Cyber realism and just war*

Luke M. Perez

March 17, 2021

Introduction

Cyberwar—or cyber attacks used in war—is, to paraphrase Carl von Clausewitz, acts of force to compel the enemy to do one's will through electronic, or virtual means by the use of malicious code.[1] The concept of cyberwar is at least as old as the idea of computers and networked systems. More recently cyberwar has come into widespread use. The most well known to Americans is the infamous Stuxnet worm which damaged the Iranian centrifuges brought the concept that states were already actively using such virtual weapons.[2] In the ten years since knowledge of Operation Olympic Games (for which Stuxnet was developed and deployed), many other high profile cases of political cyberattacks have occurred, including well-known instances such as those against the G20 in Paris (2011), Sony (2014), the U.S. Office of Personal Management (2015), and Democratic National Committee (2015-2016). Such attacks will not likely abate in the coming years. Indeed, all prognoses suggest that both their frequency and intensity will only increase. In response to these, and other threats, Congress authorized a cyber-solarium commission.[3]

*Assistant Professor at Arizona State University. Paper prepared for the Just War Colloquium at Wheaton College, March 18, 20201. Citations permitted, but comments and suggestions on how to improve the draft are very much encouraged. Corresponding email: lukemperez@asu.edu

1. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (1832; repr., Princeton, NJ: Princeton University Press, 1976), 75; Clausewitz' definition has been described by Thomas Rid as having three criteria: (1) Force to compel, force as instrumental (means), and (3) force use to achieve a political objective (ends). See, Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 7–8, doi:10.1080/01402390.2011.608939.

2. "The Meaning of Stuxnet," *The Economist*, October 2nd 2010 Edition, https://www.economist.com/leaders/2010/09/30/the-meaning-of-stuxnet, Date Accessed February 17, 2020.

3. The choice of a name is telling. It, intentionally, echoes Dwight D. Eisenhower's 1953 Solarium Project which produced NSC 162/2, which formalized containment as the guiding national security strategy during the Cold War. The current Cyber-Solarium report was released in March 2020 and can be found here:

And yet, although much of contemporary scholarship has investigated whether and to what extent cyberwar will (or will not) have a role in the future of warfare, many ethical questions remain either unanswered or insufficiently so. What is at stake, as with any new technological advancement, is the potential that cyberwars will undermine our ethical thinking, invite abuse, and potentially lead to an increase of human suffering. Unlike other technological innovations, the risk is not that the new technology is more deadly (nuclear weapons) or blurs traditional just war categories in order to gain more precision in others (drones). Rather, cyberwar's defensive vulnerabilities are overemphasized, while the offensive risks are underemphasized. That is, we have come think of only "Cyber-Pearl Harbors"—to use the words of Leon Panetta—while simultaneously characterizing our offensive capabilities as *always* a just response in the escalation of coercive force by the state.

This paper advances the argument that whatever the critcisms of cyberwar, not only is it warfighting, but also that the just war tradition is more than adequate for dealing with the novel challenges unique to cyber. It also advances caution for two risks on the horizon to which military and strategic ethicists must remain attentive. The first is legalist-atrophy from an myopically technical approach which seeks ever granular definitions, categories, and procedure. The second is a mirror, wherein overly optimistic analyses of cyberwar invite moral hazard—creating conditions that increase human suffering and risk escalating physical violence when none would other have occurred. In short, rather than focusing our moral anlysis on the quite modern *jus ad bellum-jus in bello* distinctions, we should remember that the just war tradition is about the prudential, just ordering of statecraft writ large. In this vein, the main categories of the just war tradition are more akin to principles of thinking, not formal laws.

---

https://www.solarium.gov/

What is Cyberwar, and is it war-fighting?

The 2015 novel *Ghost Fleet* begins with a premise that captures the worst fears about the growing power of cyberwar: Malware embedded in a video message of a groundskeeper who works at DIA finds it way onto the phone of a security analyst who unwittingly carries the computer virus into the secure military networks.[4] Written by two analysts who relied on contemporary research to imagine what war will look like in the not-to-distant future, the book takes seriously what happens when the United States is fighting from a technologically inferior position. Such a premise is not far fetched. Even as recently as 2012, Leon Panetta warned that a cyber-Pearl Harbor was among the CIA's and DOD's most serious concerns regarding cyberwar.[5] Such an attack could make victory a *fait accompli*.

