# Chapter 1
# Fog in the Fifth Dimension: The Ethics of Cyber-War

**Brian Orend**

**Abstract** Cyber-warfare is a cutting-edge topic in armed conflict. It can be defined, at least initially, as attempting to use the Internet, and related advanced computer technologies, to substantially harm the fundamental interests of a political community. And cyber-space has been referred to as "the fifth dimension of warfare," after: land; water; air; and space. Yet, much confusion (or "fog") surrounds cyber-warfare, both regarding its present realities and its future potential. How much damage can cyber-attacks actually do? Is it even appropriate to liken computer-based cyber-attacks to physical ("kinetic") violence? Is "informational warfare", as cyber-war is otherwise known, changing the very nature of political conflict in our time (indeed, for all time)? This chapter aspires to clear up some—but certainly not all—of this fog which surrounds the fifth dimension. It will do so by means of critically examining three important distinctions in this regard. But first, some workable definitions are required.

> *All action takes place, so to speak, in a kind of twilight which, like a fog or moonlight, often tends to make things seem grotesque and larger than they really are.* (Clausewitz 1995)
> Carl von Clausewitz, ***On War***

Cyber-warfare is a cutting-edge topic in armed conflict. It can be defined, at least initially, as attempting to use the Internet, and related advanced computer technologies, to substantially harm the fundamental interests of a political community. And cyber-space has been referred to as "**the fifth dimension of warfare**," after: land; water; air; and space (The Economist 2010). Yet, much confusion (or "fog") surrounds cyber-warfare, both regarding its present realities and its future potential. How much damage can cyber-attacks actually do? Is it even appropriate to liken computer-based cyber-attacks to physical ("kinetic") violence? Is "**informational warfare**", as cyber-war is otherwise known, changing the very nature of political

B. Orend (✉)
University of Waterloo, Waterloo, Canada
e-mail: bdorend@uwaterloo.ca

L. Floridi, M. Taddeo (eds.), *The Ethics of Information Warfare,*
Law, Governance and Technology Series 14, DOI 10.1007/978-3-319-04135-3_1,

conflict in our time (indeed, for all time)? This chapter aspires to clear up some—but certainly not all—of this fog which surrounds the fifth dimension. It will do so by means of critically examining three important distinctions in this regard. But first, some workable definitions are required.

## 1.1 Quick Definitions

As offered above, "**cyber-warfare**" is an umbrella term, referring to the aggressive use of advanced computer technologies in a way deliberately designed to substantially harm the fundamental interests of a political community (Carr 2010). A **political community** can be considered a country, state, or nation, but was perhaps most suggestively defined by Aristotle as an on-going human partnership, formed for the sake of the common good of its members and aimed at achieving both *justice for all* and *happiness for each* (Aristotle 1984). Political communities have many interests, but among the most fundamental are: peace and security; access to vital resources; the right to govern themselves free from foreign domination; the right to grow their economy and try to improve their lives; and finding a balance between creative innovation and reliable stability in their way of life. Most basic, perhaps, of a country's **fundamental interests** are: freedom from invasion; freedom from domination; and secure possession of those resources truly needed to survive on an on-going basis (Orend 2013).

Cyber-warfare, generally, can take one of three forms:

1. **espionage** (i.e., using the Internet, etc., to gather information which a country has taken steps to protect as a matter of national security, such as secret-, confidential-, or classified information);
2. **the spread of disinformation**, via the same means, in a manner which harms the security interests of the target country; and/or
3. **sabotage** (i.e., using these means to bring about the non-functioning, or destruction, of various systems which are integral to the basic interests of a political community. The systems most often mentioned include: electricity and power; water and fuel distribution; computerized parts of manufacturing facilities; transportation systems, such as air or rail; banking and the stock market; and even the Internet itself, or at least the most used web-sites (like Google or Facebook), Internet service providers, and/or the most basic operating systems.) (Clarke 2010)

**Cyber-attacks** would then refer to any *specific* use of any of 1–3 above, as tools within the overall cyber-warfare *strategy*. The countries most frequently mentioned today with reference to cyber-war technology include: America; Britain; China; France; India; Israel; Pakistan; and Russia (Clarke 2012).

## 1.2 The First Distinction: "Cyber-War-Skeptic" Vs. "Cyber-War-Salesman"

A **cyber-war-skeptic** would be someone, like Howard Schmidt, who declares that "there is no such thing as cyber-warfare." (Schmidt 2006) A cyber-war-skeptic believes that the threat from such measures (as 1–3 above) is minimal or, at least, not at all on a level where talking about a military response is appropriate. A cyber-war-skeptic might also believe that the whole extended analogy—between information attacks and computer viruses, on the one hand, and kinetic warfare and physical casualties, on the other—is: 1) crude and factually incorrect, perhaps even a "category mistake" confusing two completely different things; 2) fear-mongering, capitalizing on the common person's (relative) intimidation by, and lack of knowledge regarding, advanced computer technology; and 3) deliberate exaggeration, or even fraud, communicated by those with a vested interest in the business of cyber-security, ranging from cash-strapped military departments looking for fresh resources to greedy software programmers drooling at the prospects for profit. (And the financial stakes *are* very considerable: The Pentagon has publicly disclosed that, in the first half of 2009 alone, it spent over $ 100 million USD "responding to, and repairing damage from, cyber-attacks.") (Clarke 2010).

A **cyber-war-salesman**, on the other hand, would be someone who wildly exaggerates the threat of cyber-war, and the disruption to be suffered from such. It needs to be stressed that such a figure doesn't have to be a cyber-war profiteer, as just mentioned at the end of last paragraph. Consider that the influential 2010 *Lipman Report*—i.e., the US Congress' formal study of cyber-warfare, for American foreign policy purposes—warned that threats of "crippling attacks on computer networks are sharply on the rise." (U.S. Congressional House 2011) The US mainstream broadcasting company CBS reported, in an evening national TV broadcast, that, in 2007, the US federal government suffered "an espionage Pearl Harbour" when some unknown sources downloaded "terabytes of classified government and even military information." (Note the similarity between the spoken sound of "terabytes" and "terror bites.") (CBS News 2009) Indeed, in 2010, the U.S. Joint Forces Command issued a statement expressing its conviction that "adversaries have already taken advantage of computer networks and the power of information technology… to plan and execute savage acts of terrorism." (USJFC 2010) Even the normally staid *New York Times* reported that a **malware program** (i.e., a malicious software virus) which had infected some U.S. factory computers should be "considered the first attack on critical industrial infrastructure that sits at the foundation of modern economies." (New York Times 2010) Finally, consider the closing lines in one of distinguished journalist Michael Gross' important articles about information warfare in general, and a virus called "Stuxnet" (more below) in particular:

> Cyber-conflict makes military action more like a never-ending game of uncle, where the fingers of weaker nations are perpetually bent back. The wars would be secret, waged by members of anonymous, elite brain trusts, none of whom would ever have to look an enemy in the eye. For people whose lives are connected to the targets, the results could be as cata-

> strophic as a bombing raid, but would be even more disorienting. People would suffer, but would never be certain whom to blame.
> Stuxnet is the Hiroshima of cyber-war. That is its true significance, and all the speculation about its target and its source should not blind us to that larger reality. We have crossed a threshold, and there is no turning back. (Gross 2011a)

Within these various dramatic comments, one takes special note of the multiple references to terrorism and to the Second World War.

