Philos. Technol. (2015) 28:333–338
DOI 10.1007/s13347-015-0197-8

EDITORIAL NOTES

Cyber Conflicts: Addressing the Regulatory Gap

Ludovica Glorioso[1]

Received: 7 March 2015 / Accepted: 9 March 2015 / Published online: 20 March 2015

This special issue gathers together a selection of papers presented by international experts during a workshop entitled 'Ethics of Cyber-Conflicts', which was devoted to fostering interdisciplinary debate on the ethical and legal problems and the regulatory gap concerning cyber conflicts. The workshop was held in 2013 at the Centro Alti Studi Difesa in Rome under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). This NATO-accredited international military organisation that has always placed a high value on an interdisciplinary approach to cyber defence, uniting as it does perspectives from technical, policy, legal, and strategic domains. The Centre's mission is to enhance capability, cooperation, and information-sharing between NATO, its member states, and partner countries in the area of cyber defence by virtue of research, education, and consultation. The workshop was one of the projects supported by the Centre to achieve this mission.

Readers may already be familiar with the term 'cyber conflict', which is understood as any use of information and communication technologies (ICTs) that may have disruptive or destructive consequences. Cyber conflicts are an umbrella phenomenon encompassing several instances ranging from cyber warfare and *hacktivism* to cyber crime and cyber terrorism. As contemporary societies grow dependent from ICTs, any form of conflict that uses these technologies, both as a means and as a target, poses serious threats to their stability, security, and welfare.

As recently reported by the *Financial Times*, "the ultimate impact [of cyber-conflicts] could be as much as $3 trillion in lost productivity and growth".[1] Furthermore, should cyber conflicts propagate without an adequate response then contemporary societies may risk a *cyber backlash* in the shape of a deceleration to the digitization process imposed by governments and international institutions in order to prevent this

[1] www.ft.com/cms/s/0/1c4115e8-885a-11e3-85a2-00144feab7de.html#axzz3RpxcLjt0

Ludovica Glorioso is a Captain of the Italian Army and a legal and policy researcher of the NATO Cooperative Cyber Defence Centre of Excellence.

✉ Ludovica Glorioso
ludovica.glorioso@ccdcoe.org

[1] NATO Cooperative Cyber Defence Centre of Excellence, Filtri tee 12, Tallinn 10132, Estonia

kind of conflict, to erode trust in the economy. The need to define policies and laws to regulate cyber conflicts is thus much felt and grows more compelling as cyber conflicts become so more common.

The modes, targets, and effects of cyber conflicts are unprecedented, and as such, regulating the phenomenon continues to prove problematic and is at the centre of lively and interdisciplinary debate. This is polarised around two main approaches, the *analogy* and the *discontinuous approach* (Taddeo, 2014). The first approach stresses that the regulatory gap concerning cyber conflicts is only apparent insofar as cyber conflicts are not radically different from any other form of conflict.

According to those endorsing this approach (Barrett, 2013; Lucas, 2012; Schmitt, 2013), the existing legal framework governing armed conflict is sufficient to regulate the cyber battlefield. All that is needed is an in-depth analysis of such laws and an adequate interpretation. As Schmitt puts it, "a thick web of international law norms suffuses cyber-space. These norms both outlaw many malevolent cyber-operations and allow states to mount robust responses" (Schmitt, 2013, p. 177). The legal framework that is referred to mainly encompasses the four Geneva Conventions and their first two Additional Protocols,[2] the international customary law and general principle of law[3] Convention restricting or prohibiting the use of certain conventional weapons,[4] and judicial decisions. This framework has been developed over the years to restrict the freedom of states in the conduct of hostilities during armed conflicts to discipline the behaviour of belligerents in their mutual relations, as well as to manage the attitude of the organs of military violence against civilian populations. Initially referred to as the laws and customs of war and codified by the Hague Conventions of 1899 and 1907, in 1949 (GC I–IV), it became the law of war, laws of armed conflict.[5] These days, we refer to this body of laws as international humanitarian law, and it is considered the product of the influence of universal human rights theories on this area of international law.[6] It rests on the conceptual framework of just war theory.

