Chapter 3
Is Warfare the Right Frame for the Cyber Debate?

Patrick Lin, Fritz Allhoff and Keith Abney

Abstract Nation-states are struggling to formulate cyberpolicy, especially against foreign-based intrusions and attacks on domestic computer systems. These incidents are often framed in the context of cyberwarfare, which naturally implies that military organizations should respond to these incidents. This chapter will discuss why cyberwarfare is ethically difficult and why, until responsible cyberpolicy is developed, we may plausibly reframe the problem not as warfare but as private defense, i.e., self-defense by private parties, especially commercial companies, as distinct from a nation-state's right to self-defense. The distinction between private defense and national defense is relevant, since victims of cyberattacks have been primarily industry targets and not so much government targets, at least with respect to measurable harm. And we focus on foreign-based cyberattacks since, unlike domestic-based attacks that are usually considered to be mere crimes and therefore a matter for domestic law enforcement, foreign-based attacks tend to raise special alarms and panic about more sinister motives. More than a mere criminal act, a foreign cyberattack is often perceived as an aggression so serious that it may plausibly count as an act of war, or *casus belli*, and so we are quick to invoke national security. But insofar as the state is currently not protecting industry from such cyberattacks—in part because it is difficult to arrive at a sound cyberpolicy—we should consider interim solutions outside the military framework.

Nation-states are struggling to formulate cyberpolicy, especially against foreign-based intrusions and attacks on domestic computer systems. These incidents are

P. Lin (✉) · K. Abney
Department of Philosophy, California Polytechnic State University, San Luis Obispo, USA
e-mail: palin@calpoly.edu

K. Abney
e-mail: kabney@calpoly.edu

F. Allhoff
Department of Philosophy, Western Michigan University, Kalamazoo, USA
e-mail: fritz.allhoff@wmich.edu

L. Floridi, M. Taddeo (eds.), *The Ethics of Information Warfare*,
Law, Governance and Technology Series 14, DOI 10.1007/978-3-319-04135-3_3,

often framed in the context of cyberwarfare, which naturally implies that military organizations should respond to these incidents (Arquilla 2012). This chapter will discuss why cyberwarfare is ethically difficult and why, until responsible cyberpolicy is developed, we may plausibly reframe the problem not as warfare but as private defense, i.e., self-defense by private parties, especially commercial companies, as distinct from a nation-state's right to self-defense.

The distinction between private defense and national defense is relevant, since victims of cyberattacks have been primarily industry targets and not so much government targets, at least with respect to measurable harm (Clarke 2010, esp. Chap. 3; Riley and Walcott 2011). And we focus on foreign-based cyberattacks since, unlike domestic-based attacks that are usually considered to be mere crimes and therefore a matter for domestic law enforcement, foreign-based attacks tend to raise special alarms and panic about more sinister motives. More than a mere criminal act, a foreign cyberattack is often perceived as an aggression so serious that it may plausibly count as an act of war, or *casus belli*, and so we are quick to invoke national security (Gorman and Barnes 2011). But insofar as the state is currently not protecting industry from such cyberattacks—in part because it is difficult to arrive at a sound cyberpolicy—we should consider interim solutions outside the military framework.

In this chapter, though we speak primarily from the US perspective as the one with which we are most familiar, the discussion can apply to cyberpolicies in other nation-states. Further, the issues we identify and discuss are not meant to be exhaustive but only a *prima facie* case for thinking about cyberattacks in a nonmilitary framework.

3.1 Cyberpolicy and Just-War Theory (Lin et al. 2012)

Why it is so difficult to develop responsible policy for cyberwarfare? If we understand war as "actual, intentional, and widespread armed conflict between political communities" (Orend 2005), it is first unclear that a cyberincident is an "attack" or even "armed" conflict. And even if they are acts of war, cyberattacks and counterattacks must adhere to international humanitarian law (IHL), otherwise known as the laws of war. These laws include the Geneva and Hague Conventions, as well as many other international agreements. Much of IHL is rooted in just-war theory, the philosophical tradition meant to establish the moral boundaries of warfare (Aquinas 1948; Walzer 2006; Reichberg et al. 2006). As a general discussion about the ethics of cyberwarfare, let us explain why cyberpolicy is so difficult to reconcile with just-war theory on at least the following five points:

3.1.1 Aggression

By the laws of war, there is historically only one "just cause" for war, a defense to aggression (Walzer 2006, esp. pt. 2). But it is not clear at *what kinds* of cyberincidents are so aggressive that they may be considered to be attacks (never mind

"armed" attacks), as opposed to espionage or vandalism. Traditional just-war theory doesn't consider mere (non-military) property damage as *casus belli;* to count as warlike aggression, the act needs to be more serious, such as an actual loss of lives or serious threat of economic harm, e.g., blockade of a trading route (Walzer 2006, Chap. 10). So, on the face of it, taking down a website does not seem to be *casus belli*, to the extent that it is only damage to property.

But in the Digital World, intellectual property is the coin of the realm. A cyberattack that erased financial data could wipe out entire bank accounts, leaving their owners penniless; this seems to be as severe as a naval blockade. And while the cyber domain (not counting physical substrate, e.g., routers and servers) is composed of only information bits, some of these bits control real-world property, e.g., power grids, nuclear centrifuges, and so on. Therefore, corrupting information data could lead to physical harms. It is a more complicated question, then, whether or not theft of intellectual property, or damage to virtual property, should fall under the threshold for war. Again, it may make a difference as to whether a military website is defaced, as opposed to a commercial website.

Complicating matters further, it is unclear *when* a cyberincident becomes an attack, even if we agree that it is an attack. Is it *casus belli* to install malicious software on an adversary's computer systems but not yet activate it? Or maybe the act of installing malicious software is an attack itself, much like installing a land mine? What about unsuccessful attempts to install malicious software? Do these scenarios count as war-triggering aggression—or are they mere crimes, which do not fall under the laws of war? These questions feature in debates over the legitimacy of preemptive and preventative war (Dipert 2006; Willson 2010).

Another question: Insofar as most cyberattacks do not directly target lives, are they as serious? The organized vandalism of cyberattacks could be serious if it prevents a society from meeting basic human needs like providing food or power, and so could indirectly cause death and injury. A lesser but still serious case was the denial-of-service cyberattacks on media websites in the country of Georgia in 2008, which prevented the government from communicating with its citizens (Markoff 2008). However, the traditional understanding of aggression in just-war theory says that human lives must be directly in jeopardy. This makes it difficult to justify going to war in response to a cyberattack.

3.1.2 Discrimination

The laws of war mandate that noncombatants be avoided in attacks, since they do not pose a military threat (McMahan 2009). Most theorists accept some version of a double effect in which some noncombatants could be unintentionally harmed as "collateral damage" in pursuing important military objectives (Aquinas 1948), though some have more stringent requirements (Walzer 2006). Some challenge whether noncombatant immunity is really a preeminent value (Allhoff 2012), but the issue undoubtedly has taken center stage in just-war theory and therefore the laws of war.

