Preprint from http://rosariataddeo.net
This is a preprint version of an article accepted for publication in *APA Newsletter on Philosophy and Computers*

Information warfare: the ontological and regulatory gap*

Mariarosaria Taddeo
Department of Politics and International Studies, University of Warwick, UK
m.taddeo@warwick.ac.uk

1. Introduction

In his 1985 paper "What is Computer Ethics?" Moor discussed the changes that the information revolution was prompting as well as the relevance and the need for conceptual analysis addressing such changes. In his words: "although a problem … may seem clear initially, a little reflection reveals a *conceptual muddle*. What is needed in such cases is an analysis which provides a coherent *conceptual framework within which to formulate a policy for action*" ((Moor 1985), emphasis added).

Almost three decades later, with contemporary societies turning into information societies, the policy vacuum and the conceptual muddle underpinning it have become not just evident but pressing issues to be solved. Understanding and regulating privacy, anonymity, as well as security and well-being in the information age have become crucial to the existence and functioning of our societies and the well-being of their citizens. Information warfare (IW) is one of the most compelling cases to be addressed.

Historically, technological breakthroughs determine changes affecting the structure of both civil society and military organisations. As described by Toffler and Toffler (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 (L. Floridi 2014). Information and communication technologies (ICTs) have reshaped social interactions; they provide new tools for the management of information and bureaucracy; and when considered with respect to warfare, ICTs determine the latest revolution in military affairs, making IW the warfare of the information age.

IW raises a number of ethical and regulatory problems, all of which rest on a key feature, namely its transversality (M. Taddeo 2012). IW may arise and target physical as

well as non-physical objects, it may go from non-violent to highly violent, and also prompts an increasing blurring of the distinction between military and civilian, as it no longer reflects the distinction between combatant and non-combatant. The transversality of IW, coupled with the growing dependency of contemporary societies on ICTs, unveils the potential for IW to become a new form of *total war*. For, the scope of the mobilisation, targets and resources increasingly overlaps with resources, agents and infrastructures of contemporary societies.

Regulating IW to ensure its fairness and avoid escalation risk is therefore pivotal. Since the first cyber-attack to Estonian websites in 2008, the debate surrounding the regulation of IW has grown fast and has accompanied concrete efforts to understand whether and how existing international laws and treaties could be endorsed to regulate it. Such efforts have proven to be quite demanding and were not the exclusive concern of the military; they have also had a bearing on ethicists and policy-makers, since existing ethical theories of war and national and international regulations struggle to address the novelties of this phenomenon.

In the rest of this article I will analyse how some of the most relevant tenets of Just War Theory (JTW), and the international laws and treaties implementing them, are applied to the case of IW. In doing so I will mainly focus on the interpretations of existing laws and regulations given in the so-called Tallinn Manual (NATO Cooperative Cyber Defence Centre of Excellence 2013). This has been the first and, so far, the most exhaustive work devoted to offer guidance in their application to the case of IW. The manual offers a valuable contribution to the debate over the regulation of IW, for it shows that extant laws and treaties can be stretched to address this phenomenon and that when it comes to the international ground, the cyber-sphere is not a new Wild West. I will argue, however, that it would be a mistake to consider the stretching of existing laws and treaties as the ultimate and perfectly satisfying strategy to regulate IW, for existing laws and treaties struggle to fully address the changes prompted by this phenomenon and the ethical problems that it poses.

While the application of existing laws and treaties to IW is indeed possible, it is at the same time a *stretch*, which will eventually reach its limits and generate a regulatory vacuum. To overcome the latter, a theoretical effort is needed to fully understand the nature of this new phenomenon, its ethical, political and social implications, and so to design new norms and principles that will allow for regulating IW not by stretching an old blanket but by properly and adequately addressing the novelty of this new phenomenon. I

shall begin this analysis by offering a definition of IW, in order to clear the ground of any possible misunderstandings.