If such concerns were all, or even the majority, of what cyberwar is, then questions regarding its moral and strategic concerns would be moot. In those cases, the just war tradition is clear that most questions would be merely ones of military necessity and proportionality. (Self-defense from catastrophic cyber attack is not only permitted, it might even be obligatory to protect civilians.) Secondary questions would be mostly relegated to whether and under what conditions could kinetic force be used to deter or retaliate against cyber attacks of that scale.[6]

Beyond these scenarios which capture the imagination, in practice some scholars have questioned whether or not cyberwar, or cyber-operations are warfighting. Indeed, at first blush, cyber-operations do not even appear to be warfighting in the sense it has carried for thousands of years. As Rebecca Slayton put it many cyber warriors "spend their time focused on defensive work that differs very little, if at all, from that of civilian computer security experts."[7] Cyberwar operators do not, it is plain to see, experience war

4. P. W. Singer and August Cole, *Ghost Fleet* (New York, NY: Houghton Mifflin Harcourt, 2015), 37–39.

5. Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times*, October 11, 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

6. To be sure, these are important moral questions to consider but are not the main topic of this paper.

7. Rebecca Slayton, "What Is a Cyber Warrior? The Emergence of u.s. Military Cyber Expertise, 1967–2018," *Texas National Security Review* 4, no. 1 (2021): 62–63.

in the same way that infantry soldiers experience close quarter firefights, for example. What's more, there is a substantial literature contending that cyberwar is a chimera. Erik Gartzke argues that cyberwar, whatever that means, is not war.[8] We cannot form logical connections from opportunity to consequence. He adds, "[c]yber pemissim rests heavily on capabilities (means), with little thought to a companion logic of consequences (ends)."[9] Cyber Skeptics further contend that when we consider the elements of war, cyber fails to meet the standard.[10]

In some ways, these cyber skeptics are half-right. Cyberwar is not likely to become the final arbiter of competition in international politics but will rather be a secondary, "adjunct" status to conventional warfighting.[11] What the skeptics miss, however, is how these auxillaries can enhance and strengthen the preponderance of military power.[12] Alongside the skeptics are cyber moderates and radicals. Radicals assert that cyber has fundamentally disrupted our understanding of ethics because it has moved the concept of violence beyond the anthropocentric world of physical force.[13] This debate over the status of cyberwar is critically important. As already mentioned, if cyberwar were strictly adjunct, we might merely conclude that using cyber weapons is morally unjust, prohibit their use along side chemical and biological weapons, and punish violators. Such a world does not exist.

The cyber-realist position, in turn recognizes that technology "drives a wedge

8. "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth," *International Security* 38, no. 2, Fall (2013): 41–73, doi:10.1162/.

9. Ibid., 42.

10. See, Thomas Rid, "Cyber War Will Not Take Place"; Rid relies on Clausewitz to develop a three-pronged test of whether something is war: (1) It is an act of force, (2) It is instrumental, (3) It is always political. Given the frequence of cyber attacks in a military setting in the eight years since writing "Cyber war will not take place," one might wonder whether Rid's theory is in need of revision.

11. Gartzke, "The Myth of Cyberwar," 42, 66, and 72.

12. Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton University Press, 2006), 53, 73.

13. The phrasing of cyber "skeptic, moderate, radical" is Matt Sleat's. For an elaboration on the categories as well as a summary of the radical view, see, Matt Sleat, "Just Cyber War? *Casus Belli*, Information Ethics, and the Human Perspective," *Review of International Studies* 44, no. 2 (2017): 324–42, doi:10.1017/S026021051700047X, 325–326.

between the real capability" of modern armies.[14] It is a more fitting term than moderate because it captures and echoes the realist traditional of international relations.[15] Its use is not only already here,[16] those who wage cyberwar are warfighters. A simple thought experiment suggests why: would be permissible under the Law of Armed Conflict to target military cyber operators who are actively engaging in a cyber attack? Of course they would be. They are lawful targets in the same way an tank mechanic or aircraft radio maintainer would be lawful targets. Cyber operations contributes to and enhances the warfighting effort. Put differently, the proximity and severity of the risk inured by those in distinct professions is not the rubric by which we can evaluate whether or not a particular task is warfighting. Thus, while electronically storming an enemy network mainframe is not identical to storming the beaches at Normandy, in some ways the stakes of a cyber operation might be higher because cyber does blur the lines between civilian and military targets, capabilities, and uses.

