Philos. Technol. (2015) 28:407–425
DOI 10.1007/s13347-014-0177-4

SPECIAL ISSUE

Cyber Force and the Role of Sovereign States in Informational Warfare

Ugo Pagallo

Received: 31 March 2014 / Accepted: 7 October 2014 / Published online: 17 October 2014

Abstract The use of cyber force can be as severe and disruptive as traditional armed attacks are. Cyber attacks may neither provoke physical injuries nor cause property damages and still, they can affect essential functions of today's societies, such as governmental services, business processes or communication systems that progressively depend on information as a vital resource. Whereas several scholars claim that an international treaty, much as new forms of international cooperation, are necessary, a further challenge should be stressed: authors of cyber attacks can be non-state actors, and identifying the party responsible for such a use of force, whether non-state actors or national sovereign states, is often impossible. Accordingly, several programmes on online security and national defence have been developed by sovereign states to tackle this menace and yet, the endurance of Western democracies and their aim to protect basic rights have already been tested by such programmes over the past years. The new scenarios of cyber force do not only concern the field of international law, since they may represent the main threat in the fields of national and constitutional law as well.

Keywords Cyber attack · Force · Information ethics · International humanitarian law · Laws of war · Sovereignty

1 Introduction

Two thousand years of debate on the characteristics of a just war were eclipsed three centuries ago in the modern Western world. Older just war theories no longer made sense after the triumph of modern legal positivism and the "paradigm of Westphalia", so-called after the 1648 series of peace treaties signed in Germany to conclude the Thirty Years War. In the classical phrasing of Thomas Hobbes in *Leviathan*,"[it] is annexed to the sovereignty the right of making war and peace with other nations and Commonwealths; that is to say, of judging when it is for the public good, and how great forces are to be assembled, armed and paid for that end" (Hobbes, Th 1999). By

U. Pagallo (✉)
Department of Law, University of Turin, Lungo Dora Siena 100, 10153 Torino, Italy
e-mail: ugo.pagallo@unito.it

admitting that no one is set to judge the decisions of sovereign states, no room was left to ascertain the lawfulness of the causes of war, as the law is made up by a set of rules effectively established by national sovereigns. The immunity of sovereigns finally ended with the Nuremberg trials (1945–1946), and projects for a permanent International Criminal Court (ICC) culminated with the Treaty of Rome in October 1999 and the ICC's work in The Hague from 1 July 2002. Far from claiming that a Kantian cosmopolitan paradigm has replaced the old legal system within current international humanitarian law, it was only with the end of the Cold War (1989) and the first Gulf War (1991) that the topic of just war again became a popular topic of debate among lawyers.

Legal scholars have increasingly debated in the past 25 years the many conditions that make a war just, such as whether a legitimate claim exists and violence can be admitted as a last resort, whether there is a probability of success and proportionality in the use of force, down to matters of proper authority and whether a declaration of war is always necessary. Such conditions are traditionally distinguished between the causes legitimating war in the sense of *jus ad bellum*, and the behaviour admitted in warfare in the sense of *jus in bello*.[1] As to the preconditions for war to be deemed just, we have to further distinguish between formal and substantial criteria. On the one hand, the formal preconditions that make a war just include a basic tenet of the Westphalian paradigm, such as the Leviathan's monopoly on the legitimate use of force: wars need to be declared by the competent authority of national sovereign states, so that such authority can be held responsible for operations occurring in the course of the war. The substantial reasons of just war in the sense of *jus ad bellum*, on the other hand, traditionally comprise the good intention of the war-declaring authority, the reasonable success of war and especially in today's context, the use of force as the last option. In the phrasing of Article 51 of the United Nations (UN) Charter, "nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations", and thus, an armed attack, save in self-defence, can only be used if authorised by the UN Security Council. Moreover, the use of force should be proportional to the good achieved by war, so that, as a necessary condition for legal *jus ad bellum*, states cannot wage a massive war to remedy a trivial wrongdoing, as it occurred with the 1969 Soccer War between El Salvador and Honduras.

In addition to the causes of just war, a second set of legal provisions concerns principles of military conduct and rules of engagement as criteria of just war in the sense of *jus in bello*. When analysing the conditions rendering conduct lawful on the battlefield, scholars usually distinguish between discrimination and non-combatant immunity, the doctrine of double effect and the principle of proportionality. The focus of the legal analysis is therefore on the military necessity in fixing criteria for the target identified as a legitimate combatant: once political and military authorities have granted the use of force, such "military necessity" may allow collateral damage, in accordance with the doctrine of double effect and the tactics for engagement, approach and standoff

[1] Besides the traditional distinction between causes (*jus ad bellum*) and conditions (*jus belli*) of just wars, lawmakers have added a third scenario, that is the provisions for the aftermath of warfare, or *jus post bellum*. In this paper, the classical bifurcation between *jus ad bellum* and *jus belli* suffices to describe basic tenets of today's legal framework that may be affected by a new generation of informational attacks.

distance. Such a use of force, however, should be further understood in connection with the aforementioned principle of discrimination and non-combatant immunity that requires distinguishing between civilians and combatants and between friends and foes, so as to direct force only against enemy military objectives. The principle of proportionality also sets the necessary conditions for legal *jus in bello* that impose further restrictions on war fighting techniques: no unnecessary violence can be used in order to attain one's military ends; rather, the level of force should be proportioned to the goal of attaining such ends.

In light of this framework on the current laws of war (LOW), much as the rules of international humanitarian law (IHL),[2] scholars have further debated in the last years whether the information revolution has affected both principles and clauses of LOW and IHL. Here, we should take into account a basic fact: whereas, over the past centuries, human societies have used information and communication technology (ICT), but have been mainly dependent on technologies that revolve around energy and basic resources, today's societies are increasingly dependent on ICT and, furthermore, on information as a vital resource. Essential functions of today's societies, such as governmental services, transportation and communication systems, business processes or energy production and distribution networks, depend on the use of computer platforms. Face-to-face with the benefits of this profound transformation, such ICT-dependency entails however its own risks, because "the near absolute dependence of critical infrastructure on cyberspace looms particularly large as a security concern" (Schmitt 2014, p. 273). Consequently, scholars have focused on a new class of aggressions, dubbed as informational attacks or cyber attacks, conceived as "any action taken to undermine the function of a computer network for a political or national security purpose" (Hathaway et al. 2012, p. 826). A typical illustration is given by the distributed denial-of-service (DDOS)-attacks against both the Republic of Estonia in April 2007 and Georgia in summer 2008, which interrupted, or paralyzed, some critical services and infrastructures of those countries. Further forms of digital assaults comprise the syntactic and semantic attacks: in the former case, the aim is to infect a computer's operating system through viruses, worms and Trojan horses, namely programs that aim to produce the malfunctioning of a computer network. In the case of semantic attacks, the purpose is either to insert inaccurate information in the computer system, or to modify correct information processed by such system, so that computers seem to work properly, even as they malfunction (Libicki 1995). As a result, how then, and to what extent, do such attacks affect current LOW and IHL?

