscriminate, those advocating for the bomb’s use argued persuasively that it was proportionate relative to the alternative of

117 Gray, *International Law and the Use of Force*, 150.

118 Hurka, “Proportionality and the Morality of War,” 38.

119 Walzer, *Just and Unjust Wars*, 129.

120 Barrie Paskins and Michael Dockrill, *The Ethics of War* (Minneapolis: University of Minnesota Press, 1979), 45.

121 Brian Orend, *The Morality of War* (Ontario, CA: Broadview Press, 2006), 60.



invading Japan, both in terms of Allied and Japanese lives lost.¹²² They were probably correct: If one considered only this factor, then dropping the two atomic bombs was arguably proportionate. The fact that dropping the bombs remains morally

● **Thus, intending to kill someone with a low probability of success is proportionally equal to intending a lesser harm even though it comes with the same low probability that it will result in death.** ●

questionable is due to their indiscriminate nature.

What this example shows is that when it comes to a new technology, it is not sufficient to simply consider discrete instances of its employment, even if one does so cumulatively. Given that two bombs were sufficient to bring the war to an end, one might concede the proportionality of proceeding with dropping them.¹²³ However, it is difficult to take back a technology once it is introduced. Thus, when considered more broadly, the introduction of nuclear weapons technology could reasonably be expected to lead to proliferation and an arms race as actors adjust to the new rules of competition these weapons bring with them. In fact, these issues were raised during the deliberations on their use, but apparently were discounted.¹²⁴

Even if one could come up with a way to commensurately measure goods and harms, there are deeper problems with simple comparisons, especially under conditions of uncertainty. In military contexts, proportionality is typically measured by comparing the intended good of achieving a particular military objective against the foreseen, but unintended, harms associated with achieving that objective. Under conditions of certainty, such a calculation would be relatively simple, if not straightforward. If the amount of collateral harm associated with accomplishing a military mission is known, then one has a basis on which to judge, on balance, whether a particular act is proportional. Moreover, this does not require precision. If one knows that an objective is of low value but that a significant amount of civilians or friendly combatants will die, one can judge it to be disproportionate. It just does not make moral sense to destroy a village to save it.

Under conditions of uncertainty, however, probabilities associated with any expected harm would seem to matter. As Patrick Tomlin points out, however, by taking probabilities into account one can end up with the result that intending a larger harm with a low probability of success could be just as proportionate as intending to inflict a much smaller harm but with an equally low probability of resulting in the larger harm. Thus, intending to kill someone with a low probability of success is proportionally equal to intending a lesser harm even though it comes with the same low probability that it will result in death.¹²⁵ It seems counterintuitive, however, that killing could, under any circumstances, be as proportionate as breaking a finger, assuming both resulted in a successful defense.

What Tomlin is underscoring here is that intent matters. As he writes, "It matters what the defensive agent is aiming for, and the significance of that cannot be fully accounted for in a calculation which discounts that significance according to the likelihood of occurring."¹²⁶ A cyber operation to shut down an air traffic control system to force fatal aircraft collisions, even if it is unlikely to be successful, would be less proportionate than a cyber operation that disrupts an adversary's electric grid, as Iran did to Turkey, even if there was similar loss of life. In the former, loss of life is intended, but unlikely. In the

122 Henry Stimson, "The Decision to Use the Atomic Bomb," *Harper's Weekly* 194, no. 1161 (February 1947), quoted in, Stephen Coleman, *Military Ethics: An Introduction with Case Studies* (Oxford: Oxford University Press, 2013), 15–16. See, Michael Kort, *The Columbia Guide to Hiroshima and the Bomb* (New York: Columbia University Press, 2007), 102.

123 Kort, *The Columbia Guide to Hiroshima and the Bomb*, 87. Kort points out that a number of U.S. officials involved in the decision to employ the atomic bombs believed that it would take at least three, if not more, bombs to force a Japanese surrender.

124 Kort, *The Columbia Guide to Hiroshima and the Bomb*, 96.

125 Patrick Tomlin, "Subjective Proportionality," *Ethics* 129, no. 2 (January 2019): 265–66, <https://doi.org/10.1086/700031>.

126 Tomlin, "Subjective Proportionality," 267.

latter, loss of life is unintended, but, depending on the scope of the outage and the resiliency of back-up power systems, could have the same probability of causing loss of life as the air traffic control example. The widespread disruption of electric power could affect life-sustaining systems in hospitals and care facilities as well as cause traffic accidents due to inoperable traffic lights.