Space does not permit a fuller treatment of the debate. Suffice to say, we can summarize the relevant point this way: on the one hand, we cannot put into clear words what cyberwar *is*, nor why it should be considered warfighting. On the other hand, the scope and scale of the risk inherent to cyber's military context matches or exceeds the risk of previous technological advancements. Moreover, where cyber has the potential risk approaching the scale of nuclear war, unlike nuclear weapons, it can scale down into smaller one-off events akin to burglary or espionage. Cyberwar's scalability naturally invite us to consider the role of prudence, since it is through the prudential use of cyber operations in a military context which the just war tradition has always been intended.

14. Biddle, *Military Power*, 73.

15. I do not wish to get into debates over classical, neo-, and neoclassical variants of realism here. Suffice it to say, some "realists" might hold a cyber-skeptical view and my use of the term is intentionally aimed at drawing such a distinction.

16. John Arquilla, "Twenty Years of Cyber War," *Journal of Military Ethics* 12, no. 1 (2013): 80–87, doi:10.1080/15027570.2013.782632.

Technology does not change the principles of just war

In the opening section of this paper, I asserted that the just war tradition was more than capable of dealing with cyberwar. Whatever novel complications accompany the virtual domain of war, the principles of just war are timeless. Time and again, they have adapted to changes in technology. When Saint Augustine wrote what is widely considered to be the origin of the just war tradition, he could never have imagined the advent of the firearm, mechanized weaponry, nuclear weapons, or hypersonic kinetic missiles.[17] For critics of just war's suitability, those developments should have buried the just war and any pretension for restricting war on moral grounds. And for them, cyberwar *a fortori* should foreclose any hope of a suitable just war approach to contemporary war.

Those views are flawed because what has not changed over the millenia is human nature. Humans are flawed yet aspirational creatures who at once have high moral standards and fail to achieve them in great and small affairs. To reframe Gartzke's criticism of pessimistic views of cyberwar, we should not conflate or confuse revolutions in the means of warfare without also considering both the logic of ends and the logic that binds the means-ends relationship. It is the field ethics which captures all of these and vis-a-vis war, just war is still quite ready for the task.

The clearest exposition of what is required for a war to be just can be found in Thomas Aquinas. His well-known treatment of the topic is found in the *Summa Theologae* II-II Q. 40. Here, Thomas raises the question whether war is always unjust. In rejecting the proposition that war is always unjust he delineates three criteria which make war just. Fist, it must be waged by a proper public authority (i.e., no private wars); Second, it must have a just cause; Third, those who wage the war must have the right intention.

17. Students of western philosophy might point out that theories of just war can be found long before Augustine, in pagan texts (Greek and Roman) as well as religious ones (Old Testament). But Augustine might be credited with fusing the two, mainly in his efforts to refute Christian pacifism. A wonderful resource for the primary sources in the just war tradition can be found in Gregory M. Reichberg, Henrik Syse, and Endre Begby, eds., *The Ethics of War: Classic and Contemporary Readings* (Malden, MA & Oxford, UK: Blackwell Publishing, 2006).

Thomas' formulation of war must be read in the larger context of the *Summa* and of all his works on ethics and politics. He expects his readers to be familiar with other relevant sections, including those on human acts (I-II QQ. 6–21), prudence, especially military prudence (II-II, QQ. 47–56, esp. Q.50 a. 4), and peace (II-II Q. 29).[18] Since war is a function of politics, one cannot reason about war in moral terms without also reasoning about politics in moral terms. Such reasoning, Thomas suggests, turns explicitly on the importance of charity (Christian love) for God and for neighbor. Politics for Thomas, as for Augustine, directs the political community toward the heavenly community through the prudential use of political power.

