Regulating cyber conflicts and shaping information societies

Mariarosaria Taddeo,[1,2,*] Ludovica Glorioso [3]

[1] Oxford Internet Institute, University of Oxford

[2] Alan Turing Institute, London

[3]Cpt ITA A, Legal & Policy Scientist/Senior Analyst, NATO Cooperative Cyber Defence Centre of Excellence, Tallin Estonia

*mariarosaria.taddeo@oii.ox.ac.uk

A relation of mutual influence exists between the way conflicts are waged and the societies waging them. As Clausewitz remarked, more than an art or a science, conflicts are a social activity. And much like other social activities, conflicts mirror the values of societies while relying on their technological and scientific developments. In turn, the principles endorsed to regulate conflicts play a crucial role in shaping societies.

Think about the design, deployment, and regulation of weapons of mass destruction (WMDs). During World War II, WMDs were made possible by scientific breakthroughs in nuclear physics, which was a central area of research in the years leading to the War. Yet, their deployment proved to be destructive and violent beyond what the post-war world was willing to accept. The Cold War that followed and the nuclear treaties that ended it defined the modes in which nuclear technologies and WMDs can be used, drawing a line between conflicts and atrocities. In doing so, treaties and regulations for the use of WMDs contributed to shape contemporary societies as societies rejecting the belligerent rhetoric of the early twentieth century and to striving for peace and stability.

The same mutual relation exists between information societies and cyber conflicts, making the regulation of the latter a crucial aspect, which will contribute to define current and future societies. In the short term, regulations are needed to avoid a digital wild west, as remarked by Harold Hongju Koh, the former Legal Advisor U.S. Department of State. For this reason, over the past few years, efforts have been devoted to analysing and interpreting the existing corpus of laws to guide states in engaging in international cyber conflicts.

Interpretations often highlight that existing norms raise substantial barriers to the use of cyber weapons and to the use of force to defend cyberspace. It is claimed that international law contains coercive means of permitting lawful responses to cyber provocations and threats of any kind. The legal framework that is referred to mainly encompasses the four Geneva Conventions and their first two Additional Protocols, the international customary law and general principle of law, the Convention restricting or prohibiting the use of certain conventional weapons, and judicial decisions (Glorioso 2015). Arms control treaties, such as the Nuclear Non-Proliferation Treaty and the Chemical Weapons Convention, are often mentioned as providing guidance for action in the case of kinetic cyber attacks (Schmitt 2013). At the same time, coercive measures addressing economic violations are generally considered legitimate in the case of cyber attacks that do not cause physical damage (Lin 2012; O'Connell 2012).

However, the problem at stake is not whether cyber conflicts can be interpreted in such a way as to fit the parameters of kinetic conflicts, economic transgressions, and conventional warfare, and hence whether they fall within the domain of international humanitarian law, as we know it. The problem rests at a deeper level and questions the very normative and conceptual framework of international humanitarian law and its ability to *satisfactorily* and *fairly* accommodate in the medium- and long-term the changes prompted by cyber conflicts (Floridi and Taddeo 2014, Taddeo and Floridi 2014).

In the medium- and long-term, regulations need to be defined so to ensure security and stability of societies, and avoid risks of escalation. To achieve this end, efforts to regulate cyber conflicts will have to rely on an in-depth understanding of this new phenomenon; identify the changes brought about by cyber conflicts and the information revolution (Floridi 2014; Taddeo and Buchanan 2015); and define a set of shared values that will guide the stakeholders operating in the international arena.

Efforts to regulate cyber conflicts cannot afford to be future-blind and disregard questions concerning the impact of these new forms of conflicts on future information societies, on their values, the rights, and security of their citizens, and on national and international politics. Conceptual and ethical questions need to be addressed now, while efforts to regulate this phenomenon are still nascent, to ensure fair and effective regulations, which will contribute to shaping open, pluralistic, peaceful information societies.

Regulation of cyber conflicts need to be developed consistently to (a) Just War Theory, (b) human rights, and (c) international humanitarian laws. However, applying (a)-(c) to the case of cyber conflicts proves to be problematic given the changes in military affairs that they prompted (Dipert 2010; Taddeo 2012a; Floridi and Taddeo 2014). When compared to kinetic warfare, cyber conflicts show fundamental differences: their domain ranges from the virtual to the physical; the nature of their actors and targets involves artificial and virtual entities alongside human beings and physical objects; and their level of violence may range from non-violent to potentially highly violent phenomena. These differences are redefining our understanding of key concepts such as harm, violence, target, combatants, weapons, and attack, and pose serious challenges to any attempt to regulate conflicts in cyberspace (Dipert 2010; Taddeo 2012b; Taddeo 2014a; Floridi and Taddeo 2014; Taddeo 2014b).