2. Dissolving the mist of information warfare

The expression 'information warfare' has already been used in the extant literature to refer solely to the uses of ICTs devoted to breaching the opponent's informational infrastructure in order to either disrupt it or acquire relevant data and information about the opponent's resources, military strategies and so on; see for example (Libicki 1996) (Waltz 1998) (Schwartau 1994).

Distributed denials of service (DDoS) attacks, like the ones launched in Burma during the 2010 elections,[1] the injection of Stuxnet in the Iranian nuclear facilities of Bushehr,[2] as well as 'Red October' (discovered in 2013) are all famous examples of how ICTs can be used to conduct cyber-attacks.[3] Nonetheless, such attacks are only one instance of IW. In what follows I will use a definition of IW that I provided in (Taddeo 2012) and refer to IW to indicate a wide spectrum of phenomena, encompassing cyber-attacks as well as the deployment of robotic weapons and ICT-based communication protocols.[4]

IW is thus defined as follows:

> "Information Warfare is the use of ICTs within an offensive or defensive military strategy endorsed by a [political authority] and aimed at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging across the physical and non-physical domains and whose level of violence may vary upon circumstances." (Mariarosaria Taddeo 2014) (p. 3)

The informational nature and transversality of IW can be properly appreciated once they are considered within the framework of the so-called information revolution (Floridi 2014). The information revolution has a wide impact on many of our daily practices: from our social and professional lives to our interactions with the environment that surrounds

[1] http://www.bbc.co.uk/news/technology-11693214 http://news.bbc.co.uk/2/hi/europe/6665145.stm
[2] http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml
[3] For an annotated time line of cyber attacks see NATO's website http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm
[4] The reader may refer to (Taddeo 2012 and Taddeo 2014) for a more detailed analysis of the reasons supporting such a definition.

us. With the information revolution we have witnessed a shift, which has brought the *non-physical domain* to the fore and made it as important and valuable as the physical one (Taddeo 2012).

IW is one of the most compelling instances of such a shift. It shows that there is a new environment, where physical and non-physical entities coexist and are equally valuable, and in which states have to prove their authority and new modes of warfare are being specifically developed for this purpose.[5] The shift towards the non-physical domain provides the ground for the transversality of IW. This is a complex aspect, and it can be better understood when IW is compared with traditional forms of warfare.

Traditionally, war entails the use of a state's *violence* through the state *military forces* to determine the conditions of governance over a determined territory (Gelven 1994). It is a necessarily violent phenomenon, which implies the sacrifice of human lives and damage to both military and civilian infrastructures. Here, the state faces the problem of how to minimise damage and losses while ensuring the enemy is overpowered.

IW is different from traditional warfare in several respects, mainly because it is not a necessarily violent and destructive phenomenon (Arquilla 1998) (Dipert 2010) (Barrett 2013). For example, IW may involve a computer virus capable of disrupting or denying access to the enemy's database, and in so doing it may cause severe damage to the opponent without exerting *physical* force or violence. In the same way, IW does not necessarily involve human beings. In this context, an autonomous artificial agent can conduct an action of war, such as, for example, in the cases of EADS Barracuda, and the Northrop Grumman X-47B,[6] or in the case of autonomous cruising computer viruses (Abiola, Munoz, and Buchanan 2004) targeting other artificial agents or informational infrastructures, like a database or a website. IW can be waged exclusively in a digital context without ever involving physical targets; nevertheless it may escalate to more violent forms (Arquilla 2013) (Clarke 2012) (Brenner 2011) (Bowden 2011).

