Just & Unjust War, Uses of Force & Coercion: An Ethical Inquiry with Cyber Illustrations

David P. Fidler

Abstract: The emergence of cyber means and methods of war, force, and coercion raises ethical questions under just war theory different from those historically generated by the development of ever more destructive instruments of war. Whether in armed conflict or contexts not considered war, cyber technologies create political and ethical incentives for their use. However, this attractiveness poses potential risks and dangers that, at present, are largely speculative but invite more ethical deliberation. Unfortunately, the convergence of political and ethical incentives on cyber in a context of increasing geopolitical competition and conflict make the prospects for ethical consensus on just and unjust cyber coercion, force, and war unlikely.

DAVID P. FIDLER is the James Louis Calamaras Professor at the Indiana University Maurer School of Law and an Adjunct Senior Fellow for Cybersecurity at the Council on Foreign Relations. His publications include *The Snowden Reader* (2015), *India and Counterinsurgency: Lessons Learned* (2009), *Responding to National Security Letters: A Practical Guide for Legal Counsel* (2009), and *Biosecurity in the Global Age: Biological Weapons, Public Health, and the Rule of Law* (2008).

Among new technologies affecting ethical deliberations about war, none is as enigmatic as cyber. Within just war theory, cyber warfare exhibits attractive characteristics. Unlike the development of more violent weaponry, cyber does not endanger ethical objectives as directly in the just war tradition. Cyber weapons take a different trajectory within just war theory: away from extremes that threaten to obliterate ethics and toward scenarios in which the ethical compass functions but struggles to find true north.

This trajectory also appears in how cyber technologies highlight differences between war and force, which recalls Michael Walzer's argument for "a theory of just and unjust uses of force."[1] Cyber creates possibilities for force "short-of-war"[2] and coercion short-of-force and thus raises questions about the relationship among force, coercion, and ethical objectives of the just war tradition, such as protecting civilians. Cyber incidents often require analyzing concepts found in just war theory, such as reprisals and

doi:10.1162/DAED_a_00410

deterrence, in situations not amounting to war, creating complicated ethical contexts.

This essay, first, identifies how cyber technologies affect just war theory. Cyber warfare presents different challenges from those that have dominated just war thinking and invites ethical deliberations rather than marginalizing them.[3] Cyber is not putting the Athenians before Melos. Second, concerning uses of cyber technologies that fall short of war and thus outside just war theory, the essay examines Walzer's ideas on just uses of coercion and force and applies them to cyber. Thinking through the ethics of coercion and force short-of-war proves disorienting because arguments go in various directions. But the disorientation is important because cyber is not rendering ethics inert.

After a decade of effort, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) reached a consensus in 2013 that international law applies to cyberspace, including the prohibition on the use of force.[4] Prior GGE failure to reach agreement on this issue reflected many factors, including whether cyberspace is so different that it requires new rules.

GGE delegations for and against applying international law made ethical arguments, at least rhetorically. China resisted – and continues to resist – including the law of armed conflict in the consensus because applying this law legitimizes the "militarization" of cyberspace. Under this position, cyberspace is, and should be considered, different. The United States embraced the law of armed conflict because it provides legal and ethical guidance in cyberspace. These opposed positions force us to consider whether cyberspace is, or should be considered, distinct from traditional realms of armed conflict.

Perhaps those against applying the law of armed conflict bear the burden of justifying this position. However, things get complicated when we consider other controversies. China and the United States also disagree about Internet governance. China favors "Internet sovereignty," in which states govern the Internet through international law and organizations. The United States supports "multistakeholder" governance involving state and nonstate actors, an approach associated with "Internet freedom."

Friction between these positions intensified at the 2012 World Conference on International Telecommunications (WCIT) organized by the International Telecommunication Union (ITU). The Chinese wanted international law and institutions to control Internet governance, as done with other communication technologies. The Americans advocated keeping international law and the ITU at arm's length – a stance that the Internet is, and should be considered, distinct.

In the GGE and WCIT, we have claims that cyberspace and the Internet are different and these differences should affect how we think about them. But we do not have consistency about which states support cyber exceptionalism or in what contexts. Instead, these examples illustrate normative and political complexities lurking in cyberspace. How these complexities affect ethical considerations bears watching in analyses of cyber activities and armed conflict.