For the military, cyber-counterattacks (or, euphemistically, "active defense") must comply with the principle of discrimination or distinction. But it is unclear how discriminatory cyberwarfare can be: If victims use fixed Internet addresses for their key infrastructure systems, and these could be found by an adversary, then they could be targeted precisely—but victims are unlikely to be so cooperative. Therefore, effective cyberattacks need to search for targets and spread the attack; yet, as with viruses, this risks involving noncombatants.

For instance, consider the uncontrolled propagation of a computer worm such as Stuxnet (Schneier 2010; Sanger 2012). Stuxnet's designers had taken pains in designing it to target only Iranian nuclear processing facilities, yet it had spread far beyond intended targets. If the US is behind Stuxnet, then its own weapon has boomeranged back to US computer systems. Although its damage was highly constrained, Stuxnet's quick broad infection was noticed and required upgrades to antivirus software worldwide, incurring a cost to everyone. The worm also provided excellent ideas for new exploits that are already being used, another cost to everyone. Arguably, then, Stuxnet did incur some collateral damage.

Cyberattackers could presumably appeal to the doctrine of double effect, arguing that effects on noncombatants would be foreseen but unintended. This may not be plausible, given how precise computers can be when we want them to be. Alternatively, cyberattackers could argue that their attacks were not directly against noncombatants but against infrastructure. However, attacking a human body's immune system as the AIDS virus does can be worse than causing bodily harm directly. Details matter; for instance, if it knocks out electricity and the refrigeration that is necessary for the protection of the food supply, starvation could ensue from a modest cyberattack. Disrupting other crucial services, such as hospitals, could also result in deaths, as well as the foreseeable social unrest that routinely accompanies widespread power outages in urban areas.

A serious unintended effect to consider is that any cyberattack or counterattack may need to involve one's own civilian infrastructure (e.g., routers). This is problematic, because in providing material assistance for an attack, the civilian assets involved then can be marked by adversaries as a legitimate target of attack, either cyber or kinetic. For instance, if a counterstrike required the use of Google's servers or programming help from their engineers, then just-war theory holds that Google's facilities may be legitimately bombed and its personnel attacked.

3.1.3 Proportionality

Proportionality in just-war theory is the idea is that it would be wrong to use more force than necessary to achieve one's legitimate military objective, including as a punitive or deterrent response to an attack. For example, a cyberattack that causes little harm should not be answered by a conventional attack that kills hundreds (Walzer 2006; Coady 2004); that would seem to be a disproportionate response, in that less force could have achieved the same goals. This is not to say that a kinetic

attack cannot be a just response to a cyberattack, depending on the severity of either. As one US official described the nation's cyberstrategy, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks" (Gorman and Barnes 2011).

A challenge to proportionality is that certain cyberattacks, like viruses, might spiral out of control regardless of the attackers' intentions. While those consequences could be tolerated to prevent even worse consequences, lack of control means an attack might not be able to be called off after the victim surrenders, violating another key law of war. Such attacks thus raise issues of unintended proliferation and the possibility of widespread conflict, as attacks and counterattacks may spread beyond intended victims, undermining principles of both discrimination and proportionality. Another issue is that the target of a cyberattack may have difficulty in assessing how much damage they have received. A single malfunction in software can cause widely varied symptoms; thus a victim may think they have been damaged more than they really have, and counterattack disproportionately. Therefore, counterattack—a key deterrent to unprovoked attacks—is now fraught with ethical dilemmas.

3.1.4 Attribution

Discrimination in just-war theory also requires that combatants be identifiable to clarify legitimate targets—the principle of attribution of attackers and defenders. Terrorism ignores this requirement and therefore elicits moral condemnation. A problem with cyberwarfare is that it is very easy to mask the identities of combatants (Dipert 2010). Then counterattack risks hurting innocent victims. For example, the lack of attribution of Stuxnet raises ethical concerns because it removed the ability of Iran to counterattack, encouraging them towards ever more extreme behavior.

Attribution is an issue not only of moral responsibility but also of criminal and civil liability: we need to know whom to blame and, conversely, who can be absolved of blame. To make attribution work, we need international agreements. We first could agree that cyberattacks should carry a digital signature. Signatures are easy to compute, and their presence can itself be concealed with the techniques of steganography, so there are no particular technical obstacles to using them. Countries could also agree to use networking protocols, such as IPv6, that make attribution easier, and they could cooperate better on international network monitoring to trace sources of attacks. Economic incentives can make such agreements desirable.

3.1.5 Treacherous Deceit

Perfidy, or deception that abuses the necessary trust for the fair conduct of warfare, is prohibited by both Hague and Geneva Conventions. For instance, soldiers are not permitted to impersonate Red Cross workers and adversary soldiers. However,

some ruses, misinformation, false operations, camouflage, and ambush of combatants are permissible. Cyberattacks almost inevitably involve an element of deception to make operations of a computer or network appear to be normal when they are not, as with tricking a user to click on a malicious link.

So, to what extent might cyberattacks count as perfidy and therefore be illegal given international humanitarian law (Rowe 2009)? Consider, for instance, an email virus that purports to come from the International Committee of the Red Cross: this would seem to be a reasonable analogue to the prohibited act of posing as a humanitarian worker. Similarly, an email virus that purports to come from one's own military organization would breach the same shared trust as impersonating an enemy soldier does.

The moral impermissibility of perfidy is tied to the concept of treachery, and a prototypical example of a treacherous (and illegal) act in war is to kill with poison. Yet there are poisons that can kill quickly and painlessly, much more humanly than a bullet to the head. And spraying poisons in open battle is prohibited chemical or biological warfare. This apparent paradox suggests that the concept of treachery (and therefore perfidy) is fuzzy and hard to apply. We don't get as angry when software betrays us as when people betray us. But maybe we should—software would be better if users were less complacent.

3.1.6 What Now?

The above issues do not exhaust the moral and philosophical controversies surrounding cyberwarfare. For instance, just-war theory also requires that wars are publicly declared by the proper authority. Yet the ambiguity of the attacker's identity is a major part of cyberwarfare's allure, as is therefore waging a secret war. These issues suggest that either we need to quickly figure out how cyberwarfare fits into the extant framework of IHL and just-war theory (Cook 2010), or if emerging capabilities to cyberattack require rewriting the rules of war (Dipert 2010). Some scholars have cast doubt that cyberwarfare is much different from previous forms of warfare or that it requires a "new ethics" (Crisp 2012; Rid 2012). Whether or not they are right, it should be clear that cyberwarfare is burdened with legal and moral hazards, some of which we described above. These hazards are perhaps solvable, but they are not solved now. And this makes "active defense" or counter-cyberattacks, at least by the nation-state, morally problematic.

