JUST WAR THEORY AND INFORMATION WARFARE

Keywords: Information Ethics, Information Warfare, Just War Theory.

1. Introduction

This article is devoted to develop an ethical analysis of information warfare (IW), the warfare waged in the domain of information, with the twofold goal of overcoming the theoretical vacuum surrounding this phenomenon and of providing the conceptual grounding for an ethical regulation for IW.

The proposed analysis rests on a conceptual investigation of IW proposed in (reference removed for blind review), which highlights the informational nature of this phenomenon as well as its relation to the so-called Information Revolution. In the rest of this paper it will be argued that Just War Theory (JWT) is a necessary but not sufficient instrument for the ethical analysis of IW. It will be maintained that analysing IW through the lenses of JWT allows for unveiling the fundamental ethical issues that this phenomenon brings to the fore, but that attempting to address these issues solely on the basis of JWT will leave them unsolved.

The thesis will be advanced that the problems encountered when addressing IW through JWT are overcome when the latter is merged with Information Ethics. This is a macro-ethical theory developed to take into account the features and the ethical implications of *informational phenomena*, like internet neutrality (Turilli et al. Forthcoming), online trust (Turilli et al. 2010), peer-to-peer (Taddeo and Vaccaro 2011) and IW. The goal is to develop an ethical analysis of IW able to take into account both its peculiarities and its novelty, while at the same time be consistent with the mainstream ethical analysis of warfare.

Having delineated the path of the analysis proposed in this article, we shall now begin by considering in more details the nature of IW.

2. Information Warfare

The expression 'information warfare' has already been used in part 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 information about the opponent's resources, military strategies and so on, see for example (Libicki 1996; Waltz 1998; Schwartau 1994).

The Estonian and Georgian cyber attacks provide good examples of such use of ICTs. More in general, distributed denials of service (DDoS), the dissemination of computer worms and viruses are all form of cyber attacks, which fall in the scope of the restrictive use of the label IW. Despite being cyber attacks one of the most known and debated forms of ICTs-based conflicts, they are not the only one. In the rest of this article, IW will refer to a wide spectrum phenomenon, which encompasses cyber attacks as well as the deployment of robotic-weapons, and ICTs based communication protocols (see figure 1).[1]

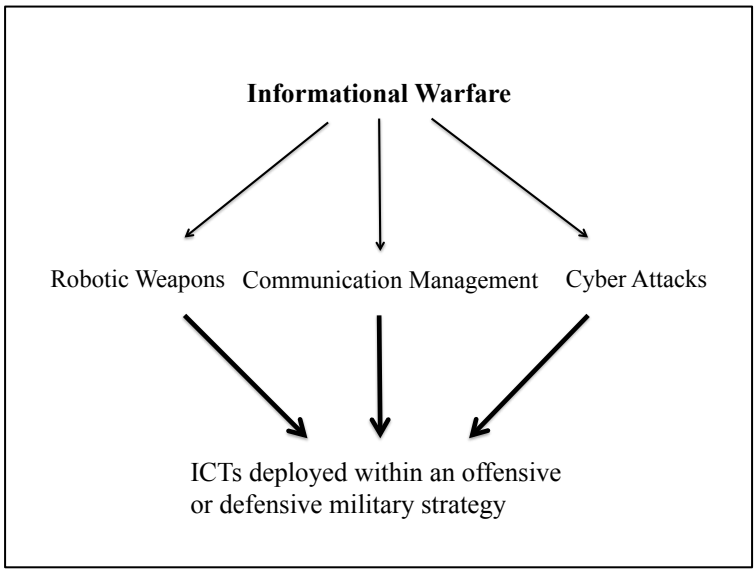

Figure 1 The deployment of robotic weapons, the launch of cyber attacks and the managing of communications through ICTs as instances of Information Warfare (figure from (reference removed for blind review)).

Following the analysis proposed in (reference removed for blind review) all these cases are instances of the same phenomenon, namely IW, which 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

[1] See (reference removed for blind review) for a detailed analysis of such a use of the expression 'information warfare'.

> informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances (reference removed for blind review).

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 elaborate, manage and communicate data and information. With this respect IW shows to be related to the so-called Information revolution.