The second approach, the *discontinuous approach* (Denning, 2007; Durante, 2014; Taddeo, 2012; Toffler & Toffler, 1997), stresses the novelty of cyber conflicts and maintains that existing ethical principles and laws are not adequate to regulate this phenomenon. This view sees cyber conflicts as one of the most compelling signs of the information revolution (Taddeo, 2012); as Floridi puts it, "those who live by the digit, die by the digit" (Floridi, 2014a). Scholars endorsing this approach maintain that the information revolution is a conceptual revolution and not just a technological upheaval. It is reshaping the very way in which we understand ourselves, the reality in which we live, and the way we interact with the environment and with other agents (L. Floridi, 2014b). Elsewhere, Taddeo has referred to it as the "shift toward the non-physical domain. *This shift makes the boundaries of reality stretch to include non-physical*

[2] The Geneva Conventions of 1949 and their Additional Protocols (Additional Protocol I and II, 1977). See www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/

[3] *Ius cogens* norms. Examples are the prohibition against genocide and torture.

[4] Convention restricting or prohibiting the use of certain conventional weapons which may be deemed to be excessively injurious or to have indiscriminate effects. Geneva, 10 October 1980. See www.icrc.org/ihl.nsf/385ec082b509e76c41256739003e636d/f6426235883f9d62c125641e0052d53d

[5] Nils Melzer, 2011, "Cyberwarfare and International Law", United Nations Institute for Disarmament Research (UNIDIR). See www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

[6] Tadic, IT-94-1, 2 October 1995, par. 87.

objects, *actions and interactions as well as physical ones* … [*Cyber warfare*] *shows that there is a new environment*, *where physical and non-physical entities coexist*, *in which states have to prove their authority and new modes of warfare are being developed specifically for deployment in such a new environment*" (Taddeo, 2012). As such, according to the discontinuous approach, any successful attempt to regulate the different instances of cyber conflicts cannot prescind from considering such radical changes.

Although debate over the regulation of cyber conflicts involves all the different instances of this phenomenon, cyber warfare has emerged as one of the key topics of discussion. Further, the definition of *cyber attack* offers a good example of the scope and nature of the debate. Before leaving readers to the rest of this issue, I shall now briefly describe it.

There are quite a few definitions of *cyber attack*. The *Tallinn Manual on the International Law Applicable to Cyber Warfare*, for example, describes cyber attack as "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (NATO Cooperative Cyber Defence Centre of Excellence, 2013) (p. 106). However, as at the present time, the definition remains disputable. For example, the USA National Research Council defines cyber attacks as "the use if deliberate actions—perhaps over an extended period of time—to alter, disrupt deceive, degrade or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (p. 80).[7] This definition has a different characterisation of cyber attacks, for it also considers the damage caused to physical as well as to non-physical (*intangible*) objects such as data, information, and informational infrastructure. The *Tallinn Manual* gives another definition: rule 10 stresses that under *jus ad bellum*[8], a cyber attack is unlawful if it constitutes a threat or *use of force* against a state. Rule 11 refines Rule 10 by stressing that a cyber operation amounts to a use of force if its scale and effects are similar to a kinetic attack. Rule 11 of the manual offers a good example of the position held by those following the analogy approach, as it compares the effects of a cyber attack with the scale of effects of a conventional attack in order to determine whether a use of force should be regarded as an armed attack.[9] In order to support such an assessment, several tests can be run, the most famous one being the Pictet's test,[10] which focuses on the scope, duration, and intensity of the attack.

Those who agree with the discontinuous approach would argue that this is quite uncontroversial, for a cyber attack that has the same or similar effects to a conventional attack, i.e. when a cyber attack is destructive, should be considered as a kinetic attack in the eye of the law. The conundrums emerge when focusing on those cyber attacks that

[7] The debate remains open. For example, Hayes and Kesan criticised the USA National Research Council definition, arguing that it does not allow for distinguishing between military (state-based) and non-military uses (e.g. cyber-crime) of ICTs (Hayes & Kesan, 2014).