3.2 Stand Your (Cyber)Ground: An Interim Solution?

If we could conduct cyberdefense outside the military frame, then we can avoid at least the legal issues above, if not also the moral ones. But do we have a good reason—other than to sidestep these issues—to use a different frame? In this section, we will suggest that we do (Lin 2012).

First, it is still an open question of whether or not military organizations should take the lead in national cyberdefense, even against foreign-based attacks. Currently in the US, a major controversy with cybersecurity legislation is whether the US Department of Homeland Security (DHS) or the US Department of Defense (DoD) should bear responsibility for defending the nation's digital borders (Jensen 2011; Jackson 2012). Reasonable arguments can be made to support and criticize either one as the lead agency for cybersecurity, but these arguments are not relevant to our discussion here. Rather, the point is simply that we are using a law-enforcement—as distinct from military—frame if we believe that DHS should take the lead, which is not unreasonable.

However, we are not proposing a law-enforcement frame here. Instead, we want to offer a third option that government need not be involved—a solution that would avoid the DHS versus DoD debate, as well as the aforementioned difficult issues related to IHL and just-war theory. This option models the "Stand Your Ground" laws in the US that are rooted in the basic human right to self-defense, and it authorizes counter-cyberattacks by private companies, which have been the main victims of harmful cyberactivities by foreign actors to date. (We will present details of this option shortly).

One reason why government need not be involved is that government is, in fact, currently not involved much at all (Riley and Walcott 2011). That is, the US government has hardly protested, much less prosecuted, the perpetrators of major cyberattacks, again with industry companies as the principal victim of such attacks. Thus, it is workable to avoid governmental intervention to the extent that the status quo of nonintervention is workable or is expected to continue anyway. To be sure, part of the reason for this inaction is the difficulty of identifying the attacker with reasonable certainty for a serious state response, such as trade sanctions or a military strike against a foreign aggressor. Nevertheless, there is little, if any, state protection for industry targets in the cyber domain.

So despite existing laws against cybercrimes and related activities, there is little enforcement of these laws, and therefore the cyber domain appears to be lawless. In that regard, a natural analogy to which we might look for consistent policy is the "Wild West" of American history. Both the Wild West and cyberspace now are marked by general lawlessness; bad guys often operate with impunity against private individuals and companies, as well as what government exists in those realms, such as the lone sheriff. The distinctively American solution to the Wild West was found in the second amendment to the US Constitution: the right to bear arms. As more private citizens and organizations carried firearms and could defend themselves, the more outlaws were deterred, and society as well as the rule of law could then stabilize and flourish.

We also find this thinking in current "Stand Your Ground" laws in the US that authorize the use of force by individual citizens. If such laws make sense, could this model work for cyberspace?

3.2.1 *Why it is Reasonable*

Not to endorse this solution (or "Stand Your Ground" laws) but merely to offer it for consideration as a new option: what if we authorized *commercial companies* to fight cyberfire with cyberfire? Some have already started to explore the legality of active defense (White Wolf Security 2007; Owens et al. 2009; Willson 2012), i.e., offensive operations, but let us further consider its ethical foundation here. As in the Wild West, civilians are the main victims of pernicious cyberactivities. Some estimate that industrial cyberespionage costs US companies billions of dollars a year in lost intellectual property and other harms (Goldman 2011); UK companies also report annual losses in the billions (Blitz 2012). As in the Wild West, they now look to government for protection, but government is struggling badly in this role, for the above-mentioned reasons and others. If we consider the US (or any other nation) as one member of the world community, there is no clear authority governing international relationships, and this make our situation look like a "state of nature" where no obvious legal norms exist, at least with respect to cyber.

This option isn't completely outlandish, because precedents or similar models exist for the physical, nondigital world today. In the open sea, commercial ships are permitted to shoot and kill would-be pirates (United Nations 1982). Security guards for banks are allowed to shoot fleeing robbers (e.g., New York Penal Law 2012). Again, "Stand Your Ground" laws—which give some authority and immunity to citizens who are being threatened or attacked—also operate on the same basic principle of self-defense, especially where few other options exist.

A key virtue of "Stand Your *Cyber*ground" is that it avoids the unsolved and paralyzing question of what a state's response can be, legally and ethically, against foreign-based attacks; the state is no longer involved. If the state were to make a wrong move, it could become a war crime or provide an adversary with just cause to respond with force. Again, the point of reframing cybersecurity as a nonmilitary issue isn't so much to avoid stringent but sensible requirements in IHL and just-war theory, though that might be a benefit if there are independent reasons to support a different frame.

As useful a model as it is for thinking through at least some issues in cyberwarfare, just-war theory is also limited, for at least the following reasons. First, just-war theory is most powerful when applied to state actors, particularly ones engaged in traditional warfare. This is not to say that just-war theory tells us nothing about other forms of conflict; for example, it clearly inveighs against some form of asymmetric warfare, e.g., terrorism. Rather, this gives rise to a second consideration, already discussed above: much of cyberconflict takes place among private citizens or, in many cases, between private citizens and corporations. Just-war theory would typically not be applied to this sort of dynamic, but rather we would turn to the strictures of criminal law; and, as we will see in the following, there is some promise in this regard.

3.2.2 *Controversy in "Stand Your Ground" Laws*

Of course, "Stand Your Ground" laws are not without significant controversies. In recent history, this is represented by the following criminal case in the US: On February 26, 2012, outrage broke out when George Zimmerman, a neighborhood watch coordinator, shot and killed Trayvon Martin, an unarmed 17-year old. The shooting took place in a Sanford, Florida gated community. The media fallout primarily seized upon Martin's race—he was African-American—and the failure of the police to arrest Zimmerman for several weeks. However, a secondary emphasis was on a Florida law that weighed in Zimmerman's favor, namely Florida's "Stand Your Ground" statutes (Florida Statutes 2011). Florida, though, is hardly alone in having "Stand Your Ground" provisions; many states have them, and others are currently considering them.

In understanding "Stand Your Ground", it is perhaps easiest to start with its contrary: a duty to retreat. Under the common law, self-defense is widely recognized, which is to say that one person can justifiably use (at least some) force against another if the former is in reasonable apprehension of imminent bodily injury. Unpacking this claim takes us too far afield, but let us at least briefly consider some basic features. First, the person invoking self-defense need not be in *actual* apprehension of imminent bodily injury; so long as the apprehension is *reasonable*, it is sufficient to mitigate liability, either criminal or civil. Second, the apprehension needs to be imminent, which is to say that self-defense cannot be used against threats or provocations. Third, the force used cannot be excessive; rather, it can only be what would be reasonable to prevent injury.