Some forms of informational aggression can be a means for real-world operations. For instance, in the words of the former US Secretary of Defence, Leon Panetta, by penetrating another nation's networks and computers "an aggressor nation… could derail passenger trains, contaminate the water supply in major cities, or shut down the power grid across large parts of the country" (in Schmidt and Cohen 2013, p. 104). Hence, it seems that the impact of an informational attack on real-world targets can be

[2] In addition to the UN Charter and customary law, LOW and IHL refer to the 1907 Hague Convention, the four Geneva Conventions from 1949, and the two 1977 additional Protocols.

properly addressed with the current provisions of LOW and IHL, either directly or by the use of analogy, in accordance with the remarks of Philip Alston in the 2010 Report to the UN General Assembly on extrajudicial, summary or arbitrary executions. As the UN Special Rapporteur affirms, "a missile fired from a drone is no different from any other commonly used weapon… The critical legal question is the same for each weapon: whether its specific use complies with IHL" (Alston 2010, § 79). However, things can be trickier both in the case of informational forms of aggression that precede, or prepare, a conventional physical assault, and in the case of informational attacks that do not entail any physical violence, for they aim to remove or annihilate informational resources from cyberspace or delete them without backup. Accordingly, "at what point does a cyber attack become an act of war?" (Schmidt and Cohen 2013, p. 114). How can we determine "when a cyber-attack constitutes an armed attack that triggers the right of armed self-defense"? (Hathaway et al. 2012, p. 845). Do such scenarios of LOW and IHL affect key elements of national law?

In order to shed light on some critical aspects of these legal issues, two challenges of information warfare will be here under scrutiny, i.e., how the notion of force and the role of sovereign states may change in the new context. The paper is presented in three parts, which are structured as follows: next, Section 2 examines the legal notion of force, how LOW and IHL have regulated it so far and to what extent the information revolution is reshaping such a notion of force with the different types of cyber attacks mentioned above. This outlook will clarify the question on the point at which a cyber attack may become an act of war, or constitute an attack that triggers the right of armed self-defence. Then, the paper dwells on the open issues of today's debate. Although scholars are increasingly stressing the uniqueness of the challenges brought on by the use of cyber force, they have failed to provide a coherent theory with which canonical targets of real-world operations on the battlefield can be compared with the new means of informational warfare. Section 3 aims to fill this gap by reinterpreting traditional causes and conditions of just war theory in light of Luciano Floridi's ethics of information (Floridi 2013). In accordance with such a moral common framework for real-world and cyber operations, the paper considers how the role of sovereign states may change. Four different scenarios of cyber attacks are taken into account in Section 4, so as to pinpoint some legal challenges of informational warfare that concern the field of national, rather than international, law. In addition to the problematic notion of force in cyberspace or the assumption that sovereign states represent the only war-declaring authorities in the international arena, further cases related to the fields of criminal and constitutional law should be examined, such as the reaction of sovereign states against non-state actors deemed as the responsible party for a cyber attack, and the protection of basic rights in the national law field vis-à-vis the claim of sovereign states to monopolize the legitimate use of force within a given territory. Whilst most scholars admit that current LOW and IHL may fall short in coping with the new scenarios of informational warfare, would the latter similarly impact crucial tenets of national law? How about the difference between cybercrimes and cyber attacks? Moreover, how about the balance that should be struck between the protection of fundamental rights and national security purposes?

2 The Use of Force in Cyberspace

There are four different ways in which scholars usually address the connection between force and law:

(i) Force as a state of conflict opposed to the legally regulated human interaction, e.g. Thomas Hobbes's version of the "state-of-nature" in which the man is a wolf to the other men, as contrasting with the "civil society" of modern contractualism;
(ii) Force as the fundamental principle of both politics and legal systems, e.g. Trasimacus's idea of justice as the "advantage of the stronger" as discussed in the first book of Plato's *Republic*;
(iii) Force as a means of legal enforcement, e.g. Hans Kelsen's idea of the law as a set of commands enforced through the menace of physical sanctions, so that "the decisive criterion is the element of force—that means that the act prescribed by the order as a consequence of socially detrimental facts ought to be executed even against the will of the individual and, if he resists, by physical force" (Kelsen 1967: 34);
(iv) Force as the subject of legal regulation, e.g. the rules of criminal, civil or administrative law, determining how the acts prescribed by the legal order should be executed in a given case.

Some of these different levels of analysis are, of course, strictly connected: for instance, once the inquiry dwells on force as the decisive criterion of the law, i.e. level (iii) of the analysis, we should further understand the ways in which such a use of force is regulated by the legal system, i.e. level (iv) of the analysis. In this context, however, suffice it to mention the latter connection between force and law, in order to comprehend how force, as the subject of legal regulation, may change with the new scenarios of informational warfare. Accordingly, this section is divided in three parts: first, attention is drawn to the traditional regulation of force in the international law field (Section 2.1). Then, focus is on whether this framework is evolving in connection with different types of cyber attacks (Section 2.2). Finally, the aim is to stress the set of issues that are still open at this level of analysis in the legal field (Section 2.3).

2.1 The Use of Force in International Law

Articles 2, 39 and 51 of the UN Charter define the conditions that make the use of force lawful in the international field. As a general rule, the fourth paragraph of Article 2 states "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." As mentioned above in Section 1, there are nonetheless two exceptions to this general prohibition on the threat or use of force. Besides cases of self-defence pursuant to Article 51, Article 39 establishes the power of the Security Council to "determine the existence of any threat to the peace, breach of the peace or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security."

