Topoi (2016) 35:213–224
DOI 10.1007/s11245-014-9245-8

Just Information Warfare

Mariarosaria Taddeo

Published online: 16 April 2014

Abstract In this article I propose an ethical analysis of information warfare, the warfare waged in the cyber domain. The goal is twofold: filling the theoretical vacuum surrounding this phenomenon and providing the conceptual grounding for the definition of new ethical regulations for information warfare. I argue that Just War Theory is a necessary but not sufficient instrument for considering the ethical implications of information warfare and that a suitable ethical analysis of this kind of warfare is developed when Just War Theory is merged with Information Ethics. In the initial part of the article, I describe information warfare and its main features and highlight the problems that arise when Just War Theory is endorsed as a means of addressing ethical problems engendered by this kind of warfare. In the final part, I introduce the main aspects of Information Ethics and define three principles for a just information warfare resulting from the integration of Just War Theory and Information Ethics.

Keywords Cyber conflicts · Entropy · Information Ethics · Information war · Just War Theory · War

1 Introduction

Since 2010, cyberspace has been officially listed among the domains in which war may be waged these days. It is ranked fifth after land, sea, air and space, because the ability to control, disrupt or manipulate the enemy's informational infrastructure has become as decisive as weapon superiority in determining the outcome of conflicts. Information and communication technologies (ICTs) have proved to be a useful and convenient technology for waging war, and 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 1997; Taddeo 2012).[1] Such a revolution is not the exclusive concern of the military; it also has 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.

In this article, I propose an ethical analysis of information warfare (IW) with 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 that I provided in (Taddeo 2012), where I highlight the informational nature of this phenomenon and maintain that IW represents a profound novelty, which is reshaping the very concept of war and raises the need for new ethical guidelines.

Following on from that analysis, I argue that considering IW through the lens of Just War Theory (JWT) allows for the unveiling of fundamental ethical issues that this

M. Taddeo (✉)
Department of Political and International Studies, University of Warwick, Coventry, UK
e-mail: m.taddeo@warwick.ac.uk

M. Taddeo
Uehiro Centre for Practical Ethics, University of Oxford, Oxford, UK

[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 2011).

phenomenon brings to the fore, yet that attempting to address these issues solely on the basis of this theory will leave them unresolved. I then suggest that problems encountered when addressing IW through JWT are overcome if the latter is merged with Information Ethics (Floridi 2013). This is an ethical theory, which is particularly suitable for taking into account the features and the ethical implications of *informational phenomena*; for example, internet neutrality (Turilli et al. 2011) and transparency (Turilli and Floridi 2009), online trust (Turilli et al. 2010), peer-to-peer (Taddeo and Vaccaro 2011) and IW. Merging the principles of JWT with the 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; 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).

In the initial part of this article, I describe IW and its main features, I 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 I describe the principles for a just IW and discuss how JWT can be applied to IW without leading to ethical conundrums. Having delineated the path ahead of us, we should now begin our analysis by considering the nature of IW in greater detail.

2 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,[2] the injection of Stuxnet in the Iranian nuclear facilities of Bushehr,[3] as well as 'Red October' discovered in 2013 are all famous examples of how ICTs can be used to conduct cyber attacks.[4] Nonetheless, such attacks are only one instance of IW. In the rest of this article, I will use IW to 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. 1).

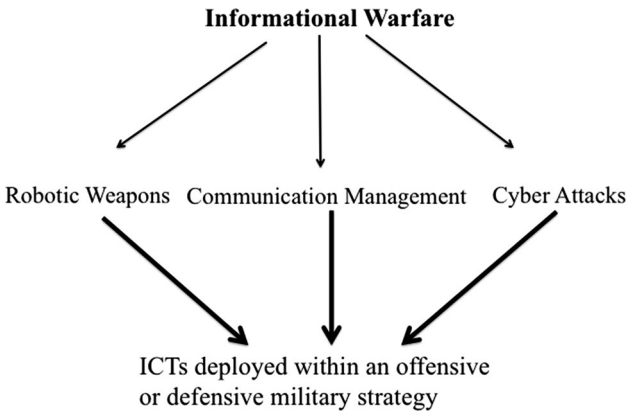

Fig. 1 The different uses of ICTs in military strategies (Taddeo 2012, p. 110)