In 2010, the Stuxnet worm was discovered, and analysis revealed it was used to attack uranium-enrichment centrifuges in Iran. The attack damaged hundreds of centrifuges. The worm was so sophisticated that only a state or states could have developed it. Evidence suggests that Stuxnet was a U.S.-Israeli effort, but neither country has admitted involvement. Stuxnet is the first known use by a state of a pur-

pose-built cyber weapon designed to damage property in another state. In *jus ad bellum* terms, did the attack constitute an act of war or a crime of aggression?

The incident reopened debates about what "force" and "armed attack" mean. Whether Stuxnet was an illegal use of force or armed attack produced disagreement about whether the damage constituted force or an armed attack in international law.[5] State reactions to this episode were subdued. Had conventional weaponry damaged hundreds of centrifuges, international lawyers would not have considered the use-of-force and armed-attack questions difficult. Diplomats would have been more vocal. Did use of a *cyber weapon* affect perspectives on this seminal incident?

This question implies that cyber creates the potential for a type of aggression we might not consider criminal. Stuxnet did not trigger war. But if war is an act of force, as Clausewitz argued, then Stuxnet – a weapon designed to damage property in a specific country – was an instrument of force. Without a justification, it looks like an act of war that we are not sure how to evaluate.

Two options to avoid this quandary are apparent. First, we could read Stuxnet as not amounting to war or aggression because of the limited damage it caused, particularly the absence of injuries or deaths. It is a type of force outside *jus ad bellum* made possible by the less lethal and destructive options cyber technologies create. Second, perhaps the perpetrators were justified in attacking, in which case Stuxnet was not an act of war or aggression. The most plausible justification involves preventing Iran from developing a nuclear-weapons capability. We are not talking about preventive war. Stuxnet involved, in Walzer's phrase, "preventive use of force-short-of-war" outside *jus ad bellum*,[6] thus highlighting the need to extend just war thinking to force short-of-war.

Both options take analysis away from *jus ad bellum*. This trajectory resonates with debates about whether Stuxnet violated the legal prohibition on the use of force. Even if Stuxnet was an illegal use of force, it did not generate controversies typically seen when states use force in violation of international law. Given the ability to limit and tailor damage, can a cyber weapon provide ethical ways of violating the legal prohibition on the use of force?

This analysis assumed that a state was responsible for Stuxnet. However, Stuxnet touches another aspect of cyber technologies that affects ethical deliberations: the attribution problem. When a cyber incident happens, we want to know who did it. Cyber technologies provide opportunities for instigators to make attribution difficult. In law, attribution is critical because it determines which actor is involved, what policy prescriptions and legal rules apply, and what evidence is required to hold the perpetrator accountable. Attribution is also important in ethics. We could assert that "a state perpetrated an unjust cyber attack," but if we cannot identify the state, then the statement loses ethical force.

In just war theory, having a just cause to go to war requires identifying the state that committed the initial wrong triggering the right to use force. The inability to do so with a high level of certainty counsels against the victim state waging war. This position perhaps explains why analyses of just war theory often do not focus on attribution. With perhaps one exception, Walzer's historical illustrations involve known perpetrators. The exception involves General Yamashita, who was, many believe, unjustly executed for crimes committed by soldiers under his command. But no one questioned that Japanese soldiers committed the atrocities.

In cyber, attribution is a problem. Although claims are made that attribution is becoming more feasible, accusations based on evidence and means of detection that

remain secret agitate attribution controversies. In addition, the law imposes evidentiary requirements that those seeking to hold states accountable for violating legal rules must meet. Tracing a cyber attack to an Internet address in a specific location might be technically accurate, but might not meet the evidence thresholds international law requires for assigning state responsibility.[7] Just war theory creates a similar challenge given its high threshold for attributing wrongs capable of starting wars.[8]

The attribution problem has stimulated efforts to overcome it, including the argument that, rather than perceive the problem as intractable, "attribution is what states make of it."[9] However, alternative approaches have to achieve collective acceptance given cyber's global scope. This challenge requires surmounting the triple burden in the attribution problem – the technological difficulties, the legal demands, and the ethical strictures – in an international political context that has not proved receptive to the development of new cyber norms.

Stuxnet is the only existing example of a cyber incident that approaches *jus ad bellum*, but states and terrorists could try to use cyber weapons to kill and destroy on a massive scale. U.S. policy-makers have warned that states could cause a "cyber Pearl Harbor" or terrorists could launch a "cyber 9/11." However, these scenarios are not difficult in just war terms. If, unprovoked, a state attacked with cyber and caused death and destruction on the scale of Pearl Harbor, then it launched an unjust war and committed criminal aggression. The slaughter of thousands and large-scale destruction of property by cyber terrorists would trigger the victim state's right to use force in self-defense. In both cases, ethical analysis would shift to whether belligerents fight in accordance with *jus in bello*.