So, the question naturally arises: who's right? Who, between the cyber-war skeptic and the cyber-war salesman, is more correct? It will be an on-going theme of this chapter that the truth between each of the three distinctions to be drawn and addressed probably rests somewhere in the middle, in a Rawlsian over-lapping consensus (as it were) (Rawls 1993). Where does the middle ground properly lay in this present case?

### *1.2.1 Middle Ground Judgment*

On the one hand, there is no denying that cyber-attacks *are* real, and they have had some surprisingly serious consequences, at times very much akin to actual, kinetic warfare. So, in this sense, the cyber-war skeptic is wrong and the cyber-war salesman, right. Several quick, illustrative examples:

- In 1982, during the height of The Cold War, a Canadian oil and gas company thought they had a Soviet (Russian) spy in their midst. They contacted America's military. The Canadians and Americans launched a joint scheme: they would let the spy steal what he was after: a computer-control system for regulating the flow of oil and gas. (The Russians wanted this to modernize their pipeline system in Siberia.) But the Americans programmed the computer system with "a logic bomb", designed to make the pipelines malfunction and eventually explode after it was implemented. And that is exactly what happened, with some loss of life and a substantial set-back for a key sector of the Soviet economy (The Economist 2010).
- In 2007, Russia launched a cyber-attack on Estonia, a neighbouring country. There was a dispute between them regarding the movement of a war statue of great meaning to the Russians. When the Estonians moved it, Russia responded with a crippling cyber-attack on the websites of the Estonian government, media, and its richest banks. For nearly a week, these institutions could not conduct any business online, nor could their citizens/customers contact them, or access anything through them. The attack came to an end only when Russia decided to release its grip (Karatzogianni 2008).
- From May to December, 2010, India and Pakistan traded over 1,000 separate cyber-attacks against each other, directed not only against official government- and military web-sites but also selected high-profile companies, universities, and research institutes. While most of these attacks were mere "**defacements**" of the various web-sites (and thus more a form of disinformation, or graffiti, than

sabotage), they nevertheless revealed both the involvement of these countries in cyber-war activities as well as the degree to which they were capable of gaining access and demonstrating control (Hyacinthe 2011).

- More seriously, in 2010, Iran was attacked by a computer virus or "worm" commonly believed to have been the joint-creation of both America and Israel (nicknamed "**Stuxnet**"). A piece of malware, this very sophisticated computer virus was planted in a German-made component of one of Iran's nuclear reactors. When it was activated, the virus eventually disabled the reactor, forcing it to shut down—lest it melt-down and cause enormous damage—for an unspecified time (thought to be at least for months, and perhaps even over 1 year). The goal, reputedly, was to set-back Iran's progress towards developing nuclear weapons (Gross 2011a).
- Perhaps relatedly, in 2012 the "**Flame**" virus entered public knowledge. Reputedly, Flame went undetected for over 5 years. Its main purpose seems to have been espionage or information-gathering. Experts have pronounced it "more than 20 times more powerful" in its sophistication than Stuxnet and, by time of discovery, it was confirmed to be present in over 5,000 computers, almost all in the Middle East, with a special concentration in Egypt, Iran and Israel (Stallwood 2012).
- The country most associated with cyber-attacks today is China. Unlike American and Russian attacks, though, which have tended to feature sabotage, the Chinese seem to prefer espionage, both of the commercial- and political variety. Many of the top US high-tech firms, such as Google, Microsoft, Apple, and various weapons companies, have complained of sustained cyber-attacks from China which have accessed tons of their highest-security information, including especially product design- and patent information (as well as, intriguingly, human resources data, such as personal information about top executives). The companies have pressed the US government to respond, but thus far all that have been issued are verbal warnings by Hilary Clinton, the US Secretary of State (Gross 2011b).

Thus, informational warfare is truly real; and it can have—and has had—very serious consequences, including loss of life. (Though, admittedly, these most serious consequences seem more rare and exceptional rather than regular and expected, as with direct kinetic warfare.) On the other hand, the cyber-war skeptic seems correct to insist that it's important not to exaggerate people's fears about the likelihood of themselves being victimized by such strikes, or to make colourful but unhelpful analogies to weapons (such as at Hiroshima) which can kill hundreds of thousands of people. And it certainly seems compelling to note that all this talk, and all this activity, surrounding cyber-warfare *does serve some vested interests*, out to gain narrow advantage, and we should regard their claims with some sober second thought, and make them prove such. After all, if The Pentagon is spending $ 100 million USD every 6 months on cyber-defence, one must admit that a pot of money *that* large is likely to attract not only legitimate, but also questionable, attention.

## 1.3 The Second Distinction: Realism Vs. Just-War Theory

### *1.3.1 No Law*

Cyber-warfare is here, and it's real; and so the question arises: what, if anything, should we do about it? An obvious response would be to try to regulate it with the law. Presently, there is no international law whatsoever regarding informational warfare. In 2011, America, China and Russia got together for a high-level meeting of officials, one branded as being "talks about talks" regarding a possible negotiated treaty between them on the acceptable methods and means of cyber-war (analogous to the many such treaties on kinetic warfare). But the talks fell apart, amidst bitter mutual accusations (Dinniss 2012).

It is vital to note that, in the absence of an international treaty on this, all the major countries have simply (and resoundingly) declared that, as a matter of their foreign policy, they will consider any "severe" cyber-attack against them as a ***casus belli***, i.e.: a cause for war, a reason to resort to war (presumably, either of the new informational-, or the traditional physical, kind) (Carr 2010; Lynn 2010).

### *1.3.2 Thus, Ethics*

In the absence of law, one turns to ethics for guidance. Traditionally, there are three major traditions of thought about the ethics of war and peace: realism; just war theory; and pacifism.