As remarked above, the transversality of IW is the key feature of this phenomenon; it is the aspect that most differentiates it from traditional warfare. Transversality is also the feature that engenders the ethical problems posed by IW. The

---

[5] The USA only spent $400 million in developing technologies for cyber conflicts: http://www.wired.com/dangerroom/2010/05/cyberwar-cassandras-get-400-million-in-conflict-cash/ The UK devoted £650 million to the same purpose: http://www.theinquirer.net/inquirer/news/1896098/british-military-spend-gbp650-million-cyber-warfare

[6] Note that MQ-1 Predators and EADS Barracuda, and the Northrop Grumman X-47B are Unmanned Combat Aerial Vehicles used for combat actions and they are different from Unmanned Air Vehicles, like for example Northrop Grumman MQ-8 Fire Scout, which are used for patrolling and recognition purposes only.

potential bloodless and non-destructive nature of IW (Denning 2007) (Arquilla 2013) makes it desirable from both an ethical and a political perspective, since at first glance it seems to avoid bloodshed and it liberates political authority from the burden of justifying military actions to the public. However, the disruptive outcomes of IW can inflict serious damage to contemporary information societies and at the same time may potentially lead to highly violent and destructive consequences – dangerous for both military forces and civil society. Consider, for example, the data diffused for GridExII.[7] This is a simulation that was conducted in the US in November 2013. More than two hundred utility companies collaborated with the US government to simulate a massive cyber-attack on the US's basic infrastructure. Had the attack been real, estimates mention hundreds of injuries and tens of deaths, while millions of US citizens would have been left in darkness.

The need for strict regulations for declaring and waging a fair IW is now compelling. To this end an analysis that discloses the ethical issues related to IW while pointing in the direction of their solution is a preliminary and necessary step. This will be the task of the next section.

3. Regulating IW: *jus ad bellum*

I will now focus on the application of *jus ad bellum* to cases of IW. Part of the problem relating to *jus ad bellum* concerns the so-called attribution problem and the difficulties of tracing back the author of a cyber-attack. As this seems to be more a technically related problem than a conceptual one, I shall not focus on it here. Also, I shall not focus on the problems related to *jus ad bellum*, as they have been extensively analysed elsewhere (Taddeo 2014) (L. Floridi and Taddeo 2014). Rather, my attention will be devoted to the definition of what counts as an use of force in IW and what, as such, can trigger the waging of a war or a conflict.

I shall first consider some of the most common definitions of cyber-attacks, for they underpin the application of existing tenets of *jus ad bellum* to the case of IW. In this respect it is quite useful to compare two definitions, the one provided by the National Research Council in its 2009 report on cyber-attack capabilities (*Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* 2014), and the one offered in the Tallinn Manual. In the former, a cyber-attack is defined as "the use if deliberate actions – perhaps over an extended period of time – to alter, disrupt deceive, degrade or

[7] http://www.nytimes.com/2013/11/15/us/coast-to-coast-simulating-onslaught-against-power-grid.html

destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (p. 80).

The Tallinn Manual defines cyber-attacks as "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to object" (NATO Cooperative Cyber Defence Centre of Excellence 2013)(p. 106). The National Research Council's definition offers a more specific characterisation of cyber-attacks, including non-physical damages as well as physical ones, while the scope of the definition offered by the Tallinn Manual remains undecided, for it depends on the definition of 'objects'. If these are understood as *physical* objects, then the manual is by default considering as attacks only kinetic uses of cyber-technologies. This seems actually to be the case if one considers the focus of the definition on physical damages and the absence of any reference to damages to intangible objects, e.g. data, information, informational infrastructure.

The consequences of such an approach are extremely relevant for they affect the application of *jus ad bellum* as well as of *jus in bello*. For example, rule 10 of the Tallinn Manual stresses that under *jus ad bellum* 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-attack amounts to a use of force if its scale and effects are similar to those of non-cyber-operations. In this sense the Tallinn Manual follows Hoisington (Hoisington 2009), according to whom cyber-attacks that are intended to cause physical damage should be categorized as uses of force.

Criteria based on the magnitude and effects of a cyber-attack have been proposed to assess if the former amounts to a use of force or to an armed attack, like the one described in Rule 11 of the Tallinn Manual. This compares the effects of a cyber-attack with the scale of effects of a conventional attack in order. To support such an assessment several tests can be run, the most famous one being the Pictet's[8] test, which focuses on the scope, duration and intensity of the attack. Heyes and Kesan (Hayes and Kesan 2014) report that there are three models that can be used to apply the test to the case of cyber-attacks: "[I]nstrument-based models look at whether the damage caused was of the kind that previously would have required a kinetic attack, such as shutting down a power grid. Effects-based models focus on the overall effect on the victim state, such as an information attack on financial institutions that causes significant damage to the economic

[8] Jean Pictet was a Swiss jurist and the General Editor for the Geneva Conventions of 12 August 1949.

well-being of the victim state. Finally, a strict liability model would consider any cyber-attack directed at critical infrastructure to be an armed attack" (p. 10).