Thus, what matters is not just a collective assessment of goods and harms, but how they pair up. If the intended harm pairs with a disproportionate outcome, then the act is disproportionate, even if the chances of the outcome occurring are low. Thus, under conditions of uncertainty, proportionality calculations should give greater weight to the intended harm, independent of its likelihood, and in so doing amplify the weight given to unintended harms.¹²⁷

It is not enough to account for intended consequences and unintended, albeit foreseen, consequences. One must take into account unforeseen consequences as well. Of course, specific unforeseen consequences cannot be taken into account since they are, by definition, unforeseen. But one could imagine that while the designers of the atomic bomb were aware of its destructive effects, they may not have fully foreseen the evolution of that technology into the fusion bomb, whose destructive capabilities risked global annihilation. Given that “ought implies can,” one cannot be morally faulted for a failure of the imagination. But what a person can be faulted for is not taking into account that failure of imagination.

This suggests that proportionality requires actors to consider how to manage the proliferation and evolution of any technology in advance of introducing it, not because they have an idea of what the negative effects will be, but because they do not. One may not know how a technology will affect matters of autonomy, justice, well-being, and social stability, but the fact that it could affect these things suggests that identifying measures to control the technology as well as minimize any disruptive impacts is morally required.

There are therefore three conditions that must be met when calculating the proportionality of developing and employing disruptive technologies. First, there is an obligation to demonstrate that the intended outcome is not disproportionate, calculated in terms of the intended disruptive effects. Second, one must consider foreseen but unintended harms independent of how likely they are to occur. Doing so forces the question, “If the harm were to occur, would introducing the technology still have been

worth it?” It also requires considering measures to prevent the foreseen harm from occurring, or at least minimizing its impact. Finally, it is necessary to ensure there are controls on the technology so that when *unforeseen* harms arise, there are tools available to minimize their impact.

Conclusion

The development of military technologies does not occur in isolation. Eventually, their unique attributes will find a civilian use and they will find their way into civilian markets. Of course, each disruptive technology will come with its own challenges. However, the fact that they are disruptive raises a common set of ethical concerns that should be addressed in advance of their acquisition and employment.

The first concern is identifying which technologies are disruptive. What matters is not how advanced or new a particular technology is, but rather how its attributes find utility among a community of users. What makes those attributes disruptive is that they change the way actors compete. This change can be both revolutionary and evolutionary. The advantage represented by a disruptive technology places pressure on actors to use the technology in non-normative ways, much like the submarine in World War I and II. To the extent that the community of users accepts that use at the expense of the norm it violates, its introduction is revolutionary.

That revolution can have far-reaching consequences. Had the international community simply accepted that merchant vessels were legitimate targets for submarines, it could have opened up other defenseless targets to attack, at least by weapon systems that shared similar vulnerabilities as the submarine. The fact that did not happen suggests that some norms, such as prohibitions on attacking the defenseless, are resilient. However, the utility of the submarine forced an evolution in norms that made room for its use. In so doing, it set conditions for the evolution of the submarine itself to make it more compatible with established norms.

The submarine is not the only disruptive technology whose introduction caused considerable harm before it and the norms that govern it found equilibrium. The most obvious takeaway is that one should not develop technologies that are inherently norm-violating. Having said that, however, it can be difficult to predict how a technology’s various attributes will find utility. So one must be prepared for such harms to occur and have taken measures and

127 Tomlin, “Subjective Proportionality,” 271.



adopted policies in advance to mitigate them.

Because the benefits of these technologies are associated with national security, there is a *prima facie* imperative to develop them. As previously discussed, the social contract obligates states to provide security for their citizens. Even if we only recognize, as Thomas Hobbes did, the right to self-preservation, entrusting that right to the state obligates it to defend its citizens from internal and external threat.¹²⁸ That obligation has to fall to someone, so states raise police forces and armies to provide security. Those who take up that task are further obligated to make decisions about how best to see to that defense. As Samuel Huntington argued, the military officer has a responsibility to the state, and by extension to the people it governs, to provide expert advice on national defense.¹²⁹ That means advising not only on *when* to wage war, but also *how* to wage it.

That responsibility entails two imperatives. First, decisions about whether to develop disruptive technologies cannot be abandoned without incurring a moral failure. Second, there will be times when developing disruptive technologies is not only permissible, but obligatory.

Avoiding Moral Failure

Regarding the first point, as discussed, there are conditions that should hold when developing disruptive technologies. Moreover, there are a number of measures and policies that should be adopted to maintain those conditions as the technology is developed and implemented:

First, it is necessary to allow for soldier consent to the extent possible when employing and integrating new technologies. This involves avoiding inherently coercive situations where soldiers bear significant costs should they not consent to a particular technology's use. When consent is not possible, it is necessary to ensure no one is worse off and at least some are better off than if the technology had not been developed or employed.

Second, one must ensure measures are put in place when beginning research on potentially disruptive technologies to manage proliferation.

Third, soldier well-being must be taken into account throughout the acquisition process and the

technology's effect on operators must be tested for all possible expected uses.