### *1.3.3 Pacifism*

#### 1.3.3.1 In General

Pacifism is a species of idealism regarding international affairs. **Idealism** is the view that one's goal as a country, when dealing with others, ought to be to *do one's part in making the world a better place*. It's like a form of national altruism, or unselfishness. When dealing with the outside world, use one's resources and influence to improve the world: make it richer, happier, more secure, and so on. Be a good international citizen. Give a damn, so to speak, and act accordingly. Commonly, idealists tend to divide into those favouring small-scale, concrete, and gradual improvements versus those attracted to larger-scale, sweeping, and more sudden shifts in international politics. Prominent idealist thinkers would include Immanuel Kant, whereas prominent idealist politicians would include former US President Woodrow Wilson (Orend 2013; Price 2007; Kant 1983).

#### 1.3.3.2 On War and Cyber-War

The essence of **pacifism**, obviously, is a rejection of war. War is always wrong; there is always some superior alternative to war, such as non-violent resistance. For better or worse, pacifism thus far plays no effective role in the debate about cyber-warfare. While there *has* been a pacifist-inspired idea to have a treaty banning all forms of cyber-war, and to have the Internet declared "part of the common cultural heritage of humanity" (and thus, *not* a proper battlefield), it has thus far gone nowhere (Menthe 1998). (Mathieu Doucet has suggested that perhaps pacifists could actually endorse cyber-warfare, as a tool of nonviolent resistance designed to shut down, or seriously complicate, the use of kinetic war, with its violent, bloody consequences. That is an intriguing idea but one which, thus far, remains underdeveloped—and, further, it would need to account for, and ethically grapple with, those forms of cyber-war where killing force *has* resulted, such as in the Soviet logic bomb case described above. Pacifists, presumably, could neither logically nor morally endorse those forms: care would need to be taken to show which kinds of cyber-war might be permitted and which not.)

### *1.3.4 Realism*

#### 1.3.4.1 In General

**Realism** is the view that, as a country, one's goal should be *to advance one's national interests*. **National interests** are those things that improve, benefit, or enhance the position of one's country. They boil down to having both hard- and soft power. **Hard power** is the use of economic resources, and/or armed force, to get what one wants in international relations. Summarized as "the bucks-and-bullets" approach to foreign policy, it means either buying or forcing the compliance of others to one's will. **Soft power**, by contrast, is the use of one's language, ideas, values, and culture to bring about the compliance of others to one's will. The spread of one's culture is thought to create a commonality of world-view, a mutuality of interest, and a reservoir of good will, which bolsters one's ability to get what one wants. Realism is thus like a form of national egoism or selfishness. When dealing with the outside world, or "the international community," one ought to (as they say) "Look Out For Number One." Do the best one can for one's own society, especially in terms of: national security and defence; growing the economy, optimizing one's population and its access to natural resources; and augmenting one's cultural and political influence around the world. Prominent realist thinkers would include Machiavelli and Hans Morgenthau. Prominent realist politicians would include Henry Kissinger and former US President Richard Nixon (Orend 2013; Machiavelli 1998; Kissinger 1995; Morgenthau 1970).

#### 1.3.4.2 On War and Cyber-War

In terms of warfare, realism clearly clashes with pacifism. Indeed, whereas pacifism seems to say "nothing goes" in terms of violent warfare, realism replies with an equally sweeping "anything goes." The most important thing to note with warfare, according to many realists, is that history shows that it is a dreadful thing to lose a war, and such is almost never in the interests of any country. Thus, the over-riding objective is to *do whatever one deems required to win*. It all becomes a calculus of national self-interest and advantage.

The realist thus views the development of informational warfare as just the latest permutation in human history's endless cycle of violent conflict. Countries constantly seek advantage in war, including especially through mastery of new weapons. Cyber-technology is a new, and potentially very important, technology which could have deep implications for armed conflict, in particular, and for the hierarchy of nations in general. Thus, countries *should* be doing exactly what they *are* doing right now: investing in its development; experimenting with its use; not tolerating any strikes against themselves; threatening others over its use; using it against others to gauge its impact; and ascertaining how best to use this new weapon in their overall war-fighting, and foreign policy, objectives.

### *1.3.5 Just War Theory*

In-between the extreme views of realism and pacifism resides just war theory. Like pacifism (and unlike realism), just war theory believes that there *is* both sense and value in applying ethics and moral values to issues of international relations. But unlike pacifism (and like realism), just war theory believes that there *can sometimes* be instances where resorting to war is justified, if only as "the least-worst" option. Thus, if pacifism says "nothing goes" with regard to the ethics of war, and realism declares that "anything goes", just war theory opines that "something, sometimes goes." While war *can* be morally permissible, just war theory nevertheless views war dimly and dangerously, and insists that it's too risky and lacking in restraint to allow for "anything goes." Just war theory seeks to substitute, for that realist permissiveness, a set of sensible rules to restrain and guide those considering warfare as a tool for solving some serious foreign policy problem. The just war approach has been deeply influential on the international laws of armed conflict, for instance as contained in the *Hague*- and *Geneva Conventions*, as well as in the *UN Charter* and the various resolutions of the UN Security Council (UNSC) (Walzer 1977; Orend 2006; Roberts and Guelff 1999).

Elsewhere, I've further explained, and defended at length, the claims and rationale of just war theory against its two major rivals. I still believe it is the most sophisticated, detailed, comprehensive, and well-defended system of thought about the ethics of war and peace (Orend 2006, 2000a, 2009). As such, it profits us to consider further *how* the just war rules and categories can shed light on informational

warfare. The method will be as follows: to explain just war rules in general (as they've applied traditionally to regular, physical warfare); and then to suggest how they might apply to our analysis of informational warfare.

#### 1.3.5.1 Jus ad Bellum

This is Latin for "the justice of war." When, if ever, may states fight?

The just war answer is that states may fight *only if* they satisfy *all* of the following rules: just cause; right intention; public declaration of war by a proper authority; last resort; probability of success; and proportionality. Those with "the war power" (usually the executive branch in non-democratic societies, and the legislative branch in democratic ones) are to ensure they satisfy these principles before embarking on war.

- **Just Cause**

The way international law renders just war theory in this regard is very clear and quite helpful. Most experts agree that, when it comes to a just cause for war, three general principles are at play:

1. All countries have the inherent, or "natural," right to go to war in **self-defence** from aggression. **Aggression** is defined as any unjustified use of force against another country. Any armed attack which crosses an international border constitutes aggression and is a *casus belli*, i.e., "a cause for war."
2. All countries have the further natural, or inherent, right of **other-defence**—otherwise known as "**collective security**"—to go to war as an act of aid, or assistance, to *any* country victimized by aggression; and
3. *Any other* use of force—e.g., pre-emptive strike, or armed humanitarian intervention—is *not* an inherent, or natural, right of states. Any country wishing to engage in such is supposed to get *the prior approval* of the UNSC. Failing to receive such prior authorization renders any such use of force illegal, itself an act of aggression (Orend 2006, 2013; Regan 1996; Roberts and Guelff 1999).