Critics of the Christian tradition of just war often claim that war is the opposite of charity. For how can killing in any way be an act of love? Thomas is silent to that objection, but only formally. Informally, the placement of "On War" reveals much about his thinking toward such critics. Question 40 is in a cluster of questions on the theological virtue of charity. War's limited permissibility suggests what later scholars would make more explicit; when just, war is an act of charity. The virtue of charity obliges all to look out for the good of the other, and in a political context for the good of the political community. Threats to those good, proper and common, must be met. And at times, force must be used if the threat is from other humans who have or are threatening to use illicit violence. It is an act of love, therefore, to maintain justice in political communities. A just war framework does not begin with a presumption against war but injustice.[19] Its primary aim is peace, but peace rightly understood as more than merely the absence of conflict.

If war is therefore an instrument toward peace, then its use must be calibrated

18. Of course, Thomas also expects his readers to know of his explicitly political works (*Commentary on Aristotle's Politics*, *On Kingship*.

19. Francisco Suarez, *Disputations on Charity* XIII, §1.2: "Unde ad confirmationem, negatur bellum esse contrarium honestae paci, sed iniquae; est enim potius medium ad veram et tutam pacem obtinendam." http://cdigital.dgb.uanl.mx/la/1080042136_C/1080042067_T12/1080042067_162.pdf Suarez' position runs counter to his contemporary fellow Jesuit, Pope Francis, who has recently called the just war tradition into question in the encyclical *Fratelli Tutti*. For a discussion of its implications, see Joseph E. Capizzi, "Pope Francis and the Problem of War in *Fratelli Tutti*," *Providence*, October 15, 2020. url: https://providencemag.com/2020/10/pope-francis-and-the-problem-of-war-in-fratelli-tutti/, date accessed March 1, 2021.>

toward that goal. All instruments of war are subordinate to this precept. Cyber operations are no different. Policymakers must therefore calibrate the role of cyberwar along side other instruments of statecraft to ensure its use does not endanger the more important task of peace understood in the terms sketched above. It is neither cyber, nor any other particular tool of war, that is inherently just or unjust, but rather particular *applications* which can be just or unjust according to the precepts of just war. The subcategories of *jus ad bellum* and *jus in bello* are helpful here since they are better understood as auxiliary tools of moral analysis to the antecedent analysis of any given war's moral status. In other words, unless the intention is right, the cause just, and the decision to wage war made by legitimate authority, questions over proportionality, probability of success, and whether the use of force is a last resort are moot.

Placing Thomas' formulation strengthens the application of *jus ad bellum* and *jus in bello* for war broadly and cyberwar narrowly. Right intention always includes self-defense. But the strength of the argument weakens when thinking about preemptive and preventive war.[20] In cases of preemption, it is not immediately obvious how a virtual attack is necessarily justified. Likewise, the principles of last resort and discrimination.[21] Cyber is presumably non-lethal (though, even there its secondary effects may not be) and paradoxically lowers the threshold to the use of coercion and force. The Thomistic model helps address this. If a fact pattern meets standard for just war, then whether cyber operations can be used is a prudential question to be weighed alongside other—lethal and non-lethal—means to restore or preserve justice.

Thus far I have not considered whether cyber attacks on any country can themselves be a sufficient cause for initiating a non-cyber counter offensive. I think the answer is obvious if, for this paper, unsatisfying. It depends. The scale and severity of any cyber attack would have to be evaluated. And as noted in the introduction, there are already real cases to consider. Here, an outline will have to do. A small scale probe of a government

20. Arquilla, "Twenty Years of Cyber War," 83.
21. Ibid., 83–84.

website would not by itself justify a deployment of F-35s to flatten a military base that conducted the operation. But a large scale attack which crippled critical infrastructure and contributed to the loss of GDP and lives would certainly justify a kinetic response.[22] The hypothetical cases are easier to assess than some of the real world examples because attribution of who conducted the attack are not easily discerned, and often it is the pattern of many small and medium size cyber operations that suggest but do not prove that a state or other actor is engaging in asymmetric coercive competition. Still, even when military force is an inappropriate response to those patterns, policymakers can rely on sanctions, counter-cyber operations, and other tools of statecraft that fit within a just war framework.

