Information Warfare: a Philosophical Perspective

University of Hertfordshire, University of Oxford
m.taddeo@herts.ac.uk

Abstract

This paper focuses on Information Warfare – the warfare characterised by the use of information and communication technologies. This is a fast growing phenomenon, which poses a number of issues ranging from the military use of such technologies to its political and ethical implications. The paper presents a conceptual analysis of this phenomenon with the goal of investigating its nature. Such an analysis is deemed to be necessary in order to lay the groundwork for future investigations into this topic, addressing the ethical problems engendered by this kind of warfare. The conceptual analysis is developed in three parts. First, it delineates the relation between Informational Warfare and the Information revolution. It then focuses attention on the effects that the diffusion of this phenomenon has on the concepts of state and war. On the basis of this analysis, a definition of Information Warfare is provided as a phenomenon not necessarily sanguinary and violent, and rather *transversal* concerning the environment in which it is waged, the way it is waged and the ontological and social status of its agents. The paper concludes by taking into consideration Just War Theory and the problems arising from its application to the case of Informational Warfare.

Key words: Cyber Attack; Information Revolution; Information Warfare; Robotic Weapon; Just War Theory; War.

1. Introduction

The use of Information and Communication Technologies (ICTs) in warfare scenarios has been of central interest to governments, intelligence agencies, computer scientists and security experts for the past two decades (Arquilla and Ronfeldt 1997; Campen and Dearth 1998; Singer 2009). ICTs support war-waging in two ways: providing new weapons to be deployed on the battlefield – like drones and semi-autonomous robots used to hit ground targets, defuse bombs and patrolling actions - and allowing for the so-called *information superiority*, the ability to collect, process, and disseminate

information while exploiting or denying the adversary's ability to do the same.

ICTs prove to be effective and advantageous war technologies, as they are efficient and relatively cheap when compared to the general costs of traditional warfare (Arquilla and Borer 2007; Steinhoff 2007b; Brenner 2008). For this reason, the use of ICTs in warfare has grown rapidly in the last decade determining some deep changes in the way war is waged. ICTs gave rise to the latest revolution in military affairs (RMA)[1] by providing new tools and processes of waging war - like network-centric warfare (NCW), and integrated command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR).

This RMA concerns *in primis* military forces, as they have to deal with "the 5th dimension of warfare, *information*, in addition to land, sea, air and space" [emphasis added].[2] It also concerns strategy planners, policy-makers and ethicists, as rules for this new form of warfare are much needed and the existing international regulations, like the Geneva and Hague Conventions, provide only partial guidelines (Wall 2000; Barnett 1998; Saydjari et al. 2002). In the same way, traditional ethical theories of war, which should provide the framework for policies and regulations, struggle to address the ethical problems that arise with this new form of warfare (Arquilla 1999; DeGeorge 2003; Powers 2004; Weber 2009).

In particular there are three categories of problems on which both policy-makers and ethicists focus their attention, and these are the *risks*, *rights* and *responsibilities*. In the rest of this paper I shall refer to these problems as the 3R problems. ICT-based modes of conflicts do not relate exclusively to military affairs. Rather, they represent a wide spectrum phenomenon, which is rapidly changing the dynamics of combat as well as the role warfare plays in political negotiations and the dynamics of civil society. These changes are the origins of the 3R problems, so the conceptual analysis of such changes and of the nature of this phenomenon is deemed to be a necessary and preliminary step for addressing these problems.

Altogether, the 3R problems pose a new ethical challenge with which most of the extant literature on the use of ICTs in warfare is concerned. Nevertheless, the 3R problems will not be the focus of this paper, which will instead concentrate on the analysis of the nature of ICTs-based warfare. The task of the proposed analysis is to

[1] For an analysis of RMA considering both the history of such revolutions and the effects of the development of the most recent technologies on warfare see (Benbow 2004; Blackmore 2005).
[2] http://www.defencejournal.com/2000/sept/military.htm

lay down the conceptual foundation for the solution of the 3R problems, which will be provided elsewhere.

