Chapter 8
Information Warfare and Just War Theory

Mariarosaria Taddeo

Abstract This article is devoted to developing an ethical analysis of information warfare, the warfare waged in the cyber domain. It has the twofold goal of filling the theoretical vacuum surrounding this phenomenon and of providing the grounding for the definition of new ethical regulations for information warfare. The article maintains that Just War Theory is a necessary but not sufficient instrument for considering the ethical implications of information warfare and argues that a suitable ethical analysis of this kind of warfare is developed when Just War theory is merged with Information Ethics. The initial part of the article describes information 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 information warfare. The final part introduces the main aspects of Information Ethics and defines three principles for a just information warfare.

8.1 Introduction

The cyberspace is nowadays conceived as the fifth domain in which war may be waged, along with land, sea, air and space, for the ability to control, disrupt or manipulate the enemy's informational infrastructure has become as decisive with respect to the outcome of conflicts as weapon superiority. In this respect, information and communication technologies (ICTs) have proved to be a useful and convenient technology for waging war.

The military deployment of ICTs has radically changed the way wars are declared and waged nowadays. It has actually determined the latest revolution in military affairs, i.e. the informational turn in military affairs (Toffler and Toffler

M. Taddeo (✉)
Cyber Security & Ethics, Department of Politics and International Studies,
University of Warwick, Coventry, United Kingdom
e-mail: M.Taddeo@warwick.ac.uk

Uehiro Centre for Practical Ethics, University of Oxford, Oxford, United Kingdom

L. Floridi, M. Taddeo (eds.), *The Ethics of Information Warfare,*
Law, Governance and Technology Series 14, DOI 10.1007/978-3-319-04135-3_8,
© Springer International Publishing Switzerland 2014

1997).[1] Such a revolution is not the exclusive concern of the military; it has also a bearing on ethicists and policymakers, since existing ethical theories of war and national and international regulations struggle to address the novelties of this phenomenon.

This article is devoted to developing an ethical analysis of information warfare (IW). It has the twofold goal of filling the theoretical vacuum surrounding this phenomenon and of providing the conceptual grounding for the definition of new ethical regulations for IW. The proposed analysis rests on the conceptual investigation of IW provided in (Taddeo 2012), which highlights the informational nature of this phenomenon, and argues that IW represents a profound novelty, which reshapes the very concept of war and raises the need for new ethical guidelines.

On the basis of this analysis, the article maintains that Just War Theory (JWT) is a necessary but not sufficient instrument for considering the ethical implications of IW. It is argued that investigating IW through the lens of JWT allows for the unveiling of fundamental ethical issues that this phenomenon brings to the fore, yet that attempting to address these issues solely on the basis of this theory will leave them unsolved.

It is suggested that problems encountered when addressing IW through JWT are overcome if the latter is merged with Information Ethics (Floridi 2013). This is a macro-ethical theory, which is particularly suitable for taking into account the features and the ethical implications of *informational phenomena*, like internet neutrality (Turilli et al. 2012), online trust (Turilli et al. 2010), peer-to-peer (Taddeo and Vaccaro 2011) and IW.

Merging the principles of JWT with the macro-ethical framework provided by Information Ethics has two advantages; it allows the development of an ethical analysis of IW capable of taking into account the peculiarities and the novelty of this phenomenon; and it also extends the validity of JWT to a new kind of warfare, which at first glance seemed to fall outside its scope (Taddeo 2012).

The initial part of this article will describe IW and its main features. It will then focus on JWT and on the problems that arise when this theory is endorsed as a means of addressing the case for IW. Information Ethics will then be introduced. Its four principles will provide the grounds for the analysis proposed in the final part of this article, where the principles for a just IW are defined. Finally, it is discussed how JWT can be applied to IW without leading to ethical conundrums. Having delineated the path ahead, we should now begin our analysis by considering in more detail the nature of IW.

8.2 Information Warfare

The expression ‘information warfare’ has already been used in some parts of 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

[1] For an analysis of revolution in military affairs considering both the history of such revolutions and the effects of the development of the most recent technologies on warfare see (Benbow 2004; Blackmore 2005).