Information revolution determines a shift, which brings the *non-physical domain* to the fore and makes it as important and valuable as the physical one (reference removed for blind review). 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 be deployed in such a new environment.[2]

The shift toward the non-physical domain provides the ground for the transversality of IW. This is a complex aspect, and can be better grasped when IW is compared with traditional form of warfare. Traditional war is understood as 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 the damage of both military and civilian infrastructures. The problem to be faced when waging traditional warfare is how to reduce to the minimum such damages while ensuring to overpower the enemy.

IW shows to be different from traditional warfare, as it is not a necessarily violent and destructive phenomenon (Arquilla 1999). IW may involve a computer virus able to disrupt or deny access to the enemy's database, and in so doing cause a severe damage to the enemy 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, or by a computer virus, targeting other

[2] 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

artificial agents or informational infrastructures, like a database or a website. Nevertheless, IW is to be feared as much as traditional warfare, for it is transversal with resect to the level of violence and 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 with respect to the levels of violence, the nature of the agents and the waging domain is the key feature of this phenomenon, the aspect that differentiates it the most from traditional warfare, and also the feature that engenders the ethical problems posed by IW.

Transversality makes IW extremely appealing from both an ethical and political perspectives (Arquilla and Ronfeldt 1997). At first glance, IW seems to avoid bloodshed and human commitment and therefore it liberates political authorities of the burden of justifying military actions to the public opinion. A more attentive analysis unveils that IW should be feared as much as traditional warfare as it can lead to highly violent and destructive consequences, which could be dangerous for both the military forces and civil society.

For this reason, declaring and waging IW require a strict ethical regulation to guarantee its fairness. An analysis of IW unveiling the ethical issues that it engenders and pointing at the direction for their solution is a necessary step toward the achievement of such goal.

3. Just War Theory and IW

JWT refers to war as to a violent and sanguinary phenomenon, declared by states and their official leaders and waged by military forces. Such a scenario is quite different from the one determined by IW, the difference between the two forms of warfare is the origin of the problems arising when the principles of JWT are applied to IW. In this respect, there are three issues that deserve attention; they follow from the application of the principles of ‘war as last resort’, of ‘more good than harm’, and of ‘non-combatants immunity’ to 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 not casualties. The attack could also lead to resolution of the tension and avoid 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, which could probably be sanctioned by international regulations.

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, which make 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. At the same time, even the soft cases of IW have a disruptive purpose - disrupting the enemy's (informational) resources (Floridi 2008) - which need to be taken in consideration by any analysis aiming at providing ethical guidelines for IW. Even when the disruption of the enemy's informational infrastructure is not achieved through violent and sanguinary means.[3]

The second problem to be considered concerns the principle of 'more good than harm'. According to such a 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. A state is justified in declaring war only when the goods are proportional to the evils. This balance is easily assessed in case of traditional warfare, where the

[3] For a more in depth analysis of the non-violent cases of IW and their assessment as acts of war or of espionage see (Arquilla 1998) and (references remove for blind review).

evils are mainly considered in terms of the casualties and physical damages. The equilibrium between the goods and the evils becomes more problematic to determine when IW is taken under consideration.

IW is likely to cause none or very little casualties, and as it targets informational infrastructures it is unlikely to cause the destruction of physical obejcts, like buildings for example. Although it is possible for IW to turn in a violent warfare, in the most of the cases it does not determine physical damages, nonetheless IW may result in unethical actions. If the only criteria for the assessment of the harm in warfare scenario remain the consideration of the physical damages 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 database or erasing a digital archive containing important historical records of a nation are all deemed to be ethical actions as they do not constitute *per se* a physical damage.

In the case of this principle, it is not the prescription that the goods should be grater than the harm in order to justify the decision to wage a war to be shaken. It is rather the set of criteria to assess the good and the harm, which show to be inadequate when considering IW.

The last problem concerns the principle of 'discrimination and non-combatant immunity'. Also this principle refers to a classic war scenario and aims at reducing the bloodshed and prohibits any form of violence against non-combatants, like civilians. 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. Hence it forbids targeting not only civilians but also civilian infrastructures, like hospitals or civilian food and water supply chains. In the last century, the diffusion 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).

The blurring leads to the involvement of civilians in war actions and poses two issues. The first one concerns the discrimination itself: in the IW scenario it is difficult to distinguish combatants from non-combatants, wearing a uniform is no

longer a sufficient criterion to identify someone's 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.