In the rest of this paper ICTs-based warfare will be analysed within the framework of the Information revolution (Floridi 2009). In particular, a general definition of this kind of warfare will be provided as a starting point of the analysis. Then it will be argued that this form of warfare is one of the most compelling cases of the *shift toward the non-physical domain* brought to the fore by the Information revolution. Attention will be focused upon the effects of such a shift on the concept of war and upon a structural aspect of contemporary society, such as the distinction between civil society and military organisations. Finally, the paper will focus on Just War Theory and its application to the case of ICTs-based warfare.

Before analysing in detail the nature of this new form of warfare, I will describe concisely the 3R problems. The examination of these problems is not the goal of this analysis, but since this paper is devoted to preparing the ground for their solution, the reader may benefit from being acquainted with them.

Risks. The risks involved with ICTs-based warfare concern the potential increase in the number of conflicts and casualties. ICTs-based conflicts are virtually bloodless for the army that deploys them. This advantage has the drawback of making war less problematic for the force that can implement these technologies, and therefore making it easier not only for governments, but also for criminal or terrorist organisations, to engage in ICT-based conflicts around the world (Arquilla and Borer 2007; Steinhoff 2007a; Brenner 2008).

Rights. ICTs-based conflicts are pervasive for they not only target civilian infrastructures but may also be launched *through* civilian computers and websites. This may initiate a policy of higher levels of control enforced by governments in order to detect and defend their citizens from possible hidden forms of attacks. In this circumstance, the ethical rights of individual liberty, privacy and anonymity may come under sharp, devaluating pressure (Arquilla 1999; Denning 1999).

Responsibilities. The problem concerns the assessment of responsibilities when using semi-autonomous robotic weapons and cyber attacks. In the case of robotic weapons, it is becoming increasingly unclear who, or what, is accountable and responsible for the actions performed by complex, hybrid, man-machine systems on the battlefield (Matthias 2004; Sparrow 2007). The assessment of responsibility

becomes an even more pressing issue in the case of cyber attacks, as it is potentially impossible to track back the author of such attacks (Denning 2007).

We are now ready to look more carefully into the nature of ICTs-based warfare; this will be the task of the next section.

2. Information Warfare and Information Revolution

ICTs are used in several combat activities, from cyber attacks to the deployment of robotic weapons and the management of communications among the fighting units. Such a wide spectrum of uses makes it difficult to identify the peculiarities of this phenomenon. Help in respect to this will come from considering in more detail the different uses of ICTs in warfare. Let us begin by describing a very powerful kind of cyber attack, the 'smurf' attack.

A smurf attack is an implementation of distributed denial of service (DDoS) attacks. A DDoS is a cyber attack whose aim is to disrupt the functionality of a computer, a network or a website. In a smurf attack, the attacker sends a request for return packets to some intermediary network's broadcast address, which in turn automatically communicates the request to all the peers on that network. All the peers then reply with a return packet. In the original packet, the author of the attack replaces her source address with the address of the intended victim. The victim is then flooded with replies from all the peers in the network. The author of the attack can send similar packets to other networks at the same time to intensify the attack and cause so much network congestion at the victim's site that it will be impossible for the victim to perform any work or provide any services. This form of attack was deployed in 2007 against institutional Estonian websites, and more recently similar attacks have been launched to block the Internet communication in Burma during the 2010 elections.[3]

The use of robotic weapons in the battlefield is another way to use ICTs in warfare. It is a growing phenomenon, coming to widespread public notice with US army, which deployed 150 robotic weapons in Iraq's war in 2004, culminating in 12,000 robots by 2008. Nowadays, several armies around the world are developing and using tele-operated robotic weapons, they have been deployed in Iraq and Afghanistan, and more sophisticated machines are being used at the borders between

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

Israel and Palestine in the so-called 'automatic kill zone'. These robots are trusted to detect the presence of potential enemies and to mediate the action of the human soldiers and hence to fire on potential enemy's targets when these are within the range patrolled by the robots.[4] Several armies also invested their resources to deploy unmanned vehicles, like the MQ-1 predators, which have then been used to hit ground targets, and to develop unmanned combat air vehicles, which are designed to deliver weapons and can potentially act autonomously, like the EADS Barracuda, and the Northrop Grumman X-47B.[5] One of the latest kinds of robotic weapon - SGR-A1 – has been deployed by South Korea to patrol the border with North Korea.