As to the meaning of these clauses, scholars commonly agree that the prohibition of Article 2 (4) does not include any type of political, or economic, coercion; vice versa, every kind of armed attack should be understood as a use of force. More particularly, according to the jurisprudence of the International Court of Justice (ICJ) in the *Nicaragua case* from 27 June 1986, an attack need not to entail either the use of kinetic force or non-kinetic operations with similar effects, in order to be deemed as a use of force. Still, such attack should represent "most grave forms of the use of force" to trigger a nation's right to self-defence. For instance, cross-border incursions that are minor in their "scale and effects", can be conceived as a "frontier incident" rather than "armed attacks"; yet, a state that arms and trains guerrilla forces to engage them in hostilities against another state, should be considered as a use of force (ICJ 1986, §§ 195 and 228). In these latter cases, the customary law norm of non-intervention which prohibits states from interfering in the internal affairs of other states, complements the general prohibition of Article 2 (4), for "acts constituting a breach of the customary principle of non-intervention will also, if they directly or indirectly involve the use of force, constitute a breach of the principle of non-use of force in international relations" (ICJ 1986, § 209). On this basis, we should distinguish three possible scenarios:

(i) An attack that does not amount to the use of force;
(ii) An attack that can be properly understood as a use of force pursuant to Article 2 (4) and eventually, in accordance with the customary principle of non-intervention;
(iii) The use of force that triggers the right to self-defence pursuant to Article 51.

Leaving aside the first case, scholars have debated over the past years whether scenarios (ii) and (iii) make sense in the case of cyber attacks (Roscini 2010; Schmitt 2011; Waxman 2011; etc.). The discussion has correspondingly revolved around whether a non-destructive cyber operation can amount to an un/lawful use of force (scenario ii), much as whether a cyber attack can rise to the level of an armed attack (scenario iii). Although scholars have progressively conceded the first hypothesis, crucial doubts persist when comparing traditional "grave forms of the use of force", according to the phrasing of ICJ, with new forms of cyber attacks. After all, how about the distinction between cyber attacks as a means for real-world operations and the class of strict informational attacks mentioned above in the introduction?

2.2 The Evolution of Force in Cyberspace

Most scholars admit that even non-destructive cyber attacks can represent a use of force in the sense of the UN Charter's Article 2 (4). For example, the group of experts that drafted the "Tallinn Manual on the International Law Applicable to Cyber Warfare", reckons that the Stuxnet virus, which halted almost one fifth of the Iranian nuclear facilities in 2010, should be considered as a use of force (Schmitt 2013: p. 45). Moreover, some are keen to declare that even strict informational attacks can force states to desist from—or to engage in—a particular course of action (Schmitt 2014). Consequently, most of today's debate does not centre on whether a cyber attack should be understood as a use of force, that is, the second scenario mentioned above in Section 2.1. Rather, the

discussion concerns whether such a use of cyber force can rise to the level of an armed attack, thus triggering a nation's right to self-defence pursuant to Article 51 of the UN Charter.

Three different approaches should be mentioned: to start with, some affirm that strict informational attacks cannot rise to the level of an armed attack, since they lack "the physical characteristics traditionally associated with military coercion" (Hollis 2007, p. 1041). Yet, most reject this approach "as dangerously outdated… because cyber-attacks have the potential to cause catastrophic harm without employing traditional military weapons" (Hathaway et al. 2012, p. 817).

Others claim that a cyber attack should be considered as an armed attack whenever it targets a critically important computer system of a nation's infrastructure network, regardless of whether such attack has provoked physical damages, casualties or destruction (Sharp 1999, p. 129). However, most scholars criticize this target approach, because it perilously lowers the threshold of entry into war, by legitimizing a nation's use of anticipatory self-defence in response to any attempt to infiltrate critically important computer networks of that nation (Sklerov 2009; Hathaway et al. 2012; etc.).

The limits of both the traditional stance and the target approach to the new scenarios of informational warfare have suggested scholars to increasingly draw the attention to the effects of a cyber attack. As the Tallinn Manual recommends, such effects should include (not only but also) the severity of the attack, its immediacy, directness, invasiveness, military character, state involvement and presumptive legality (Schmitt 2013, p. 47–52). Whilst the Tallinn Manual's criteria can be used to determine if a cyber attack is a use of force, these criteria do not address whether a cyber attack goes far enough to be an armed attack for the purpose of self-defence under Article 51. Some, as the former General Counsel of CIA and National Security Agency (NSA), Daniel Silver, have thus proposed to restrict such criteria, by justifying a nation's right to self defence in response to a cyber attack "only if its foreseeable consequence is to cause physical injury or property damage and, even then, only if the severity of those foreseeable consequences resembles the consequences that are associated with armed coercion" (Silver 2001, p. 90–91).

There are a number of reasons why this latter approach, namely the foreseeable severity-perspective, has become popular. By avoiding the shortcomings of both the traditional and target approaches, the foreseeable severity-perspective focuses on a limited set of criteria, such as the foreseeable severity of physical injuries or of property damages provoked by a cyber attack. This limited focus reduces the risk that the use of cyber force may lead to war. In the wording of *The Law of Cyber-Attack*, "this final version of the effects-based approach provides the best balance between enabling states to adequately respond to catastrophic cyber-attacks and preventing states from resorting to armed force too easily" (Hathaway et al. 2012, p. 848). Such a balance, however, presents some limits of its own, once we take into account such a class of cyber-attacks, previously dubbed as strict informational attacks, which can be as disruptive as traditional armed attacks are and nevertheless, aim to provoke neither physical injuries nor property damages but rather, to affect informational resources in cyberspace. All in all, the more we deal with ICT-driven societies, i.e. societies that depend on information as a vital resource, the more it is likely that scholars and decision makers should take this neither physical nor property approach seriously.

Some advocates of the effects-based approach concede this point, when examining further restrictions on the use of force, such as the IHL rules governing the conduct of attacks, pursuant to Articles 51 and 57 of the 1977 Protocol I to the Geneva Conventions; whilst such rules prohibit any form of indiscriminate attack or prescribe special precautions with respect to attacks that can cause damage to civilian objects, "it can be difficult to evaluate whether an attack would be proportional according to the relevant categories of" IHL (Hathaway et al. 2012, p. 851). Since essential functions of today's societies progressively depend on the processing of data, it follows that crucial categories of IHL, such as notions of "damage" and "object" will likely evolve, so as to include the impairment of cyber infrastructures, much as the destruction of data. In the words of Michael N. Schmitt, the overall idea is that "IHL will assuredly evolve to meet the shift in the relative importance of physical and virtual entities" (Schmitt 2014, p. 297). By complementing the effects-based approach with the virtual effects of strict informational attacks, let us explore how far this idea goes separately.