The second issue concerns the effects of this difficulty in distinguishing combatants from non-combatants and unveils an ethical conundrum. If combatants can easily hide themselves among the civilian population, then states may be justified in endorsing high levels of surveillance over the entire population, thereby breaching individual rights, like privacy and anonymity, in order to identify the combatants and guarantee the security of the entire community. For the sake of these goals, public authorities could also be justified in persecuting certain sections of the civilian population, which are profiled and deemed to be potentially dangerous for the community. Therefore, on the one side respecting the principle of discrimination may lead to the violation of individual rights. On the other side, waiving the principle of discrimination leads to bloodshed and dissemination of violence over the entire civil population, because the policy could be endorsed to target everyone or everything a soldier encounters in her way, as being potentially involved in the conflict.

It would be misleading to consider the problems described in this section as reasons to disregard JWT when analysing IW. The ideal of just warfare provided by JWT and its principles remain valid even when considering this new kind of warfare. Yet, the analysis proposed in this section points to a more fundamental problem, namely the need to provide an ethical framework for the regulation of IW able to address the novelty of this phenomenon. In the next section, Information Ethics will be introduced as the suitable ethical framework for this purpose.

4. Just IW

Following the ontocentric approach, all (informational) entities enjoy some minimal rights to exist and flourish in the Infosphere. As such all entities, would they be leaving things or non-living things, physical or virtual, deserve some minimal respect. When applied to IW, this principle allows for considering as moral patients all the entities that may be affected by an action of war within IW. A human being, who suffers the consequences of a cyber attack and an informational infrastructure that is disrupted by a cyber attack are both to be consider the receiver of the moral action.

The morality of that action will be assessed on the basis on its effect on their rights to exist and flourish.[4]

The first question when considering the conditions for a just IW concerns the rights of the informational entities, namely what and whose rights should be preserved. The answer to this question follows from the rationale of Information Ethics. Information Ethics states that an entity looses it rights to exist and flourish when it comes into conflict with the rights of other entities or with the well being of the Infosphere. Therefore, any entity that causes entropy in the Infosphere looses its informational rights as it conflicts with the well being of the other entities and ultimately of the Infosphere. It is a moral duty of the other inhabitants of the Infosphere to *remove* such a malicious entity from the Infosphere, as it is a cause of entropy, or to impede it to perpetrate more evil.

This 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 restore the *status quo* in the Infosphere before the malicious entity began increasing the entropy in it. According to the second principle, IW should have the same role that police forces have in a democratic state, i.e. it should act only when some evil has been or is about to be perpetrated with the goal of stopping it. Police forces do not act in order to ameliorate the aesthetics of the cities or the fairness of the laws, but only focus on reducing or stopping crimes to be committed. Likewise, IW ought to be endorsed as an *active* measure in response to the increasing of the evil and not as *proactive* measure to foster the flourishing of the Infosphere. This is explicitly forbidden by the third principle, which prescribes that

[4] While assuming that all entities share some initial rights to exist and flourish, Information Ethics does not claim that there is no hierarchy among the entities. It specifies that the rights are overridable and hence that an entity ceases to hold the rights to exist and flourish, should it contravene the well being of other entities or of the Infosphere. Further more, according to Information Ethics, the position in the hierarchy of an entity depends on its contribution to the flourishing of the Infosphere. For a more in depth analysis of the criteria to override the entities initial rights see (Floridi 2008).

the promoting of the well being of the Infosphere does not pertain to the scope of a just IW.

The time has come to consider how JWT can be applied to the case for IW without leading to the conundrums described in section 3.

5. Three principles for a just IW

The application of the principle of 'last resort' provides the first instance of how JWT and Information Ethics are merged. The reader may recall that the 'principle of last resort' forbids to embrace IW as an 'early move', even in those circumstances in which waging an IW may avoid 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 the resort to war only in case of 'self-defence'. As much as rightful this approach is when referred to traditional (violent) form of warfare, it shows to be inadequate when IW is taken under 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 looses its basic rights and becomes a licit target. Therefore, a state can rightly endorse IW as an early move against a malicious entity. The choice to resort to IW is furthermore justified if it allows a state to avoid the possibility of a traditional warfare, as this one would determine casualties and destructions in the Infosphere, and as such it is deemed to be a greater evil 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 means endorsed to win the enemy must be sufficient to stop the malicious entity, yet they ought not to generate more entropy than the one a state is aiming to remove from the Infosphere. This leads us to consider in mode detail the principle of more good than harm.