All this is quite uncontroversial, for a cyber-attack that has the same or similar effects to a conventional attack should be treated as a kinetic attack in the eye of the law. In this case it is true what Schmitt states: "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).

However, while very interesting and important, this approach inevitably finds its own limit as it overlooks the conceptual roots, i.e. JWT, on which laws regulating IW rest. In doing so, it misses the possibility of truly expanding the scope of existing laws by reshaping their conceptual framework. The consequence is that the approach fails to consider and to account for the conceptual changes prompted by IW and risks confusing an *ad hoc* remedy with the long-term solution, and, in the long run, risks imposing conceptual limitations on the laws and regulation for IW.

A good example in this respect concerns the application of the principle of just cause to IW. As Barrett (Barrett 2013) noted: "Since damage to property may constitute a just cause, can temporary losses of computer functionality also qualify as a *casus belli*? Like kinetic weapons, cyber-weapons can physically destroy or damage computers. But offensive computer operations, because of their potential to be transitory or reversible, can also merely compromise functionality. While permanent loss of functionality create the same effect as physical destruction, temporary functionality losses are unique to cyber-operations and require additional analysis" (p. 6).

The issue is not whether the case of IW can be considered in such a way as to fit the parameters of kinetic warfare and hence to fall within the domain of JWT, 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 JWT rests and its ability to *satisfactory* and *fairly* accommodate the changes brought to the fore by the information revolution. The time has come to consider in more detail such changes, this will be the task of the next section.

4. The ontological gap

JWT mainly focuses on the use of force in international contexts and surmises sanguinary and violent warfare occurring in the physical domain. As the cyber-domain is virtual and IW mainly involves abstract entities, the application of JWT becomes less direct and

intuitive. The struggle encountered when applying JWT to the cases of IW becomes even more evident if one considers how pivotal concepts such as harm, target, and attack have been reshaped by the dissemination of IW. The very notion of harm, for example, which is at the basis of JWT, struggles to apply to the case of IW. This is a problem that has been already highlighted in the extant literature; see for example Dipert, who argues that any moral analysis of this kind of warfare needs to be able to account for a notion of harm "[focusing] away from strictly injury to human beings and physical objects toward a notion of the (mal-) functioning of information systems, and the other systems (economic, communication, industrial production) that depend on them" (Dipert 2010) (p. 386).[9]

The transversality of the ontological status of the entities involved in IW is particularly relevant as we try to shed some light on IW's novelty. Traditional warfare concerns human beings and physical objects, while IW involves artificial and non-physical entities alongside human beings and physical objects. Therefore, there is a *hiatus* between the ontology of the entities involved in traditional warfare and those involved in IW. Such a hiatus affects the ethical analysis, for JWT rests on an anthropocentric ontology, i.e. moral discourse is solely concerned with respect for human rights and disregards all non-human entities, and for this reason it does not provide sufficient means for addressing the case of IW (more details on this aspect presently).

The gap between the ontology assumed by JWT and the ontology of IW has also been described by Dipert, who stresses that "[s]ince cyber-warfare is by its very nature information warfare, an ontology of cyber-warfare would necessarily include [a] way of specifying *information objects* …, *the disruption and the corruption of data and the nature and the properties of malware*. This would be in addition to what would be required of a domain-neutral upper-level ontology, which addresses this type of characteristics of the most basic categories of entity that are used virtually in sciences and domain: material entity, event, quality of an object, physical object. A cyber-warfare ontology would also go beyond … a military ontology, such as agents, intentional actions, unintended effects, organizations, artefacts, commands, attacks and so on" (Dipert 2013, p. 36; emphasis added).