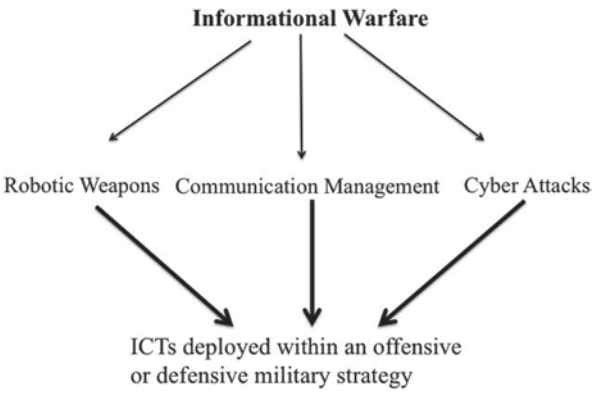

Fig. 8.1 The different uses of ICTs in military strategies. (Taddeo 2012)

information about the opponent's resources, military strategies and so on; see for example (Libicki 1996; Waltz 1998; Schwartau 1994).

The distributed denials of service (DDoS) attacks conducted in 2007 against institutional Estonian websites, the attacks launched to block the Internet communication in Burma during the 2010 elections[2] or the injection of Stuxnet, a computer-worm in the Iranian nuclear facilities of Bushehr [3] provide good examples of how ICTs can be used to conduct so-called cyber attacks. Cyber attacks are surely one of the most well-known and debated forms of ICT-based conflicts, but they should be considered only one form of IW. Equating IW with cyber attacks would lead to a too restrictive use of the label IW.

In the rest of this article, IW will refer to a wide spectrum of phenomena, encompassing cyber-attacks as well as the deployment of robotic-weapons and ICT-based communication protocols (see Fig. 8.1).

The reason for endorsing such a wide spectrum definition is twofold. On the one side, it allows for focusing on the purpose for the military deployment of ICTs rather than on the mode of their deployment. In the case of IW, the endorsement of ICTs—be it the use of (semi)autonomous weapons, of a computer virus, or of digital devices to enhance the performance of forces on the battlefield—has a *disruptive* intent. Such an intent is the main concern of the ethical analysis proposed in this article. On the other side, endorsing a wide spectrum definition has also methodological advantage. For by considering indiscriminately the different uses of ICTs in warfare, the analysis provides ethical principles addressing the totality of the cases of IW rather than some of its specific occurrences.

A parallel with the ethical analysis of traditional warfare will support such a methodological choice. JWT is concerned with warfare in general, its principles are valid in any theatre of traditional warfare, be it waged with swords or guns or by deploying nuclear weapons as long as the weapons are used with the same intent, namely to inflict physical damage on the enemy. Likewise, the analysis proposed

[2] http://www.bbc.co.uk/news/technology-11693214 http://news.bbc.co.uk/2/hi/europe/6665145.stm.

[3] http://www.cbsnews.com/stories/2010/11/29/world/main7100197.shtml.

in this article aims to provide ethical principles for a just IW valid for every mode of conducting it.

This approach neither undermines the differences between the use of a computer virus and a robotic weapon nor denies that such different uses generate different ethical issues. Rather, it asks the reader to be patient and to focus first on the aspects that are common among the different military uses of ICTs, since the analysis of these aspects provides the groundwork for addressing specific ethical problems brought to the fore by specific military uses of ICTs.

Following this approach, IW is defined as follows:

> **Information Warfare** is the use of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemy's resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances. (Taddeo 2012)

This definition highlights two aspects of IW: its *informational nature* and its *transversality*. The informational nature of IW is a consequence of the fact that this kind of warfare rests on the military deployment of technological artefacts devoted to elaborating, managing and communicating data and information. In this respect, IW shows how it is related to the so-called Information revolution.

