2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

An Analysis For A Just Cyber Warfare

Mariarosaria Taddeo[1]
Department of Philosophy –
School of Humanities
University of Hertfordshire
Hatfield, UK
m.taddeo@herts.ac.uk

Abstract: This article focuses on the ethical analysis of cyber warfare, the warfare characterised by the deployment of information and communication technologies. It addresses the vacuum of ethical principles surrounding this phenomenon by providing an ethical framework for the definition of such principles. The article is divided in three parts. The first one considers cyber warfare in relation to the so-called information revolution and provides a conceptual analysis of this kind of warfare. The second part focuses on the ethical problems posed by cyber warfare and describes the issues that arise when Just War Theory is endorsed to address them. The final part introduces Information Ethics as a suitable ethical framework for the analysis of cyber warfare, and argues that the vacuum of ethical principles for this kind warfare is overcome when Just War Theory and Information Ethics are merged together.

Keywords: *cyber warfare, information ethics, Just War Theory*

1. INTRODUCTION

During the past two decades, information and communication technologies (ICTs) proved to be a useful and convenient for war waging, so much so that they have been deployed in most of the conflicts since the second Iraq's war.[2] The military deployment of ICTs has radically changed the way wars are waged nowadays. It has actually determined the latest revolution in military affairs, making the cyber space the fifth domain of war, along with land, sea, air and space.

The informational turn in military affairs is not of exclusive concern of the militaries; it also concerns ethicists and policymakers. For existing ethical theories of war and national and international regulations struggle to address the novelties of this phenomenon. This article is devoted to develop an ethical analysis of cyber warfare (CW), with the twofold goal of overcoming the theoretical vacuum surrounding this phenomenon and of providing the grounding for an ethical regulation for CW.

The proposed analysis rests on the investigation of CW proposed in (Taddeo 2012), which highlights the informational nature of this phenomenon as well as its relation to the so-called

1 This paper is part of the research supported by the Marie Curie Intra-European Fellowships.
2 *See* http://www.economist.com/node/16478792.

Information Revolution. In this paper it will be argued that Just War Theory (JWT) is a necessary but not sufficient instrument for the ethical analysis of CW. It will be maintained that analysing CW 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 CW through JWT are overcome when the latter is merged with Information Ethics (Floridi 2008). 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 CW. The goal is to develop an ethical analysis of CW 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 CW.

2. CYBER WARFARE

For the purpose of this article CW is defined as follows:

> "**[Cyber] Warfare** is [the warfare grounded on certain] uses 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, 114).

This definition highlights two aspects of CW, its *informational nature* and its *transversality*[3]. The informational nature of CW 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 CW shows to be related to the so-called Information Revolution.

The Information Revolution is a multi-faced phenomenon. It rests on the development and the capillary dissemination of the use of ICTs, which have a wide impact on several of our daily practises, from working, to interacting with other human beings, to driving around and planning holidays. The dissemination of ICTs has important philosophical implications (Floridi 2010), for the Information Revolution changes fundamentally the way reality is perceived and understood.

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. CW 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

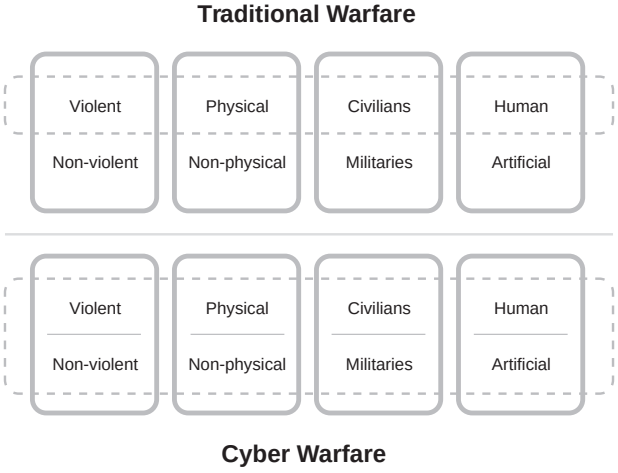
3 'Transversality' is used in this article to indicate that CW cuts across any qualifying couple such as 'violent-non violent', 'civil-military', 'human agents-artificial agents'. This aspect is quite different from traditional warfare, which is violent, conducted by militaries and mainly by human agents.

authority and new modes of warfare are being developed specifically to be deployed in such a new environment (Taddeo 2012).[4]

The shift toward the non-physical domain provides the ground for the transversality of CW. This is a complex aspect, and can be better grasped when CW 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.

CW shows to be different from traditional warfare, as it is not a necessarily violent and destructive phenomenon (Arquilla 1999). CW 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, CW does not necessarily involve human beings. An action of war in this context can be conducted by a computer virus, targeting other artificial agents or informational infrastructures, like a database or a website (see Figure 1). Nevertheless, CW is to be feared as much as traditional warfare, for it is transversal with respect to the level of violence and may escalate from non-violent 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 CW 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 CW.

