The Ethics of Information Warfare – An Overview

M. Taddeo
University of Warwick, University of Oxford
M.Taddeo@warwick.ac.uk

L. Floridi
University of Hertfordshire, University of Oxford
luciano.floridi@philosophy.ox.ac.uk

The Ethics of Information Warfare – An Overview

> *"By the word 'information' we denote all the knowledge which we have of the enemy and his country; therefore, in fact, the foundation of all our ideas and actions [in war]."*
> (C.Von Clausewitz, F. N Maude et al. 2008, p. 81).

This volume collects twelve original contributions addressing some of the most important ethical problems raised by Information Warfare (IW), the complex set of new phenomena associated with the use of Information and Communications Technologies (ICTs) in fighting scenarios. IW is redefining how war is waged. In doing so, it is reshaping the concept of war itself, raising new ethical problems and challenging old solutions. These transformations are at the core of the current debates in research fields such as ethics, philosophy of technologies, war studies, and political philosophy. The main purpose of this volume is to provide an interdisciplinary investigation of some of the most compelling ethical problems posed by IW and to present innovative analyses for their solutions.

Before the pervasive dissemination of ICTs, the expression 'information warfare' referred to the importance of information, understood as the semantic content (Floridi 2010), within military strategies. Information as semantic content is relevant to war-waging both in relation to intelligence-gathering and as a means for propaganda aimed at demoralising the enemy's military forces and civilians. However, with the advent of the information revolution and the capillary dissemination of ICTs, the role of information in warfare radically evolved. ICTs further support war-waging in two new ways: by providing unmanned weapons to be deployed on the battlefield – like drones and semi-autonomous robots used to hit ground targets, defuse bombs, and patrolling actions – and by creating an entirely new battlefield, called the 'cyber domain', where warfare is waged with software tools, e.g. computer viruses or security packages. During the past two decades, such new uses of ICTs in warfare proved to be convenient and effective and gained a central role in militaries strategies. Nowadays, IW indicates a heterogeneous phenomenon concerning the deployment of robotic weapons, of cyber weapons, and the use of ICTs to foster coordination among militaries on the battlefield and for propaganda, the so-called C4ISR (integrated command, control, communications, computers, intelligence, surveillance, and reconnaissance) (Libicki 1996), (Taddeo 2012).

The rise of IW is not surprising. Historically, technological breakthroughs determine changes affecting the structure of both civil society and military organisations. As described by (Toffler and Toffler 1997), this was the case with the Neolithic revolution, when human beings first made weapons out of wood and rocks, and with the Industrial revolution, which provided the means for industrialised warfare and for the dissemination of weapons of mass destruction. The Information revolution is the latest example. It has changed our activities in several ways and at several levels (Floridi 2010). The use of ICTs changed the way individuals manage their communications and daily practices, from working and reading books, listening to music and driving. At a social level, ICTs reshaped social interactions; at the institutional level they provide new tools for the management of information and bureaucracy (Ciborra 2005) (Saxena 2005); and when considered with respect to warfare, ICTs determine the latest revolution in military affairs. In this sense, IW is the warfare of the information age.

Nonetheless, it would be misleading to consider this new type of warfare simply as the latest evolution of war fighting techniques. For IW engenders radical changes, which concern the very way in which we understand war, not just how it is waged. War is traditionally understood as the use of violence by a state through the latter's deployment of military forces, in order to determine the conditions of governance over a determined territory (Gelven 1994). As Oppenheim put it: "war is a contention between two or more states through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases", (Lauterpacht 1952, p. 202). The choice to undertake a (traditional) war usually involves a substantial commitment, given its heavy human, moral, economical, and political costs. Such aspects of war-waging have been radically changed by IW, which provides the means to carry out war in a completely different manner. The changes determined by IW are of astounding importance as they concern both the way the military and politicians consider and wage war, and the way war is perceived by the civil society. Like traditional warfare, IW is very powerful and potentially highly disruptive. However, unlike traditional warfare, IW is potentially bloodless, cost effective, and does not require military expertise. In short, ICTs have modified the costs of war, and hence our understanding and evaluation of them.

Furthermore, the information revolution brought to the fore a new domain, the cyber domain, which has become an important part of the environment in which we live and interact and plays crucial role for the development of contemporary societies (Floridi 2010). The management of national health systems, the regulation of energy, water and food supply-chains are only some examples of the aspects of contemporary societies that largely depend on the efficient functioning of the cyber domain. In this context, the ability

to control, disrupt or manipulate the enemy's informational infrastructures has become as decisive, with respect to the outcome of conflicts, as weapon superiority. Ethical analyses of IW need to take into account these aspects, for they pose important ethical problems concerning, for example, the moral stance of the entities existing in the cyber domain and the moral responsibilities for the actions performed by autonomous artificial agents, such as cyber viruses or robotic weapons, and increasingly hybrid agents, represented by human-machine systems.