2.3 Open Issues of Force in Informational Warfare

In order to fully appreciate a key legal challenge of informational warfare, i.e. new forms of cyber force that rise to the level of armed attacks, consider the following scenarios. First, a strict informational attack against key governmental functions, or services in the public health sector, for social protection and education, labour and so forth, with the aim to bring these services to a halt. Similarly, contemplate a strict informational attack against a nation's air traffic control system, or the traffic light system of cities, that shuts these systems down through a series of syntactic attacks. Here, people would finally stop flying or driving, because of the insecurity of the entire communication system. To cut to the chase, what these examples show is a class of cyber attacks that are neither physical nor strictly property-related and still, can be as "severe" as armed attacks typically are. Once a state finds itself trapped in this sort of informational stalemate, a mere resort to the customary international law of countermeasures seems hardly viable or at least, "far from panacea" (Hathaway et al. 2012, p. 858). It is unclear how effective countermeasures will be in response to a cyber attack. If active defence is deployed to interrupt an ongoing attack, it may be ineffective. If the countermeasure targets the systems of the alleged responsible party, that also may not mitigate the harm to the systems of the original victim. As a result, a number of such situations will likely justify a nation's right to self-defence pursuant to Article 51 of the UN Charter.

Interestingly, this is the scenario stressed by Michael N. Schmitt's (2014) paper on *The Law of Cyber Warfare*: *Quo Vadis*? In his view, non-destructive cyber attacks may be interpreted as "presumptive uses of force", much as the destruction of data that severely disrupts societal, economic or governmental functions, may come to be viewed "as the functional equivalent of physical destruction for use of force characterization purposes" (Schmitt 2014, p. 281). A way to overcome the shortcomings of the effects-based approach introduced above in the previous section, can thus be expanding the notion of "foreseeable severity" so as to add cases of informational severity to those of physical injury and property damage. Because we are increasingly dealing with ICT-driven societies, considering the virtual severity of the attack as important as its physical, or proprietary,

counterpart makes a lot of sense, since undermining the function of critical computer networks, much as destroying or removing data without backups, can be of much greater impediment than their physical equivalents.

The principle of informational severity, to be sure, concerns both the causes legitimating war in the legal sense of *jus ad bellum*, and what is admitted on the battlefield in the legal sense of *jus in bello*. In addition to the cases in which a non-destructive cyber attack can rise to the level of an armed attack, thereby triggering the right to self-defence pursuant to Article 51 of the UN Charter, a broad interpretation of the notions of "damage" and "object" in accordance with Articles 51 and 57 of the 1977 Protocol I to the Geneva Conventions should equally be expected. Whilst the legal definition of object will probably evolve so as to include the notion of data, the notion of damage will likely comprise some effects of strict informational attacks on the functionality of essential cyber infrastructure, much as the act of obstructing basic services. Still, by complementing the effects-based approach with the principle of informational severity, we have to face two further problems.

First, it remains unclear how, in the words of Schmitt, "as cyber activities become even more central to the functioning of modern societies, the law will impose obligations on States to act as responsible inhabitants of cyberspace, lower the point at which cyber operations violate the prohibition on the use of force, allow States to respond forcefully to some non-destructive cyber operations, and enhance the protection of cyber infrastructure, data and activities during armed conflicts" (Schmitt 2014, p. 299). Even though this overall picture on current trends of informational warfare may look sound, a normative standpoint should provide the measuring stick for such conclusions. What kind of new obligations, if any, shall the law impose on states as "responsible inhabitants of cyberspace"? What does it mean responsibility in this new informational context? How much would the latter lower the threshold of entry to war? We return to this in Section 3.

Second, a tenet of the effects-based approach, namely the notion of "foreseeability", is problematic. In order to determine whether the "foreseeable consequence" of a cyber attack has to do with the materialization of injuries and damages (Silver 2001, p. 90–91), the level of risk for the use of different types of cyber force that can trigger a nation's right to self defence, should be determined on the basis of the probability of the events, their consequences and costs. As it occurs in other fields of informational warfare, e.g. robotic weapons, it can be tricky and even impossible to predict the consequences of such attacks (Pagallo 2013a). As a 2007 US Navy-sponsored research admits in the field of *Autonomous military robotics*, "we may paradoxically need to use the first deaths to determine the level of risk" (Lin et al. 2007, p. 68). Of course, if it is likely that the use of cyber force will continue to increase, we still can hold military commanders and competent political authorities strictly responsible for all the consequences of such cyber attacks. And yet, the unpredictable consequences of the use of cyber force reverberate on further aspects of LOW and IHL. Even advocates of the effects-based approach admit this point: consider, for example, a DDOS-attack that blocks the communications of vital information in hospitals and hence, leads to loss of life. As Hathaway et al. stress in the paragraph on *in bello proportionality* (in Hathaway et al. 2012), a DDOS attack

may carry a much greater degree of uncertainty than would a conventional attack, because anticipating the probable consequences of such an action can be "much more difficult in the cyber context. As a result, cyber-attacks may change the weight given to temporary consequences, and may force states to confront more uncertainty" (*op. cit.*, p. 851).

The difficulty brings us back to the peculiarity of strict informational attacks and the ways in which the good achieved by such attacks can be compared with the evil of waging them in cyberspace. Since we lack specific rules on the subject matter, such as provisions that regulate the use of strict informational attacks in LOW and IHL, how can scholars address this set of legal issues?