The Information revolution is a multi-faceted phenomenon. It rests on the development and the ubiquitous dissemination of the use of ICTs, which have a wide impact on many of our daily practises: from working and interacting with other human beings, to driving and planning holidays. ICTs allow for developing and acting in a new domain, the digital or informational one (Floridi 2009). This is a completely virtual, non-physical domain, which has grown important and hosts a considerable relevant part of our lives. With the information revolution we witness 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 developed specifically for deployment in such a new environment.[4]

The shift toward the non-physical domain provides the ground for the transversality of IW. This is a complex aspect that 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. The problem

[4] 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.

to be faced when waging traditional warfare is how to minimise damage and losses while ensuring the enemy is overpowered.

IW is different from traditional warfare in several respects. It is not a necessarily violent and destructive phenomenon (Arquilla 1998). 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. An action of war in this context can be conducted by an autonomous robot, such as, for example, the EADS Barracuda, and the Northrop Grumman X-47B,[5] or by an autonomous cruising computer virus (Abiola et al. 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 concrete targets. Nevertheless, IW may escalate to more violent forms. Consider for example the consequences of a cyber attack targeting a military aerial control system causing aircraft to crash (Waltz 1998).

As remarked above, the transversality of IW is the key feature of this phenomenon; it is the aspect that differentiates it the most from traditional warfare. Transversality is also the feature that engenders the ethical problems posed by IW. The potential bloodless and non-destructive nature of IW (Denning 2009; Arquilla 1998) 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. A more attentive analysis unveils that IW can lead to highly violent and destructive consequences, which would be dangerous for both military forces and civil society. For this reason declaring and waging IW requires strict regulation to guarantee its fairness.

To this end an analysis that discloses the ethical issues that IW engenders and points at the direction for their solution is a preliminary and necessary step. The development of such analysis will be the task of the next section.

8.3 IW and Just War Theory

Ethical analyses of war are developed following three main paradigms: JWT, Pacifism or Realism. In the rest of this paper, the analysis will focus only on JWT. Two reasons support this choice: (i) the ethical problems with which JWT is concerned are generated by the very same decision to declare and to wage war, be it a traditional or an informational war. Therefore JWT sheds light on the analysis of the ethical issues posed by IW; (ii) The criteria for a *just* war proposed by this theory remain valid when considering IW, for the justification to resort to war and the cri-

[5] 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.

teria for *jus in bello* and *post bellum* proposed by JWT rest on the defence of basic human rights of life and liberty, see for example (Walzer 2000). There is no doubt that such rights and their preservation hold in the case of traditional warfare as well as in the case of IW.

Nevertheless, despite the relevance of these two reasons, it would be mistaken to consider JWT both the necessary and sufficient ethical framework for the analysis of IW, for addressing this new form of warfare solely on the basis of JWT generates more ethical conundrums than it solves. In the words of Arquilla (Arquilla 1998):

> it appears that […] information war [has] left a good part of 'just war theory' in tatters. For IW may now make preventive war far more thinkable (and practical), straining the limits of the concept of 'right purpose'. And the manner in which the information revolution empowers small groups and individuals to wage IW suggests that the notion of 'duly constituted authority' may also have lost meaning. Finally, the ease in undertaking IW operations, and the fact that they are disruptive, but not very destructive, weakens notions of justice as requiring that war be started only as a 'last resort'. (p. 208)

The ethical problems encountered when addressing IW on the basis of JWT originate from the differences between IW and traditional warfare. Such differences need to be taken into account in developing an ethical analysis of IW. Otherwise, the risk is twofold. On the one side, if the peculiarities of IW are not taken in consideration one is caused to disregard all those cases of IW that do not correspond to the parameters of traditional warfare (mainly the non-violent cases of IW). These are nevertheless potentially dangerous cases and need to be regulated as they remain disruptive and may cause extensive damage. On the other side, not taking into account the novelty posed by IW and focusing only on traditional criteria when analysing this phenomenon leads to a focus only on those cases which fall within the scope of traditional warfare, namely the violent cases of IW. In this case, the ethical analysis equates these instances of IW to traditional warfare, and leaves unexplored the peculiarities of IW and its specific ethical implications.