Endorsing a wide spectrum definition of IW offers important advantages, both conceptual and methodological. The conceptual advantage revolves around the identification of the informational nature of this phenomenon. In all three cases, information plays a crucial role, it is either the target, the source or the medium for the accomplishment of a given goal. Now, while this is evident for the cases of communication management and cyber attacks, further explanation may be needed to highlight the informational nature of the deployment of (semi)autonomous robotic weapons, which may be less obvious. Such weapons are usually deployed (or designed to be deployed) to participate in traditional military actions and usually have destructive purposes, see for example Harpi [5] or Taranis.[6]

Nonetheless, while (semi) autonomous weapons may be used to perform tasks and achieve goals not dissimilar to those pursued in traditional warfare, their modes of operation are quite different from traditional ones as they rely extensively on the collection and elaboration of information. The ability and the way in which a machine collects, manipulates and checks information against the requirements for an action to be performed are crucial for the accomplishment of the given task. Information is in this case the means for the achievement of the goal and it shows an aspect common to all three cases. Henceforth, I endorse

[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.

[4] For an annotated time line of cyber attacks see NATO's website http://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm.

[5] This is an autonomous weapon system designed to detect and destroy radar emitters http://www.israeli-weapons.com/weapons/aircraft/uav/harpy/harpy.html.

[6] This is a UK drone which can autonomously search, identify and locate enemies although it should be stressed that it can only engage with a target upon the authorization of mission command http://en.wikipedia.org/wiki/BAE_Systems_Taranis.

an informational level of abstraction (LoA) to focus on such a common factor.

A brief digression from the analysis of IW is in order here to introduce LoAs. Any given system, for example a car, can be observed by focusing on certain aspects and disregarding others, and the choice of these aspects, i.e. the observables, depends on the observer's purpose or goal. An engineer interested in maximising the aerodynamics of a car would likely focus upon the shape of its parts, their weight and the materials. A customer interested in the aesthetics of the car will focus on its colour and on the overall look. The engineer and the customer observe the same car endorsing different LoAs. A LoA is a finite but non-empty set of observables accompanied by a statement of what feature of the system under consideration such a LoA stands for. 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. It is important to stress that a single LoA does not reduce a car to merely the aerodynamics of its parts or to its overall look. Rather, a LoA is a tool that helps to make explicit the observation perspective and constrain it to only those elements that are relevant in a particular observation.[7]

Endorsing an informational LoA to analyse cyber attacks, the deployment of robotic-weapons and ICT-based communication protocols allows us to reveal the factor common to these three phenomenon rather than their differences. A different (lower) LoA can be endorsed later in order to analyse the specific occurrences of these three phenomena and their ethical implications. This approach neither undermines the differences between the use of a computer virus, ICT-based communication protocols and robotic weapons nor denies that such different uses generate different ethical issues. Rather, it aims at focusing first on the aspects that are common among the military uses of ICTs, since the analysis of these aspects provides the groundwork for addressing specific ethical problems brought to the fore by the different modes of military deployment of ICTs.

The methodological advantage of endorsing a wide spectrum definition concerns the scope of the analysis, by considering indiscriminately the different uses of ICTs in warfare, the analysis will address the totality of the cases of IW rather than focusing solely on some of its specific occurrences.

Information warfare 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 (Taddeo 2012).

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; Taddeo 2013). The information revolution is a complex phenomenon. It rests on the development, the ubiquitous dissemination and use of ICTs, which have a wide impact on many of our daily practices: from our social and professional lives to our interactions with the environment surrounding 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).

Information warfare 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.[8] 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. Here, 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) and (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

[7] For a more detailed analysis of LoA see (Floridi 2008).

[8] The USA only spent $400 million in developing technologies for cyber conflicts: http://www.wired.com/dangerroom/2010/05/cyber war-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.

X-47B,[9] or of in the case of autonomous cruising computer viruses (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 physical targets, nevertheless it may escalate to more violent forms (Arquilla 2013), (Waltz 1998), (Clarke 2012), (Brenner 2011), and (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 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, it 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.[10] This is a simulation that has been conducted in the US in November 2013. More than two hundred utility companies collaborated with US government to simulate a massive cyber attack on US 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 IW and Just War Theory

Ethical analyses of war are developed following three main paradigms: JWT, Pacifism or Realism. The analysis in this paper will focus only on JWT. Two reasons support this choice: 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 possible declaration of IW. More generally, the criteria for a *just* war proposed by this theory remain valid even when considering IW; the justification to resort to war and the proposed criteria for *jus in bello* and *post bellum* are also desirable in the case of IW and there is no doubt that just war principles and their preservation hold in the case of traditional warfare as well as in the case of IW.