3 A Common Framework for Real-World and Cyber Operations

So far, we have seen how scholars resort, either directly or by the use of analogy, to the current provisions of LOW and IHL, in order to address the challenges of information warfare. Although this approach is at times useful, e.g. applying such provisions to the class of cyber attacks as a means of real-world operations, further cases show the limits of this method. Analogy, let alone literal interpretations of today's legal framework, often falls short in coping with the new dimensions of informational warfare, once we take into account how the notion of force is changing with the class of strict informational attacks and some open issues of cyber proportionality, such as the temporary consequences of DDOS attacks. Moreover, the clause of immunity summed up, in continental Europe, with the formula of the principle of legality, i.e. "no crime, nor punishment without a criminal law," sets further limits to the applicability of analogy. As established, for example, by Article 7 of the 1950 European Convention on Human Rights (ECHR), individuals can be held criminally liable for a given behaviour, only on the basis of an explicit criminal norm. So, scholars have increasingly been claiming that an international treaty, much as new forms of international cooperation on evidence collection and criminal prosecution, are necessary (Clarke and Knake 2010; Hathaway et al. 2012; etc.). Yet, a new international agreement on some critical aspects of informational warfare may not only take a long time, but this stalemate will likely continue as long as sovereign states think they can exploit the loopholes of the current legal framework due to their technological superiority or strategic advantage. Waiting for a new agreement in the long run, how should we address today's legal challenges?

A fruitful approach is given by a morally coherent theory, such as Luciano Floridi's ethics of information. This perspective allows us to reinterpret traditional causes and conditions of just war theory, so as to fill some gaps of current LOW and IHL through a common framework for both real-world and cyber operations. In a nutshell, Floridi's ethics of information can be presented as an "ontocentric", "patient-oriented" and "ecological macro ethics" (Floridi 2008, 2013). By rejecting a rigid methodological anthropocentrism, this theory calls for a wider perspective than that based exclusively on the role of human agents. The informational outlook also suggests a different understanding of the interaction between agents and receivers or reagents, assuming the "level of abstraction" which asserts that all entities should be represented in terms of information. In the phrasing of (Floridi 2008, p. 21), "all entities, *qua* informational objects, have an intrinsic moral value, although possibly quite minimal and overridable,

and hence can count as moral patients, subject to some equally minimal degree of moral respect understood as a disinterested, appreciative and careful attention." The aim is not only to explain how interacting agents communicate and share informational resources by means of positive or negative messages: in accordance with the ontocentric stance of this theory, the tenets of information ethics provide a unified perspective for varying statuses and regimes that concern the content of such resources, regardless of the specific technologies with which we are dealing and in an impartial and universal way (Pagallo and Durante 2009). What Floridi calls the ontological equality principle means that the resources of the system are deemed informational entities that should morally be treated as part of the environment or infosphere, bringing to "ultimate completion the process of enlargement of the concept of what may count as a center of moral claim" (Floridi 2008, p. 12). As a result, a universal normative framework should govern the life cycle of information within the infosphere in a field-independent way and in connection with the ontological equality principle, in an impartial manner. More specifically, this normative framework hinges on the concept of informational entropy, which is structured according to four moral laws. Whilst informational entropy "refers to any kind of destruction or corruption of informational objects (mind, not of information), that is, any form of impoverishment of being" (Floridi 2008, p. 11), the four moral laws command that:

1. Entropy ought not to be caused in the infosphere (null law)
2. Entropy ought to be prevented in the infosphere
3. Entropy ought to be removed from the infosphere
4. The flourishing of informational entities, as well as the whole infosphere, ought to be promoted by preserving, cultivating, enhancing and enriching their properties

In light of this normative framework, let us go back to the open issues of informational warfare, so as to bridge the gap between the traditional principles of LOW and IHL, and the set of parameters that should regulate cases of cyber warfare. First, canonical causes and conditions of just war can be reinterpreted in accordance with these moral laws, that is, as just exceptions to them. For instance, in light of the laws which prescribe that entropy shall not be caused, or it should be prevented in the informational environment, causes of just war as self-defence (*jus ad bellum*), much as conditions of *jus in bello* like the principle of proportionality, should be deemed exceptional cases in which the use of force is necessary. The reasons for this legitimate necessity are traditionally given as either the aim of removing entropy from the infosphere, for example, by defeating another nation's unjust aggression, or preventing the creation of further entropy through the means of self-defence, a pre-emptive attack and so forth. The tenets of information ethics allow us to grasp the common ground between traditional targets of real-world operations and the new means of informational warfare, because all the entities that are at stake can be understood in terms of information. This is why, in the words of Michael N. Schmitt, the law has to impose obligations on states as "responsible inhabitants of cyberspace" (Schmitt 2014, p. 299). In addition to cases of physical injury or property damage, we should consider the virtual severity of a cyber attack as important as its traditional real-world counterparts.

Second, the ontological equality principle does not aim to equate, say, human resources with such informational tools as networks and computers. Rather, the

informational outlook intends to provide a universal normative framework with which to govern the life cycle of information in an impartial manner. The lawfulness of virtual, as opposed to physical, force can thus be determined and compared with the legitimacy of the military goals that a nation aims to attain in the real world, by tracing them back to the second and third laws of information ethics. As previously stated, the causes legitimating war, much as the behaviour admitted in warfare, concern either the aim to prevent the creation of further entropy on the battlefield, or the goal of removing such entropy from the informational environment. Although these scenarios are closely related to the principle of proportionality, attention is drawn to a different aspect of the problem. Focus is here on the proportion, and comparison, between real-world operations, tactics and ends of just war that are traditionally associated with armed coercion, and their informational counterparts in cyber warfare. The notion of entropy in the second and third laws of information ethics paves the way for a sound definition of responsibility in cyberspace that shall prevent that challenges of informational warfare may lower the threshold of entry to war. Whereas, in accordance with the null law of information ethics, the point at which cyber operations violate the prohibition on the use of force should be lowered (Schmitt 2014, p. 299), the virtual effects of cyber attacks have to be as severe as the entropy related to armed coercion, in order to justify a nation's right to self defence.

Third, the outlook of information ethics allows us to deepen the scenarios illustrated in Section 2.3, i.e. the conditions rendering a strict informational attack lawful. Consider a cyber attack against a nation's air traffic control system vis-à-vis a frontier incident, or in response to a state's unjust aggression. To start with, we have to pay attention to the amount of entropy that is caused by such an attack aiming to obstruct, remove or annihilate the informational resources in cyberspace. Then, in light of the null law of information ethics, we have to evaluate the amount of entropy provoked by the attack with the second and third laws mentioned above, that is, the amount of entropy which was prevented by that cyber attack (second law), or the amount of entropy which was removed from the infosphere via the cyber attack (third law). Here, the set of criteria developed by advocates of the effects-based approach, either physical or property-related, can appropriately be complemented with the principle of informational severity. The aim is not only to determine the different ways in which a cyber attack should be viewed as a new use of force in LOW and IHL (null law); but moreover, whether such a use of cyber force is legitimate (second and third laws). On this basis, the laws of information ethics help us to tackle the tricky scenarios of proportionality conceived as both a cause and a condition of just war.