Particularly relevant in considering the differences between traditional and informational warfare is the transversality of the ontological status of the entities involved in the latter. 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 of those involved in IW. Such a hiatus affects the ethical analysis, for JWT rests on an anthropocentric ontology, i.e. it is concerned with respect for *human* rights and disregards all non-human entities as part of the moral discourse, and for this reason it does not provide sufficient means for addressing the case for IW (more details on this aspect presently).

The case of the autonomous cruising computer virus will help in clarifying the problems at stake (Abiola et al. 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 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 such a role should be attributed to the designer or to the agency that decided to deploy 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 questions 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.

These questions indicate that IW includes informational infrastructures, computer systems, and databases. In doing so, it brings new objects into the moral discourse. The first step toward 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 Sect. 4. Before focusing on Information Ethics, we shall first consider in detail some of the problems encountered when applying three principles of JWT to IW.

8.3.1 The Tenets of JWT and IW

For the purpose of this analysis, we shall consider whether and how the tenets of *last resort*, *more good than harm*, and *non-combatants immunity* can be applied in the case of IW.

The principle of 'war as last resort' prescribes that a state may resort to war only if it has exhausted all plausible, peaceful alternatives to resolve the conflict in question, in particular diplomatic negotiations. This principle rests on the assumption that war is a violent and sanguinary phenomenon and as such it has to be avoided until it remains the only reasonable way for a state to defend itself. The application of this principle is shaken when IW is taken in consideration, because in this case war may be bloodless and may not involve physical violence at all. In these circumstances, the use of the principle of war as last resort becomes less immediate.

Imagine, for example, the case of tense relations between two states and that the tension could be resolved if one of the states decide to launch a cyber attack on the other state's informational infrastructure. The attack would be bloodless as it would affect only the informational grid of the other state and there would be no casualties. The attack could also lead to resolution of the tension and avert the possibility of a traditional war in the foreseeable future. Nevertheless, according to JWT, the attack would be an act of war, and as such it is forbidden as a first strike move.

The impasse is quite dramatic, for if the state decides not to launch the cyber attack it will be probably forced to engage in a sanguinary war in the future, but if the

state authorises the cyber attack it will breach the principle of war as last resort and commit an unethical action.

This example is emblematic of the problems encountered in the attempt to establish ethical guidelines for IW. In this case, the main problem is due to the transversality of the modes of combat described in Sect. 2, which makes it difficult to define unequivocal ethical guidelines. In the light of the principle of last resort, soft and non-violent cases of IW can be approved as means for avoiding traditional war (Perry 1995), as they can be considered a viable alternative to bloodshed, which may be justly endorsed to avoid traditional warfare (Bok 1978). At the same time, even the soft cases of IW have a disruptive purpose—disrupting the enemy's (informational) resources (Arquilla and Ronfeldt 1997). Such a disruptive intent, even when it is not achieved through violent and sanguinary means, must be taken in consideration by any analysis aiming at providing ethical guidelines for IW.[6]

Another problem arises when considering the principle of 'more good than harm'. According to this principle, before declaring war a state must consider the *universal* goods expected to follow from the decision to wage war, against the *universal* evils expected to result, namely the casualties that the war is likely to determine. The state is justified in declaring war only when the goods are proportional to the evils. This is a fine balance, which is straightforwardly assessed in the case of traditional warfare, where evil is mainly considered in terms of casualties and physical damages which may result from a war. The equilibrium between the goods and the evils becomes more problematic to calculate when IW is taken into consideration.

As the reader may recall, IW is transversal with respect to the level of violence. If strictly applied to the non-violent instances of IW, the principle of more good than harm leads to problematic consequences. For it may be argued that, since IW can lead to the victory over the enemy without determining casualties, it is a kind of warfare (or at least the soft, non-violent instances of IW) that is always morally justified, as the good to be achieved will always be greater than the evil that could potentially be caused.