Fourth, it is required to pay attention to how the introduction of a new technology affects the distribution of reward and risk. This includes avoiding the establishment of a class of soldiers who bear most of the risk and a class that bears little. This outcome can be avoided by ensuring that, in general, soldiers rotate through assignments that involve varying degrees of risk such that over an enlistment or career risk and rewards are evenly distributed. This could require significant changes in career-field management. For example, individual servicemembers may need a range of physical and mental attributes to take on a variety of assignments new technologies make possible. It could also require servicemembers to acquire multiple skills to ensure they are capable of handling that range of possible assignments.

Fifth, it is necessary to manage the transfer of technology to society. This involves considering how technological attributes will be utilized in civilian markets and ensuring that military research is not conducted in a way that eliminates technology that is better suited for civilian use.

Sixth, all sustainable alternatives to the development and employment of a new technology must be considered, not just the most efficient ones.

Seventh, one must calculate disproportionality to take into account any intended harm independent of its likelihood, and in so doing amplify the weight given to unintended, but foreseen, harms.

Eighth, norm-violating technologies are to be developed only as a means to promote their ban or deter their proliferation and use. Efforts to ban or restrict such a technology must occur simultaneously with its development.¹³⁰

Obligation

Regarding the second point, there are two conditions that must hold to obligate developing disruptive technologies. The first condition is that, where the expected disruption promotes better moral outcomes, whatever form that may take, one arguably should pursue it. As mentioned earlier, changing the way actors compete is not necessarily a bad thing. If artificial intelligence, for example, re-

128 Thomas Hobbes, *Leviathan*, ed. Richard Tuck (Cambridge, UK: Cambridge University Press, 1991), 89–91 in *The Ethics of War: Classic and Contemporary Readings*, ed. Gregory M. Reichberg, Henrik Syse, and Endre Begby (Malden, MA: Blackwell Publishing, 2006), 445–47.

129 Samuel P. Huntington, "Officership as Profession," in *War, Morality, and the Military Profession*, ed. Malham M. Wakin (Boulder, CO: Westview Press, 1986), 3031.

130 For example, the use of lasers to blind pilots led to an international agreement to ban such use as early as 1995. "Annex A: Protocol on Blinding Laser Weapons (Protocol IV)," in "Additional Protocol 'Review Conference of the States Parties to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Indiscriminate Effects,'" United Nations, 1996, https://treaties.un.org/doc/source/docs/CCW_CONF.I_16_Part%20I-E.pdf.

ally can make war more humane and any negative effects can be mitigated to the extent that at least some are better off and no one is worse off, then one *should* develop that technology. This last point is important. Simply having a moral benefit is not sufficient to obligate the development of disruptive technologies. On the other hand, simply having a morally negative effect is not sufficient to prevent such obligation. Nor is this simply a matter of utility. What matters is how the technology promotes the good, understood broadly here to include a range of moral concerns including rights, principles, virtues, and other universally held moral commitments that shape our sense of justice.

The second condition follows from the conjunction of the social contract and necessity. To the extent a disruptive technology avoids a disadvantage relative to an adversary, the pressure to develop it will be directly proportional to the disadvantage it avoids. This suggests that while not every disadvantage will entail obligation, some will. Technologies that meet this criterion are those whose possession by an adversary would undermine the state's ability to fulfill the social contract. Weapons of mass destruction serve as one obvious example. To the extent their possession allows an adversary to coerce concessions affecting the security and well-being of a state's citizens, then that state has an obligation to resist that coercion.

More needs to be said regarding what counts as security and well-being. As disruptive as the 2007 Russian cyber operations directed at Estonia were, it is not clear they would justify developing a prohibited technology in response.¹³¹ However, to the extent possession of a technology enables that resistance, and there is no other less morally risky alternative, then arguably the state *should* develop that technology. However, developing that technology brings with it a further obligation to work toward preventing its proliferation and use. Otherwise, one risks an "arms race" that, like last century's nuclear arms race, can increase the risk of the technology's use. The fact that nuclear weapons have not been used since 1945, however, suggests that if the consequences are severe enough, even the most self-interested actors can be persuaded to forego a technology's use.

The preceding account is not intended to be comprehensive. However, it does serve as a starting point to avoid Boris Johnson's nightmare scenarios of technology run amok. While much of what concerned him is extremely unlikely to occur, it is the case that these technologies will not only change

how we fight and who we fight, but what counts as fighting as well. This uncertainty is unresolvable. It is also inevitable. The advantages of such technologies frequently impose pressures that ensure their development. Thus the challenge is not to prevent their development, but to manage it to the extent possible, and to avoid the moral harms that their introduction invariably brings. 

Dr. C. Anthony Pfaff is a research professor for strategy, the military profession, and ethics at the U.S. Army War College's Strategic Studies Institute and a senior non-resident fellow at the Atlantic Council. The views represented here are the author's and do not necessarily reflect those of the United States government.

Photo: Maj. Penny Zamora

131 George R. Lucas, "Emerging Norms for Cyber Warfare," in *Binary Bullets: The Ethics of Cyberwarfare*, ed. George R. Lucas et al. (Oxford: Oxford University Press, 2016), 26–27.