The Just War Theory principle of proportionality, as specified in the ethical tradition, offers a good example of the case in point. The principle prescribes a balance identifying the necessary and sufficient means to achieve a legitimate goal. Enforcing and respecting this principle is thus crucial while planning and waging cyber conflicts. However, proportionality rests on an assessment of the gains and damages received and caused by a cyber operation, and this assessment is highly problematic. The conventional conceptual framework for calculating pain and gains accounts for casualties, physical and economic damages, and territorial advantages, but proves to be challenging when endorsed to assess damage to virtual objects in cyberspace (Dipert 2013). This highlights an ontological hiatus between the entities involved in cyber conflicts and those taken in consideration in conventional wars (Taddeo 2016). This hiatus demands immediate attention as it encroaches our understanding of cyber conflicts, and any attempts to regulate them.

Such attempts are further complicated when we consider state and non-state actors operating in cyberspace. The use of a state's coercive power is coupled with the concept of state's sovereignty over a given territory. However, the absence of clear national boundaries, the distributed and interconnected nature of cyberspace, as well as the global sharing of information that it enables, make it difficult to define state sovereignty in this domain (Brenner 2009; Chadwick and Howard 2009; Cornish 2015).

This has serious implications for the definition of state authority and military power and hence on our understanding of the state and non-state actors involved in conflicts, as

well as for the definition of lawful and unlawful conducts and the body of law that should be applied. Understanding such conceptual changes, and identifying their medium- and long-term impact on international relations and military strategies is a preliminary and necessary step to any effort for regulating cyber conflicts.

Things are not less problematic when considering ethical issues. Cyber conflicts bring about three kinds of problems, concerning risks, rights, and responsibilities (3R problems) (Taddeo 2012). The more contemporary societies are dependent on ICTs, the more the 3R problems become pressing and undermine ethically blind attempts to regulate cyber conflicts. Consider, for example, the risks of escalation. Estimates indicate that the cyber security market will grow from US$106 billion in 2015 to US$170 billion by 2020, posing the risk of a progressive weaponization and militarisation of cyberspace. At the same time, the reliance on malware for state-run cyber operations (like Titan Rain, Red October, and Stuxnet) risks sparking a cyber arms race and competition for digital supremacy, hence increasing the possibility of escalation and conflicts (MarketsandMarkets 2015). Regulations of cyber conflicts need to address and reduce this risk by encompassing principles to foster cyber stability, trust, and transparency among states (Arquilla and Borer 2007; Steinhoff 2007; European Union 2015).

At the same time, cyber threats are pervasive. They can target, but can also be launched through, civilian infrastructures, e.g. civilian computers and websites. This may (and in some cases already has) initiate policies of higher levels of control, enforced by governments in order to detect and deter possible threats. In these circumstances, individual rights, such as privacy and anonymity may come under sharp, devaluating pressure (Arquilla 1999; Denning 2007). Ascribing responsibilities also prove to be problematic when considering cyber conflicts. Cyberspace affords a certain level of anonymity, often exploited by states or state-sponsored groups and non-state actors. Difficulties in attributing attacks allow perpetrators to deny responsibility, and pose an escalatory risk in cases of erroneous attribution. These risks have been faced, for example, by the international community in 2014, when malware initially assessed as capable of destroying the content of the entire stock exchange was discovered on Nasdaq's central servers and allegations were made of a Russian origin for the software;[1]

[1] http://arstechnica.com/security/2014/07/how-elite-hackers-almost-stole-the-nasdaq/

and later in 2015, when cyber attacks against TV5 Monde were initially attributed to ISIL/Da'esh.[2]

The volume is multidisciplinary as it collects contributions by leading experts in international law, war studies, philosophy and ethics of war, philosophy of law, information and computer ethics, as well as policy-makers focusing on of the problems prompted by cyber conflicts. The eleven chapters of this volume are either invited contributions or papers presented during the workshop "Ethics and policies for cyber warfare" organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) in collaboration with the University of Oxford and held at the Magdalen College Oxford, in November 2014. This was the second workshop organised by the Centre (and chaired by the editors of this volume) with the goal of identifying and defining the most pressing issues concerning the regulation of cyber conflicts.[3]

Each chapter provides a detailed analysis of a key problem concerning the ethical or legal implications of cyber conflicts. In more details, the book offers an analysis of the following topics: the conceptual novelty of cyber conflicts and the ethical problems that this engenders; the applicability of existing conceptual and regulatory frameworks to cyber conflicts; the analysis of models to foster cooperation in managing cyber crises; and how to regulate cyber operations through international law.