Nonetheless, IW may result in unethical actions—destroying a database with rare and important historical information, for example. If the only criteria for the assessment of harm in warfare scenarios remain the consideration of the physical damage caused by war, then an unwelcome consequence follows for all the non-

[6] It is worthwhile noticing that the problem engendered by the application of the principle of last resort to the soft-cases of IW may also be addressed by stressing that these cases do not fall within the scope of JWT as they may be considered cases of espionage rather than cases of war, and as such they do not represent a 'first strike' and the principle of last resort should not be applied to them. One consequence of this approach is that JWT would address war scenarios by focusing on traditional cases of warfare, such as physical attacks, and on the deployment of robotic weapons, disregarding the use of cyber attacks. This would be quite a problematic consequence because, despite the academic distinction between IW and traditional warfare, the two phenomena are actually not so distinct in reality. Robotic weapons fight on the battlefield side by side with human soldiers, and military strategies comprise both physical and cyber attacks. By disregarding cyber attacks, JWT would be able to address only partially contemporary warfare, while it should take into consideration the whole range of phenomena related to war waging in order to address the ethical issues posed by it (for a more in depth analysis of this aspect see (Taddeo 2012)).

violent cases of IW comply by default to this principle. Therefore, destroying a digital resource containing important records is deemed to be an ethical action, as it does not constitute physical damage *per se*.

The problem that arose with the application of this principle to the case of IW does not concern the validity *in se* of the principle. It is rather the framework in which the principle has been provided that becomes problematic. In this case, it is not the prescription that the goods should be greater than the harm in order to justify the decision to conduct a war, but rather is the set of criteria endorsed to assess the good and the harm that shows its inadequacy when considering IW.

A similar problem arises when considering the principle of 'discrimination and non-combatant immunity'. This principle refers to a classic war scenario and aims at reducing bloodshed, prohibiting any form of violence against non-combatants, like civilians. It is part of the *jus in bello* criteria and states that soldiers can use their weapons to target exclusively those who are "engaged in harm" (Walzer 2000, p. 82). Casualties inflicted on non-combatants are excused only if they are a consequence of a non-deliberate act. This principle is of paramount importance, as it prevents massacres of individuals not actively involved in the conflict. Its correctness is not questionable yet its application is quite difficult in the context of IW.

In classic warfare, the distinction between combatants and non-combatants reflects the distinction between military and civil society. In the last century, the spread of terrorism and guerrilla warfare weakened the association between non-combatants and civilians. In the case of IW such association becomes even feebler, due to the blurring between civil society and military organisations. (Schmitt 1999; Shulman 1999; Taddeo 2012).

The blurring of the distinction between military and civil society leads to the involvement of civilians in war actions and raises a problem concerning the discrimination itself: in the IW scenario it is difficult to distinguish combatants from non-combatants. Wearing a uniform or being deployed on the battlefield are no longer sufficient criteria to identify someone's social status. Civilians may take part in a combat action from the comfort of their homes, while carrying on with their civilian life and hiding their status as informational warriors.

It would be misleading to consider the problems described in this sections as reasons for dismissing JWT when analysing IW. These problems rather point to a more fundamental problem; namely the need to consider more carefully the case of IW, and to take into account its peculiarities.

8.4 Information Ethics

The time has come to introduce Information Ethics. This 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 one sentence Information Ethics is defined as a *patient-oriented*, *ontocentric*, and *ecological* macroethics. Information Ethics is patient-oriented because it considers the morality of an action with respect to its effects on the receiver of the action. It is ontocentric, for it endorses a non-anthropocentric approach for the ethical analysis. It attributes a moral value to all the 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, *overridable*, 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, 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.

By endorsing such a principle, Information Ethics guarantees a judgment of the moral scenario free from a biological or anthropological bias, for, following the principle of ontological equality, minimal and overridable rights to exist and flourish pertain to all existing things, and not just to human or living things. From this perspective, the Colosseum, Jane Austin's writings, a human being and computer software all share the right to exist and flourish, as they are all informational entities.[7]

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

In this respect, 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 are overridden whenever they conflict with the rights of other (more morally valuable) entities. 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*, includes all existing things, be they digital or analogical, physical or non-physical and the relations occurring among them, and 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 and destruction of informational entities or of the Infosphere is referred to as *entropy*. Lest the reader be confused, in this case entropy refers to "any kind of *destruction* or *corruption* of informational

[7] For more details on the information-based ontology see (Floridi 2003). The reader interested in the debate on the Informational ontology and the principles of Information Ethics may whish to see (Floridi 2007).