So, if Country A commits an armed attack against Country B, then B (and any other country C) is entitled to go to war against A as an act of *defence from*, *resistance to*, and *punishment of*, aggression. Aggression is seen as a wrong so severe that war is a fitting response because it violates the most basic rights of groups, and individuals, to life and security, and to freedom and well-being—i.e., to go about their lives peacefully, on a territory where their people reside. Classic examples of international aggression include: Imperial Germany's invasion of Belgium in 1914, sparking WWI; Nazi Germany's invasion of Poland in 1939, sparking WWII; Japan's invasion of China in 1937, and its attack on the USA at Pearl Harbour in 1941, sparking the Pacific part of WWII; the USSR's invasion of Afghanistan in 1979; and Iraq's invasion of Kuwait in 1990, sparking the Persian Gulf War. There are actually thousands of historical examples of international aggression (Orend 2006, 2013; Walzer 1977; Keegan 1990, 1994).

- **Proportionality**

In every kind of law or rule, there is supposed to be a **proportion**, or balance, between problem and solution (or between violation and response), which is here to say that international law commands that the problem in question really must be so serious that war is a proper reply. Since war is so costly, bloody, and unpredictable, it follows that only a very few problems in international life are truly so bad that war will be a proportionate response to them. The function of this rule is to get those with the war power to think again, deeply, whether there isn't some other thing to be tried—say, one of the other foreign policy tools, such as diplomacy or sanctions—before resorting to force. What, if anything, might be a problem truly so severe that war is a proportionate response? *The answer of international law, and just war theory (for reasons stated above) is: aggression.* When confronted with an aggressive invader—like Nazi Germany, Imperial Japan, or the Soviet Union—who's intent on conquering and essentially enslaving other nations, it's deemed reasonable to stand up to such a dark threat to life and liberty and to resist it, and beat it back, with force if need be. Just as dangerous criminals must be resisted and not be allowed to get away with their crimes, countries are entitled to stand up to aggressors, and to resist and defeat them (Orend 2006; Walzer 1977).

- **Public Declaration of War by a Proper Authority**

War is supposed to be declared out in the open, officially and honestly, by the proper authority for doing so. In every country, some branch of government has "**the war power**:" i.e., the authority to order the use of force and warfare. In Canada and Britain, the war power rests with Parliament; in America, the war power likewise rests with the legislature: i.e., Congress. But the American President—as Commander-in-Chief of the Armed Forces—has enormous factual power to order the American military into action. As a result, many experts argue that the war power in the US is actually split—in classic American "**checks-and-balances**" style—between the legislative and executive branches of government. (This became an issue of struggle between the branches during both the Korean War (1950–1953) and especially the Vietnam War (1954–1974), when Congress felt successive presidents were running a ***de facto*** war without actually publicly declaring it and getting ***de jure*** authority for doing so—i.e., getting a clear vote of support from Congress.) (Regan 1996) Generally, in most democracies, the legislature has the war power whereas, in most non-democratic societies, it's the executive—i.e., the president or dictator—which has the authority to order war. We have seen, further, how in all cases where non-defensive armed force is being considered, the UNSC must also approve of the action, and beforehand. This is to say that, with non-defensive war, both domestic and international authorization must be satisfied (Orend 2006, 2013).

- **Last Resort**

State governments are only supposed to go to war as a **last resort**, only after all other reasonable means of problem-solving have been tried, and failed. It's said that countries have four basic tools in their foreign policy tool-box: diplomacy; economic incentives; sanctions; and force. Obviously, you want to exhaust all other means of problem-solving before engaging in something as expensive, bloody, and

risky as war. A nice illustration of this rule in action happened during the run-up to the Persian Gulf War of 1991. In August 1990, Saddam Hussein's Iraq invaded its tiny neighbour, Kuwait. International allies, as led by the USA and UK, tried to talk to Saddam and threaten him, to no avail. They then slapped sweeping sanctions on him, and got most of his neighbours to agree and also put pressure on Iraq. Still nothing. As a result, the international community felt it was the last resort to go to war to push Saddam out of Kuwait, and back into his own borders. This they did, within 2 months, in early 1991 (Johnson and Weigel 1991; Orend 2006).

The above *jus ad bellum* rules are all part of the international laws of armed conflict. Just war theory, as a theory of ethics, levies two additional moral requirements:

- **Right Intention**

The notion here is that one's motives need to be ethically proper. It's not enough merely that one's *actions* comply with the above rules but that, furthermore, one acts with *the right frame-of-mind* and, in particular, that seedy, ulterior motives—such as greed—play no role. In the case of a just war, then, the idea would be that one's intentions in acting are to resist, repulse, and punish aggression, and nothing more. Though this rule is *not* part of international law—largely owing to the difficulty involved discerning the true intentions of a complex, multi-part actor like a state government—it is frequently invoked in common moral discussion of warfare. It was, e.g., a popular criticism of the Bush Administration's decision to invade Iraq in 2003 to suggest that the decision had as much, or more, to do with the desire to gain secure access to oil as it did with, say, ensuring Iraq wasn't about to deploy weapons of mass destruction (WMD) against the USA (Murray and Scales 2003; Woodward 2004; Orend 2006).

- **Probability of Success**

The rule here is that one should not begin a war one knows in advance is going to be futile. The point is *to prohibit pointless killing and suffering*: one should have some probability of success before resorting to war. At the same time, this can be very difficult to predict at the start of war, and history has shown that, sometimes, long-shots can actually win. Moreover, this rule seems biased in favour of powerful states, who (for that very reason) have better chance of winning their wars. This probably explains the absence of this rule from international law, which is based around theoretical ideals regarding the equality of sovereign states: if a country—any country, big or small—has been victimized by aggression, who are we to say that they shouldn't go to war, because at the outset it looks like such a risky venture? (Orend 2006)

#### 1.3.5.2 Application of Jus ad Bellum Rules to Cyber-War

- **Just Cause**

As shown above, the gold standard of *casus belli* is a kinetic physical attack, usually involving some kind of armed invasion across a border. As such, a cyber-strike does

*not* seem to constitute aggression in the traditional meaning of the term. But two thoughts suggest themselves:

1. sometimes, as we've seen, cyber-attacks can actually lead to traditional, physical damage, including loss of life. Such would have to be construed as straight-forward instances of aggression, ethically and legally enabling a forceful response.
2. an argument could be made that the concept of aggression itself needs to be amplified and expanded (but responsibly so) precisely to allow for cyber-attacks as a kind of aggression. This thinking would need to stress the new and pervasive role which advanced computer technologies have come to play in our lives (especially in the developed world), and the degree to which damage aimed at them could rise to the level of a very serious, society-wide strike. Indeed, some might even argue that, say, a cyber-attack on the stock market, causing it to crash and costing millions of people billions of dollars, might actually be more damaging in long-term consequence than, e.g., an army unit lobbing a missile across a border, resulting in the physical injury (or death) of only, say, 3 soldiers on border patrol. This is to say that: a) a powerful cyber-strike might actually be more damaging than a physical strike; and b) if the latter counts as aggression, then the former ought to, as well. The key notion here would be that our thinking of what constitutes aggression needs to keep pace with the times and the new technological realities of our lives (Floridi 2010a, b).