With these scenarios, people argue not about ethics, but whether states or terrorists could or would cause such slaughter and devastation with cyber weapons. From the technological perspective, doubt exists that cyber weapons could kill and destroy on the scales of Pearl Harbor or 9/11. More realistic scenarios involve less dramatic consequences, which would raise questions, again, about whether uses of cyber weapons cross into *jus ad bellum*. Politically, scary scenarios do not explain why a state or terrorists would court full-scale war by launching killer cyber attacks.

In 2008, Russia and Georgia fought a war that featured depressingly familiar aspects of armed conflict, including alleged war crimes. However, the war stands out because Georgia experienced distributed denial of service (DDOS) attacks. Once war is underway, just war theory analyzes whether "the war is being fought justly or unjustly."[10] Lawyers have analyzed the cyber aspects of the Russia-Georgia war under the law of armed conflict. The hardest question involved the attribution problem: was Russia responsible? Efforts to answer this question did not find sufficient evidence that Russia was legally responsible. Although this outcome does not preclude ethical deliberations, facts – or the lack of them – still matter for determining accountability.

In addition, attribution does not matter if no wrong is done. In the Russia-Georgia war, did the DDOS attacks against governmental and civilian institutions violate *jus in bello* rules about "fighting well"?[11] Under the law of armed conflict, the disruptions did not qualify as an "attack" – an act intended or foreseeably likely to cause death, injury, destruction, or damage – subject to legal rules, including those protecting civilians. With no violation, there is no accountability to assign, which makes attribution legally irrelevant.

In just war theory, international law does not determine the scope of ethical delib-

eration. However, where ethics go when the law of armed conflict is not violated is unclear. Most debates about the actions of soldiers and commanders address whether violating established rules – Walzer's "war convention"[12] – are justified. How do we evaluate acts of force or coercion short-of-an-attack during war? When we evaluate such acts, will we not look favorably on them compared to violent, kinetic attacks? Aren't we going to want, ethically, weapons that do not produce the death, injury, destruction, and damage that belligerents can legally inflict during war?

Let's return to Stuxnet. Assume Iran and the United States were at war, and the United States deployed Stuxnet. This weapon was built to cause damage, and it caused damage, qualifying as an attack in the law of armed conflict. Under this law, the United States attacked a military target, the attack and weapon complied with the principles of distinction and discrimination, the damage was not disproportionate, and the methods used to attack were, as far as we know, not perfidious. Stuxnet's performance, particularly under the discrimination and proportionality principles, provided a glimpse of "the possibility of an age of precise warfare that is truly unprecedented."[13]

This hypothetical highlights cyber's attractiveness under the war convention.[14] Underscoring this attractiveness is the U.S. government's acknowledgement in early 2016 that it was launching cyber attacks against the so-called Islamic State's social media operations and military command-and-control capabilities in the armed conflict being waged against this group.[15] Given its position on cyber and *jus in bello*, the United States clearly believes that its cyber weapons and attacks comply with the law of armed conflict and with this law's ethical functions in the just war tradition. The U.S. acknowledgement represents the first time a state has admitted to using cyber weapons in armed conflict, and the U.S. cyber attacks are a seminal development in the long-predicted integration of offensive cyber capabilities into strategies and tactics for waging war.

The attractiveness of cyber in the war convention does not mean that all cyber weapons will be as sophisticated as Stuxnet or that all cyber attacks during war would comply with *jus in bello*. Belligerents could use cyber weapons in illegal and unethical ways, with "the most serious ethical problem … [being] their potential for collateral damage to civilians."[16] However, the cyber threat to the war convention appears, at present, more limited than threats posed by kinetic weapons. We are unlikely to see cyber equivalents of the Dresden firebombing or the My Lai massacre. Indeed, cyber's less lethal and destructive possibilities raise the question whether belligerents should use them before, or instead of, kinetic weapons.[17]

Cyber weapons might also be preferable if a belligerent decides that military necessity or supreme emergency requires breaching the war convention. If a belligerent believes it must neutralize civilian targets, an attack would violate the principle of civilian immunity, whatever weapon is used. However, a cyber attack might cause less death, injury, destruction, or damage than conventional weaponry, and thus be an ethically better way to fight unjustly.