The case of the autonomous cruising computer virus will help to clarify the problems at stake (Abiola, Munoz and Buchanan 2004). These viruses are able to navigate through the web and identify autonomously their targets and attack them without requiring any supervision. The targets are chosen on the basis of parameters that the

[9] The need to define concepts such as those of harm, target and violence is stressed both by scholar who argue in favor of the ontological difference of the cyber warfare (Dipert 2013) and exploit this point to claim that JWT is not an adequate framework to address IW and by those who actually maintain that JWT provides sufficient element to address the case of IW (Lucas 2012).

designers encode in the virus, so there is a boundary to the autonomy of these agents. Still, once the target has been identified, the virus attacks without having to receive 'authorisation' from the designer or any human agent.

In considering the moral scenario in which the virus is launched, three main questions arise. The first question revolves around the identification of the moral agents, for it is unclear whether the virus itself should be considered the moral agent, or whether this role should be attributed to the designer or to the agency that deployed the virus, or even to the person who actually launched it. The second question focuses on moral patients. The issue arises as to whether the attacked computer system itself should be considered the moral receiver of the action, or whether the computer system and its users should be considered the moral patients. Finally, the third question concerns the rights that should be defended in the case of a cyber-attack. In this case, the problem is whether any rights should be attributed to the informational infrastructures or to the system compounded by the informational infrastructure and the users.

As noted by Dipert (Dipert 2012), IW includes informational infrastructures, computer systems and databases. In doing so, it brings new objects, some of which are intangible, into the moral discourse. The first step towards an ethical analysis of IW is to determine the moral status of such (informational) objects and their rights. Help in this respect is provided by Information Ethics, which will be introduced in the Section 5.

5. Information ethics

Information Ethics is a macro-ethics which is concerned with the whole realm of reality and provides an analysis of ethical issues by endorsing an informational perspective. Such an approach rests on the consideration that "ICTs, by radically changing the informational context in which moral issues arise, not only add interesting new dimensions to old problems, but lead us to rethink, methodologically, the very grounds on which our ethical positions are based" (Floridi 2006) (p. 23).

In just one sentence Information Ethics is defined as a *patient-oriented*, *ontocentric*, and *ecological* macro-ethics. It is patient-oriented, because it considers the morality of an action with respect to its effects on the receiver of that action. It is ontocentric, for it endorses a non-anthropocentric approach for the ethical analysis. It attributes a moral value to all existing entities (both physical and non-physical) by applying the principle of ontological equality: "This ontological equality principle means that any form of reality …, simply for the fact of being what it is, enjoys a minimal, initial, *overrideable*, equal right to

exist and develop in a way which is appropriate to its nature" (Floridi 2013). The principle of ontological equality is grounded on an information-based ontology,[10] according to which all existing things can be considered from an informational standpoint and are understood as informational entities, all sharing the same informational nature.

The principle of ontological equality shifts the standpoint for the assessment of the moral value of entities, including technological artefacts. At first glance, an artefact, a computer, a book or the Colosseum seems to enjoy only an instrumental value. This is because one endorses an anthropocentric Levels of Abstraction (LoA)[11] (Luciano Floridi 2008); in other words, one considers these objects as a user, a reader, a tourist. In all these cases, the moral value of the observed entities depends on the agent interacting with them and on her purpose in doing so.

The claim put forward by Information Ethics is that these LoAs are not adequate to support an effective analysis of the moral scenario in which the artefacts may be involved. The anthropocentric, or even the biocentric, LoA prevent us from properly considering the nature and the role of such artefacts in the reality in which we live. The argument is that all existing things have an informational nature, which is shared across the entire spectrum; from abstract to physical and tangible entities, from rocks and books to robots and human beings. Further, all entities enjoy some minimal initial moral value *qua informational* entities.