I think these reflections would need to be made in greater detail than here, but I do support the general notion that these concepts, to remain relevant, must be considered in light of the latest technologies and deep, ongoing developments in the contours of our lives. My own considered view is that *a cyber-strike probably will not justify anything more than an in-kind cyber-response*, and that the burden of proof rests on anyone arguing that it may justify something further, such as an armed kinetic attack in reply. While there is much defensive, deterrent-based wisdom in the status quo—i.e., of warning others that any "severe" cyber-strike will be considered a *casus belli* (especially one involving sabotage against core, society-wide, infrastructure)—more sustained efforts at deeply developing these concepts need be made (Brenner 2009; Cook 2010; Lucas 2011).

- **Proportionality (and Probability of Success)**

Proportionality would clearly support the notion that a cyber-strike probably justifies *only* an in-kind cyber-response, and *not* an armed kinetic war in reply. And probability of success demands that we ask, for any such cyber-strike: is it likely to achieve its aims? How so? What kind of confidence can one have in that regard, especially as regards the minimization of any over-spill onto civilians and the likelihood that one can have favourable control over the consequences?

- **Last Resort**

There is a real danger, and some evidence from the actual uses thus far, that a major temptation with cyber-strikes is that they be used *not* as a last resort, but rather as a **first-strike capability**, either on their own or else to disorient and "soften up" the

target for an actual kinetic attack, such as with drones, missiles, or even an armed invasion.

It might be argued that cyber-war could be rendered consistent with this principle, and find its own proper slot in the moral hierarchy of foreign policy tools, with diplomacy at the ground floor, as the most accessible (and encouraged) level, and with kinetic force at the top: the rarest, riskiest, and most controversial. Cyber-strikes could be located either just beneath kinetic warfare, or else perhaps on par with sweeping economic sanctions, which often are similarly targeted at foundational aspects of the target country's economy.

- **Public Declaration by a Proper Authority**

Here there is no question that the vast majority of actual cyber-attacks thus far have violated this rule of just war. Indeed, has any government publicly declared, and accepted responsibility, for any cyber-attack? One of the seductions of this technology is its supposed anonymity (though, almost always, the doer's identity *does* come to be known: see more below). We know that, historically, those with the war power prefer to use it in secret and with few, or no, checks-and-balances on them. Cyber-war may thus provide terrible temptations in favour of "easy war" and "secret war" which ought, obviously, to be resisted.

Experts in the field talk repeatedly of "**the attribution problem**", noting how cyber-attackers—especially those suspected to be linked, in some way, with China—go out of their way to hide their tracks and conceal the ultimate source of the strike. This is of great concern, as it would no doubt colour our judgment of whom it is permissible to strike back at (Clarke 2010). Yet, while being ignorant of the sophisticated details of how these things get determined, I would want to point out, as mentioned above, that eventually—and rather quickly, actually—the cyber-community seems to have been able, thus far, to come with pretty reliable attributions. Is cyber-strike attribution really so different from, and so much more difficult than, say, the investigations which went into determining who was responsible for the 9/11 attacks (i.e., al-Qaeda), and how the then-government of Afghanistan was complicit in them as well?

### *1.3.6 Traditional Rules of Jus in Bello*

Whereas the rules of *jus ad bellum* are aimed at those with the war power—often the head of state—the rules of *jus in bello* are aimed at soldiers and officers, i.e., those who actually do the fighting. If they violate these rules, they can find themselves—after the conflict—facing war crimes charges, either domestically through their own military justice system or internationally through The Hague. There are many rules of *jus in bello*, but most of them concern only physical, kinetic warfare, and they are not directly applicable to cyber-war. The one principle which most clearly is, though, is *jus in bello*'s most important: discrimination and non-combatant immunity. Let us consider this first in the traditional sense, and then the potential implication for information warfare.

- **Discrimination and Non-Combatant Immunity**

"**Discrimination**" here means the need for fighters to distinguish, or discriminate, between legitimate and illegitimate targets, and to take aim only at the former. A **legitimate target** is anyone, or anything, which is part of the war machine of the enemy society. "**The war machine**" refers to the military-industrial-political complex which guides the war and fights it. Loosely speaking, it is anything which is a source of potential physical harm, or armed force, directed against oneself. More specifically, legitimate targets include: soldiers, sailors, marines, pilots, and their officers; their weapons and equipment; their barracks and training areas; their means of transportation; their supply and communications lines; and the industrial sites which produce their supply. Core political- and bureaucratic institutions are also legitimate objects of attack, in particular things like the Defence Ministry. **Illegitimate targets** include residential areas, schools, hospitals, farms, churches, cultural institutions, and non-military industrial sites. *In general, anyone or anything not demonstrably engaged in military supply, or military activity, is immune from direct, intentional attack*. Thus, **non-combatants**—i.e., civilians—are "immune" from intentional attack. This is seen as probably the worst war crime: the intentional killing of civilians (Walzer 1977; Orend 2006).

Strange as it may sound, the non-combatant immunity principle does *not* mean that it's illegal for civilians to die in wartime. What is illegal is *taking deliberate and intentional aim* at civilians with armed force. If a fighting side has taken every reasonable effort to avoid and minimize civilian casualties—but some civilians still die accidentally, or in the indirect way just noted—then that is *not* a war crime. Such civilians are viewed as "**collateral damage**"—i.e., accidental, un-intended, casualties of the fighting. An example would be an air-bombing raid on an enemy's industrial sites, during which a few bombs accidentally go astray and hit a close-by residential area, wounding and killing some civilians.