Analyzing cyber warfare has a surreal quality at the moment because there has been no cyber warfare, at least not as just war theory describes war. However, as the U.S. cyber attacks against the Islamic State demonstrate, cyber technologies are being integrated with other weaponry and tactics in armed conflict, a trend that will continue. The future might also see more examples of the "hybrid warfare" Russia has conducted in Eastern Ukraine by combining kinetic operations, infor-

mation warfare, and covert cyber activities,[18] or of Russia's "gray zone combat" against NATO members and partners involving disruptive cyber attacks, cyber espionage, and online propaganda.[19] In such activities, cyber technologies are useful for many purposes, most of which do not constitute attacks under the law of armed conflict, but challenge adversaries and complicate calculations of outside actors.

The Islamic State also integrates kinetic operations with cyber activities in its war-fighting. Although its "cyber caliphate" has claimed responsibility for incidents, including one against U.S. Central Command, its signature activity is exploiting social media to spread propaganda and recruit adherents.[20] The Islamic State's use of social media in waging war is unprecedented, and it has produced not only U.S. cyber attacks against the Islamic State's social media operations, but also U.S. kinetic attacks against members of the cyber caliphate.

Although not works of ethics, the *Tallinn Manual on the International Law Applicable to Cyber Warfare* and the U.S. Department of Defense's *Law of War Manual* address how *jus in bello* applies to cyber.[21] These manuals indicate that cyber weapons do not create the stark ethical dilemmas that the militarization of other technologies has. Ever more destructive weaponry has strained ethical strictures in *jus in bello*, but cyber technologies do not follow this pattern.

Cyber raises different issues, particularly whether *jus in bello* should protect civilians from the full range of harms cyber operations can inflict on Internet-dependent services important to civilian well-being. Should the threshold at which civilian immunity is triggered be *lowered* to regulate less violent and lethal effects cyber operations can cause? Interfering with civilian cyber systems can be coercive, but, according to the *Tallinn Manual*, damaging code and data on computers does not by itself qualify as an attack in the law of armed conflict and is not subject to rules protecting civilian objects from attack.

Where the attack threshold is set legally makes cyber attractive to coerce an adversary without violating *jus in bello*. Here, the question is whether cyber coercion directed at civilians during war is ethical. At first glance, this question seems superficial given that the law of armed conflict permits belligerents to use kinetic weapons, including in ways that produce civilian collateral damage. However, civilian dependence on computer systems makes unrestricted cyber coercion suspect, especially given the principle of military necessity. Allowing unrestricted cyber coercion underneath the attack threshold would privilege a new capability to coerce civilians over the ethical imperative in war not to harm civilians without compelling reasons.

Norms guiding the transition from war to peace – *jus post bellum* – are not prominent in just war theory. Advocates for these norms identify the need to think about how wars end in order to inform war's ends and means. What *jus post bellum* seeks is daunting because a "just peace is one that vindicates the human rights of all parties to the conflict."[22]

In 2011, the UN Security Council authorized the use of force under the responsibility to protect (R2P) principle to protect Libyan civilians. According to news reports, the U.S. government considered, but rejected, cyber attacks against Libyan air defense systems, which NATO disabled through bombing. With Security Council authorization, NATO's operations were legal, and the attacks on the air defense systems complied with the law of armed conflict. The Libyan intervention was hailed as a successful application of R2P, until post-conflict Libya descended into chaos.

R2P includes the "responsibility to rebuild" after military interventions, which

links with *jus post bellum*. What happened in Libya supports those seeking more attention on the transition from war to peace. NATO forces complied with *jus ad bellum* and *jus in bello*, but the post-conflict phase tainted the notion that the intervention was a just war. Even so, how more emphasis on *jus post bellum* would have affected the decision to use military force or choices NATO made in waging war is hard to see. The Security Council acted under R2P to prevent atrocities in urgent circumstances that did not permit much contemplation about how the conflict might end. The U.S. government decided, in part, against cyber attacks because it believed preventing atrocities required immediate action that conventional weapons could accomplish. *Jus post bellum* does not seem relevant to that decision.

The Libya incident does not nullify the ethical importance of transitioning from war to peace, but it raises questions about how *jus post bellum* informs decisions about war's ends and means. What these questions mean for use of cyber technologies in war is harder to fathom. Cyber weapons might produce less death and destruction, which might help post-conflict efforts. But the more we use the Internet for military purposes, the more we might undermine cyberspace as a tool for post-conflict development. However, these musings seem trite because Libya's post-intervention collapse had nothing to do with cyber technologies.