This robot has low-light camera and pattern recognition software to distinguish humans from animals or other objects. It also has a colour camera, which can locate a target up to 500 metres, and if necessary, can fire its built-in machine gun. Up until now, robotic weapons were *tele-operated* by militaries sitting miles away from the combat zone. Human were kept in the loop and were the ones who decided whether to shoot the target and to manoeuvre the robot on the battlefield. The case of SGR-A1 constitutes quite a novelty, as it has an *automatic* mode, in which it can open fire on the given target without waiting for the human soldier to validate the operation.

Finally, the management of communication among the units of an army has been revolutionized radically by the use of ICTs. Communication is a very important aspect of warfare. It concerns the analysis of the enemy's resources and strategy and the definition of an army's own tactics on the battlefield. NCW and C4ISR represent a major revolution in this respect. An example of such revolution is the use of iPhone and Android devices. Today, the US army is testing the use of these devices to access intelligence data, display videos made by drones flying over the battlefields, constantly update maps and information on tactics and strategy, and, generally speaking, gather all the necessary information to overwhelm the enemy.[6]

Before looking more carefully in the nature of Information Warfare (IW) it is worthwhile to recall the reader's attention on the method of the analysis proposed in this article. In order to do so it is necessary to introduce the levels of abstractions

[4] http://blog.wired.com/defense/2007/08/httpwwwnational.html
http://blog.wired.com/defense/2007/06/for_years_and_y.html
[5] Note that MQ-1 Predators and EADS Barracuda, and the Northrop Grumman X-47B are Unmanned *Combat* Aerial Vehicles used for combat actions and they are different from Unmanned Air Vehicles, like for example Northrop Grumman MQ-8 Fire Scout, which are used for patrolling and recognition purposes only.
[6] http://www.geohot.us/2010/12/american-soldiers-are-testing-iphone.html

(LoAs) (Floridi 2008b).

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

The goal is to analyse the nature of IW as a phenomenon; in order to do so the different occurrences of such a phenomenon, i.e. the deployment of robotic weapons, cyber attacks and the use of ICTs for communication management, are all considered at a high LoA. At such a level, the different occurrences of military uses of ICTs are considered only with respect to their common factor rather than their differences. The analysis developed in this way allows for focusing on the nature of IW and for unveiling its characteristic aspects. Once these aspects are considered, a lower LoA will be endorsed in order to study the specific occurrences of IW and their ethical implications.

Despite the differences between the uses of ICTs in warfare, there is one aspect that is common to all the circumstances, and this is the deployment of ICTs with an *immediate disruptive* intent – be it the use of (semi)autonomous weapons, the disruption of some informational infrastructure or the deployment of digital devises to enhance the performance of the forces on the battlefield. This common factor provides the first step towards the definition of this new kind of warfare. We are now able to provide a general definition (GD).

> **GD.** Information Warfare is the use of ICTs with either offensive or defensive purpose to immediately *intrude*, *disrupt*, or *control* the opponent's resources.

The expression *Information Warfare* is meant to stress the informational nature of this phenomenon. The label '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). In this paper, IW will be used to indicate a wide spectrum phenomenon with different occurrences – ranging from cyber attacks, to the use of (semi)autonomous weapons, NCW and C4ISR protocols – which all share the same informational nature, as they are all grounded on some implementation of ICTs (Figure 1).

Figure 1 The deployment of robotic weapons, the launch of cyber attacks and the managing of communications through ICTs as instances of InformationWarfare.

GD focuses only on the *minimum* common factor to all the occurrences of IW and it does not take into consideration other important features of this phenomenon. In particular, GD does not tell us whether there are other fundamental aspects of IW that need to be taken in consideration and what these are. Also, it does not allow for distinguishing between IW, information crime, terrorism or activism. For this reason, the reader should not consider it a conclusive definition but rather the starting point of our analysis, which will eventually allow for its refinement.