So, civilians are *only* entitled to "due care" from fighters; they are *not* entitled to absolute and fail-safe immunity from warfare. What does "**due care**" include? It includes all serious and sustained efforts, from the top of the military chain of command down to the bottom, to protect civilian lives as best as can be amidst the difficult circumstances of war. So, e.g., strategists must make their plans with an eye to minimizing civilian casualties; intelligence needs to be gathered and analyzed regarding which are the permissible targets; soldiers need to be trained exhaustively in proper—i.e., restrained and discriminating—ways of fighting; and any rough treatment of civilians needs to be investigated and punished; and so on (Orend 2006; Walzer 1977).

What about so-called "**dual-use**" targets? The question arises: what about things used *both* by the military and civilians during war: e.g., roads, bridges, radio and TV networks and transmitters, railway lines, harbours, and airports? International law forbids targeting them but, in reality, they often are, as they are so useful in helping military planners communicate with their troops and to move them around to where they can fight. More controversial, and thus more criticized, is targeting basic infrastructure, like farms, food supply, sewers, water treatment plants, irrigation systems, water pipelines, oil and gas pipelines, electricity generators, and power and

telephone lines. The civilian population pays a huge price for any damage inflicted on such vital social infrastructure, and so it seems to violate civilian immunity to go after them. America did this recently twice. During the opening days of both the 1999 Kosovo War, and the 2003 Iraq attack, America launched a so-called "**shock and awe**" campaign—relying on air power, bombing raids, and cruise missiles—to inflict heavy damage on basic infrastructure (especially communications and electricity) on Serbia and Baghdad, respectively. The military goal of such a strike is to hit the enemy as fast and furiously as possible, dazing them, and "softening them up" for a subsequent ground invasion by army soldiers. It is also to shock the civilians in that society into putting pressure on their regime to give up and surrender quickly (Clark 2002; Ignatieff 2001; Orend 1999, 2006).

#### 1.3.6.1 Application of Jus in Bello to Cyber-War

The inference for cyber-warfare is clear: if one engages in a cyber-strike, one ought to take every effort to ensure that civilians are left out of it, and that only legitimate targets bear the brunt of the cyber-attack. The best, contrasting examples from the above list of cases would be the Russian cyber-strike on Estonia, on the one hand, and Stuxnet, on the other. The Russian strike clearly impacted every citizen in Estonia, as for the week or so in which it was on-going, such citizens could not have contact with their democratically-elected government online, nor could they access personal funds from their own bank accounts, and so on. This, clearly, was a substantial and intended interference with the basic rhythms of their daily lives. Ironically, Estonia (and the other Baltic states) had been, up until that point, at the fore-front of so-called "**e-government"**: i.e., making as many government services deliverable over the Internet as possible. The cyber-strike from Russia, unfortunately, showed the potential disadvantages of such a progressive and technologically advanced approach. In any event, it clearly violated non-combatant immunity.

Stuxnet, by contrast, was elaborately constructed to harm only the nuclear power capability of the Iranian government. And it seems to have succeeded in that regard, and not one civilian was even harmed—much less killed—in the process. (The virus, after it struck, was programmed to "evaporate;" i.e., write itself out of existence so it could do no further harm.) Now, I suppose one could talk about the *potentia*l harm to the public, had the Iranians not known how to handle the situation: things may, indeed, have taken a frightening turn. Obviously, the perpetrators (rumoured to be the US and Israel) had confidence that the Iranians *would* recognize what was happening, and would have the wherewithal to shut the reactor down and not risk broader public damage. In any event, these two broad examples show what just war theory would view as a permissible cyber-strike: a discriminate one aimed only at a legitimate target, and with clear measures taken to minimize or eliminate any negative consequences on civilian populations. Especially to be ruled out—as the equivalent, really, of WMD—are potent, society-wide, cyber-strikes involving sabotage of basic core infrastructure (like, say, water treatment) seeing as how such would predictably involve large-scale damage, harm, and loss of life (Lucas 2011, Cook 2010).

### *1.3.7 Jus Post Bellum: The Aftermath of War*

The final phase of war is when the conflict is coming to an end. *Jus post bellum* concerns "justice after war." There is, perhaps surprisingly, very little international law regulating things in this regard. The preference, historically, has been for "the winner to enjoy the spoils of war:" i.e., for the war winner to impose whichever terms of peace it prefers upon the loser (Orend 2000a, 2002b). Generally, one of two approaches tends to be followed in this regard: retribution or rehabilitation.

- **Retribution**

According to **the retribution model,** the basic aspects of a decent post-war peace are these (and, crucially, they assume that "the good side" won, and that the aggressive side lost):

- A public peace treaty.
- Exchange of Prisoners of War (POWs).
- Apology from the Aggressor.
- War crimes trials for those responsible.
- Aggressor must give up any gains made during the war.
- Aggressor must be demilitarized, at least to avoid a repeat.
- Aggressor must suffer further losses. What makes this model one of **retribution** is the conviction that it is *not enough* for the defeated aggressor merely to give up what it wrongly took, plus some weapons. *The aggressor must be made worse off than it was prior to the war.* Why? The defenders of this model suggest several reasons. First, it is thought that justice itself demands retribution of this nature—the aggressor must be made to feel the wrongness, and sting, of the war which it unjustly began. Second, consider an analogy to an individual criminal: in domestic society, when a thief has stolen a diamond ring, we don't just make him give the ring back and take away his thieving tools. We also make him pay a fine, or send him to jail, to impress upon him the wrongness of his conduct. And this ties into the third reason: by punishing the aggressor, we hope *to deter or prevent* future aggression, both by him (so to speak) and by any others who might be having similar ideas.

But what will make the aggressor worse off? Demilitarization, sure. But two further things get frequently employed: *reparations payments* to the victims of the aggressor, plus *sanctions* slapped onto the aggressor as a whole. These are the post-war equivalent of fines, so to speak, on all of the aggressive society. Reparations payments are due, in the first instance, to the countries victimized and hurt by the aggressor's aggression and then, secondly, to the broader international community. The reparations payments are *backward-looking* in that sense, whereas the sanctions are more *forward-looking* in the sense that they are designed to hurt and curb the aggressor's future economic growth opportunities, at least for a period of time (a sort of probation) and especially in connection with any goods and services which might enable the aggressor to commit aggression again (Orend 2002b, 2006).