In contrast with the paucity of cyber warfare examples, states are using cyber technologies in ways that are not acts of war, do not take place during armed conflict, and thus fall outside just war theory. For example, certain disclosures made by Edward Snowden revealed the U.S. government's interest in, policies on, and conduct of offensive cyber operations that can achieve a range of potential effects.[23] But the United States is not the only country interested in the coercive possibilities of cyber technologies.

The occurrence of offensive cyber acts demonstrates that cyber technologies make coercion and force short-of-war possible and attractive. The U.S. government has started to emphasize cyber threats short-of-war more than cyber Pearl Harbor or cyber 9/11 scenarios. This shift suggests that cyber force and coercion, not cyber war, are more pressing challenges. The following examples illustrate that forceful and coercive cyber actions, and threats of such actions, have become frequent.

Cyber Sabotage. In 2015, Reuters reported that the United States attempted, but failed, to damage North Korea's nuclear weapons program with a Stuxnet-like attack at approximately the same time it allegedly used Stuxnet to damage Iran's centrifuge facility. If these reports and allegations are accurate, the United States attempted cyber sabotage against two countries for reasons related to threats posed by the proliferation of nuclear weapons.

Cyber Vandalism. In 2014, the United States accused North Korea of "cyber vandalism" in hacking Sony Entertainment and damaging stored data and networks. Allegedly, North Korea did so in response to Sony's crude comedy about a fictional assassination of North Korea's leader. The hacking was a coercive act, but the choice of vandalism to describe it illustrates the difficulties of characterizing cyber coercion short-of-force.

Cyber Reprisal. In 2012, Iran is believed to have launched a cyber attack against Saudi Aramco, damaging approximately thirty thousand computers, and DDOS attacks against U.S. financial institutions. Experts argued that these attacks were reprisals against Saudi Arabia for being a U.S. ally and the United States for the Stuxnet attack. In 2015, the United States accused Iran of hacking the Sands Hotel in

Las Vegas, an apparent retaliation for remarks the hotel's owner – a supporter of Israel – made about Iran.

Cyber Attrition. For years, South Korea has experienced cyber incidents it believes North Korea has perpetrated. One incident involved the hacking of a company that operates South Korean nuclear energy facilities. These events form part of the political and military struggle on the peninsula, and North Korea uses cyber to threaten, weaken, and distract South Korea.

Cyber Espionage. Traditionally, states have not considered espionage a coercive act that violates the legal prohibition on intervention in the domestic affairs of other states. However, the scale and intensity of cyber espionage have generated claims that it has become coercive, destabilizing, and "a proscribed intervention under customary international law."[24] The United States has accused China of persistent, large-scale, and harmful cyber espionage against the U.S. government and U.S. companies. Significantly, in 2015, the United States accused Chinese government hackers of stealing information from the Office of Personnel Management (OPM) on millions of government employees. The Obama administration believed this act of spying went beyond normal espionage and justified retaliation. Likewise, China has complained about intrusive U.S. cyber espionage, complaints Snowden's leaks amplified.

Cyber Deterrence. In 2015, the U.S. Department of Defense released a new cyber strategy that emphasized deterrence, which "works by convincing a potential adversary that it will suffer unacceptable costs if it conducts an attack on the United States, and by decreasing the likelihood that a potential adversary's attack will succeed."[25] The U.S. government has threatened to retaliate against China to deter it from undertaking certain kinds of cyber espionage. In thinking about how to retaliate for the OPM hack, the Obama administration considered offensive cyber operations against China's "Great Firewall" to undermine the Chinese government's control of the Internet. As in other contexts, deterrence in cyber requires credible threats backed by attribution and offensive capabilities sufficient to identify and hurt an adversary, and thereby change its behavior. Deterrence in cyber appears in other ways as well. Demonstrating offensive capacity and cyber espionage skills sends signals intended to induce caution in adversaries, features connected with cyber attacks that temporarily disrupted electrical supplies in Ukraine at the end of 2015.[26]

In short, states have developed interests and capabilities in using, and threatening to use, cyber as a means of force and coercion short-of-war. The examples reveal a spectrum of harm that includes destructive, damaging, degrading, disruptive, and deterrent effects. This spectrum highlights the complications that cyber technologies introduce when attempting to distinguish force short-of-war from coercion short-of-force. The range of effects also creates the risk that cyber actions short-of-war might trigger escalation, which raises particular questions about automated responses to cyber incidents.[27] The spectrum, and its dangers, counsels thinking about just and unjust cyber coercion in addition to cyber force short-of-war.