In the case of *jus ad bellum* and whether the good achieved by an informational attack is proportionate to the evil of waging it, we can determine that good in conformity with the second and third laws of information ethics so as to compare the military ends with the evil that is defined by the null law in terms of entropy. Going back to the example of a cyber attack against a nation's air traffic control system, the entropy provoked by such an attack (null law), may be justified in response to the unjust aggression of a nation state (third law), but deemed excessive in the case of a frontier incident (second law). A similar ratio is at work in the case of *jus in bello* and whether the level of virtual, as opposed to physical, force is proportionate to attain a nation's military end: the evil of the null law, which is provoked by the cyber attack against a nation's air traffic control system, should be grasped in accordance with the

good that is illustrated by the second and third laws. The aim is to determine whether the level of that informational attack has to be deemed excessive vis-à-vis a frontier incident (second law), a nation's unjust aggression (third law), etc. Notwithstanding such a similar ratio, which is, after all, the reason why scholars usually refer to proportionality as both a cause and condition of just war, a crucial difference has to be stressed: whereas a proportionate cause to go to war may be ruined by an excessive use of violence, either virtual or real, a reasonable use of force cannot redeem a futile motive for fighting.

Admittedly, the devil is in the detail. From a legal point of view, a number of issues are fated to remain open in the new context, including whether a nation's resort to war abides by such a context-dependent and fact-intensive principle, as the non-excessive use of cyber force in the name of the proportionality principle. However, the realignment of these problems through the lens of information ethics does not mean that these issues are over, but rather that we can properly address them by taking into account both the ways in which these problems are reshaped by the means of the information revolution and how a normative framework, such as the moral laws of information ethics, can guide us throughout this huge transformation. Think about such uncertainties that have traditionally affected both LOW and IHL, as the good intention of the war-declaring authority and the reasonable success of war in the field of *jus ad bellum*, much as the principle of distinction between civilian and military objectives, i.e. the "dual use" issue in the field of *jus in bello* (Hathaway et al. 2012, p. 851–852; Schmitt 2014, p. 298; etc.).

Still, we have to widen the spectrum of the analysis: so far, attention has been drawn to the content of current LOW and IHL in terms of the causes and conditions that make wars just. Yet, the information revolution also impacts on the pillars of this traditional framework as a matter of procedure, rather than substance, in order to define the authority that may properly enter the informational wars. Is there any crucial difference between old and new scenarios?[3]

4 New Scenarios of Sovereignty

The current legal framework of LOW and IHL can be grasped as a sort of compromise between a basic tenet of the Westphalian paradigm, i.e. the sovereignty of nation states, and a post-Westphalian model of international law that restrains what Hobbes called the sovereign right of making war and peace with other nations and commonwealths. Pursuant to the UN Charter and save in cases of self-defence, force can only be used if the UN Security Council authorises it, and yet, states are deemed the only relevant actors in the field of international law and more specifically, the only proper authority to declare and enter wars. The information revolution, much as the expansion of the

[3] By examining causes and conditions of just war through the lens of the moral laws of information ethics, you may wonder what role the fourth law plays in this context, namely the aim to promote "the flourishing of informational entities as well as the whole infosphere… by preserving, cultivating, enhancing and enriching their properties" (Floridi 2008). This moral law is very important for the laws of war, particularly in the field which scholars traditionally sum up as *jus post bellum. This* paper only deals with the challenges of *jus ad bellum* and *jus in bello*, and so I have skipped this part of the analysis on *jus post bellum*, on which see chapter 7 of Schmidt and Cohen (2013).

international community and the globalization of environmental and economic issues, are however affecting this traditional role of nation states: the increasing dependence of societies on information as a vital resource challenges the aim of sovereign states to monopolise the use of force in cyberspace, the new domain of military operations. Moreover, authors of the new generation of informational attacks can be non-state actors, and identifying the party responsible for such attacks, whether non-state actors or traditional sovereign states, is often impossible. Whilst this very difficulty affects the principle that wars need to be declared by competent authorities, it also lowers the traditional barriers to enter into war, since anonymity may trigger new temptations for exploitative attacks and shelter the anonymous informational offender from the reaction of others. Some insist on such trends as the privatisation of war and the role of "corporate warriors" (Singer 2008); others have attempted to define a "new paradigm of international law" (e.g. Schreuer 1993); "a new paradigm of inter-state relations" (e.g. Cullet 1999); etc. In this context, suffice it to stress the different ways in which the information revolution may impact a crucial aspect of LOW and IHL, i.e. the procedural precondition for legitimating the war as the proper war-declaring authority, in order to cast light on how nation states may react against this further set of legal challenges. Four different scenarios with their variables are taken into account: the common ground is given by a nation state that identifies or submits evidence as to the identity of the party responsible for a cyber attack. How should a state react in these cases?

The first scenario can be dubbed as the constitutional one: the party responsible for a cyber attack is a non-state actor and in response to such aggression, a nation state intends to prosecute it pursuant to its own criminal laws and eventually, in accordance with such international provisions as the rules of the Budapest Convention on cybercrime. Although the aim of the non-state actor was to undermine the function of a computer network for a political or national security purpose, the constitutional response of the state can depend on two different views. On the one hand, as suggested by *The Law of Cyber-Attack*, we can imagine that "the consequences of this act would not rise to the level of an armed attack" (Hathaway et al. 2012, p. 836), so that such a cyber attack by the non-state actor should be properly conceived as a cybercrime.[4] On the other hand, *pace* Hathaway et al., such attack may amount to an armed attack, thereby constituting an act of cyber warfare and still, the nation state proceeds in accordance with its criminal laws. The latter is the case of most European antiterrorism laws vis-à-vis the right to a fair trial under Article 6 of the European Convention on Human Rights (ECHR).