The application of this principle is of paramount importance for the waging of a just warfare, would it be a traditional or an informational one. As noted in section 3, the issues concerning IW are due to the definition of the criteria for the assessment of the 'good' and the 'harm' that warfare may cause. Traditionally, they are defined with respect to the collateral damage, casualties, damages to the physical infrastructures of

both the parts involved in the war. Such criteria do not take in consideration the harm that IW may cause.

In the case of IW, the damage to non-physical entities needs to be considered as well as the damage to the physical ones. More precisely, the assessment of the good and the harm should be determined considering the general condition of the Infosphere 'before and after' waging the war. A just war never determines greater entropy (evil) than the one that it intended to remove from the Infosphere in the first place. Once considered in 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 it never increases the level of entropy in the Infosphere.

The assessment of the entropy in the Infosphere allows also for reconsidering the application of the principle of non-combatants immunity to IW. Two problems accompany the application of this principle, the consequences of its endorsement on the individuals' rights of privacy and anonymity, and the very distinction between combatants and non-combatants. The rest of this section will focus only on the latter issue, the former does not pertain to the scope of this paper and as such will not be considered here.[5]

The distinction between combatants and non-combatants promoted by this principle rests on a hidden distinction, namely the distinction between militaries and civilians that it is inherited from traditional warfare. This distinction is then mirrored in the one between combatants and non-combatants. Such approach cannot be endorsed in the case of IW. As we have seen, IW is transversal with respect to the social status of the combatants, for it does not require military skills to be waged. This makes problematic the application of the principle, which nevertheless has to be maintained as it prescribes the distinction between enemies and 'innocents'.

Help in applying this principle to IW comes from the first principle for just IW, which allows for overcoming the distinction between militaries and civilians, and for substituting it with the distinction between licit targets and non-licit ones, the former being the malicious entities that endangered or disrupted the well being of the Infosphere.

The time has arrived to pull together the threads of the analysis proposed in this article.

[5] For an in depth analysis of this issue see (reference removed for blind review).

6. Conclusion

This article rests on the conceptual analysis of IW provided in section 2. Such analysis stresses the novelty of this phenomenon, its relation with the Information revolution and argues that transversality is its main feature. Transversality is dimmed to be the characteristics of IW that differentiates it the most from traditional warfare and also the one from which all the ethical issues posed by IW originate.

It has been argued that, given the radical novelty posed by IW, the ethical analysis of this phenomenon and the definition of the ethical principles for a just IW cannot rest solely on JWT. For such a theory does not provide 'the right sieve' for the work to do. JWT does not take into account the main features of IW, namely the transversality of the levels of violence, of the domain (physical and non-physical) in which it is waged, and finally the transversality of the nature and social status of agents who may be involved in this warfare. Yet, the article maintains that it would be mistaken to reject JWT altogether when addressing IW.

It is rather argued that the ideal of just warfare and the principles prescribed by JWT are still valid when referred to IW, and that they can be endorsed to regulate this new form of warfare if they are combined with a macro-ethical framework able to take into account the peculiarities of this phenomenon.

Three principles for just IW, encompassing both the rationale of JWT and the one of Information Ethics, have been provided. Such principles constitute the grounding for the development of more detailed ethical guidelines for IW, that is for the next step of this research.

References

Arquilla, J. (1998). Can information warfare ever be just? *Ethics and Information Technology, 1*(3), 203-212.

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

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

Floridi, L. (2008). Information Ethics, its Nature and Scope. In J. v. d. Hoven, & J. Weckert (Eds.), *Information Technology and Moral Philosophy* (Vol. 40-65). Cambridge: Cambridge University Press.

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

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

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

Perry, D. L. (1995). Repugnant Philosophy:Ethics, Espionage, and Covert Action. *Journal of Conflict Studies, Spring*.

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, USA: Thunder's Mouth Press.

Shulman, M. R. (1999). Discrimination in the Laws of Information Warfare. *Pace Law Faculty Publications, 37*, 939-968.

Taddeo, M., & Vaccaro, A. (2011). Analyzing peer-to-peer technology using information ethics. *The Information Society, 27*(2), 105 - 112.

Turilli, M., Vaccaro, A., & Taddeo, M. (2010). The Case of on-line Trust. *knoweldge, Technology and Policy*.

Turilli, M., Vaccaro, A., & Taddeo, M. (Forthcoming). Internet Neutrality: Ethical Issues in the Internet Environment.

Waltz, E. L. (1998). *Information Warfare Principles and Operations*. Norwood, USA: Publisher Artech House, Inc.