Two interwoven sets of problems are of particular relevance, when considering the ethical implications of IW. The first one concerns the definition of IW and its properties. As Orend puts it in his chapter, there is a conceptual fog shrouding this type of warfare. Scholars are still debating on issues such as the nature of non-kinetic cyber attacks (Schmitt) (Arquilla 1998), the definition of IW, its long-term effects on the concept of war (see, for example, Dipert's chapter) and its role in the future development of international politics and economy. Casting some light through this fog is the preliminary and necessary step toward the solution of the second set of problems. These are ethical problems that range from the consideration of the most adequate ethical framework to prescribe principles for conducting a *just* war (Dipert 2011) to the solution of more applied issues. In this respect, three categories of applied ethical problems are at the centre of the contemporary debate on IW, attracting the attention of both ethicists and policy-makers; these are the *risks*, *rights* and *responsibilities* - the 3R problems (Arquilla and Ronfeldt 1997) (Taddeo 2012).

Risks. The risks involved in IW concern the potential increase in the number of conflicts and casualties. ICTs-based conflicts may be virtually bloodless for those involved. This advantage has the drawback of making war less problematic for the force that can implement these technologies, therefore making it easier not only for governments, but also for criminal or terrorist organisations, to engage in such conflicts around the world (Arquilla and Borer 2007), (Steinhoff 2007), (Brenner 2008).

Rights. IW is pervasive since not only can it target civilian infrastructures, it can also be launched through civilian computers and websites. This may initiate a policy of higher levels of control, enforced by governments in order to detect and defend their citizens from possible hidden forms of attacks. In this circumstance, the ethical rights of individual liberty, privacy and anonymity may come under sharp, devaluating pressure (Arquilla 1999), (Denning 1999).

Responsibilities. The problem concerns the assessment of responsibilities when using semi-autonomous robotic weapons and cyber viruses. In the case of robotic weapons, it is becoming increasingly unclear who, or what, is accountable and responsible

for the actions performed by complex, hybrid, man-machine systems on the battlefield (Matthias 2004), (Sparrow 2007). The assessment of responsibility becomes an even more pressing issue in the case of cyber attacks, as it is potentially impossible to trace back the author of such attacks (Denning 2007).

The twelve chapters of this volume address the changes and the problems caused by IW, with different focuses and approaches. The volume is divided into three parts. The first part focuses on issues pertaining to the concept of IW and the clarifications that need to be made in order to address its ethical implications. It includes four chapters: *Fog in the Fifth Dimension: The Ethics of Cyber-war*, by Brian Orend; *The Future Impact of a Long Period of Limited Cyber warfare on the Ethics of Warfare*, by Randall Dipert; *Is Warfare the Right Frame for the Cyber Debate?*, by Patrick Lin, Fritz Allhoff, and Keith Abney; and *Technology, Information, and Modern Warfare: Challenges and Prospects in the 21st Century*, by Wayne McCormack and Deen Chatterjee.

Orend's chapter opens the volume by first addressing the conceptual confusion surrounding IW and outlining some useful clarifications and distinctions. The focus is then shifted on to the analysis of Just War Theory and on how it can be embraced to provide some guidance in waging IW. The contribution stresses that Just War Theory remains the core conceptual framework for evaluating the ethics of political violence in general, and the ethics of IW in particular, but at the same time the chapter acknowledges the patches of darkness and confusion that remain unaddressed by Just War Theory.

Dipert's analysis adopts quite a different approach from Orend's. The chapter focuses mainly on cyber attacks and cyber warfare. He first provides a detailed taxonomy of the different instances of this phenomenon, then discusses possible alternative defensive strategies that may be put in place in the long term by governments in order to guarantee cyber defence.

The contribution by Lin, Allhoff, and Abney concerns above all cyber attacks. They highlight the relation between the policy vacuum concerning the launching of such attacks and the absence of ethical principles that provide guidance for the waging of cyber warfare. The chapter concludes by suggesting that the ethical problems posed by the occurrences of cyber attacks are overcome if such attacks are considered as attacks to privates rather than instances of warfare, which may give rise to private defence, i.e. self-defence by private parties, especially commercial companies, as distinct from a nation-state's right to self-defence.