[8] Specifically, the manual refers to Article 2(4) of the United Nations Charter and its specific prohibition of threats or use of force against the territorial integrity or political independence of any state.

[9] The International Court of Justice *Nicaragua Case* (*Nicar* v. *US*), 1986 I.C.J. 14 (June 27) distinguished the most grave forms of the use of force from other less grave forms and addressed the matter defining certain actions that were not kinetic in nature as uses of force.

[10] http://resources.infosecinstitute.com/fitting-cyber-attacks-to-jus-ad-bellum-consequence-based-approach-part-ii/

do not cause any physical damage and yet can still be disruptive. A good example of this can be found in Barrett's contribution to this special issue: "since damage to property may constitute a just cause, can temporary losses of computer functionality also qualify as a casus belli?" Offensive cyber attacks, because of their potential to be transitory or reversible, can also merely compromise functionality, which is a unique feature of cyber and deserves to be further investigated.

As Taddeo remarked: "the issue is not whether the case of [cyber-attack] can be considered in such a way as to fit the parameters of kinetic warfare and hence to fall within the domain [existing laws], as we know it. This result is easily achieved if the focus is restricted to physical damage and tangible objects. Rather, the problem lays at a deeper level and questions the very conceptual framework on which Just War Theory rests and its ability to satisfactory and fairly accommodate the changes brought to the fore by the information revolution" (Taddeo, 2014).

The novelty of cyber conflicts, and in particular of cyber warfare, is the object of analysis of Bringsjord and Licato's essay "By Disanalogy, Cyberwarfare is Utterly New". The first part of the paper offers an argument in support of the differences between cyber warfare and other forms of warfare. The authors propose necessary conditions (one each for kinetic warfare, espionage, and cyber warfare) sufficient to support their argument. They then use deductive meta-reasoning to show the disanalogy between cyber and kinetic warfare and to argue that cyber warfare is a fundamentally new phenomenon given the environment in which it is waged and the role that artificial agents play in it. The second part of the article relies on the first one to make the case for a revision of just war theory.

This contribution is also the target paper of this issue, and as such, it is followed by a commentary by Bruce Christianson. The commentary offers an insightful application of the meta-argument proposed in Bringsjord and Licato's essay to other kinetic forms of warfare, the use of the crossbow being the case in point, to argue that any interpretation of Just War Theory replying on the use of analogy is invalid.

The applicability of just war theory to cyber warfare is also the topic of Durante's essay "Violence, Just Cyber War and Information". This contribution argues for the need to reconsider pivotal concepts such as those of "force", "violence", and "attack" as a preliminary and necessary step for the application of just war theory to cyber warfare. The essay dwells upon the definition of cyber attack and argues that such a definition depends on "how force is to be interpreted in the cyber age. We need a unified approach to our understanding of a cyber attack, which may encompass the two dimensions of a cyber war: destruction and exploitation". The author endorses an informational approach, à la Floridi, to offer such a definition. Following information ethics' four principles (Luciano Floridi, 2013), which couple moral and physical violence, Durante's contribution offers an insightful analysis of what violence and force are in the age of cyber warfare.

Barrett's essay "Reliable Old Wineskins: the Applicability of the Just War Tradition to Military Cyber Operations" also focuses on just war theory. It supports the analogous approach and maintains that the principles of just war theory are fully applicable to the cases of cyber warfare. First, it analyses the notion of liability to defensive harm and then it offers a criticism to the need to develop alternative frameworks to just war theory. The final part addresses ethical issues such as casus belli, moral aspects of "the attribution problem", and respective rights and duties when attacks involve innocent third-party states to support the analogous approach.

In his paper "Cyber Force and the Role of Sovereign States in Informational Warfare", Pagallo addresses two problems: "how the notion of force and the role of sovereign states may change in the new context". The analysis of such issues leads Pagallo to consider the role of both state and non-state actors in cyber-warfare and the difficulties prompted by the latter in cyber-conflict scenarios, e.g. attribution, transparency, and accountability. The paper argues that national constitutional laws are affected by the emergence of cyber conflicts as much as international laws are, insofar as the response of sovereign states to cyber attacks attributed to non-state actors may involve a breach of individual rights such as privacy, anonymity, and free speech. As the author puts it, there is then a pressing need to examine "the reaction of sovereign states against non-states 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".