Nevertheless, it would be mistaken to consider JWT both the necessary and sufficient ethical framework for the analysis of IW, since addressing this new form of warfare solely on the basis of JWT generates more ethical conundrums than it solves. The problem arises because 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 the ones of harm, target, attack have been reshaped by the dissemination of IW. The very notion of harm for example, which is at the basis of JWT, struggle to apply to the case of IW. This a problem has been already highlighted in the extant literature, see for example (Dipert 2010) 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" (p. 386).[11]

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 of 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 one 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 way of specifying *information objects* […], *the*

[9] 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.

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

[11] 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 2013).

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 […] of a military ontology, such as agents, intentional actions, unintended effects, organizations, artefacts', commands, attacks and so on" (emphasis added) (Dipert 2013 p. 36).

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 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 (2010), 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 Sect. 4. Before focusing on that, we shall first consider in detail some of the problems encountered when applying JWT to IW.

3.1 The Tenets of JWT and IW

Let me begin this section by stressing that the proposed analysis does not claim that JWT does not adequately respond to contemporary global politics or to new methods for waging violent warfare.[12] In the rest of this section I shall analyse the tenets of *last resort*, *more good than harm*, and *non-combatants immunity* to consider the problems that arise when these principles, which are desirable also in case of IW, are applied to the occurrences of a war in the cyber (non-physical) domain. I argue that the nexus of the ethical problems posed by IW rest on the ontological hiatus between IW and JWT, for the latter focuses on violent warfare, bloodshed and physical damage, and these aspects are essential characteristics of kinetic warfare but they are not peculiar 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 considered, because here 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 resolve the tension and avert the possibility of kinetic 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 dramatic: if the state decides not to launch the cyber attack it may be 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 2006), as they can be considered a viable alternative to bloodshed, which may be justly endorsed to avoid traditional warfare (Bok 1999). At the same time, even soft cases of IW have a disruptive pur-

[12] See (Withman 2013) for an analysis of validity of JWT with respect to contemporary violent warfare.

pose—disrupting the enemy's (informational) infrastructures (Arquilla and Ronfeldt 1997) (Arquilla 2013). Such a disruptive intent, even when it is not achieved through violent and sanguinary means, must be taken into consideration by any analysis aiming at providing ethical guidelines for IW.[13]

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 produce. 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 damage that may result from a war. The equilibrium between the goods and the evils becomes more problematic to calculate when considering IW.

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 victory over the enemy without incurring 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-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 *tout court*, 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 *per 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 it 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 2006, 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) (reference removed for blind review).

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.

This case provides also a good example of the policy gap surrounding IW, for one of the most important aspects of the distinction between military and civilian concerns the identification of the so-called civilian objects, i.e. buildings, places and objects that should not be considered military targets. Chapter III of the Protocol I of the Geneva Convention [14] defines civilian objects as tokens, which are further categorised according to cultural or religious type,

[13] 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)).

[14] "ICRC Databases on International Humanitarian Law".

environmental or necessary to the survival of the population. This chapter proves to be ontologically limited as it considers as 'objects' only physical, tangible entities.[15]

Furthermore, civilian objects are distinguished from military ones, as the latter are deemed to be objects that "make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage". The reader may easily see how such a definition may be used to qualify a civilian informational infrastructure in time of IW, making the line between civilian and military even less evident and making even more compelling the need for policies able to accommodate a more inclusive definition of objects, and generally more able to address the conceptual changes posed by this new kind of warfare.

Before introducing Information Ethics, I shall remark that several analyses have been proposed claiming that JWT, as it is distilled in the existing apparatus of laws, is adequate and sufficient to address cases of IW (see for example (Schmitt 2013) and (NATO CCD COE 2013), "[…] a thick web of international law norms suffuses cyberspace. These norms both outlaw many malevolent cyberoperations and allow states to mount robust responses" (Schmitt 2013, p. 177).

This is an interesting and useful approach, it allows the application of current international laws to IW and it has prevented the cyber sphere from becoming an unregulated domain by considering how existing laws and regulations can be applied to the cases of IW. The approach recognises the novelty posed by IW and focuses on interpreting existing international laws to understand how to apply them to the case of IW: "[w]e must, at least, attempt […] to extrapolate from the known to the unknown, by means of *analogy*, *comparison*, and *interpretation*. At least we must make the attempt, and explore the intuitive soundness of the results, before abandoning such resources altogether." (emphasis added) (Lucas 2013, p. 372).