For state actions that fall underneath the legal prohibition on the use of force associated with *jus ad bellum*, international law contains obligations, including to settle disputes peacefully, respect the sovereignty of other states, and refrain from intervening in the domestic affairs of other states.[28] Violation of these principles permits the victim state to respond with proportionate countermeasures not involving the use of force intended to bring the state committing the wrongful act into compliance with international law.

The cyber acts short-of-war described above suggest that these legal rules do not adequately regulate state behavior. This problem connects to precyber controversies about the nonintervention principle, including the principle's nonapplication to espionage or other coercive acts, such as economic sanctions. These issues create challenges for ethical analysis. To illustrate, the United States proposed to the GGE in 2015 some voluntary cyber norms for peacetime. One norm the GGE accepted holds that countries should not conduct cyber operations that intentionally damage critical infrastructure in other states.[29] Such attacks would violate legal duties to settle disputes peacefully, respect sovereignty, and refrain from coercive interference in another country's domestic affairs. It is a sign of how bad things are in cyberspace when a nonbinding norm is proposed to accomplish what binding international law prohibits.

Turning to ethics, Walzer posited that a theory of just uses of force short-of-war should reflect just war theory. We can extend this proposition to coercion short-of-force as well. First, coercion and force short-of-war must have a just cause. Walzer argued that just causes for force short-of-war "will certainly be more permissive than the theory of just and unjust war."[30] How much more permissive is not clear, which raises the question of whether just causes for coercion short-of-force are even broader. The need to prevent escalation should inform the additional permissiveness, and avoiding escalation requires that coercion and force be proportionate to the just cause and the context be one in which escalation is not likely.

Second, Walzer argued that force short-of-war "should be limited in the same way that the conduct of war is limited, so as to shield civilians."[31] In essence, *jus in bello* –type rules should apply. But this step is more complicated than it might appear. Do we need a rule to determine when coercion and force short-of-war trigger the obligation to shield civilians, as the concept of "attack" does in the law of armed conflict? What are the peacetime equivalents of the "military necessity" principle, or "combatants" that would be legitimate targets? Does it even make sense to subject coercion or force short-of-war to a rule against targeting civilians when such acts do not threaten a civilian's right to life? What rules should guide the responses of states victimized by cyber coercion and force short-of-war?

Cyber technologies do not clarify what just causes should be included in a theory of just coercion and force short-of-war. The scope of just-cause permissiveness would stimulate disagreement, just as the legitimacy of going to war for reasons beyond self-defense and Security Council authorization is hotly contested. Potential just causes, such as responding to atrocities or preventing proliferation of weapons of mass destruction, do not come with political or ethical consensus about the propriety of using coercion or force short-of-war for these purposes. Does Stuxnet's role in helping the United States persuade Iran to enter into an agreement on its nuclear program make the operation ethically palatable sabotage?[32]

However, cyber's coercive possibilities might provide incentives for countries to explore the boundaries of coercion and force short-of-war. Capabilities associated with cyber could make deliberations about just causes for coercion and force short-of-war less exacting, with emphasis shifting to the proportionality of the means used. If so, we would expect frequent but calibrated cyber incidents undertaken for diverse reasons. The examples described above prove this expectation is not far-fetched.

Drawing a line between force short-of-war and coercion short-of-force might avoid this problem by centering ethical de-

liberations on actions closer to war. Leaving aside the difficulty of reaching consensus on where to draw this line, cyber technologies might stimulate resistance to establishing clarity between force and lesser forms of coercion. The ability to argue that a coercive cyber operation did not constitute a use of force short-of-war would be politically useful and would create headwinds for achieving ethical consensus. This dynamic could produce the ethics equivalent of controversies about the scope, substance, and effectiveness of the nonintervention principle in international law.

Similarly, arguing that *jus in bello*–type rules should regulate coercion and force short-of-war – and responses to such acts – might encourage countries to resist clarifying what qualifies as coercion short-of-force and what constitutes force short-of-war. The possibilities that cyber technologies support could feed this resistance so that states can maximize offensive and defensive options. Even for activities that would produce coercion or force short-of-war, states can tailor cyber attacks in ways that are discriminating and do not cause significant collateral damage, as happened with Stuxnet. Even with ethically dubious attacks, such as the Sony hack, indiscriminate harm to people or property did not occur. Further, states hit by acts of cyber coercion or force should also react under the discrimination and proportionality principles.[33] So, just and unjust acts of cyber coercion or force – and responses to them – can comply with *jus in bello*–type rules.