McReynolds' paper "How to Think About Cyber Conflicts Involving Non-State Actors" also investigates the role of non-state actors in cyber conflicts. The focus in this case is shifted from cyber warfare to other forms of cyber conflicts, for example digilantism and hacktivism. The article first distinguishes between different kinds of non-state actors, i.e. insurgents, vigilantes, and civil disobedience. It then argues that, albeit illegal, some actions taken by non-state actors may be morally acceptable.

Rao, Jongerden, Lemmens, and Ruivenkamp's contribution to this issue is entitled "Technological Mediation and Power: Postphenomenology, Critical Theory, and Autonomist Marxism" and focuses on the power of technological mediation from the point of view of autonomist Marxism. The essay first compares the analyses of power embedded in technological artefacts provided by both postphenomenologial theories of technological mediation and by the critical theory of technology. It then relies on the Foucauldian dispositifs of biopower to argue that resistance should be understood in terms of practice that subverts the technically mediated circuit of production itself.

The special issue is concluded by an insightful commentary written by Maurizio D' Urso, a member of the Italian Defence General Staff, Legal Affairs General Office (SMD–UGAG). D' Urso focuses on the status of *cyber combatant*, as a new status for those engaging in cyber warfare. The commentary dwells on the status of lawful combatants in cyber-warfare scenarios, and its goal is to discuss whether the concept of 'direct participation in hostilities' is valid also in cases of cyber warfare. In doing so, it addresses a problem, the distinction between lawful and unlawful combatants in cyber warfare, which is a focal point of the debate on the regulation of cyber warfare.

Before leaving the reader to the essays included in this special issue, I would like to thank all the authors who have kindly contributed to it and also the reviewers. Finally, I would like to express my gratitude to the NATO CCD COE for fostering this project, to Mariarosaria Taddeo for her participation and support in organising the workshop and to the editor-in-chief of this journal, Professor Luciano Floridi, for having made this special issue possible.

References

Barrett, E. T. (2013). Warfare in a new domain: the ethics of military cyber-operations. *Journal of Military Ethics, 12*(1), 4–17. doi:10.1080/15027570.2013.782633.

Denning. (2007). The ethics of cyber conflict. In *In information and computer ethics*. Hoboken, USA: Wiley.
Durante, M. (2014). Violence, just cyber war and information. *Philosophy and Technology*. doi:10.1007/s13347-014-0176-5. October, 1–17.
Floridi, L. (2013). *The Ethics of Information*. Also available as: eBook.
Floridi, L. (2014a). *The Onlife Manifesto - Being Human in a Hyperconnected Era*. Dordrecht: Springer. http://www.springer.com/philosophy/epistemology+and+philosophy+of+science/book/978-3-319-04092-9.
Floridi, L. (2014b). *The fourth revolution, how the infosphere is reshaping human reality*. Oxford: Oxford University Press.
Hayes, C.M., and Kesan J.P. (2014). *Law of Cyber Warfare*. SSRN Scholarly Paper ID 2396078. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2396078.
Lucas, G. R. (2012). "Just War and cyber conflict 'can there be an "ethical" cyber war?'" presented at the Naval Academy Class 2014.
NATO Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO cooperative cyber defence centre of excellence*. New York: Cambridge University Press.
Schmitt, M. (2013). Cyberspace and international law: the penumbral mist of uncertainty. *Harvard, 126*(176), 176–80.
Taddeo, M. (2012). Information warfare: a philosophical perspective. *Philosophy and Technology, 25*(1), 105–20.
Taddeo, M. (2014). Information warfare: the ontological and regulatory gap. *Newsletter on Philosophy and Computers, 14*(1), 13–20. fall 2014.
Toffler, A., and Toffler A. (1997). "Foreword: the new intangibles." In: *In Athena's camp preparing for conflict in the Information Age*, edited by John Arquilla and David F Ronfeldt. Santa Monica, Calif.: Rand.