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 1999, 2001). On the basis of this approach Information Ethics provides four principles to identify right and wrong and the moral duties of an agent. The four moral principles are:

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

8.5 Just IW

The first step toward the 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 we can now answer the questions posed in Sect. 3 concerning the identification of moral agents, moral patients and the rights that have to be respected in the case of IW. The remainder of this article will focus on the problems regarding moral patients and their rights. The issue concerning the identification of moral agents in IW requires an in-depth analysis (see for example (Asaro 2008)) which falls outside the scope of this article. I shall clarify a few aspects concerning morality of artificial agents relevant to the scope of this analysis, before setting this issue aside.

The debate on morality of artificial agents is usually associated to the issues of ascribing to artificial agents moral responsibility for their actions. (Floridi and Sanders 2004) provide a different approach to this problem decoupling the moral *accountability* of an artificial agent, i.e. its ability to perform morally qualifiable actions, from the moral *responsibility* for the actions that such an agent may perform.

Floridi and Sanders argue that an action is morally qualifiable when it as morally qualifiable effects on its patient, and that every entity that qualifies as an interactive, autonomous and adapTable (transition) system and which performs a morally qualifiable action is (independently from its ontological nature) considered a morally accountable agent. So when considering the case for IW, a robotic weapon and

a computer virus are considered moral agents as long as they show some degree of autonomy in interacting and adapting to the environment and perform actions that may cause either moral good or moral evil.

As argued by Floridi and Sanders, attributing moral accountability to artificial agents extends the scope of ethical analysis to the actions of such agents and permits prescribable moral principles for their actions. This approach particularly suits the purpose of the present analysis, for the reader may accept suspending judgment on the moral responsibility for the actions that artificial agents may perform in case of IW, and agree that such actions are nevertheless morally qualifiable, and that as such they should be the objects of a prescriptive analysis.

Once we have put aside the issue concerning the morality of artificial agents, we are left with questions concerning the moral stance of the receivers of the actions performed by such agents and of the rights that ought to be respected in the case of IW. The principle of ontological equality states that all (informational) entities enjoy some minimal 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 allows for considering all entities that may be affected by an action of war as moral patients. A human being, who enjoys the consequences of a cyber attack and an informational infrastructure that is disrupted by a cyber attack are both to be held 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 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 Infosphere or at least to impede it from perpetrating more evil.

This framework lays the ground for the first principle for just IW. The principle prescribes the condition under which the choice 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 began increasing the entropy within it. IW is just as long 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 increasing of evil and not as 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 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 Sect. 3, and provide the framework for applying JWT to the case of IW without leading to the ethical conundrums analysed in Sect. 3.1. The description of how JWT is merged with Information Ethics is the task of the next section.

8.6 Three Principles for a Just IW

The application of the principle of 'last resort' provides the first instance of the merging of JWT and Information Ethics. The reader may recall that the principles forbids embracing IW as an 'early move' even in those circumstances in which IW may avert the possibility of waging a traditional war. The principle takes into account traditional (violent) forms of warfare, and it is coupled with the principle of 'right cause', which justifies resort to war only in case of 'self-defence'. However right this approach may be when applied to traditional (violent) forms of warfare, it proves inadequate when IW is taken into consideration. The impasse is overcome when considering the principles for just IW.

The first principle prescribes that any entity that endangers or disrupts the well-being of the Infosphere loses its basic rights and becomes a licit target. The second principle prescribes that a state is within its rights to wage IW to re-establish the *status quo* in the Infosphere and to repair the damage caused by a malicious entity. These two principles allow for breaking the deadlock described in Sect. 3.1, because a state can rightly endorse IW as an early move to avoid the possibility of a traditional warfare, as the latter threatens greater disruption of the Infosphere, and as such it is deemed to be a greater evil (source of entropy) than IW.