Intuitively, self-defense protections strike most of us as eminently plausible: we hardly expect people to suffer preventable injuries at the hands of others. The key to understanding "Stand Your Ground", though, is in recognizing that it provides even greater protections to those who wield protective force than does the traditional doctrine of self-defense. Specifically, this distinction trades on the duty to retreat. Under self-defense, if the person being attacked could have escaped without injuring his assailant, he is usually expected to do so; if he does not, he may be found liable for the injuries that he causes. "Stand Your Ground", however, is more forgiving insofar it does not require the attacker to exercise the option of retreat before using force.

Surely we can understand why reasonable retreat would be required, so why does "Stand Your Ground" jettison it? Progenitors to contemporary statutes ran under the "Castle doctrine", which provides extra protections for a person's residence and has been widely adopted. Under this doctrine, whether a person has a duty to retreat depends on where he is, and the duty is absent when he is in his own house. In fact, the "Stand Your Ground" locution originated in a case deriving from just this sort of situation: "[the homeowner] may stand his ground, and, if need be, kill his adversary" (Beard v. US 1895). In the contemporary legislative landscape, "Stand Your Ground" extends beyond just domestic contexts. The basic rationale for this

expansion is one that Oliver Wendell Holmes expressed a long ago, "detached reflection cannot be demanded in the presence of an uplifted knife" (Brown v. US 1921); in other words, the duty to retreat is simply unfair to the person who is attacked.

3.2.3 *How it Could Work*

Our exploration—but not necessarily an endorsement—of a "Stand Your *Cyber*-ground" policy starts from a similar assumption of a basic right to self-defense, as found in extant "Stand Your Ground" and other laws. And as imperfect as any analogy inevitably is, but nonetheless useful (Hollis 2008), there are important similarities here. In both cases, the victim does not have access to government protection, for all practical purposes: in the home-invasion case where seconds matter, that the police may be minutes away is little consolation or protection; and in the corporate cyberattack case where there is no prosecution, that we have laws against cyberattacks are also of little help. In both cases, there's nowhere to reasonably retreat, even if there were such a duty to retreat. Even considering some of the other analogies proposed for cyberspace—e.g., outer space and Antarctica—it's reasonable to assume that something like "Stand Your Ground" would also apply in those lawless frontiers, if an attack were to occur against a private party there. This also suggests a correlative policy that at least some cyberattacks, perhaps even between nation-states, should be treated as "frontier incidents" rather than the more serious "acts of war", to the extent that cyberspace is still a frontier (Watts 2011; Schmitt 2010).

Where "frontier justice" may evoke images of brutal eye-for-an-eye retaliation, or *lex talionis*, this need not be the case for cyberpolicy. A counter-cyberstrike by a defending company does not have to be as dramatic as the initial attack or anything else we usually associate with an "attack." For instance, the response could be to forcibly install software patches and anti-malware applications on an attacking "botnet" or network of zombie computer systems, usually hijacked without their owners' knowledge; or it could be to encrypt an attacking computer's data and operating system until some remedy is achieved; or, as Microsoft had done in 2012, the response could be to render a botnet inoperable (Infosec Island 2012). Other remedies include creating a "honeypot" or diversionary target (Rowe et al. 2007), e.g., a fake directory of trade secrets, in order to misdirect the cyberattacker, plant false information for attackers to "discover", keep attackers occupied to buy time for defense and evidence-collection, and other ends. Compare these to decoys, mock operations, camouflage, and other tactics that militaries and intelligence agencies are permitted to conduct to mislead adversaries.

If we like, "Stand Your Cyberground" could require a judicial warrant prior to a cyber-counterstrike, that is, *ex ante* justification or authorization before the event. However, this may be unnecessary, since there could be also *ex post* justification, that is, authorization in virtue of an initial attack. Again, in open-seas piracy and other scenarios today, a victim does not need to request approval prior to defending itself with a counterattack. As further safeguards, the state (or industry, to avoid

the state's involvement) may require that counter-cyberattacks be reported, either before or after the fact, to ensure there is reasonable cause in those actions, or else face some penalty for negligence or other deficiencies.

As with the counterattacking of pirates, a cyber-counterattack has many potential benefits, including neutralizing the threat, deterring future threats, and providing some measure of justice, in contrast to doing nothing. Further, where initial cyber-attacks are often anonymous or conducted through an unwitting proxy, a counter-strike on an "innocent" third-party's system—say, computers owned by China but hijacked and used for an attack by unknown hackers—could elicit pressure from the third-party (in this case, China, a nation of significant influence) to identify the real aggressor. (We will say more about the innocence of these third-parties below.) Short of a sound or responsible national cyberpolicy that accounts for IHL and just-war theory, a counterstrike outside the military frame helps to avoid a larger cyberwar as well as kinetic war. If this is still unsatisfying or unsustainable, then "Stand Your Cyberground" may help motivate lawmakers to more quickly develop a sensible national cyberpolicy.

3.3 Possible Objections and Replies

Here we briefly consider several objections to the "Stand Your Cyberground" policy, as it is undoubtedly controversial. In the process, we clarify how such a proposal might work, in case it is ultimately defensible. Again, this is not an exhaustive list of objections but only some immediate worries, which may be overcome to make a *prima facie* case for "Stand Your Cyberground."

3.3.1 Only the State has a Monopoly on Violence

Objection: Only the state can engage in war or otherwise violent actions; companies legally cannot, as governments have a legitimate monopoly on warfare and violence.

Reply: There are certainly areas in which government intervention is required to regulate or even supplant private interactions; political parties routinely argue over the appropriate extent of such government usurpation of individual sovereignty. But almost everyone agrees that government should have the sole legitimate use of violent force against other people. The most basic argument for this requirement is that vigilante justice runs into a regression problem, when friends or loved ones of private individuals retaliate for their loved one's murder, and then the loved ones of the original transgressor return the favor, and on and on as some legendary family and ethnic feuds have continued.

If governments must have a monopoly on the legitimate use of violence, must they also have the sole legitimate use of cyberattacks? No, not necessarily. To say

that a state has a monopoly on violence seems to imply it is capable of inflicting violence or otherwise enforcing laws so that individuals need not resort to violence themselves. With industry cyberattacks, if the state does have this power, it has not been exercising it, as justice may demand. Again, part of the problem is that it's difficult to identify the aggressor, as ethics generally would seem to require; so this is not so much the state's fault as it is the nature of cyberattacks. Nevertheless, the state is not living up to its implicit promise to protect its citizens, which was the basis for claiming a monopoly on violence. Further, it is not true that governments claim a monopoly on violence, to the extent that they allow commercial ships to defend themselves against pirates, or bank security guards to shoot fleeing robbers, or private citizens to counterattack given "Stand Your Ground" laws.