The second scenario resembles the first with one crucial difference: here, in response to an informational attack, the state conceives the non-state actor as a combatant enemy under current LOW or regardless of such rules, due to the evil nature of the aggression, e.g. derailing passenger trains by penetrating a nation's computer network. Whereas the national constitutional laws of the first scenario often provide for a stronger level of

[4] Theoretically speaking, we can imagine a cyber attack by non-state actors that does not rise to the level of an armed attack and still, does not constitute a cybercrime. However, authors of *The Law of Cyber-Attack* admit that "it is unlikely for a private actor to purposefully undermine the function of a computer network without also violating the law" (*op. cit.*, p. 835).

protection than terms and conditions of international LOW, three different hypotheses can lead to the second scenario:

(i) The cyber attack by the non-state actor rose to the level of an armed attack and thus, *pace* most European antiterrorism acts, such attack entails a cyber warfare scenario that should be regulated by LOW (e.g. Hathaway et al. 2012: p. 835);
(ii) The cyber attack by the non-state actor was carried out in the context of an armed conflict, "provided those actions could not be considered cyber-crimes, either because they do not constitute war crimes, or do not employ computer-based means, or both" (Hathaway et al. 2012, p. 836);
(iii) The state prosecutes such attacks regardless of LOW, in accordance with the George W. Bush doctrine of the "war on terrorism."

The third scenario is a Hobbesian one: an informational attack is carried out by a sovereign state and the targeted nation mulls over the counter-attack that may be appropriate in the absence of parameters and conditions which, in conformity with international law, govern such cases of informational aggression. A first option is given by the good will of the sovereign: the latter decides to constrain itself and abide by the "precept, or general rule, found out by reason," according to Hobbes's definition of the laws of nature in Chapter 14 of *Leviathan*. Either for moral causes or for simple matters of convenience under the pressure of the public opinion, the state may end up following, for example, the moral laws of information ethics illustrated in the previous section. As a result, a state's response to a cyber attack by another nation state can lawfully resort to the use of force, either virtual or physical, if (and only if) the original attack rises to the level of "informational severity." In accordance with Hobbes' standpoint and the old Roman maxim *salus rei publicae suprema lex esto*, i.e. the health of the nation represents the supreme law, we should be prepared however for the other way around; that is, a Hobbesian state-of-nature between sovereign states. Here, it is up to the discretion and power of the state to determine forms and means of its response to a critical informational aggression.

The final scenario is closely related to the previous one, because it concerns the attempt to find a way out of the new international state-of-nature of the information era. After all, previous technological advancements have given rise to the drafting of international conventions and agreements to discipline and regulate the use of chemical, biological and nuclear weapons; land mines and the like. As mentioned in Section 3, however, a new international agreement on some critical aspects of informational warfare may take a long time and still, the lack of an international agreement does not mean that each man will be a threat to his neighbour in informational warfare. Going back to the difference between strict informational attacks and such attacks as a means for real-world operations, we have seen that most of the latter can be properly addressed with the current provisions of LOW and IHL, either directly or by the use of analogy. Moreover, even in the case of strict informational attacks, a number of these attacks seem to fall within the loopholes of current legal frameworks and yet some outlooks, such as the moral laws of information ethics, allow us to approach them conveniently. In addition, scholars have insisted on how further international legal frameworks, such as telecommunication law, aviation law and law of space and of sea, can help us to work out

satisfactory solutions to the challenges of informational warfare (e.g. Hathaway et al. 2012, p. 866–873).

Paradoxically, since we are dealing with a field that traditionally concerns problems of international law, i.e. the relationship between sovereign states, one of the main threats of informational warfare may pertain to the realm of constitutional law. As nations are progressively unable to monopolise the use of force in cyberspace, it is likely that non-state actors will have a crucial role in this new domain of military operations. But, the more non-state actors shape the new scenarios of cyber warfare, the more attention should be drawn to the alternatives between the first and second scenarios examined in this section, i.e. between standard criminal law safeguards for alleged cyber terrorists and their treatment under current LOW, down to the slippery slope approach of the second scenario that ends up with some variants of the "war on terror". This trend is further illustrated by a number of national programmes on online security and defence, much as national laws in the field of data retention, e.g. the EU directive 24 from 2006. As shown by the 2013 scandal of the US National Security Agency (NSA)'s Prism project, much as the UK's GCHQ files,[5] what is at stake here suggests a Hobbesian approach to issues of national security, rather than a Hobbesian state-of-nature in the international affairs of informational warfare. All in all, unconventional challenges of cyber attacks are increasingly testing the framework of legal safeguards that have represented, so far, the salient quality of Western democracies (Pagallo 2013b).

On one side, a zero sum game approach to issues of security and defence is still popular among Western scholars and national lawmakers. Some believe that providing basic security must be the first priority in policy considerations, at least in international affairs, because security drives democracy, and not the other way around (Etzioni 2007). Others claim that "calls for tighter trammels on security agencies come from a movement that fuses the libertarian right with a certain kind of left-winger for whom the big state is a wonderful thing in every aspect of life apart from the basic provision of safety."[6] Yet, on the other side, several recent rulings of both US and EU courts stress, *pace* the comments in the *Financial Times*, that the issue is not only about "liberal lawyers and privacy campaigners" shuddering at people's insouciance. Consider the decisions with which several European constitutional courts have annulled the national implementation laws of the aforementioned EU data retention directive 2006/24, as the German *Bundesverfassungsgericht* did on 2 March 2010, because of the balance that should be struck between national security purposes and the protection of fundamental rights. Similarly, reflect on the reasons why, in the name of the proportionality principle, the EU Court of Justice declared the 2006 data retention directive invalid on 8 April 2014 (joined cases C-293/12 and C-594/12). Likewise, contemplate the legal grounds on which the US district court of Columbia entered on 16 December 2013 an order that bars the Government from collecting telephony metadata as part of the NSA's bulk telephony metadata programme (*Klayman* et al. *v. Obama*, no. 13–0851). Whilst

[5] See John Lanchester, The Snowden files: why the British public should be worried about GCHQ, The Guardian, 3 October 2013, at http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester (last accessed 29 August 2014).

[6] See Janan Ganesh, Cynicism is no match for the mortal threat posed by Isis, *Financial Times*, 26 August 2014, p. 9.

several programmes and national statutes on online security and defence have been developed by sovereign states so as to tackle the menace of a new generation of cyber attacks carried out by other sovereign states or non-state actors, what these rulings show is not only the reaction of the legal immunity system. Such cases illustrate how the threat to constitutional rights does materialise in the field of national law.