The chapter by McCormack and Chatterjee addresses the normative and legal challenges that ICTs pose for modern warfare. They first examine the ethical and legal implications of IW in relation to the internal affairs of nations facing armed uprising or

undergoing similar violent turmoil. Then, they focus on the ethical consequences of the growing reliance on ICTs in modern warfare and analyse the blurring of the distinction between pre-emption and prevention in self-defence wars.

The second part of the volume collects four contributions focusing on Just War Theory and its application to the case of IW: *Permissible Preventive Cyberwar: Restricting Cyber Conflict to Justified Military Targets*, by George R. Lucas; *Moral Cyber Weapons: The Duty to Employ Cyber Attacks*, by Dorothy Denning and Bradley J. Strawser; *The Ethics of Cyber attack*, by Steven Lee; and *Just Information Warfare*, by Mariarosaria Taddeo.

Lucas' chapter investigates the conditions for preventive cyber warfare. The chapter first distinguishes permissible from impermissible forms of cyber conflicts as well as genuine warfare from criminal or terrorist enterprises. It then stresses the lack of discrimination often encountered in the formulation of cyber strategy and development of cyber weapons. The chapter concludes by considering the case of Stuxnet and arguing in favour of establishing international governance and guidance that (with respect to proportionality, discrimination, and the principle of last resort) may provide regulations for the use of cyber weapons. Lucas argues that cyber warfare is permissible "if it aims primarily at harming military infrastructure, degrades an adversary's ability to undertake highly destructive offensive operations, harms no civilians and/or destroys little or no civilian infrastructure in the process, and is waged as a last resort in the sense that all reasonable alternatives short of attack have been attempted to no avail, and further delay would only make the situation worse."

The contribution by Denning and Strawser also concerns the ethical principles for the deployment of cyber weapons. In particular, this contribution focuses on the international law of armed conflict. It defends the thesis that, at least in some circumstances, the use of cyber weapons not only respects the principles of Just War Theory, but that a "positive duty to employ" such weapons may arise in certain contexts. It is argued that in some cases the option of using cyber weapons is not just permissible for a state, it is actually a moral duty. The moral obligation rests on the consideration that non-kinetic cyber attacks may reduce the risk of bloodshed.

Lee's analysis focuses on cyber attacks and the suitability of Just War Theory for providing some guidance to them. The chapter first investigates the nature of cyber attacks and cyberwar. It then considers cyber attacks on the basis of the principles of *jus ad bellum* and *jus in bello*. Finally, it concludes that while cyber attacks are a novel form of conflict, their ethical dimensions can be understood for the most part in terms of the traditional categories of Just War Theory. At the same time, Lee maintains that the principle of last resort cannot be applied in case of cyber attacks, since each side's fear

that the other is about to attack will make it impossible for either side to explore effectively options short of war for resolving the conflict.

Taddeo's chapter has the twofold goal of filling the theoretical vacuum surrounding IW and of grounding the definition of new ethical principles for this phenomenon. The chapter argues that Just War Theory is a necessary but insufficient instrument for evaluating the ethical implications of IW and that a suitable ethical analysis of this kind of warfare may be developed by merging Just War Theory with Information Ethics. The initial part of the chapter describes IW and its main features, and highlights the problems that arise when Just War Theory is endorsed as a means of addressing ethical problems caused by IW. The final part introduces the main aspects of Information Ethics and defines three principles for a Just IW.

The third section comprises three chapters that adopt alternative approaches to Just War Theory for analysing the ethical implications of IW: *The Ethics of Cyber Attacks*, by Thomas W. Simpson; *Virtue in Cyber Conflict*, by Don Howard; *Armed Robots and Military Virtue*", by Shannon Vallor; and *Deception and Virtue in Robotic and Cyber Warfare,* by John Sullins.

Simpson's chapter addresses the circumstances under which it is permissible to attack ICTs' infrastructures. It analyses Just War Theory in relation to IW and it is argued that Just War Theory is appropriate for assessing the permissibility of cyber attacks in some, but not in all, contexts. The thesis defended is that the concept of *harm to property* provides the right framework to evaluate a great proportion of the moral significance of cyber attacks, which otherwise escapes the principles of Just War Theory.

Howard's analysis adopts virtue ethics to investigate the ethical issues raised by the deployment of tele-operated robotic weapons. The analysis first describes the role of virtue ethics in decision-making processes in general and in war-related circumstances in particular. It then addresses two fundamental questions: whether the technologizing of war made honour and courage irrelevant; and how relying upon the integrity of the cyber warrior (the soldier who remotely controls robotic weapons) may ensure ethical action in cyber conflicts. The analysis concludes by considering how the principles of virtue ethics should be included in the training and evaluation processes of cyber warriors.