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 rather than revising the conceptual roots of JWT in order to address the novelty posed by IW, the latter is 'forced' to fit in the parameters set for kinetic warfare.

Hence, the approach fails to consider and to account for the conceptual changes prompted by IW (see the discussion in Sects. 2 and 3) and risks confusing an *ad hoc* remedy with the long-term solution and, in the long run, 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 "[s]ince 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 focus is restricted to physical damage and tangible objects. 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, which are affecting not only the way we wage war, but also the way in which we conduct our lives, perceive ourselves and the very concepts of harm, warfare, property, and state.

As it has been noted by Schmitt himself (Schmitt 2013) "Indeed, interpretive endeavors seldom survive intact because international law, crafted as it is by states through treaty and practice, necessarily reflects the contemporary values of the international community. As these values evolve, so too will international law's prevailing interpretations" (p. 179–180). It would be misleading to consider the problems described in this section as reasons for dismissing JWT when analysing IW. Instead these problems point 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.

4 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)

[15] On this point see also (Dipert 2010, p. 400).

In just 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 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,[16] 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 standing point 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 LoA; 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, and that 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 writings, a human being and computer software all share *initial* rights to exist and flourish, as they are all informational entities.[17]

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. The four moral principles are:

[16] The reader may recall the informational LoA mentioned in Sect. 2. Information Ethics endorses an informational LoA, as such it focuses on the informational nature as a common ground of all existing things.

[17] 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).

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.

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 not 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 simply clarify a few aspects concerning morality of artificial agents relevant to the scope of this analysis, before setting this issue aside.

The debate on the morality of artificial agents is usually associated with the issues of ascribing to artificial agents moral responsibility for their actions. Floridi and Sanders (Floridi and Sanders 2004) provide a different approach to this problem by 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.

The authors argue that an action is morally qualifiable when it has morally qualifiable effects, 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 include actions performed by artificial agents and allows us to determine moral principles to regulate such actions. This approach particularly suits the purpose of the present analysis, for the reader may agree to suspend judgment on the moral responsibility for artificial agents' actions performed in cases of IW, but nevertheless agree that such actions are 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 IW scenarios. The principle of ontological equality 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) and (Floridi 2013).

When applied to IW, this principle enables considering 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 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 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 began increasing 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 (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 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.

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 even 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 here: 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 further 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 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.

This 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. 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.

The danger of 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 military personnel and civilians, as IW requires neither military skills nor the combatants' military status to be waged. This makes the application of this principle to IW problematic; 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 that 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 an 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 pill, which one needs to swallow to fight something even more undesirable, i.e. the uncontrolled increasing of entropy in the environment. With this clarification in mind we can now pull together the threads of the analysis proposed in this article.

7 Conclusion

The goals of this article are to fill the conceptual vacuum surrounding IW and to provide the ethical principles for a just IW. It has been 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.

This article defends the thesis 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 both human and artificial, both 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, Munoz J, Buchanan W (2004) Analysis and detection of cruising computer viruses. In: *EIWC*

Arquilla J (1998) Can information warfare ever be just? Ethics Inf Technol 1(3):203–212

Arquilla J (2013) Twenty years of cyberwar. J Mil Ethics 12(1):80–87. doi:10.1080/15027570.2013.782632

Arquilla J, Ronfeldt David F (eds) (1997) In Athena's camp: preparing for conflict in the information age. Rand, Santa Monica

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

Barrett ET (2013) Warfare in a new domain: the ethics of military cyber-operations. J Mil Ethics 12(1):4–17. doi:10.1080/15027570.2013.782633

Benbow T (2004) The magic bullet?: understanding the "revolution in military affairs". Brassey's, London

Blackmore T (2011) War X. Univ of Toronto Pr

Bok S (1999) Lying: moral choice in public and private Life, 2nd edn. Vintage Books, New York

Bowden M (2011) Worm: the first digital world war. Atlantic Monthly Press, New York

Brenner J (2011) America the vulnerable: new technology and the next threat to national security. Penguin Press, New York

Clarke RA (2012) Cyber war: the next threat to national security and what to do about it. 1st Ecco pbk. ed. New York: Ecco

Denning D (2007) The ethics of cyber conflict. In: Himma KE, Tavani HT (eds) Information and computer ethics. Wiley, Hoboken, USA