If the objection, however, is that only the state has the power to wage war, then this begs the question at hand: we have suggested that a cyberconflict does not need to be viewed through the lens of war. Suppose a cross-border kinetic attack occurs on a bank (or your house): the bank (or you) would seem to have a reasonable claim to defend itself from such attacks, including with deterrent force, especially if government is unresponsive. This is not a war-powers problem but one of basic self-defense.

3.3.2 Only the State has the Resources to Counterattack

Objection: Related to the above, many companies are typically not big enough to mount an effective counterattack. As a matter of simple utility and following the principle of division of labor, even if companies could handle cyber-counterattacks, government still should handle all cyberattacks, given its considerable resources and economies of scale.

Reply: Companies need not act alone; they could form consortiums or cooperatives to gather resources and expertise for cyber-counterattacks, if the individual company lacks resources. Or they could simply outsource the job to a third-party with cyberdefense as its core competency or product, as a bank might hire private security services. Such voluntary solutions appear to be better than involving governments, insofar as state-sponsored attacks increase the risk of formal war. Further, decentralizing this function distributes our own targets for attacks, e.g., rather than having a central government agency as a single target, an adversary could have to contend with many private organizations, if it wants to knock out cyberattack capabilities. Decentralizing this function also allows for greater diversity of solutions, with nationally and internationally recognized "best practices" emerging over time. A robust corporate culture for problem-solving can be generally preferable to government intervention, especially when that intervention could mean kinetic (and not merely cyber) war.

3.3.3 *There's Still the Problem of Attribution*

Objection: There is a great risk of misattribution in cyber-counterattacks, potentially with innocent third parties being harmed. Even if IHL is not violated by industry-sponsored counter cyberattacks, it is still immoral to attack a party without first identifying it and ensuring that it is the actual aggressor. For instance, botnets are a common form of attack, but they're victims too, not the real aggressor.

Reply: Attribution may be a red herring here. For example, the US knows China has repeatedly cyberattacked it, but the US doesn't want to do anything about it, because there are bigger political and economic issues it wants to negotiate. Even if the US doesn't "know" this, it seems to have good reason to think so (Riley and Walcott 2011). Further, there is a widespread consensus that clear attribution is not required when sailors defend against pirates, or homeowners against robbers, and so on. It is enough to know that one is being attacked and is defending oneself against the attack, even if the attacker is not the actual aggressor, e.g., if the pirate or bank-robber was really a coerced father whose family was taken hostage and threatened to be killed by true bandits.

As for innocent third parties and botnets (innocent computers hijacked by others to commit cybercrimes): again, even if we know that a pirate was really an innocent fisherman whose family was being held hostage, the fact remains that the pirate poses a threat to the safety of the targeted ship and its crew and passengers. It is therefore still not unreasonable to neutralize the threat by counterattacking the pirate, even if we know there is a puppet-master elsewhere who is responsible for the pirate's actions. Similarly, it would seem reasonable to counter-cyberattack a third party who we believe was coerced or otherwise not complicit in their initial attack.

Where we may choose to use less-than-lethal means against a fisherman we know to be an unwilling pirate, we may likewise choose less dramatic means in a counter-cyberattack. Again, such a counterattack need not be crippling or highly damaging, e.g., if it merely forces an anti-malware installation. If the cyberdefense routinely inoculates and removes malware from consumer machines, such an "attack" could actually be a great benefit to the wired world, as well as a more effective general solution to cyberattacks. This is to suggest that we may understand botnets with the public-health model of bioethics: In cases of infectious diseases, such as typhoid, patient autonomy is secondary to stopping the disease that threatens many others (Leavitt 1997). Likewise, botnets are a public-health hazard too in a sense; and even if the owners of botnet computers are not complicit in the attack and want to refuse an inoculation, the overriding greater good of public health can reasonably trump that innocent autonomy.

Botnets, however, are less innocent than the unwilling pirate above in an important sense. One can argue that the hijacked computers comprising a botnet still bear some responsibility for cyberattacks (Owens et al. 2009, p. 210). For instance, responsible owners of those computers could be said to have some positive obligation to install antivirus software and otherwise exercise due diligence in ensuring responsible use of their machines; failing to do so puts the computers at risk of

becoming hijacked and used for pernicious ends. In the bioethics model, this is analogous to something like careless or oblivious patients who don't take reasonable precautions as they enter a zone of infection; this lack of reasonable diligence weighs against their right to autonomy.

3.3.4 Counterattacks will Escalate Conflict

Objection: Cyber-counterattacks will only encourage the escalation of conflict. Violence begets more violence, so we should forgo a counterstrike option in favor of some other response.

Reply: Perhaps, though this is a general objection to any response to aggression, whether a kinetic war, cyberconflict, or a schoolyard fight. Any response—even a nonresponse—may encourage the aggressor on. This seems true for cyberconflicts, even with a national cyberpolicy in place. Note that diplomacy and negotiations may be impossible in cyberconflicts, if the victim does not know the identity of the attacker, i.e., with whom one ought to negotiate.

Insofar as deterrents work, what seems to be clear is that a nonresponse is not a deterrent. A "Stand Your Cyberground" solution could be an immediate deterrent and pressure "innocent" third-parties to help find the real aggressor for compensation and/or punishment. Further, understanding how cyberattacks occur may help us to take our computing practices more seriously and generally replace the naivete common today with a more sophisticated relationship that ultimately could engender greater, not lesser, trust. It seems possible that the current asymmetry of possible harm between elite hackers and average citizens could gradually be replaced with a grudging trust built on the possibility of mutually assured harm from cyberattacks, and hence act as a long-run general deterrent to cyberattacks; when hacking involves a considerable risk of counterattack to the hacker, it's entirely possible less hacking will result.

Hence, though the worry about escalation is reasonable (no matter what policy is adopted), ultimately it becomes an empirical question. Looking at the American debate on whether we should allow more people to carry guns, one criticism is that it'd escalate violence, especially accidental and wrongful shootings; however, others predict that more guns will force us to be more civil and therefore reduce violence, since we wouldn't want to risk offending an armed person (Debatepedia 2011). This was supposedly the case in the Wild West, which we suggested was an analogy to our current situation in the cyber domain. Where "Stand Your Cyberground" differs from the debate on guns is that there'd be little danger of an industry company launching a cyberattack by accident or without cause, like a careless, emotional, or angry gun-owner might shoot someone. Designing and implementing a complicated cyberattack is not typically an impulsive gesture. But that capacity would still remain a deterrent to others: to not cyberattack a company that could plausibly respond in kind.

The failure to defend oneself also risks escalation. After all, failing to respond to a cyberattack is an incentive for hackers to continue, if not escalate, their activities. This reasoning lies behind zero-tolerance policies for minor urban crimes and helps explain why bad, crime-ridden neighborhoods tend to get worse: because the perpetrators have no incentive to discontinue their assaults, given the absence of reliable law enforcement or self-defense. It is unclear how doing nothing will de-escalate a cyberconflict: a hacker is not like the angry drunk who will eventually run out of steam and pass out or sober up. If cyberattacks are still profitable, then they will continue or increase.