Information Ethics argues that universal moral analyses can be developed by focusing on the common nature of all existing things and by defining good and evil with respect to such a nature. The focus of ethical analysis is thereby shifted, since the initial moral value of an entity does not depend on the observer, but is defined in absolute terms and depends on the (informational) nature of the entities. Following the principle of ontological equality, minimal and overrideable rights to exist and flourish pertain to all existing things and not just to human or living things. The Colosseum, Jane Austin's

[10] The reader may recall the informational LoA mentioned in section 2. Information Ethics endorses an informational LoA, as such it focuses on the informational nature as a common ground of all existing things.
[11] A LoA is a finite but non-empty set of observables accompanied by a statement
of what feature of the system is under consideration. A collection of LoAs constitutes an interface. An interface is used when analysing a system from various points of view, that is, at varying LoAs. For example, a glass of wine observed at a chemical LoA consists of the observables of the chemical processes on going in liquid, while the same glass of wine being observed at the LoA of drinker might be identified by the observables that represent its taste and bouquet. A single LoA does not reduce a glass of wine to merely its on-going chemical processes or to its taste and bouquet. Rather, it is a tool that males explicit the observation perspective and restricts it to only those elements that are relevant in a given observation. LoAs are hierarchically organized; a high LoA enables a general perspective and allows for a general analysis of the observed system. A low LoA provides a less general perspective and allows for a more detailed analysis.

writings, a human being and computer software all share *initial* rights to exist and flourish, as they are all informational entities.[12]

A clarification is now necessary. Information Ethics endorses a minimalist approach. It considers informational nature as the minimal common denominator among all existing things. However, this minimalist approach should not be mistaken for reductionism, as Information Ethics does not claim that the informational approach is the unique LoA from which moral discourse is addressed. Rather, it maintains that the informational LoA provides a *minimal starting point*, which can then be enriched by considering other moral perspectives.

Lest the reader be mislead, it is worthwhile emphasising that the principle of ontological equality does not imply that all entities have the same moral value. The rights attributed to the entities are *initial*; they can be overridden whenever they conflict with the rights of other (more morally valuable) entities. Furthermore, the moral value of an entity is determined according to its potential contribution to the enrichment and the flourishing of the informational environment. Such an environment, the *Infosphere* (Floridi 2013), includes all existing things, be they digital or analogue, physical or non-physical, and the relations occurring among them and also between them and the environment. The blooming of the Infosphere is the ultimate good, while its corruption, or destruction, is the ultimate evil.

In particular, any form of corruption, depletion or destruction of informational entities or of the Infosphere is referred to as *entropy*. In this case, entropy refers to "any kind of *destruction* or *corruption* of informational objects (mind, not of information), that is, any form of impoverishment of *being*, including *nothingness*, to phrase it more metaphysically" (Floridi 2013) and has nothing to do with the concept developed in physics or in information theory (Floridi 2007).

Information Ethics considers the duty of any moral agent with respect to its contribution to the informational environment, and considers any action that affects the environment by corrupting or damaging it, or by damaging the informational objects existing in it, as an occurrence of entropy, and therefore as an instance of evil (Floridi and Sanders 2001). On the basis of this approach, Information Ethics provides four principles to identify right and wrong and the moral duties of an agent:

0. entropy ought not to be caused in the infosphere (null law);

[12] For more details on the information-based ontology see (Floridi 2002) . The reader interested in the debate on the Informational ontology and the principles of Information Ethics may whish to see (Floridi 2007).

1. entropy ought to be prevented in the infosphere;
2. entropy ought to be removed from the infosphere;
3. the flourishing of informational entities as well as of the whole infosphere ought to be promoted by preserving, cultivating and enriching their properties.

These four principles together with the theoretical framework of Information Ethics will provide the ground to proceed further in our analysis, and define the principles for a just IW.

6. Just IW

The first step towards a definition of the principles for a just IW is to understand the moral scenario determined by this phenomenon. The framework provided by Information Ethics proves to be useful in this regard, for it allows for answering questions concerning the moral stance of the receivers of the actions performed in IW scenarios. The principle of ontological equality is quite useful in this respect, for it states that all (informational) entities enjoy some minimal initial rights to exist and flourish in the Infosphere, and therefore every entity deserves some minimal respect, in the sense of a "disinterested, appreciative and careful attention" (Hepburn 1984), (Floridi 2013).