FIGURE 1: CW COMPARED TO TRADITIONAL WARFARE IN RESPECT TO THE COUPLES 'VIOLENT AND NON-VIOLENT', 'CIVILIANS-MILITARIES', 'HUMAN AND ARTIFICIAL AGENTS', 'PHYSICAL AND NON-PHYSICAL'. THESE COUPLES ARE EMBLEMATIC OF THE KIND OF WAR WHICH IS WAGED AS THEY IDENTIFY



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

Transversality makes CW extremely appealing from both an ethical and political perspectives (Arquilla and Ronfeldt 1997). At first glance, CW 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 CW 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 CW require a strict ethical regulation to guarantee its fairness. An analysis of CW 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 CYBER WARFARE

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 CW, the difference between the two forms of warfare is the origin of the problems arising when the principles of JWT are applied to CW. 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 CW.

As highlighted in (Taddeo 2012), the application of the principle of 'war as last resort' is shaken when CW 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 decides 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, which could probably be sanctioned by international regulations.

This example is emblematic of the problems encountered in the attempt to establish ethical guidelines for CW. 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 CW 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 CW have a disruptive purpose – disrupting the enemy's (informational) resources (Floridi 2008) –, which needs to be taken into consideration by any analysis aiming at providing ethical guidelines for CW. Even when the disruption of the enemy's informational infrastructure is not achieved through violent and sanguinary means.[5]

5 For a more in depth analysis of the non-violent cases of CW and their assessment as acts of war or of espionage *see* (Arquilla 1998) and (Taddeo 2012).

The second problem to be considered concerns the principle of 'more good than harm'. According to such a principle, 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 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 CW is taken under consideration.

CW is likely to cause none or very little casualties, and as it targets informational infrastructures it is unlikely to cause the destruction of physical objects, like buildings for example. Although it is possible for CW to turn in a violent warfare, in the most of the cases it does not determine physical damages, nonetheless CW 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 CW 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 greater 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 CW.

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. Its correctness is not questionable yet its application is quite difficult in the context of CW.

In classic warfare, the distinction between combatants and non-combatants reflects the distinction between military and civil society. Even if the diffusion of terrorism and guerrilla warfare during the 20th century weakened the association between non-combatants and civilians, in the case of CW such association becomes even feebler, due to the blurring between civil society and military organisations (Schmitt 1999; Shulman 1999).

As noted in (Taddeo 2012), the blurring leads to the involvement of civilians in war actions and poses two issues. The first one concerns the discrimination itself: in the CW 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 cyber 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 CW. 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 CW 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. INFORMATION ETHICS

Information Ethics is concerned with the ethical issues in which information is involved as a resource, as a product, and as a target (Floridi 2008a). It proposes a twofold approach: (i) considering the whole information-cycle, from creation, to communication and storage, and (ii) analysing *informationally* all entities involved in a moral scenario. The moral agents and their actions are considered as part of the informational environment to which they belong as informational entities themselves (Taddeo and Vaccaro 2011).

In this framework, two concepts are of pivotal relevance: Infosphere and informational ontology. As remarked in (Taddeo and Vaccaro 2011), the Infosphere is the totality of what exists. The Infosphere includes agents and objects, relations and processes, as well as the space within which they act. It is not to be confused with cyberspace, as it includes online as well as offline and analogue domains. Infosphere comprises e-books and trees, online websites and rocks, movies in digital format and the paintings on canvas.

The Infosphere is the environment in which animate and inanimate, digital and analogue informational objects are morally evaluated. Information Ethics endorses a universal approach, according to which all exiting things, i.e., not only human beings and living things, but also artefacts and digital artefacts enjoy some minimal and overridable moral rights (Taddeo and Vaccaro 2011).

This universal perspective is grounded in an ontocentric principle, according to which all entities, understood as informational objects, have the fundamental rights to exist and flourish. In Floridi's words: '[...], any form of reality (any instance of information/being), simply by the fact of being what it is, enjoys a minimal, initial, overridable, equal right to exist (be left alone) and develop (not to be interfered) in a way which benefits its nature' (Floridi 2007b).

In such a universal context, the morality of a given action is assessed with respect to the effects that it will have on the patients, i.e., the recipients of the action, and ultimately on the Infosphere. This is referred to as the patient-oriented perspective of Information Ethics, according to which, we can decide whether an action is evil only on the basis of a clear understanding of its effects on interacting patients.

In a nutshell, Information Ethics is an environmental ethics, which endorses an ontocentric and patient-oriented approach, and in which the morality of a course of action is evaluated on the basis of its effects on informational entities and ultimately on the Infosphere. (Floridi 2008a).