3.3.5 Malicious and Ideological Hackers will not be Deterred

Objection: Even if financially motivated hackers can be deterred or expected to not exact revenge, this may not be the case with malicious or ideological hackers, such as Anonymous. Rather, a cyber-counterattack may instead play into a hacker's agenda of anarchy.

Reply: Perhaps, but this may create political will to fight cybercrimes, if the cyber domain devolves into a Wild West—a drastic but necessary catalyst for action. And as major organizations worldwide, such as Amazon.com and various credit card companies, discovered after being attacked by Anonymous, the alternative of doing nothing seems worse. Would hackers retaliate if a company were to pull out its cybergun? Maybe if they were motivated by revenge, but again, like the average mugger, the motive in the end is usually primarily financial, even if some hackers and hooligans do it for fun. Anonymous hacked in support of WikiLeaks precisely when Amazon et al. were denying donations to WikiLeaks. Even ideological hackers need funds. And so eventually even the members of groups like Anonymous can be harmed by cyber-counterattacks, especially counterattacks that impose financial or technological hardships on the original hacker.

"Stand Your Cyberground" has the virtue of advertising to would-be attackers, whatever their motivation, that industry is not an easy target, and this has deterrent value. Perhaps some hackers will take that as a challenge, but they're not so much the rational adversary (who are motivated by profit) that this policy is meant to address. Just as some hackers and muggers may strike back harder if the victim resists or fights back, this minority group shouldn't drive policy that's otherwise reasonable and potentially more helpful than not. Of course, a rational hacker could preemptively declare a policy of striking harder if a company resists, as a way to deter deterrence, but again this would seem to be an even smaller segment of that community, and we shouldn't let these outlier (and theoretical) cases drive policy for the larger world.

3.3.6 *Even if IHL is not Violated, other International Laws may be*

Objection: Given that many companies are multinational, their counter-cyberattacks may violate other aspects of international law, even if not in violation of IHL. Conceivably, it could open the company up to international prosecution.

Reply: There's irony in prosecuting a defending company that counterstrikes but not the initial aggressor, so it's unclear what the political appetite would be for such prosecutions. If cyberattacks come to be routinely prosecuted internationally, then there would be a major step towards leaving behind the "Wild West" of current cyberconflict and moving toward international regulations, greatly obviating the need for a "Stand Your Cyberground" policy. But that would require the prosecution be carried out in such a way that companies no longer need to actively defend themselves from cyberattack, and such a vista remains distant at best. It remains hard to envisage a thoroughgoing and extensive enough international consensus on cyberlaw that could render private companies and individuals in as little need of cyberdefense as average citizens do against shootings. When assaults are common and hard to police, one must expect people to begin to actively defend themselves.

Further, it is hard to prosecute a company without clear attribution—and in principle, companies could respond in their cyber-counterattacks as anonymously as its attackers do (perhaps, if feasible, even using the same botnets), as that strategy seems to be effective for attackers. If computer forensics advances to the point in which there is a robust system for identifying and reliably attributing cyberattacks (and settled international cyberlaw for discriminating illegitimate attacks from other cyberactivities), then our proposal will be no longer needed, and attackers can be identified and prosecuted, i.e., cyberlaw can actually be enforced.

3.3.7 *A Judicial Process Implies State-Sponsorship of "Stand Your Cyberground"*

Objection: Requiring a judicial warrant or reporting of cyber-counterstrikes amounts to state-sponsorship for the "Stand Your Cyberground" policy (Owens et al. 2009, p. 211). As with states that turn a blind eye toward terrorists within their own borders, states can reasonably be blamed for any cyber-counterstrikes. This means the policy does not reduce the risk of war after all.

Reply: First, it may be the case that cyber-counterattacks could proceed without any judicial oversight at all; that would be the most *laissez faire* version and would presumably obviate any risk of war from the "Stand Your Cyberground" policy. After all, other kinds of ritualized exchanges of harm, often even those involving kinetic violence, do not threaten to lead to war, e.g., gang violence across international borders. Cross-border cyberattacks and counterattacks would be more problematic, but as we suggested above, it makes no sense to prosecute a cyber-counterattack when the initial attacker goes unpunished. It remains plausible that

transnational disputes will result from such counterattacks, but there is no reason to think they are more likely to lead to war than other types of international crime, particularly cybercrime, that already exist. Indeed, if the "Stand Your Cyberground" policy does become a credible deterrent and reduce international hacking, it may well defuse international tensions, not raise them.

If the government does become involved in cyber-counterattacks to the limited extent of requiring *post hoc* notification or *ex ante* warrants, things become more complicated. But the end result remains the same: there are multiple venues to appeal the legal findings of one country to a higher court, beginning with low-level government to government negotiations and culminating with appeals to the United Nations and the International Criminal Court. None of those involves war, and it is hard to imagine a cyber-*counter*attack—which assumes a cyberattack causing harm already took place—in which the counterattack by itself precipitated war. Cyber-counterattacks are unlike terrorism in that they are a specific response to a specific injury, in kind, and without larger political goals beyond self-defense. If nation-states begin a "first strike" cyberattack policy, that may well constitute war or an incitement to war, but that goes well beyond what "Stand Your Cyberground" is envisioned to achieve.

3.3.8 *Industry Counterattacks may Destroy Evidence Needed for Prosecution*

Objection: If we allow victims to unilaterally counter-cyberstrike, that will likely contaminate or destroy evidence needed to prosecute the initial (and presumably illegal) cyberattack (Owens et al. 2009, p. 206; Infosec Island 2012).

Reply: First of all, what prosecution? Even if prosecution of the aggressor were forthcoming, this is a problem for any act of self-defense. For instance, by allowing commercial ships to repel pirates, we risk destroying evidence on the alleged pirate's unlawful activities; by allowing individuals to counterattack assailants, we risk destroying evidence that would convict the alleged aggressors. But as real as this risk is, prosecution is secondary to self-defense and limiting the harm of the initial attack. Allowing a cyberattack to continue for the sake of a possible prosecution makes as much sense as letting a suspicious fire to keep burning so to not disturb evidence that may convict an arsonist. Further, in regulating "Stand Your Cyberground", the state or industry could require capturing and filing relevant data related to the initial attack, perhaps deploying independent emergency-response teams to document the initial attack.

3.3.9 *Cyberwarfare Doesn't Raise New Issues*

Objection: Do cyberattacks really raise new moral issues? They seem to be merely old ethical issues in a new technological dress (Crisp 2012).