But with the ability to attack targets without major collateral damage, exploiting cyber to "coerce well" might make states care even less about the ethics of coercion or force short-of-war. Leaving just causes aside, cyber attacks that produce discriminate, proportional consequences make escalation less likely. That capability has great political utility, and states are using cyber coercively in ways that have not, so far, produced escalation toward war. We get escalation avoidance through targeted, proportional cyber coercion without a theory of just coercion and force short-of-war guiding state actions.

Although cyber technologies and just war theory have been my focus, how such technologies support efforts to achieve peace – and advance *jus ad pacem* – is also important. For many, the Internet can help reduce domestic and international conflict by facilitating economic interdependence, political development, and cultural understanding. Such outlooks link a global, accessible, and free Internet with the purpose of achieving meaningful peace at home and abroad.

For *jus ad pacem*, the emphasis on the ethics of cyber warfare is worrying. The Internet's weaponization could undermine what cyber technologies can do for human betterment. These technologies prove attractive in peace and war, and perhaps too much attention is paid to shielding civilians from cyber warfare as opposed to protecting the Internet, societies, and individuals from power politics. Focusing on war, force, and coercion also does not touch human rights controversies about cyber surveillance by states seeking to prevent kinetic and cyber threats and attacks from other countries and terrorists.[34] Approaching cyber technologies through *jus ad pacem* highlights the need for demilitarizing cyberspace rather than delineating why and how states can use cyber weapons to fight wars and coerce adversaries.

In *Just and Unjust Wars*, Walzer revived the need to think about the ethics of war after the Vietnam conflict and during a Cold War dependent on nuclear terror. The digital age is different, and cyber technologies affect the ethics of war in ways that do not resemble the dilemmas Walzer

tackled. Unlike weapons and combat situations that threaten ethics in war, cyber can fit within *jus ad bellum* and *jus in bello*, but the potential for cyber coercion and force short-of-war generates ethical issues that the just war tradition does not address. Under just war theory, cyber proves attractive as a means of fighting justly and fighting well, and, outside just war theory, as a means of coercion and force short-of-war not subject to clear ethical guidance.

My claim is not that cyber technologies are intrinsically ethical when used in waging war or coercing states outside armed conflict. As has happened with other technologies, states could deploy cyber means and methods illegally and unethically in going to war, fighting armed conflicts, or coercing adversaries in peacetime. Further, political and technological developments might produce new forms of cyber warfare and less sanguine conclusions.[35] But at the moment, the possibilities cyber technologies create, along with their limitations, align with just war thinking in ways that do not produce "war is hell" outcomes.

These possibilities also make thinking prescriptively about cyber coercion and force short-of-war difficult. Following Walzer, ethical reasoning favors applying core concepts of the just war tradition – just cause, necessity, discrimination, and proportionality – to coercion and force short-of-war and responses to such acts. Anchoring ethical deliberations about coercion and force short-of-war in these principles makes theoretical sense, but murkiness arises in their application. In contexts involving conventional means of coercion and force, controversies in international law about the prohibitions against the use of force, intervention in another state's domestic affairs, and violating a foreign country's sovereignty highlight the difficult political, legal, and ethical terrain of coercion and force short-of-war as phenomena in international relations.

The great utility cyber technologies offer means states have few incentives to clarify how ethical principles from just war theory apply to cyber coercion and force short-of-war. At the same time, the possibilities cyber technologies create for discriminating and proportional acts of coercion and force that do not risk escalation make cyber options ethically attractive, in the same way the just war tradition finds ethical potential in cyber weapons.

At present, political and ethical interests converge in cyber in ways that drain urgency from revising the just war tradition and developing a theory of just coercion and force short-of-war – an outcome rarely seen in the history of politics and ethics concerning the emergence of new means and methods of coercion, force, and war.

ENDNOTES

1 Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 4th ed. (New York: Basic Books, 2006), xv.

2 Ibid.

3 Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9 (4) (2010): 384 – 410.

4 United Nations Group of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/68/98*), June 24, 2013.

5 Marco Roscini, "Cyber Operations as a Use of Force," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Cheltenham, United Kingdom: Edward Elgar, 2015), 233 – 254.