- **The Rehabilitation Model**

There is no sharp split between the retribution and rehabilitation models. They share commitment to the following aspects of a decent post-war settlement: the need for a public peace treaty; official apologies; exchange of POWs; trials for criminals; some demilitarization; and the aggressor must give up any unjust gains. Where the models differ is over three major issues. First, the rehabilitation model *rejects sanctions*, especially on grounds that they have been shown, historically, to harm civilians and thus to violate discrimination. Second, the rehabilitation model *rejects compensation payments*, for the same reason. In fact, the model favours *investing in* a defeated aggressor, to help it re-build and to help smooth over the wounds of war. Finally, the rehabilitation model *favours forcing regime change* whereas the retribution model views that as too risky and costly. That it may be, but those who favour the rehabilitative model suggest that it can be worth it over the long-term, leading to the creation of a new, better, non-aggressive, and even progressive, member of the international community. To those who scoff that such deep-rooted transformation simply can't be done, supporters of the rehabilitative model reply that, not only *can* it be done, it *has* been done. The two leading examples are West Germany and Japan after WWII (Orend 2000a, 2006).

Based on these best-case practices (Dobbins et al. 2003; Dobbins and Jones 2007), supporters of rehabilitation have devised their own list of desirable elements during the post-war period. The occupying war winner, during post-war reconstruction, ought to:

- *Adhere diligently to the laws of war during the regime take-down and occupation*.
- *Purge much of the old regime, and prosecute its war criminals*.
- *Disarm and demilitarize the society. (But then:)*
- *Provide effective military and police security for the whole country.*
- *Work with a cross-section of locals on a new, rights-respecting constitution which features checks and balances*.
- *Allow other, non-state associations, or "civil society", to flourish.*
- *Forego compensation and sanctions in favour of investing in and re-building the economy*.
- *If necessary, re-vamp educational curricula to purge past propaganda and cement new values*.
- *Ensure that the benefits of the new order will be: (1) concrete; and (2) widely, not narrowly, distributed*.
- *Follow an orderly, not-too-hasty exit strategy when the new regime can stand on its own two feet* (Orend 2006).

#### 1.3.7.1 Application of Jus post bellum to Cyber-War

It's unclear exactly how "post-war" norms apply to cyber-war, or broad-based computer attacks. I myself think there's much room for both manoeuvre, and hard,

ground-breaking work, on this subject. All I wish to point out is that there *is* a post-cyber-war phase, just as there is a post-conflict phase for every other kind of armed conflict, and so some principles of post-cyber-attack justice must come into play. I myself lean towards the rehabilitative model, more broadly, for reasons I've detailed exhaustively elsewhere (Orend 2012), and so I would insist above all on some kind of norm of potential "**Clean-up, and Aid with Restoration**" following a cyber-strike. Now, obviously, it depends crucially on the details of the strike: Stuxnet, e.g., evaporated and didn't cause spill-over damage to civilians, and so it's hard to see what duties of clean-up might meaningfully have been called for. But in the Russia/Estonia case, where people may have suffered real (mainly financial) hard-ship during their week of being blocked out from their banks, and not having access to government services, etc., some kind of actual monetary restitution might be in order.

Relatedly, it seems that there would be a *jus post bellum* norm calling for "**Public Accountability**", in terms of a public declaration of why a country resorted to a cyber-strike, and/or why it responded either kinetically or in a cyber way, to a cyber-attack. Both *jus ad bellum* and *jus post bellum* unite together to call, very strongly, for public accountability and transparency both before, and in the aftermath of, war.

As war crimes trials are called for *après la guerre*, so it would seem that cyber criminals need to be held accountable, and investigated for charges, following a cyber-strike. Such "**Trials for Cyber-Criminals**" would serve to underline and enforce the seriousness of their actions, and the attitude of the international community towards things like theft of intellectual property, espionage, and especially harm-causing acts of sabotage. Legal innovations are called for here, in order to bring such into reality (Dinniss 2012; Hyacinthe 2011).

Finally, it would seem as though some "**De-cyber-ization**" might be called for, if we follow the logic of demilitarization post-war. If cyber tools were used in an aggressive attack, then the international community, and especially any victims, are entitled to some reasonable security that they will not be made victim once more, in the near future, to the cyber-schemes of the aggressive power. How, exactly, to go about such stripping or curbing of cyber-power is, of course, beyond the ambit of this paper… and the cyber-skills of its author.

### *1.3.8 Middle Ground Judgment*

Now, this third section started off—a while ago—by saying that endorsement would be made of some kind of middle ground, in this case between realism and just war theory. Obviously, given all the effort just now put into describing the utility and sense of applying just war rules to cyber-warfare, it might be wondered how, exactly, I see a middle ground between just war theory and realism in this regard.

First, it must be noted how much middle ground there is *already* between realism and just war theory: many just war rules make not only moral sense but have clear benefits in terms of realistic self-interest. For example, there is clear over-lap

between the just war norm of proportionality and the military maxim of **an economy of force** (i.e., don't use more force than is strictly needed, as resources must be conserved and deployed only when most required). Last resort and probability of success could, straightforwardly, be stated either as moral, or as prudential, maxims of action. And, generally, many realists concur that, given war's huge costs and frightful risks, a rational leader should only contemplate war in response to an obvious and overwhelming danger, such as armed attack by an aggressive invader. Even the norm of discrimination and non-combatant immunity, which otherwise seems saturated with ethical intent, turns out to have potent prudential value as well: one only wants one's military resources, and killing force, to strike at actual sources of harm. Taking out civilians, and civilian targets, almost never directly advances military objectives: far better that one's bullets and bombs take out truly strategic targets that are part of the war machine of the enemy society. Relatedly, one can see how wrapping up a war well, and avoiding the creation of future generations of bitter enemies, can not only serve moral ends but also the long-term national interest of a self-regarding political community.

Secondly, in connection with cyber-war in particular, its very newness calls out for the combined resources of traditions of thought as formidable as realism and just war theory. Indeed, the moment today is arguably much like another moment in modern history: in the mid-1940s, when atomic weapons were just invented. (Here, indeed, *is* a legitimate sense in which reference to WWII is helpful and illustrative, as opposed to being off-key and exaggerated.) Now, as then, there's a brand-new technology of very considerable power and implication. There's absolutely no law regulating its use. Every country thus must do a calculus of self-interest to see how and whether this new tool fits into its self-image, its values, and its overall foreign-policy strategy. This is the least, we might say, that it owes its own people. From there, attempts can then be made to forge the equivalent of arms control agreements, bringing the technology into line and striving to keep it out of the hands of the most dangerous actors.