Two risks in the application of just war theory to cyberwar

Moral Atrophy

Thomas elegance comes at a cost, however. One will not find, for instance, any sustained treatment of the *jus ad bellum-jus in bello* distinction, to say nothing of the more recent addition in just war literature of a *jus post bellum*. Indeed, the dichotomy of just war doctrine into "the right to war" and "just conduct in war" may be a false one that risks moral confusion. These subcategories are recent, beginning informally with Grotius but—as far as I have been able to tell—did not become common practice until the twentieth century.[23]

This is not to suggest that the right to war and right conduct in war should be abandoned. Many just war scholars have made fruitful use of those categories. My point in raising the possible false dichotomy was to preface one of risks of just war thinking on cyberwar. Namely, that an overly legalist paradigm tends toward atrophy. In the American

22. Christopher J. Eberle, "Just War Adn Cyberwar," *Journal of Military Ethics* 12, no. 1 (2013): 58–59, doi:10.1080/15027570.2013.782638.

23. Grotius first mentions the distinction between *jus ad bellum* and *jus in bello* in the preface to his magnum opus on the laws of war. It should be noted, however, that he refers to them as common law, suggesting they were not yet positivist distinctions in international law. More than a 100 years ago, Lammasch had already pointed out that a formalized reading of *jus ad bellum* was problematic. See, Heinrich Lammasch, "Unjustifiable War and the Means to Avoid It," *The American Journal of International Law* 10, no. 4 (1916): 689–705, https://www.jstor.org/stable/2186925.

literature, Michael Walzer's *Just and Unjust Wars* advanced an updated approach of the legalist paradigm (Walzer explicitly uses the term to describe his work).[24] Walzer's formulation specifies six propositions which amount to a very restrictive view of war. Only self-defense in the face of aggression can justify war. Yet Walzer knew even in his own book that the formulation was too restrictive. He modified the paradigm, concluding that in some cases preemptive war might be justified.[25] The problem with Walzer's modifications is that the legalist paradigm does not contain a commonly agreed, objective, standard by which to judge when states used preemption wrongly but in good faith. The only way to make such a judgment would be to presume to know "the real intentions" of states and the leaders who wield state power.

More criteria must be added. But as new criteria are added, new exceptions must be made thereby accelerating the atrophy of the approach.[26] Efforts which characterize just war as somehow so novel that new rules and criteria are required would do so. Critics of just war's readiness for cyber point to three characteristics of cyberwar when making their case: cyberwar is non-physical, non-human, and non-violent.[27] This reading of cyberwar suggests that the virtual nature of cyber is somehow incommensurate with warfare as it has been traditionally understood. It shares much with those who criticized the advent of drones as somehow breaking our traditional categories of war and morality.[28]

24. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (2006; repr., Basic Books, 1977), 61–62.

25. Ibid., 85.

26. This characterization might be too unfair to Walzer who perhaps more than any other, save Paul Ramsey, helped resuscitate just war ethics in the United States. He was also aware of the criticisms and engaged them. See Michael Walzer, "The Moral Standing of States: A Response to Four Critics," *Philosophy & Public Affairs* 9, no. 3, Spring (1980): 209–29, https://www.jstor.org/stable/2265115; Michael Walzer, "The Triumph of Just War Theory (and the Dangers of Success)," *Social Research* 69, no. 4, Winter (2002): 925–44, www.jstor.org/stable/40971584; James Turner Johnson argues that Walzer was one of three legs which brought just war back in modern discourse. See, James Turner Johnson, "Paul Ramsey and the Recovery of the Just War Idea," *Providence: A Journal of Christianity & American Foreign Policy*, September 30, 2019, url: https://providencemag.com/2019/09/paul-ramsey-recovery-just-war-idea/, date accessed February 20, 2021

27. The categories are also Sleat's. See, Sleat, "Just Cyber War?". Readers should note that these criticisms seem to share the cyber skeptics idea that cyberwar is not war or violence as traditionally understood, but reason in the opposite direction toward a perceived urgency for a new, radical ethics.

28. Rosa Brooks, "Drones and the International Rule of Law," *Ethics & International Affairs* 28, no. 1 (2014): 83–103; Gregory S. McNeal, "Targeted Killing and Accountability," *The Georgetown*

For the critics of just war, the level of analysis is too narrow and must be widened.[29] It must be widened to included "non-human" approaches to conflict, and develop concepts of "cyber harm" to distinguish it from real, or physical harm.