A caveat must be stressed in this case: the waging of IW must comply with the principles of 'proportionality' and 'more good than harm'. In waging IW, the endorsed means must be sufficient to stop the malicious entity, and in doing so the means ought not to generate more entropy than a state is aiming to remove from the

Infosphere in the first place. This leads us to consider in more detail the principle of 'more good than harm'.

The issues that arose in the case of IW are due to the definition of the criteria for the assessment of the 'good' and the 'harm' that a warfare may cause. As described in Sect. 3.1, endorsing traditional criteria leads to a serious ethical conundrum, since all (the majority of) the cases of IW that do not target physical infrastructures or human life comply by default to this principle regardless of their consequences.

Such a problem is avoided if damage to non-physical entities in considered as well as physical damage. More precisely, the assessment of the good and the harm should be determined by considering the general condition of the Infosphere 'before and after' waging the war. A just war never determines greater entropy than that in the Infosphere before it was waged. Once considered from this perspective, the principle of more good than harm acts as corollary of the second principle for just IW. It ensures that a just IW is waged to restore the *status quo* and does not increase the level of entropy in the Infosphere.

Increasing entropy in the Infosphere also provides a criterion for reconsidering the application of the principle of 'discrimination and non-combatants' immunity' to IW. As it has been argued in Sect. 3.1, IW blurs the distinction between militaries and civilians, as it neither requires military skills nor does it require a military status of the combatants to be waged. This makes problematic the application of this principle to IW; nevertheless the principle has to be maintained as it prescribes the distinction between licit and illicit war targets.

Help in applying this principle to IW comes from the first principle for just IW, which allows for dispensing with the distinction between militaries and civilians, and for substituting it with the distinction between licit targets and illicit ones. The former are those malicious entities who endanger or disrupt the well-being of the Infosphere. According to the principle, IW rightfully targets only malicious entities, be they military or civilian. The social status ceases to be significant in this context, because any entity that contributes to increasing the evil in the Infosphere loses its initial rights to exist and flourish and therefore becomes a licit target. More explicitly, it becomes a moral duty for the other entities in the Infosphere to prevent such entity from causing more evil.

Before concluding this article, I shall briefly clarify an aspect of the proposed analysis, lest the reader be tempted to consider it warmongering.

The third principle provided in Sect. 5 stresses that IW is never justly waged when the goal is improving the well-being of the Infosphere. This principle rests on the very same rationale that inspires Information Ethics, according to which the flourishing of the Infosphere is determined by the blooming of informational entities, of their relations and by their well-being. IW is understood as a form of disruption and as such, by definition, it can never be a vehicle for fostering the prosperity of the Infosphere nor is it deemed to be desirable *per se*. IW is rather considered a necessary evil, the bitter medicine, which one needs to take to fight something even more undesirable, i.e. the uncontrolled increasing of the entropy in the environment. With this clarification in mind we can now pull together the threads of the analysis proposed in this article.

8.7 Conclusion

The goal of this article is to fill the conceptual vacuum surrounding IW and of providing the ethical principles for a just IW. It has been argued that to this purpose JWT provides the necessary but not sufficient tools. 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 article defends the thesis that in order to be applied to the case for IW, JWT needs to 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 to address the issues posed by this form of warfare.

The first part of this paper introduces IW and analyses its relation to the information revolution and its main feature, namely its transversality. It then describes the reasons why JWT is an insufficient tool with which to address the ethical problems engendered by IW and continues by introducing Information Ethics. The second part of the article defends the thesis according to which once the ontological hiatus between the JWT and IW it is bridged, JWT can be endorsed to address the ethical problems posed by IW.

The argument is made that such a hiatus is filled when JWT encounters Information Ethics, since its ontocentric approach and informational ontology allow for ascribing a moral status to any existing entity. In doing so, Information Ethics extends the scope of the moral discourse to all entities involved in IW and provides a new ground for JWT, allowing it to be extended to the case for IW.