[6] Walzer, *Just and Unjust Wars*, xiv.

[7] United Nations Group of Governmental Experts, *Developments in the Field of Information and Telecommunications in the Context of International Security* (A/70/174), July 22, 2015, 13.

[8] Christopher J. Eberle, "Just War and Cyberwar," *Journal of Military Ethics* 12 (1) (2013): 54 – 67, 56 – 57.

[9] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (1 – 2) (2014): 4 – 37, 7.

[10] Walzer, *Just and Unjust Wars*, 21.

[11] Ibid., 127.

[12] Ibid., 44.

[13] Ryan Jenkins, "Is Stuxnet Physical? Does It Matter?" *Journal of Military Ethics* 12 (1) (2013): 68 – 79, 74.

[14] John Arquilla, "Twenty Years of Cyberwar," *Journal of Military Ethics* 12 (1) (2013): 80 – 87.

[15] David P. Fidler, "Send in the Malware: U.S. Cyber Command Attacks the Islamic State," Net Politics, March 9, 2016, http://blogs.cfr.org/cyber/2016/03/09/send-in-the-malware-u-s-cyber-command-attacks-the-islamic-state/.

[16] Neil C. Rowe, "Distinctive Ethical Challenges of Cyberweapons," in *Research Handbook on International Law and Cyberspace*, 307 – 325, 317.

[17] Duncan B. Hollis, "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?" in *Cyberwar: Law and Ethics for Virtual Conflicts*, ed. Jens David Ohlin, Kevin Govern, and Clarie Finkelstein (Oxford: Oxford University Press, 2015), 129 – 174.

[18] Jarno Limnéll, "The Use of Cyber Power in the War between Russia and Ukraine," Net Politics, January 11, 2016, http://blogs.cfr.org/cyber/2016/01/11/the-use-of-cyber-power-in-the-war-between-russia-and-ukraine/.

[19] David E. Sanger, "As Russian Hackers Probe, NATO Has No Clear Cyberwar Strategy," *The New York Times*, June 16, 2016, http://www.nytimes.com/2016/06/17/world/europe/nato-russia-cyberwarfare.html?smprod=nytcore-ipad&smid=nytcore-ipad-share&_r=0.

[20] David P. Fidler, *Countering Islamic State Exploitation of the Internet* (New York: Council on Foreign Relations Cyber Brief, June 2015).

[21] Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013); and U.S. Department of Defense, *Law of War Manual* (Washington, D.C.: United States Department of Defense, 2015).

[22] Robert E. Williams, Jr., and Dan Caldwell, "*Jus post Bellum*: Just War Theory and the Principles of Just Peace," *International Studies Perspective* 7 (2006): 309 – 320, 317.

[23] David P. Fidler, ed., *The Snowden Reader* (Bloomington: Indiana University Press, 2015), 184 – 198.

[24] Russell Buchan, "Cyber Espionage and International Law," in *Research Handbook on International Law and Cyberspace*, 168 – 189, 189.

[25] United States Department of Defense, *The DOD Cyber Strategy 2015* (Washington, D.C.: United States Department of Defense, April 2015), 11.

[26] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

[27] David Danks and Joseph H. Danks, "The Moral Permissibility of Automated Responses during Cyberwarfare," *Journal of Military Ethics* 12 (1) (2013): 18 – 33.

[28] Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention," in *Cyberwar: Law and Ethics for Virtual Conflicts*, 249 – 270.

[29] The United Nations Group of Governmental Experts, *Developments in the Field of Information and Telecommunications* (A/70/174), 8.

[30] Walzer, *Just and Unjust Wars*, xv.

[31] Ibid., xvii.

[32] David E. Sanger, "Diplomacy and Sanctions, Yes. Left Unspoken on Iran? Sabotage," *The New York Times*, January 19, 2016.

[33] Tobias Feakin, *Developing a Proportionate Response to a Cyber Incident* (New York: Council on Foreign Relations Cyber Brief, August 2015).

[34] Edward T. Barrett, "Warfare in a New Domain: The Ethics of Military Cyber Operations," *Journal of Military Ethics* 12 (1) (2013): 4–17, 13.

[35] Randell R. Dipert, "Other-Than-Internet (OTI) Cyberwarfare: Challenges for Ethics, Law, and Policy," *Journal of Military Ethics* 12 (1) (2013): 34–53.