Dipert R (2010) The ethics of cyberwarfare. J Mil Ethics 9(4):384–410

Dipert R (2013) The essential features of an ontology for cyberwarfare. In: Panayotis Yannakogeorgos, Adam Lowther (eds) Conflict and cooperation in cyberspace. Taylor & Francis, pp 35–48. http://www.crcnetbase.com/doi/abs/10.1201/b15253-7

Floridi L (2002) On the intrinsic value of information objects and the infosphere. Ethics Inf Technol 4(4):287–304

Floridi L (2006) Information ethics, its nature and scope. SIGCAS Comput Soc 36(3):21–36

Floridi L (2007) Understanding information ethics. APA Newsl Philos Comput 7(1):3–12

Floridi L (2008) The method of levels of abstraction. Mind Mach 18(3):303–329
Floridi L (2013) Ethics of information. Oxford University Press, Oxford
Floridi L (2014) The fourth revolution, how the infosphere is reshaping human reality. Oxford University Press, Oxford
Floridi L, Sanders J (2001) Artificial evil and the foundation of computer ethics. Ethics Inf Technol 3(1):55–66
Floridi L, Sanders JW (2004) On the morality of artificial agents. Mind Mach 14(3):349–379. doi:10.1023/B:MIND.0000035461.63578.9d
Gelven M (1994) War and existence: a philosophical inquiry. Pennsylvania State University Press, University Park
Hepburn RW (1984) "Wonder" and other essays: eight studies in aesthetics and neighbouring fields. University Press, Edinburgh
ICRC Databases on International Humanitarian Law. 00:00:00.0. http://www.icrc.org/ihl/INTRO/470
Libicki M (1996) What is information warfare?. National Defense University Press, Washington
Lucas GR (2013) Jus in silico: military restrictions on the use of Cyber Warfare. In: Allhoff F, Evans NG, Henschke A (eds) Routledge handbook of war and ethics. Routledge, Oxford
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 University Press, Cambridge; New York
Perry D (2006) Repugnant philosophy': ethics, espionage, and covert action. In: Goldman J (ed) Ethics of spying: a reader for the intelligence professional
Schmitt MN (1999) The principle of discrimination in 21st century warfare. SSRN scholarly paper ID 1600631. Rochester, NY: Social science research network. http://papers.ssrn.com/abstract=1600631
Schmitt MN (2013) Cyberspace and international law: the penumbral mist of uncertainty. Harvard 126(176):176–180
Schwartau W (1994) Information warfare: Chaos on the electronic superhighway. 1st edn. Thunder's Mouth Press, New York: Emeryville, CA; Distributed by Publishers Group West
Shulman MR (1999) Discrimination in the laws of information warfare. SSRN scholarly paper ID 1287181. Rochester, NY: Social science research network. http://papers.ssrn.com/abstract=1287181
Taddeo M (2012) Information warfare: a philosophical perspective. Philos Technol 25(1):105–120
Taddeo M (2013) Cyber Security and Individual Rights, Striking the Right Balance. Philos Technol 26(4):353–356
Taddeo M, Vaccaro A (2011) Analyzing peer-to-peer technology using information ethics. Inf Soc 27(2):105–112. doi:10.1080/01972243.2011.548698
Toffler A, Toffler A (1997) Foreword: the new intangibles. In: Arquilla John, Ronfeldt David F (eds) In Athena's camp preparing for conflict in the information age. Santa Monica, Rand
Turilli M, Floridi L (2009) The ethics of information transparency. Ethics Inf Technol 11(2):105–112. doi:10.1007/s10676-009-9187-9
Turilli M, Vaccaro A, Taddeo M (2010) The case of on-line trust. Knowledge, technology and policy 23.3–4 (3–4, Special issue on Trust in Technology): 333–345
Turilli M, Vaccaro A, Taddeo M (2011) Internet neutrality: ethical issues in the internet environment. Philos Technol 25(2):133–151. doi:10.1007/s13347-011-0039-2
Waltz E (1998) Information warfare: principles and operations. Artech House, Boston
Walzer M (2006) Just and unjust wars: a moral argument with historical illustrations, 4th edn. Basic Books, New York
Withman J (2013) Is just war theory obsolete? In: Fritz Allhoff, Nicholas G. Evans, Adam Henschke (eds) Routledge handbook of ethics and war: just war theory in the 21st century, Routledge, p 23–34