Just War Theory is a central point of analysis in Cornish's chapter, which opens the volume. The chapter first delves on the understanding of key concepts, such as those of violence, attack, and cyberspace. The attention is devoted to ethical issues and to the analysis of cyberspace as an artificial environment, which is pre-political, pre-strategic, and therefore pre-ethical. The chapter argues that as such cyberspace is not yet susceptible to the forms of political organisation with which we are familiar, it is resistant to the normative constraints with which we expect to manage and moderate traditional conflicts and organised violence. The chapter concludes by stressing that the regulation of cyber conflicts requires serious, balanced public policy discourse and a new consideration of cyberspace as an arena in which diplomacy, negotiation, bargaining, compromise, concession and, therefore, moral judgement, are all considered possible and proper.

---

[2] http://www.alphr.com/security/1000604/isis-hacks-french-broadcaster-tv5-monde

[3] The first workshop 'Ethics of Cyber Conflict' was held in Rome at the 'Centre for High Defence Studies' in Rome, https://ccdcoe.org/multimedia/workshop-ethics-cyber-conflict-proceedings.html ; a special issue of Philosophy & Technology has been published collecting the papers presented during that meeting (Glorioso 2015).

McDonald's analyses three main challenges to maintaining the norm of distinction in cases of cyber attacks: (i) the significant chance that attempts of computer network exploitation may unwittingly target non-military systems; (ii) the use of civilian infrastructure or third party networks that may not be willing participants but would be targeted regardless; (iii) the design and deployment of autonomous software programmes (e.g., 'viruses', 'malware') unable to distinguish targets in all circumstances. The analysis of (i)-(iii) offers the basis for questioning the direct applicability of the Just War Theory principle of distinction to cyber attacks involving computer network exploitation.

The applicability of Just War Theory to the case of cyber conflicts and of the principle of discrimination is also focal aspect in Rowe's contribution. This chapter analyses different ways in which a military cyber attack could hit a civilian target. It focuses on both dual-uses targets and on the military advantage that may result from intentionally target civilian infrastructures and objects. This analysis highlights a vicious dynamics, i.e. cyber attacks targeting civilians objects and infrastructures encourage counter-attacks on similar targets, as such they are close to *perfidy*, which is outlawed by the laws of armed conflict. The chapter concludes with proposed principles for ethical conduct of cyber conflicts to minimize unnecessary harm to civilians, and suggests that focusing on cyber coercion and deterrence rather than cyber warfare will reduce harm to civilians.

Taylor Smith's contribution focuses on the concept of cyber harm. The chapter first offers a definition of cyber harm, whereby it occurs when the normal or intended functioning of a computer network is disrupted in ways that undermine or violate significant human interests or entitlements. The chapter argues that this view is more sophisticated than the one claiming that cyber attacks only occur in presence of *physical* harm or damage. Yet, it is not as complex as the view maintaining that the disruption of a computer system is *per se* a form cyber harm. In the second part, the provided definition of cyber harm is used to identify those occurrences of cyber attacks that count as *casus belli*, justifying unilateral military action in self-defence.

Taddeo's contribution is a reprint of an article (Taddeo 2016) delving on the applicability of Just War Theory to cyber conflicts. It proposes an ethical analysis of cyber warfare with the twofold goal of filling the theoretical vacuum surrounding this phenomenon and providing the conceptual grounding for the definition of new ethical regulations for this phenomenon. The chapter first argues that Just War Theory is a necessary but not sufficient instrument for considering the ethical implications of cyber warfare and that a

suitable ethical analysis of this kind of warfare is developed when Just War Theory is merged with Information Ethics. In the initial part, the chapter describes cyber warfare and its main features and highlights the problems that arise when Just War Theory is endorsed as a means of addressing ethical problems engendered by this kind of warfare. In the final part, the main aspects of Information Ethics are provided along to three principles for a just cyber warfare resulting from the integration of Just War Theory and Information Ethics.