In concluding this article I should like to remark that the proposed ethical analysis should in no way be understood as a way of advocating warfare or IW. Rather it is devoted to prescribing ethical principles such that if IW has to be waged then it will at least be a just warfare.

References

Abiola, A., J. M. Munoz, and W. J. Buchanan. 2004. *Analysis and detection of cruising computer viruses*. Paper presented at the 3rd International Conference on Electronic Warfare and Security.

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

Arquilla, J., and D. Ronfeldt. 1997. *In Athena's camp: Preparing for conflict in the information age*. Santa Monica: RAND Corporation.

Asaro, P. 2008. How just could a robot war be? In *Current issues in computing and philosophy,* eds. P. Brey, A. Briggle, and K. Waelbers, 50–64. Amsterdam: IOS Press.

Benbow, T. 2004. *The magic bullet?: Understanding the revolution in military affairs*. London: Brassey.
Blackmore, T. 2005. *War X*. Toronto: University of Toronto Press Incorporated.
Bok, S. 1978. *Lying: Moral Choice in Public and Private.* New York, USA: Pantheon.
Denning, D. E. 2009. The ethics of cyber conflict. In *The handbook of information and computer ethics,* eds. K. E. Himma and H. T. Tavani, 407–428. New York: Wiley.
Floridi, L. 2003. On the intrinsic value of information objects and the infosphere. *Ethics and Information Technology* 4:287–304.
Floridi, L. 2006. Information ethics, its nature and scope. *SIGCAS Computer and Society* 36:21–36.
Floridi, L. 2007. Understanding information ethics. *APA Newsletter On Philosophy and Computers* 7:3–12.
Floridi, L. 2009. The information society and its philosophy. *The Information Society* 25:153–158.
Floridi, L. 2013. *Information ethics*. Oxford University Press.
Floridi, L., and J. W. Sanders. 1999. Entropy as evil in information ethics. *Etica & Politica* 1: special issue on Computer Ethics I(2).
Floridi, L., and J. W. Sanders. 2001. Artificial evil and the foundation of computer ethics. *Ethics and Information Technology* 3:55–66.
Floridi, L., and J. W. Sanders. 2004. On the morality of artificial agents. *Minds and Machines* 14:349–379.
Gelven, M. 1994. *War and existence*. Philadelphia: Pennsylvania State University Press.
Hepburn, R. 1984. *Wonder and other essays*. Edinburgh: Edinburgh University Press.
Libicki, M. 1996. *What is information warfare*? Washington, DC: National Defense University Press.
Perry, David L. 1995. *Repugnant Philosophy: Ethics, Espionage, and Covert Action.* Journal of Conflict Studies, Springer.
Schmitt, M. N. 1999. The principle of discrimination in 21st century warfare. *Yale Humna Right and Development Law Journal* 2:143–160.
Schwartau, W. 1994. *Information warfare: Chaos on the electronic superhighway*. New York: Thunder's Mouth Press.
Shulman, M. R. 1999. Discrimination in the laws of information warfare. *Columbia Journal of Transnational Law* 37:939–968 (Pace Law Faculty Publications).
Taddeo, M. 2012. Information warfare: A philosophical perspective. *Philosophy and Technology* 25:105–120.
Taddeo, M., and A. Vaccaro. 2011. Analyzing peer-to-peer technology using information ethics. *The Information Society* 27:105–112.
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: RAND.
Turilli, M., A. Vaccaro, and M. Taddeo. 2010. The case of on-line trust. *Knoweldge, Technology and Policy* 23:333–345.
Turilli, M., A. Vaccaro, and M. Taddeo. 2012. Internet neutrality: Ethical issues in the internet environment. *Philosophy & Technology* 25:133–151.
Waltz, E. L. 1998. *Information warfare principles and operations*. Norwood: Publisher Artech House, Inc.
Walzer, M. 2000. *Just and unjust wars: A moral argument with historical illustrations*. 3rd ed. New York: Basic Books.