Reply: Given "ought implies can", as new technologies emerge with new capabilities, novel ethical questions ineluctably arise. Moral dilemmas over killing and letting die and even organ transplantation arose once medical technology forced us to redefine death: the case of Terri Schiavo would not have been an issue two centuries ago (Caplan 2005). Whenever such technological developments change the concepts currently in use, they likewise inevitably challenge our received ethics. Just-war theory is challenged by the rise of semi-autonomous robots: do drone strikes mean that the US is at war with Yemen, or not? Similarly, the distinctive nature of cyberattacks, whose very nature upends the traditional notion of kinetic force as required for attack, places extreme tension on just-war theory, law enforcement, or any other traditional frame for assessing their ethics. Hence, we believe new ethical—and philosophical (Taddeo 2012)—issues are raised by cyberattacks, and so until and unless policymakers come to grips with regulating this novel form of aggression, it falls on private individuals to work out a *modus operandi* for this new reality.

3.4 Conclusion

How we justify and prosecute a war matters. For instance, the last US presidency proposed a doctrine of preventive or preemptive war, or the "Bush doctrine": if a nation knows it will be attacked, why wait for the damage to be done before it retaliates (Tierney 2011)? But this policy breaks from the just-war tradition, which again historically gives moral permission for a nation to enter war only in self-defense. With the Bush doctrine, the US seeks to expand the triggers for war, but this could backfire spectacularly. For instance, Iran reports contemplating a preemptive attack on the U.S. and Israel, because it believes that one or both will attack Iran first (BBC 2012). Because intentions between nations are easy to misread, especially between radically different cultures and during political elections, it could very well be that the US and Israel are merely posturing as a gambit to pressure Iran to open its nuclear program to international inspection. However, if Iran were to attack first—with either kinetic or cyber means—it would seem hypocritical for the US to complain, since the US already endorsed the same policy of first strike (Wright 2012).

A key problem with a first-strike policy is that there are few scenarios in which we can confidently and accurately say that an attack is imminent. Many threats or bluffs that were never intended to escalate into armed conflict can be mistaken as "imminent" attacks. This epistemic gap in the Bush doctrine introduces a potentially catastrophic risk: that nation delivering a preemptive or preventative first strike may turn out to be the unjustified aggressor and not the would-be victim, if the adversary really was not going to attack first. Further, by not saving war as a last resort—after all negotiations have failed and after an actual attack, a clear act of war—the Bush doctrine opens the possibility that the US (and any other nation that adopts such a policy) may become ensnared in avoidable wars. At the least, this would cause harm that otherwise might not have occurred to the warring parties, and it may set up an overly stretched military for failure, if battles are not chosen more wisely.

Here's the relevance to cyberwarfare: Our world is increasingly wired, with new online channels for communication and services interwoven into our lives virtually every day. This also means new channels for warfare. Indeed, a target in cyberspace is more appealing than conventional physical targets, since the aggressor would not need to incur the expense and risk of transporting equipment and deploying troops across borders into enemy territory, not to mention the political risk of casualties. Cyberweapons could be used to attack anonymously at a distance while still causing much mayhem, on targets ranging from banks to media to military organizations. Thus, cyberweapons would seem to be an excellent choice for an unprovoked surprise strike.

Today, many nations have the capability to strike in cyberspace—but should they? The laws of war, or IHL, were not written with cyberspace in mind. So we face a large policy gap, which organizations and experts internationally have tried to address in recent years (e.g., Owens et al. 2009; Lieberthal and Singer 2012; Libicki 2009; H. Lin 2012). But there is also a gap in developing the ethics behind policies, as we described in the first section above. As an interim solution, we suggest a reframing of the cybersecurity discussion away from the military frame, i.e., away from the nation-state level, and more toward the private-defense frame, i.e., closer to the individual-actor level.

This reframing seems defensible, given related legal precedents. And, separately, it offers many benefits, including some measure of justice to victims, deterrence for aggressors, and so on. While we offer this "Stand Your Cyberground" policy as a prelude to a more complete discussion of its feasibility, we should also note that it is already being adopted by companies right now: "Frustrated by their inability to stop sophisticated hacking attacks or use the law to punish their assailants, an increasing number of US companies are taking retaliatory action" (Menn 2012; Infosec Island 2012). So regardless of whether the policy is prudent or ethical, it is apparently already a *de facto* policy for some, and this makes an examination of its details—including how it could responsibly proceed—all the more urgent.

References

Allhoff, F. 2012. *Terrorism, ticking time-bombs, and torture*. Chicago: University of Chicago Press.

Arquilla, J. 2012. Cyberwar is already upon us. Foreign policy (March/April). http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us?page=full. Accessed 22 October 2013.

Aquinas, T. 1948. *Summa Theologica* (Trans. Fathers of the English Dominican Province). New York: Benziger Books.

BBC. 2012. Iran Says Preemptive Strike on 'Enemies' Possible. BBC News, February 21. http://www.bbc.co.uk/news/world-middle-east-17116588. Accessed 22 October 2013.

Beard v. United States. 1895. 158 U.S. 550, 563 (1895). http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=158&invol=550. Accessed 22 October 2013.

Blitz, J. 2012. MI5 chief sets out price of cyber attack. Financial times. http://www.ft.com/cms/s/0/a970810c-bef2-11e1-8ccd-00144feabdc0.html#axzz1zDB9cncm. Accessed 22 October 2013.

Brown v. United States. 1921. 256 U.S. 335, 343. (1921). http://supreme.justia.com/cases/federal/us/256/335/case.html. Accessed 22 October 2013.

Caplan, A. 2005. The time has come to let terri schiavo die. MSNBC.com, March 18. http://www.msnbc.msn.com/id/7231440/ns/health-health_care/t/time-has-come-let-terri-schiavo-die/#.T-4VArWe4aw. Accessed 22 October 2013.

Clarke, R. 2010. *Cyber war: The next threat to national security and what to do about it.* New York: Ecco.

Coady, C. A. J. 2004. Terrorism, morality, and supreme emergency. *Ethics* 114: 772–789.

Cook, J. 2010. 'Cyberation' and just war doctrine: A response to randall dipert. *Journal of Military Ethics* 9 (4): 411–423.

Crisp, R. 2012. Cyberwarfare: No new ethics needed. Practical ethics: Ethics in the news. http://blog.practicalethics.ox.ac.uk/2012/06/cyberwarfare-no-new-ethics-needed/. Accessed 22 October 2013.

Debatepedia. 2011. Debate: Gun control debatepedia index. http://dbp.idebate.org/en/index.php/Debate:_Gun_control. Accessed 22 October 2013.

Dipert, R. 2006. Preventive war and the epistemological dimension of the morality of war. *Journal of Military Ethics* 5 (1): 32–54.

Dipert, R. 2010. The ethics of cyberwarfare. *Journal of Military Ethics* 9 (4): 384–410.

Florida Statutes. 2011. Chapter 776: Justifiable use of force. The Florida Senate. http://www.flsenate.gov/Laws/Statutes/2010/Chapter776/All. Accessed 22 October 2013.