With Hoisington's chapter the focus shifts to the analysis of existing laws for the regulations of cyber conflicts. This contribution distinguishes three approaches, namely '*in, out or against*' existing regulatory framework, for the regulation of cyber conflicts. It then highlights the problems that each of these approaches may rise when considering the different stakeholders acting in cyberspace. Attempts to regulate cyber conflicts relying on principles existing within *jus ad bellum* and *jus in bello* are shaken when confronted with the difficulties of applying the general principles such as proportionality and military necessity in cyberspace. The second approach, i.e. finding principles for the regulation of cyber conflicts outside the set of existing laws, describes a new set of international regulations and legal structures, including the interaction with the private sector. The third approach rests on a rebuttal of the existing framework and requires a revision of the existing rules. This analyses stresses the difficulty to amend the UN Charter, while at the same time suggesting the development of new concepts and vocabulary describing cyber operations and the need to involve new actors in the elaboration of the rules. The chapter concludes remarking that international lawyers need to be vigilant to the new developments of the cyber capabilities in order to develop the understanding and the applicability of international law in the cyber context.

Roscini's chapter explores the application of the Law of Armed Conflict's principle of distinction between military objectives and civilian objects in cyberspace. It starts by looking at what type of cyber operations are subject to the law of targeting, i.e. those qualifying as 'attacks' under Article 49(1) of Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of War. It then applies the components of the definition of 'military objective', contained in the same Protocol, to cyberspace: 'effective contribution to military action' and 'definite military advantage'. The chapter concludes that, despite current challenges posed by cyber conflicts, existing rules are flexible enough to be applied in a new domain like cyberspace.

Shackelford's, Russell's, Kuehn's chapter analyses nations' due diligence obligations to their respective private sectors and to each another in the international arena. The chapter starts off considering what steps nations and companies under their jurisdiction have to take under international law to secure their networks, and what the rights and responsibilities of transit states are. This chapter reviews the arguments surrounding the creation of a cyber security due diligence norm and argues for a proactive regime that takes into account the common but differentiated responsibilities of public and private sector in cyberspace. The analogy is drawn to cyber security due diligence in the private sector and the experience of the 2014 National Institute of Standards and Technology Framework to help guide and broaden the discussion.

Casanovas' contribution to this volume builds on the findings of two European projects-*(O)SI for (Open) Social Intelligence, and PbD for Privacy by Design* (OSINT) and *Collaborative information, Acquisition, Processing, Exploitation and Reporting* (CAPER)–devoted to embed the legal and ethical issues raised by the General Data Reform Package in Europe into security and surveillance platforms. The contribution to this volume describes a procedure to flesh out ethical principles through semantic web regulatory models that can be applied to the case of cyber warfare. New ways of designing political institutions and the possibility to build up a meta-rule of law are also discussed.

Happa's and Fairclough's chapter addresses the need for establishing a methodologies supporting different stakeholders in discussing the regulation of cyber conflicts. In particular, the chapter focuses on the difficulties law- and policy-makers, as well as military experts and ethicists and of cyber security analysts to share information, coordinate, and collaborate in defining effective regulation for cyber attacks. This chapter proposes a model enabling a collective, multidisciplinary, and collaborative approach to understand and discuss cyber attacks.

Collier's chapter compares the cyber crisis management strategies of Estonia and the UK. It argues that the two countries' strategies differ significantly. This divergence reflects broader political, historical, and cultural differences between Estonia and the UK, all of which influence the respective national cyber crisis management strategies of the two countries. The variables that affect national strategies include the countries' history, size, political views, digital dependency, and the nature of the threats and adversaries they each face in cyberspace. The chapter concludes that, given the importance of these relative factors in determining their national cyber crisis

management strategies, it is difficult to draw from these cases generalizable recommendations that apply to other states. Instead, the importance of creating a cyber crisis strategy appropriate to the specific political, historical, and cultural climate should be recognised. Although cyber attacks may be highly technical in nature, this chapter argues that a successful organisational response to the threat has significant political components.

Baylon contributed a commentary to this volume describing some of the key findings of a Chatham House 18-month project on Cyber and Nuclear Security. The project examined the challenges that ICTs pose for the nuclear industry, which include ethical problems. Using Stuxnet as a case study, the project analysed whether the deployment of this computer worm could be considered an attack on a sovereign state-thus violating Iran's right to develop a peaceful civilian nuclear energy programme–and whether Iran has a legitimate grievance against the US and Israel and would be fully entitled to retaliate.