Chasing down ever more granular and novel frameworks for just war would atrophy the tradition because no one would know which framework to use when.[30] A moral framework with too much complexity will be readily dismissed. Humans are cognitive misers who look for mental shortcuts to deal with the manifold stimuli in their daily lives.[31] Moral theories, like their empirical models, must retain a degree of simplicity so that ethicists and policymakers can think through the questions and applications during crises, when time is short, resources scarce, and consequences great.

Moral hazard

A mirror of ever increasing complexity in just war thinking is a too simplistic or caviler praise for it without sufficient reflection in the requirements of charity toward justice. The section on just war's principles mentioned in passing the paradoxical lowering of escalation thresholds. As cyberwar becomes more and more common, policymakers will come to see its use as so common place that even raising the possibility that cyberwar could be morally questionable as a laughable proposition. Cyber operations give them "more options" in a dangerous world. And when domestic constraints on executive power incentivize leaders to

Law Journal 102 (2014): 681–794; Mark Moyar, "Drones—an Evolution, Not a Revolution, in Warfare," *Strategika* (Cambridge Univ Press, 2014), http://www.hoover.org/research/drones-evolution-not-revolution-war-fare.html; Kenneth Anderson, "Efficiency in Bello and Ad Bellum: Targeted Killing Through Drone Warfare," in *Targeted Killings: Law and Morality in an Asymmetrical World*, ed. Claire Finkelstein, Jens David Ohlin, and Andrew Altman (New York, NY: Oxford University Press, 2012), http://ssrn.com/abstract=2343955; David Luban, "What Would Augustine Do? The President, Drones, and Just War Theory," 2012, https://www.bostonreview.net/david-luban-the-president-drones-augustine-just-war-theory; Daniel Brunstetter and Megan Braun, "The Implications of Drones on the Just War Tradition," *Ethics & International Affairs* 25, no. 3 (2011): 337–58.

29. Sleat, "Just Cyber War?" 328.

30. Moreover, as Sleat rightly points out, the non-physical critique is dismissed fairly quickly since cyberwar is physical "…in that it is made up of electronics, of physical matter with physical properties that obey the laws of physics" -Sleat, ibid., 335.

31. For a brief summary of how humans lessen their cognitive burden, see Robert Jervis, *How Statesmen Think: The Pyschology of International Politics* (Princton, NJ: Princeton University Press, 2017), chap. 2, "The Drunkard's Search".

exercise restraint in world affairs, the increased reticence for "boots on the ground" will be met with increased acceptance for flexible, non-lethal options like cyber.[32] But any insertion of malicious code—which is what actually happens in a cyber attack—is by definition a violation of sovereignty.[33]

The risk of moral hazard is more real and requires, I'd like to suggest, more immediate responses from scholars. Not only are policymakers and executives prone to rely on cyber without reflection, others are going so as far to claim since no physical harm occurs to people then cyber may always be justified, and even obligatory.[34] And since the tools of cyberwar are cheap relative to bombs, fighter planes and submarines, and mass mobilizations, using them will always be more attractive to leaders who lack the training in ethics or who, even if they do, want to shirk the duty of moral judgment.

Conclusion

In summary, this paper contends that just war is an adequate framework for dealing with cyberwar. It affirms that cyberwar is, in fact, war; and that whatever novelty exists in the cyber domain can be addressed with the careful application of just war precepts. Nevertheless, two challenges linger on the horizon which are endemic more to a misapplication of just war thought than to cyberwar. An over legalist approach to just war might atrophy the tradition as greater complexity will lead policymakers and ethicists to abandon its use for other approaches. And an overly optimistic use of just war could invite moral hazard as policymakers use cyber offensives and escalate human conflict faster.

Just war ethicists and strategists are wise to read the tradition less as a legal checklist and more as a handbook for prudential statecraft. The precepts of just war are

32. For a treatment of how domestic politics shapes executive power, see Peter Trubowitz, *Politics and Strategy: Partisan Ambition & American Statecraft* (Princeton, NJ: Princeton University Press, 2011).

33. David J. Lonsdale, "The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios," *Journal of Military Ethics* 19, no. 1 (2020): 34, doi:10.1080/15027570.2020.1764694.