Goldman, D. 2011. The cost of cybercrime. CNNMoney, July 22. http://money.cnn.com/galleries/2011/technology/1107/gallery.cyber_security_costs/index.html. Accessed 22 October 2013.

Gorman, S. and J. E. Barnes. 2011. Cyber combat: Act of war. *The Wall Street Journal: Technology*, May 30. http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html?mod=googlenews_wsj. Accessed 22 October 2013.

Hollis, D. 2008. New tools, new rules: International law and information operations. In *The message of war: Information, influence and perception in armed conflict*, eds. G. David and T. McKeldin. Temple University Legal studies research paper no. 2007–15. http://ssrn.com/abstract=1009224. Accessed 22 October 2013.

Infosec Island. 2012. Microsoft dismisses zeus botnet takedown criticism. Infosecisland. http://www.infosecisland.com/blogview/21036-Microsoft-Dismisses-Zeus-Botnet-Takedown-Criticism.html. Accessed 22 October 2013.

Jackson, W. 2012. DOD vs. DHS: Who should mind the US' Cyber Defense? *Defense Systems*, March 27. http://defensesystems.com/articles/2012/03/27/cyber-defense-hearing-mccain-slams-dhs-favors-dod.aspx. Accessed 22 October 2013.

Jensen, E. 2011. President Obama and the changing cyber paradigm. William Mitchell law review, vol. 37, no. 5049. http://ssrn.com/abstract=1740904. Accessed 22 October 2013.

Leavitt, J. W. 1997. *Typhoid mary: Captive to the public's health*. Boston: Beacon Press.

Lieberthal, K., and P. W. Singer. 2012. Cybersecurity and US-China Relations. The brookings institution, 21st century defense initiative. http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english. Accessed 22 October 2013.

Libicki, M. 2009. Cyberdeterrence and cyberwar. The RAND corporation. http://www.rand.org/pubs/monographs/MG877.html. Accessed 22 October 2013.

Lin, H. 2012. Arms control in cyberspace: Challenges and opportunities. *World Politics Review*, March 2012.

Lin, P. 2012. 'Stand your cyberground' law: A novel proposal for digital security. *The Atlantic*, April 30. http://www.theatlantic.com/technology/archive/2012/04/stand-your-cyberground-law-a-novel-proposal-for-digital-security/256532/. Accessed 22 October 2013.

Lin, P., F. Allhoff, and N. C. Rowe. 2012. War 2.0: Cyberweapons and ethics. *Communications of the ACM* 55 (3): 24–26.

Markoff, J. 2008. Before the Gunfire, Cyberattacks. *The New York Times: Technology*, August 12. http://www.nytimes.com/2008/08/13/technology/13cyber.html. Accessed 22 October 2013.

McMahan, J. 2009. *Killing in war*. Oxford: Oxford University Press.
Menn, J. 2012. Hacked firms fight back with vigilante justice. *The Globe and Mail*, June 18. http://www.theglobeandmail.com/technology/tech-news/hacked-firms-fight-back-with-vigilante-justice/article4321501/. Accessed 22 October 2013.
New York Penal Law. 2012. Article 35: Defense of justification. New York Laws. http://ypdcrime.com/penal.law/article35.htm. Accessed 22 October 2013.
Orend, B. 2005. War. The stanford encyclopedia of philosophy. Stanford University. http://plato.stanford.edu/entries/war/. Accessed 22 October 2013.
Owens, W., K. Dam, and H. Lin, eds. 2009. Technology, policy, law, and ethics regarding U.S. Acquisition and use of cyberattack capabilities. The National Academies Press. http://www.nap.edu/catalog.php?record_id=12651#orgs. Accessed 22 October 2013.
Reichberg, G. M., H. Syse, and E. Begby, eds. 2006. *The ethics of war: Classic and contemporary readings*. Malden: Blackwell Publishing.
Rid, T. 2012. Think again: Cyberwar. Foreign policy. http://www.foreignpolicy.com/articles/2012/02/27/cyberwar?page=full. Accessed 22 October 2013.
Riley, M., and J. Walcott. 2011. China-based hacking of 760 companies shows cyber cold war. Bloomberg, December 14. http://www.bloomberg.com/news/2011-12-13/china-based-hacking-of-760-companies-reflects-undeclared-global-cyber-war.html. Accessed 22 October 2013.
Rowe, N. 2009. The ethics of cyberweapons in warfare. *International Journal of Cyberethics*. 1:20–31.
Rowe, N., E. J. Custy, and B. T. Duong. 2007. Defending cyberspace with fake honeypots. *Journal of Computers* 2:25–36.
Sanger, D. 2012. Obama order sped up wave of cyberattacks on Iran. New York Times, June 1. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all. Accessed 22 October 2013.
Schmitt, M. 2010. Cyber operations in international law: The use of force, collective security, self-defense, and armed conflicts. The National Academies Press. http://www.nap.edu/openbook.php?record_id=12997&page=151. Accessed 22 October 2013.
Schneier, B. 2010. The story behind the stuxnet virus. Forbes, October 7. http://www.forbes.com/2010/10/06/iran-nuclear-computer-technology-security-stuxnet-worm.html. Accessed 22 October 2013.
Taddeo, M. 2012. Information warfare: A philosophical perspective. *Philosophy and Technology* 25:105–120.
Tierney, D. 2011. We don't need an Obama doctrine. The Atlantic, October 23. http://www.theatlantic.com/international/archive/2011/10/we-dont-need-an-obama-doctrine/247207/#. Accessed 22 October 2013.
United Nations. 1982. United nations convention on the law of the seas, especially Part VII. http://www.un.org/Depts/los/convention_agreements/texts/unclos/closindx.htm. Accessed 22 October 2013.
Walzer, M. 2006. *Just and unjust wars*. New York: Basic Books.
Watts, S. 2011. Low-intensity computer network attack and self-defense. *International Law Studies*. 87:59–87. http://www.law.berkeley.edu/files/watts–low_intensity_computer_network_attack.pdf. Accessed 22 October 2013.
White Wolf Security. 2007. Offensive operations in cyberspace. White Wolf Security Publications. http://www.whitewolfsecurity.com/publications/offensive_ops.php. Accessed 22 October 2013.
Willson, D. L. 2010. When does electronic espionage or a cyber attack become an 'Act of War'?. *Information Systems Security Association (ISSA) Journal* 8:20–24.
Willson, D. L. 2012. Hacking back in self-defense: Is it legal? Should it be?. *Information Systems Security Association (ISSA) Journal*. 10:7–10.
Wright, R. 2012. President Obama's hypocrisy on cyberattacks. The Atlantic, June 3. http://www.theatlantic.com/international/archive/2012/06/president-obamas-hypocrisy-on-cyberattacks/258016/. Accessed 22 October 2013.