The volume ends with a report by Cath, Glorioso, and Taddeo of the NATO CCD COE workshop "Ethics and Policies for Cyber Warfare". The report describes the discussion among ethicists, policy-makers, international lawyers, and military experts on the existing regulatory gap concerning cyber warfare and ethical problems underpinning it. The report is divided in three parts. The first one describes the discussion on the extent to which current international legal structures are able to develop cyber security norms. The second part focuses on the applicability of current legal mechanisms of warfare to cyberspace, looking specifically at the issues of deterrence, proportionality, perfidy, and *casus belli*. The final parts describes the debate occurred among the workshop delegates concerning the different mechanisms for developing ethical norms and universal principles that could be applied to cyber conflicts.

Before leaving the reader to the contributions in this volume, we would like to express our gratitude to the NATO CCD COE for supporting the organisation of the workshop 'Ethics and Policies for Cyber Conflicts'. This project allowed us to gather a number of international experts discussing cutting edge conceptual and applied problems and to identify and define the most pressing needs concerning the regulation of cyber conflicts.

References

Arquilla. 1999. "Ethics and Information Warfare." In *Strategic Appraisal: The Changing Role of Information in Warfare*, edited by Zalmay Khalilzad and John Patrick White, 379–401. Santa Monica, CA: RAND.

Arquilla, J., and Douglas A Borer. 2007. *Information Strategy and Warfare : A Guide to Theory and Practice*. New York: Routledge.

Brenner, Susan W. 2009. *Cyber Threats the Emerging Fault Lines of the Nation State*. New York [u.a.]: Oxford Univ. Press. http://www.oxfordscholarship.com/oso/public/content/law/9780195385014/toc.html.

Chadwick, Andrew, and Philip N. Howard, eds. 2009. *Routledge Handbook of Internet Politics*. Routledge Handbooks. London: Routledge.

Cornish, Paul. 2015. "Survival: Global Politics and Strategy." *Survival: Global Politics and Strategy* 57 (3): 153–76.

Denning. 2007. "The Ethics of Cyber Conflict." In *Information and Computer Ethics*. Hoboken, USA: Wiley.

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

European Union. 2015. "Cyber Diplomacy: Confidence-Building Measures - Think Tank." Brussels. http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)571302.

Floridi, L. 2014. *The Fourth Revolution, How the Infosphere Is Reshaping Human Reality*. Oxford: Oxford University Press.

Floridi, L., and M. Taddeo, eds. 2014. *The Ethics of Information Warfare*. New York: Springer.

Glorioso, Ludovica. 2015. "Cyber Conflicts: Addressing the Regulatory Gap." *Philosophy & Technology* 28 (3): 333–38. doi:10.1007/s13347-015-0197-8.

Lin, Herbert. 2012. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94 (886): 515–31. doi:10.1017/S1816383112000811.

MarketsandMarkets. 2015. "Cyber Security Market by Solutions & Services - 2020." http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html?gclid=CNb6w7mt8MgCFQoEwwodZVQD-g.

O'Connell, M. E. 2012. "Cyber Security without Cyber War." *Journal of Conflict and Security Law* 17 (2): 187–209. doi:10.1093/jcsl/krs017.

Schmitt, M. 2013. "Cyberspace and International Law: The Penumbral Mist of Uncertainty." *Harvard* 126 (176): 176–80.

Steinhoff, Uwe. 2007. *On the Ethics of War and Terrorism*. Oxford; New York: Oxford University Press.

Taddeo, M. 2012a. "An Analysis for a Just Cyber Warfare." In *2012 4th International Conference on Cyber Conflict (CYCON 2012)*, 1–10.

Taddeo, M. 2012b. "Information Warfare: A Philosophical Perspective." *Philosophy and Technology* 25 (1): 105–20.

Taddeo, M.. 2014a. "Just Information Warfare." *Topoi*, April, 1–12. doi:10.1007/s11245-014-9245-8.

Taddeo, M. 2014b. "The Struggle Between Liberties and Authorities in the Information Age." *Science and Engineering Ethics*, September, 1–14. doi:10.1007/s11948-014-9586-0.

Taddeo, M. .2016. "Just Information Warfare." *Topoi*, April, 1–12. doi:10.1007/s11245-014-9245-8. Reprint *Ethics and Policies for Cyber Operations*, Eds. Mariarosaria Taddeo & Ludovica Glorioso, Philosophical Studies, Book Series, Springer.

Taddeo, M., and Elizabeth Buchanan. 2015. "Information Societies, Ethical Enquiries." *Philosophy & Technology* 28 (1): 5–10. doi:10.1007/s13347-015-0193-z.

Taddeo, M., and Luciano Floridi. 2014. "The Ethics of Information Warfare - An Overview." In *The Ethics of Information Warfare*. Law, Governance and Technology Series. New York.