When applied to IW, this principle enables us to consider all entities that may be affected by an action of war as moral patients. A human being, who gains some benefits from the consequences of a cyber-attack, and an informational infrastructure, which is disrupted by a cyber-attack, are both to be held as moral patients, as they are both the receivers of the moral action. Following Information Ethics, the moral value of such an action is to be assessed on the basis of its effects on the patients' rights to exist and flourish, and ultimately on the flourishing of the Infosphere.

The issue then arises concerning which and whose rights should be preserved in the case of IW. The answer to this question follows from the rationale of Information Ethics, according to which an entity may lose its rights to exist and flourish when it comes into conflict (causes entropy) with the rights of other entities or with the well-being of the Infosphere. It is a moral duty of the other inhabitants of the Infosphere to *remove* such a malicious entity from the environment, or at least to impede it from perpetrating more evil.

This framework lays the ground for the first principle for just IW since it prescribes the condition under which the decision to resort to IW is morally justified.

I. IW ought to be waged only against those entities that endanger or disrupt the well-being of the Infosphere.

Two more principles regulate just IW. They are:

II. IW ought to be waged to preserve the well-being of the Infosphere.

III. IW ought not to be waged to promote the well-being of the Infosphere.

The second principle limits the task of IW to restoring the *status quo* in the Infosphere before the malicious entity begins increasing entropy within it. IW is just so long as its goal is to *repair* the Infosphere from the damage caused by the malicious entity.

The second principle can be described using an analogy, namely, IW should fulfil the same role as police forces in a democratic state. It should act only when a crime has been, or is about to be, perpetrated. Police forces do not act in order to ameliorate the aesthetics of cities or the fairness of a state's laws; they only focus on reducing or preventing crimes from being committed. Likewise, IW ought to be endorsed as an *active* measure in response to the increasing of evil, and not as a proactive strategy to foster the flourishing of the Infosphere. Indeed, this is explicitly forbidden by the third principle, which prescribes the promotion of the well-being of the Infosphere as an activity that falls beyond the scope of a just IW.

These three principles rest on the identification of the moral good with the flourishing of the Infosphere and the moral evil with the increasing of entropy in it. They endorse an informational ontology, which allows for including in the moral discourse both non-living and non-physical entities. The principles also prescribe respect for the (minimal and overrideable) rights of such entities along with those of human beings and other living things, and respect for the rights of the Infosphere as the most fundamental requirement for declaring and waging a just IW.

In doing so, the three principles overcome the ontological hiatus described in Section 3 and provide the framework for applying JWT to the case of IW. As such they point towards the direction for defining a new regulation for IW, which would be able to take into account the nature of the agents, targets and environment involved in this phenomenon.

7. Conclusion

The goals of this article have been to fill the conceptual vacuum surrounding IW and to provide the ethical principles for a just IW, which can help in filling the vacuum. I have argued that JWT provides the necessary but not sufficient tools for this purpose. For,

although its ideal of just warfare grounded on respect for basic human rights in the theatre of war holds also in the case of IW, it does not take into account the moral stance of non-human and non-physical entities which are involved and mainly affected by IW. This is the ontological hiatus, which I identified as the nexus of the ethical problems encountered by IW.

I also stressed that in order to be applicable to the case for IW, JWT must extend the scope of the moral scenario to include non-physical and non-human agents and patients. Information Ethics has been introduced as a suitable ethical framework capable of considering human and artificial, physical and non-physical entities in the moral discourse. It has been argued that the ethical analysis of IW is possible when JWT is merged with Information Ethics. In other words, JWT *per se* is too large a sieve to filter the issues posed by IW. Yet, when combined with Information Ethics, JWT acquires the necessary granularity for addressing the issues posed by this form of warfare.