Within this framework, Information Ethics provides four moral principles that ought to be respected in order to preserve the well-being and continued flourishing of the Infosphere and its inhabitants:

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 the whole Infosphere ought to be promoted by preserving, cultivating, enhancing and enriching their properties.

The concept of *entropy* adopted in the four laws indicates the result of any form of 'destruction, corruption, pollution, depletion (marked reduction in quantity, content, quality, or value) or unjustified closure of the Infosphere' (Floridi 2001). Informational entropy is the evil, which should be avoided in the Infosphere and should be understood as a metaphysical concept, and it is not related to the concept of physical entropy or the use of entropy made in Shannon's information theory.

Now that the ethical principles and the approach endorsed by Information Ethics have been described, we can focus on its application to CW.

5. JUST CYBER WARFARE

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 CW, this principle allows for considering as moral patients all the entities that may be affected by an action of war within CW. 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.[6]

The first question when considering the conditions for a just CW 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 loses 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

6 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. Furthermore, 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).

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 CW. The principle prescribes the condition under which the choice to resort to CW is morally justified:

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

Two more principles regulate just CW, they are:

II. CW ought to be waged to preserve the well-being of the Infosphere.
III. CW ought not to be waged to promote the well-being of the Infosphere.

The second principle limits the task of CW to restore the *status quo* in the Infosphere before the malicious entity began increasing the entropy in it. According to the second principle, CW should act only when some evil has been or is about to be perpetrated with the goal of stopping it. CW 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 the promoting of the well-being of the Infosphere does not pertain to the scope of a just CW.

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

6. THREE PRINCIPLES FOR A JUST CYBER WARFARE

The application of the principle of 'last resort' provides the first instance of how JWT and Information Ethics are merged. 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 CW is taken under consideration. The impasse is overcome when considering the principles for just CW.

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. Therefore, a state can rightly endorse CW as an early move against a malicious entity. The choice to resort to CW 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 CW.

A caveat must be stressed in this case; the waging of CW must comply with the principles of 'proportionality' and 'more good than harm'. In waging CW, 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 more 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 CW 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, and damages to the physical infrastructures of both the parts involved in the war. Such criteria do not take in consideration the harm that CW may cause.

In the case of CW, 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 CW. It ensures that a just CW 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 CW. 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.[7]

The distinction between combatants and non-combatants promoted by this principle rests on the distinction between militaries and civilians that is inherited from traditional warfare. As we have seen, CW 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 CW comes from the first principle for just CW, 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.

7. CONCLUSION

This article rests on the conceptual analysis of CW 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 deemed to be the characteristics of CW that differentiates it the most from traditional warfare and also the one from which all the ethical issues posed by CW originate.

It has been argued that, given the radical novelty posed by CW, the ethical analysis of this

7 For an in depth analysis of this issue *see* (Taddeo 2012).

phenomenon and the definition of the ethical principles for a just CW 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 CW, 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 CW.

It is rather argued that the ideal of just warfare and the principles prescribed by JWT are still valid when referred to CW, 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.

Information Ethics has been introduced as a suitable ethical framework for CW. This is a macro-ethics, which endorses an ontocentric, patient-oriented and ecological approach and is devoted to address the ethical problems posed by informational phenomena. In particular, the ecological facet of Information Ethics shows to be extremely relevant for the purpose of the analysis proposed in this article, as by posing the well-being of the Infosphere as the ultimate good and the creation of entropy in the Infosphere as the moral evil, it provides the criteria for the ethical assessment of the implications of CW.

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

REFERENCES

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

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

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

Floridi, Luciano. 2008. "Information Ethics, its Nature and Scope." *Information Technology and Moral Philosophy Vol. 40-65*. Cambridge: Cambridge University Press.

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

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

Perry, David L. 1995. "Repugnant Philosophy: Ethics, Espionage, and Covert Action." *Journal of Conflict Studies, Spring*.

Schmitt, Michael N. 1999. "The Principle of Discrimination in 21st Century Warfare." *Yale Humna Right and Development Law Journal* 2:143-160.

Shulman, Mark R. 1999. "Discrimination in the Laws of Information Warfare." *Pace Law Faculty Publications* 37:939-968.

Taddeo, Mariarosaria. 2012. "Information Warfare: a Philosophical Perspective." *Philosophy and Technology*, 25(1): 105-120.

Taddeo, Mariarosaria, and Vaccaro, Antonino. 2011. "Analyzing peer-to-peer technology using information ethics." *The Information Society* 27(2):105 - 112.

Turilli, Matteo, Vaccaro, Antonino, and Taddeo, Mariarosaria. (2010). The Case of on-line Trust. *Knoweldge, Technology and Policy* 23(3-4):333-345.

Turilli, Matteo, Vaccaro, Antonino, and Taddeo, Mariarosaria. (Forthcoming). *Internet Neutrality: Ethical Issues in the Internet Environment*.

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