34. Lonsdale, "The Ethics of Cyber Attack"; For clarity, this is not Lonsdale's position but rather one he evaluates and criticizes

simple, but their use requires careful thought. And although human affairs will continue to struggle with the plague of war, a constant feature of human nature is its yearning for peace. Cyberwar brings new puzzles, but as human nature has not changed, the just war tradition is worthy guide for thinking about the place of cyberwar in the quest for that elusive lasting peace among mankind.

References

Anderson, Kenneth. "Efficiency in Bello and Ad Bellum: Targeted Killing Through Drone Warfare." In *Targeted Killings: Law and Morality in an Asymmetrical World*, edited by Claire Finkelstein, Jens David Ohlin, and Andrew Altman. New York, NY: Oxford University Press, 2012. http://ssrn.com/abstract=2343955.

Arquilla, John. "Twenty Years of Cyber War." *Journal of Military Ethics* 12, no. 1 (2013): 80–87. doi:10.1080/15027570.2013.782632.

Biddle, Stephen. *Military Power: Explaining Victory and Defeat in Modern Battle*. Princeton University Press, 2006.

Brooks, Rosa. "Drones and the International Rule of Law." *Ethics & International Affairs* 28, no. 1 (2014): 83–103.

Brunstetter, Daniel, and Megan Braun. "The Implications of Drones on the Just War Tradition." *Ethics & International Affairs* 25, no. 3 (2011): 337–58.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. 1832. Reprint, Princeton, NJ: Princeton University Press, 1976.

Eberle, Christopher J. "Just War Adn Cyberwar." *Journal of Military Ethics* 12, no. 1 (2013): 54–67. doi:10.1080/15027570.2013.782638.

Gartzke, Erik. "The Myth of Cyberwar: Bringing War in Cyberspace Back down to Earth." *International Security* 38, no. 2, Fall (2013): 41–73. doi:10.1162/.

Jervis, Robert. *How Statesmen Think: The Pyschology of International Politics*. Princton, NJ: Princeton University Press, 2017.

Lammasch, Heinrich. "Unjustifiable War and the Means to Avoid It." *The American Journal of International Law* 10, no. 4 (1916): 689–705. https://www.jstor.org/stable/2186925.

Lonsdale, David J. "The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios." *Journal of Military Ethics* 19, no. 1 (2020): 20–39. doi:10.1080/15027570.2020.1764694.

Luban, David. "What Would Augustine Do? The President, Drones, and Just War Theory," 2012. https://www.bostonreview.net/david-luban-the-president-drones-augustine-just-war-theory.

McNeal, Gregory S. "Targeted Killing and Accountability." *The Georgetown Law Journal* 102 (2014): 681–794.

Moyar, Mark. "Drones—an Evolution, Not a Revolution, in Warfare." *Strategika*. Cambridge Univ Press, 2014. http://www.hoover.org/research/drones-evolution-not-revolution-war-fare.html.

Reichberg, Gregory M., Henrik Syse, and Endre Begby, eds. *The Ethics of War: Classic and Contemporary Readings*. Malden, MA & Oxford, UK: Blackwell Publishing, 2006.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32. doi:10.1080/01402390.2011.608939.

Singer, P. W., and August Cole. *Ghost Fleet*. New York, NY: Houghton Mifflin Harcourt, 2015.

Slayton, Rebecca. "What Is a Cyber Warrior? The Emergence of u.s. Military Cyber Expertise, 1967–2018." *Texas National Security Review* 4, no. 1 (2021).

Sleat, Matt. "Just Cyber War? *Casus Belli*, Information Ethics, and the Human Perspective." *Review of International Studies* 44, no. 2 (2017): 324–42. doi:10.1017/S026021051700047X.

Trubowitz, Peter. *Politics and Strategy: Partisan Ambition & American Statecraft*. Princeton, NJ: Princeton University Press, 2011.

Walzer, Michael. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*.

2006. Reprint, Basic Books, 1977.

———. "The Moral Standing of States: A Response to Four Critics." *Philosophy & Public Affairs* 9, no. 3, Spring (1980): 209–29. https://www.jstor.org/stable/2265115.

———. "The Triumph of Just War Theory (and the Dangers of Success)." *Social Research* 69, no. 4, Winter (2002): 925–44. www.jstor.org/stable/40971584.