Vallor's contribution examines the impact of the progress of military robotics on the perception of virtues in military contexts. While early reflections on the ethical implications of military robotics have focused primarily on utilitarian or deontological considerations, this chapter stresses the importance of an intensive and rigorous treatment of the virtues in the context of military robotics. Three aspects are analysed in detail: the effects of the developments in robotics on the contexts of military action in which moral

excellence is displayed; the possibilities and the modes in which robots could embody or emulate virtues, especially prudence and excellence; and the redefinition of the way in which scientists and engineers, both military and civilian, understand their ethical roles in society when 'engineering virtue' in military robotics.

Sullin's chapter considers how robotic and cyber weaponry could be deployed in such a way that our commitments to just and legal warfare are enhanced and not degraded. In particular, the chapter explores the possibilities of designing and developing information technologies that can help us make better decisions on the battlefield. A central aspect of the proposed analysis concerns the concept of deception and the implementation of deceptive strategies by virtuous artificial agents, which are considered trustworthy agents by their 'fellow soldiers'. The chapter concludes by redefining the concepts of deception and trust in relation to artificial agents.

Finally, an afterword by Neelie Kroes concludes the volume. The contribution describes the interests and commitments of the European Digital Agenda with respect to the research for the development of robots to be deployed in several circumstances, of which warfare is one. It also illustrates the goals, namely, ease of use, safety, and autonomy, of the research developed within the European Community and devoted to the design of robots in general, and robotic weapons in particular. The contribution concludes by considering the ethical problems that arise from developing and deploying machines that are autonomous to some degree, such as, for example, the assessment of the responsibility for actions performed by robots.

References

Arquilla, J. 1998. Can information warfare ever be just?. *Ethics and Information Technology*. 1: 203-212.

Arquilla, J. 1999. Ethics and information warfare. In *Strategic appraisal: the changing role of information in warfare*, eds. Z. Khalilzad, J. White and A. Marsall, 379-401. Santa Monica, USA: Rand Corporation.

Arquilla, J. and D. A. Borer, Eds. 2007. *Information Strategy and Warfare: A Guide to Theory and Practice (Contemporary Security Studies)*. New York, USA: Routledge.

Arquilla, J. and D. Ronfeldt 1997. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA: RAND Corporation.

Brenner, S. W. 2008. *Cyberthreats*. New York, USA: Oxford University Press.

C.Von Clausewitz, F. N Maude, et al. (2008). *On war*. Radford, VA: Wilder Publications.

Ciborra, C. 2005. Interpreting e-government and development: Efficiency, transparency or governance at a distance?. *Information Technology & People* 18: 260- 279.

Denning, D. 1999. *Information warfare and security*. Boston, USA: Addison-Wesley.

Denning, D. 2007. The Ethics of Cyber Conflict. In *Information and Computer Ethics.*, eds. K. E. Himma and H. T. Tavani, 407-428. Hoboken, USA: Wiley.

Dipert, R. R. 2011. The Ethics of Cyberwarfare. *Journal of Military Ethics*. 9: 384-410.

Floridi, L. 2010. The Digital Revolution as The Fourth Revolution. *Invited contribution to the BBC online program Digital Revolution*.

Floridi, L. 2010. *Information: A Very Short Introduction*. Oxford, UK: Oxford University Press.

Gelven, M. 1994. *War and Existence*. Philadelphia, PA: Pennsylvania State University Press.

Lauterpacht, H., Ed. 1952. *Oppenheim, International Law*.

Libicki, M. 1996. *What is Information Warfare?*. Washington, DC, USA: National Defense University Press.

Matthias, A. 2004. The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*. 6: 175-183.

Saxena, K. B. C. 2005. Towards excellence in e-governance. *Journal of Public Sector* Management. 18: 498 - 513.

Schmitt, M. N. 2008. *Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflicts*. Proceedings of Workshop on Deterring Cyberattacks, National Research Council: The National Academies Press.

Sparrow, R. 2007. Killer Robots. *Journal of Applied Philosophy*. 24: 62-77.

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

Taddeo, M. 2012. Information Warfare: a Philosophical Perspective. *Philosophy and Technology*. 25: 105-120.

Toffler, A. and H. Toffler 1997. Foreword: The New Intangibles. In *In Athena's Camp: Preparing for Conflict in the Information Age*, eds. J. Arquilla and D. Ronfeldt, xii-xxiv. Santa Monica, CA: RAND Corporation.