## 1.4 Optimism Vs. Pessimism

Which brings us to the final distinction: will we be able to achieve such control, such progressive agreement about when it is proper, and when illegal, to use cyber-warfare? The optimist says: why not? If we did it with something as ferocious as atomic and nuclear weaponry, we can do it with cyber-war technology. The pessimist would be inclined to cite how different cyber-technology is, how widespread and diffuse and more easily hidden it is, and comment darkly as to how, in many ways already, the world has devolved into a situation where, in cyber-terms, it is somewhat like a Hobbesian war of everyman against everyman, or at least every country against every country (Dipert 2011). The middle ground judgment here, in my view, would thus be that, while the pessimist probably provides an accurate description of the state-of-play as it presently stands, there are some historical grounds

for believing that, if we've been able to bring other forms of very destructive technology under control through international laws and arms control agreements, then we ought to be able to do the same things with the tools of cyber-war (Ventre 2010, 2011).

## 1.5 Conclusion

This paper—striving to dispel some of the fuzzy fog surrounding the fifth domain of warfare—first sought to define its terms, and then to consider in a substantial way three "big picture" distinctions surrounding informational warfare: (1) that between cyber-war-skeptic and cyber-war salesman; (2) that between realism and just war theory; and (3) that between optimist and pessimist. With regard to each distinction, it was argued that a middle ground judgment between the two seems the best and most promising way to understand the issue, and to wrestle with the many, and profound, challenges which cyber-war technology poses to the community of nations.

## References

Aristotle. 1984. *The politics*. Chicago: University of Chicago Press (Trans. by Carnes Lord.).
Brenner, S. 2009. *Cyber threats: The emerging fault lines of the nation-state*. Oxford: Oxford University Press.
Carr, J. 2010. *Inside cyber warfare*. London: O'Reilly.
CBS News. 2009. *60 min*. broadcast Nov. 06, 2009.
Clark, W. 2002. *Waging modern war*. New York: Public Affairs.
Clarke, R. 2010. *Cyber war*. New York: Harper Collins.
Clarke, R. 2012. *Cyber-war: The next threat to national security and what to do about it*. New York: Ecco.
Clausewitz, K. 1995. *On war*. Harmondsworth: Penguin, with quote at 64 (Trans. by A. Rapoport.).
Cook, M. 2010. Cyberation' and just war doctrine. *Journal of Military Ethics* 2010:417–422.
Dinniss, H. 2012. *Cyber-warfare and the laws of war*. Cambridge: Cambridge University Press.
Dipert, R. 2011. The probable impact of future cyberwarfare, paper delivered at *The First International Workshop on "The Ethics of Informational Warfare",* University of Hertfordshire (UK), July 1, 2011.
Dobbins, J., and S. Jones, eds. 2007. *The United Nations' role in nation-building.* Washington, DC: RAND.
Dobbins, J., et al. 2003. *America's role in nation-building.* Washington, DC: RAND.
Floridi, L. 2010a. *Information*. Oxford: Oxford University Press.
Floridi, L., ed. 2010b. *The cambridge handbook of information and computer ethics*. Cambridge: Cambridge University Press.
Gross, M. 2011a. The Fog of Cyber-War, *Vanity Fair* (April 2011), 155–198, with quote at 198.
Gross, M. 2011b. Enter the Cyber-Dragon, *Vanity Fair* (Sept. 2011), 220–234.
Hyacinthe, B. 2011. *Cyber-warriors at war*. New York: XLibris.
Ignatieff, M. 2001. *Virtual war: Kosovo and beyond*. London: Picador.
Johnson, J. T., and G. Weigel, eds. 1991. *Just war and gulf war*. Washington: University Press of America.

Kant, I. 1983. *Perpetual peace and other essays*. Indianapolis: Hackett (Trans. by T. Humphrey.).
Karatzogianni, A., ed. 2008. *Cyber-conflict and global politics*. London: Routledge.
Keegan, J. 1990. *The second world war*. New York: Vintage.
Keegan, J. 1994. *The first world war*. New York: Vintage.
Kissinger, H. 1995. *Diplomacy*. New York: Harper Collins.
Lucas, G. 2011. Just War Theory and Cyber-War, paper delivered at *The First International Workshop on* "*The Ethics of Informational Warfare*"*,* University of Hertfordshire (UK), July 1, 2011.
Lynn, W. J. 2010. Defending a new domain: The pentagon's cyberstrategy. *Foreign Affairs* 2010 (Sept./Oct.): 97–108.
Machiavelli, N. 1998. *The prince*. New York: Penguin Classics.
Menthe, D. 1998. Jurisdiction in cyberspace. *Michigan Technology Law Review* 69 (1998): 6–52.
Morgenthau, H. 1970. *Politics among nations*. 5th ed. New York: Knopf.
Murray, B., and R. Scales. 2003. *The Iraq war*. Cambridge: Harvard University Press.
New York Times. 2010. Malware Hits Computerized Industrial Equipment. *New York Times*, 24 Sept.
Orend, B. 1999. Crisis in Kosovo: A just use of force? *Politics* 19 (1999): 125–130.
Orend, B. 2000a. *War and international justice: A Kantian perspective*. Waterloo: Wilfrid Laurier University Press.
Orend, B. 2002b. Justice after war. *Ethics and International Affairs* 16 (1): 43–56.
Orend, B. 2006. *The morality of war*. Peterborough: Broadview.
Orend, B. 2009. *On war: A dialogue*. Lanham: Rowman Littlefield.
Orend, B. 2012. Justice after war: Towards a new Geneva convention. In *Ethics beyond war's end*, ed. E. Patterson, 175–196. Washington, DC: Georgetown University Press.
Orend, B. 2013. *Introduction to international studies*. Oxford: Oxford University Press.
Price, M. 2007. *The Wilsonian persuasion in American foreign policy*. New York: Cambria.
Rawls, J. 1993. *Political liberalism*. New York: Columbia University Press.
Regan, R. 1996. *Just war: Principles and cases*. Washington, DC: Catholic University Press of America.
Roberts, A., and R. Guelff, eds. 1999. *Documents on the laws of war*. Oxford: Oxford University Press.
Schmidt, H. 2006. *Patrolling cyberspace*. Washington, DC: Larstan.
Stallwood, O. 2012. Flame virus: How malware became the new weapon of war. *Metro News,* London, UK, 26 June.
The Economist. 2010. Special report on cyberwar: War in the fifth domain. *The Economist* 2010 (July 1): 18–26.
U.S. Congressional House. 2011. *Computer security: Cyber-attacks and war without borders*. Washington, DC: Books LLC.
USJFC. 2010. *Cyberwar report*. released Feb. 18, 2010. www.jfcom.mil.
Ventre, D. 2010. *Cyberguerre*. Paris: Hermes-Lavoisier.
Ventre, D. 2011. *Cyberespace et actueurs du cyberconflict*. Paris: Hermes-Lavoisier.
Walzer, M. 1977. *Just and unjust wars*. New York: Basic Books.
Woodward, B. 2004. *Plan of attack*. New York: Simon and Schuster.