It would be misleading to consider the problems described in this article as reasons for dismissing JWT when analysing IW, or for discarding altogether existing laws and regulations of warfare. Instead these problems point to the need to consider more carefully the case of IW, and to take into account its peculiarities, so that an adequate conceptual framework will be developed to properly take into account 'contemporary values' while developing laws to regulate IW.

References

Abiola, A, J Munoz, and W Buchanan. 2004. "Analysis and Detection of Cruising Computer Viruses." In *EIWC*.

Arquilla, J. 1998. "Can Information Warfare Ever Be Just?" *Ethics and Information Technology* 1 (3): 203–12.

Arquilla, John. 2013. "Twenty Years of Cyberwar." *Journal of Military Ethics* 12 (1): 80–87. doi:10.1080/15027570.2013.782632.

Barrett, Edward 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.

Bowden, Mark. 2011. *Worm: The First Digital World War*. New York: Atlantic Monthly Press.

Brenner, Joel. 2011. *America the Vulnerable: New Technology and the Next Threat to National Security*. New York: Penguin Press.

Clarke, Richard A. 2012. *Cyber War: The Next Threat to National Security and What to Do About It*. 1st Ecco pbk. ed. New York: Ecco.

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.

Dipert, Randall. 2013. "The Essential Features of an Ontology for Cyberwarfare." In *Conflict and Cooperation in Cyberspace*, edited by Panayotis Yannakogeorgos and Adam Lowther, 35–48. Taylor & Francis. http://www.crcnetbase.com/doi/abs/10.1201/b15253-7.

Floridi, L. 2002. "On the Intrinsic Value of Information Objects and the Infosphere." *Ethics and Information Technology* 4 (4): 287–304.

———. 2007. "Understanding Information Ethics." *APA Newsletter on Philosophy and Computers* 7 (1): 3–12.

———. 2013. *Ethics of Information*. Oxford, New York: Oxford University Press.

Floridi, L, and J Sanders. 2001. "Artificial Evil and the Foundation of Computer Ethics." *Ethics and Information Technology* 3 (1): 55–66.

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

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

Floridi, Luciano. 2006. "Information Ethics, Its Nature and Scope." *SIGCAS Comput. Soc.* 36 (3): 21–36. doi:10.1145/1195716.1195719.

———. 2008. "The Method of Levels of Abstraction." *Minds and Machines* 18 (3): 303–29. doi:10.1007/s11023-008-9113-7.

Gelven, Michael. 1994. *War and Existence: a Philosophical Inquiry*. University Park, Pa: Pennsylvania State University Press.

Hayes, Carol M., and Jay P. Kesan. 2014. *Law of Cyber Warfare*. SSRN Scholarly Paper ID 2396078. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=2396078.

Hepburn, Ronald W. 1984. *"Wonder" and Other Essays: Eight Studies in Aesthetics and Neighbouring Fields*. Edinburgh: University Press.

Hoisington, Matthew. 2009. *Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense*. SSRN Scholarly Paper ID 1542223. Rochester, NY: Social Science Research Network. http://papers.ssrn.com/abstract=1542223.

Libicki, M. 1996. *What Is Information Warfare?* Washington, D.C, USA: National Defense University Press.

Lucas, G. R. 2012. "Just War and Cyber Conflict 'Can There Be an "Ethical" Cyber War?'" presented at the Naval Academy Class 2014.

Moor, James H. 1985. "What Is Computer Ethics?*." *Metaphilosophy* 16 (4): 266–75. doi:10.1111/j.1467-9973.1985.tb00173.x.

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*. Cambridge ; New York: Cambridge University Press.

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

Schwartau, Winn. 1994. *Information Warfare: Chaos on the Electronic Superhighway*. 1st ed. New York : Emeryville, CA: Thunder's Mouth Press ; Distributed by Publishers Group West.

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

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

Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. 2014. Accessed July 31. http://www.nap.edu/catalog.php?record_id=12651.

Toffler, Alvin, and Anna Toffler. 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.

Waltz, Edward. 1998. *Information Warfare: Principles and Operations*. Boston: Artech House.