5 Conclusions

The paper has aimed to make apparent what still troubles some scholars in the international law fields of LOW and IHL; namely, how the use of cyber force can be as severe and disruptive as traditional armed attacks usually are. The more we deal with ICT-driven societies, i.e. societies that depend on information as a vital resource, the more it is likely that even strict informational attacks can force states to desist from—or to engage in—a particular course of action. Although such attacks neither provoke physical injuries nor cause property damages, they do affect essential functions of today's societies, such as governmental services, business processes or communication systems. In light of a morally coherent theory, such as Floridi's ethics of information, canonical causes and conditions of just war theory were thus reinterpreted, so as to fill some gaps of the current legal framework. In particular, the purpose was to:

i) Compare canonical targets of real-world operations on the battlefield with the new means of informational warfare, since all the entities can be understood in terms of information;
ii) Examine at what point a strict cyber attack should be viewed as an act of war due to its "severity", in accordance with the amount of entropy that is caused by the aim to remove, annihilate or delete such informational objects as the enemy's communication networks or computers; and,
iii) Clarify some scenarios of proportionality as a cause and condition of just war, by relating the amount of entropy provoked by an informational attack to the amount of entropy which is either prevented or removed by such an attack in the infosphere.

Admittedly, by examining the new scenarios and challenges of cyber warfare in connection with the severity of strict informational attacks, no one-size-fits-all answer can properly tackle the complexity of the subject matter and moreover, some critical issues are fated to remain open in the legal field. This is why, as stressed above in Section 3, several scholars claim that an international treaty, much as new forms of international cooperation, are necessary. However, a twofold peculiarity of informational warfare has to be mentioned once again: on the one hand, the lack of an international agreement does not entail a new Hobbesian state-of-nature of the information era. Although some provisions of today's LOW and IHL shall be reformulated so as to include specific rules for strict informational attacks, it does not follow a condition in which all is permitted among sovereign states. We have seen that LOW and IHL can often be interpreted in such way that, given the nature of the legal question and the background of the issue, scholars can obtain the solution that best justifies or fits

the principles of the system. On the other hand, the increasing incapacity of nation states to monopolise the use of force in cyberspace, which goes together with the difficulty and, at times, the impossibility of identifying the responsible parties of such cyber attacks, suggests a national, rather than international, legal threat. The more non-state actors will play a crucial role in cyberspace as the new domain of military operations, the more national laws on data retention, much as national programmes on online security and defence, will test the endurance of Western democracies and their aim to protect basic constitutional rights. Several recent rulings of both EU and US courts have shown that, rather than a new Hobbesian state-of-nature in the international affairs of informational warfare, a Hobbesian approach to matters of security and defence may be the main threat in the fields of national and constitutional law. The new scenarios of informational warfare do not only concern the fields of international law, such as LOW and IHL, after all.

References

Alston, P. (2010) Report of the special rapporteur on extrajudicial, summary and arbitrary executions, UN General Assembly, Human Rights Council, A/HRC/14/24/Add.6, 28 May

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: the next threat to national security and what to do about it*. New York: Harper Collins.

Cullet, P. (1999). Differential treatment in international law: towards a new paradigm of inter-state relations. *European Journal of International Law, 10*(3), 549–582.

Etzioni, A. (2007). *Security first: for a muscular, moral foreign policy*. New Haven: Yale University Press.

Floridi, L. (2008). Information ethics, its nature and scope. In J. van den Hoven & J. Weckert (Eds.), *Moral philosophy and information technology* (pp. 40–65). Cambridge: Cambridge University Press.

Floridi, L. (2013). *The ethics of information*. Oxford: Oxford University Press.

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spengel, J. (2012). The law of cyber-attack. *Southern California Law Review, 100*, 817–885.

Hobbes, Th. (1999) *Leviathan*, R. Tuck (ed.). Cambridge University Press, Cambridge.

Hollis, D. B. (2007). Why states need an international law for information operations. *Lewis and Clark Law Review, 11*, 1023–1062.

ICJ (1986) Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of the International Court of Justice from 26 November 1984, available at http://www.icjcij.org/docket/index.php?p1=3&p2=3&case=70&p3=4. Accessed 15 Oct 2014.

Kelsen, H. (1967). *The pure theory of law, M. Knight (trans.)*. Los Angeles: University of California Press.

Libicki, M. C. (1995). *What is information warfare?* Washington: National Defense University.

Lin, P., Bekey, G., & Abney, K. (2007). *Autonomous military robotics: risk, ethics, and design. Report for US Department of Navy*. San Luis Obispo, CA: Office of Naval Research. Ethics+Emerging Sciences Group at California Polytechnic State University.

Pagallo, U. (2013a). *The laws of robots: crimes, contracts, and torts*. Dordrecht: Springer.

Pagallo, U. (2013b). Online security and the protection of civil rights: a legal overview. *Philosophy and Technology, 26*(4), 381–395.

Pagallo, U., & Durante, M. (2009). Three roads to P2P systems and their impact on business ethics. *Journal of Business Ethics, 90*(4), 551–564.

Roscini, M. (2010). World Wide warfare—the jus ad bellum and the use of cyber force. *Max Planck Yearbook of United Nations Law, 14*, 85–130.

Schmidt, E., & Cohen, J. (2013). *The new digital age*. London: John Murray.

Schmitt, M. N. (2011). Cyber operations and the jus ad bellum revisited. *Villanova Law Review, 6*, 569–606.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. New York: Cambridge University Press.

Schmitt, M. N. (2014). The law of cyber warfare: quo vadis? *Stanford Law and Policy Review, 25*, 269–299.

Schreuer, C. (1993). The waning of the sovereign state: towards a new paradigm for international law? *European Journal of International Law, 4*(1), 447–471.

Sharp, W. G., Sr. (1999). *Cyber space and the use of force*. Falls Church: Aegis.

Silver, D. B. (2001). Computer network attack as a use of force under Article 2(4) of the United Nations Charter. In M. N. Schmitt & B. T. O-Donnell (Eds.), *Computer Network Attack and International Law* (pp. 73–97). Newport: Naval War College.

Singer, P. W. (2008). *Corporate warriors: the rise of the privatized military industry*. Ithaca and London: Cornell University Press.

Sklerov, M. J. (2009). Solving the dilemma of state responses to cyberattacks: a justification for the use of active defenses against states who neglect their duty to prevent. *Military Law Review, 201*, 1–85.

Waxman, M. C. (2011). Cyber-attacks and the use of force: back to the future of Article 2 (4). *Yale Journal of International Law, 26*, 421–459.