Following GD, IW is yet another phenomenon occurring thanks to the dissemination of ICTs. In this respect, IW is in line with the diffusion of other phenomena such as e-commerce, social networks, e-trust, and e-governance. Like all these phenomena, IW is related to the so-called Information revolution, i.e. the development and capillary dissemination of ICTs. The reader should not mistake this approach as a way of trivialising the issue of IW; it is rather a way of considering IW within a broad perspective, with the idea that the nature of this phenomenon and its conceptual and ethical implications will become clearer, when considered in a wider framework.

From an historical point of view, technological breakthroughs create economic upheavals, and determine changes affecting the structure of both civil society and military organisations. As described by (Toffler and Toffler 1997), this was the case in the Neolithic revolution, when human beings first made weapons out of wood and rocks, and in the Industrial revolution, which provided the means for industrialised

warfare and for the dissemination of weapons of mass destruction. The Information revolution is the latest example. It has changed our activities in several ways and at several levels. The use of ICTs changed the way individuals manage their communications and daily practices, from working and reading books and listening to music, to shopping and driving. At a social level, ICTs reshaped social interactions with the dissemination of the social networks, like Facebook, Twitter, or Flickr for example. The same applies at the institutional level, where ICTs provide new tools for the management of information and bureaucracy (Saxena 2005; Ciborra 2005), and when considered with respect to the military activities, the Information revolution determines the latest revolution in military affairs.[7]

The Information revolution is a twofold phenomenon; it has both a technological and a philosophical nature. The technological breakthrough initiated a series of transformations affecting individual and social activities, which have philosophical consequences as they radically change the way human beings interact with their environment. Floridi stresses this aspect of the Information revolution when he calls it the *fourth revolution* (Floridi 2009), to highlight that - like the previous three revolutions, Darwinian, Copernican and Freudian – the Information revolution changes deeply the way human beings perceive themselves in the universe and interact with their environment.

Among the peculiarities of the Information revolution, one is of particular relevance when considering IW. This is that the Information revolution changes fundamentally the way reality is perceived and understood. In Floridi's words: "[The Information revolution] is updating our everyday perspective on ourselves and on the ultimate nature of reality, that is, our metaphysics, from a materialist one, in which physical objects and processes play a key role, to an informational one. Objects and processes are increasingly seen as *de-physicalised*, in the sense that they tend to be treated as support-independent", ([emphasis added] Floridi 2010, p.2).

In the rest of this paper I will refer to such an updating process as a *shift toward the non-physical domain*. This shift makes the boundaries of reality stretch to include non-physical objects, actions and interactions as well as physical ones. IW is one of the most compelling instances of the shift toward the non-physical domain, for it shows that there is a new environment, where physical and non-physical entities

[7] See (Benbow 2004; Blackmore 2005) for an analysis of the debate on the on-going RMA.

coexist, in which states have to prove their authority and new modes of warfare are being developed specifically for deployment in such a new environment. Nowadays, the design of data banks and software, the ability to blindside the opponent's informational infrastructures, and ensuring the superiority of informational infrastructures of a state, are as important as the superiority of weaponry and military force. This is the reason why in the last two decades, several states have devoted huge effort and resources in order to improve their informational infrastructures and to educate experts in the relevant fields.[8]

There is no doubt about the fact that non-physical powers existed long before the advent of the Information revolution, economic and diplomatic powers being the most common examples. Yet, the novelty posed by the Information revolution is staggering, relying on the fact that informational (non-physical) powers are not backed up by physical powers but stand by themselves. Diplomatic power, for example, rests on the recognition of the military and industrial forces of a state. Informational powers, e.g. the ability to launch cyber attacks, on the contrary, are independent from any other power and, as IW shows, they may also provide the necessary support to make more effective a state's physical powers.

The shift toward the non-physical domain affects the way war is waged. The issue arises as to whether the transformation imposed by this shift is reshaping the very concept of war. The analysis of this issue will be developed in the next section.

3. War after IW

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). As Oppenheim put it: "war is a contention between two or more states through their armed forces, for the purpose of overpowering each other and imposing such conditions of peace as the victor pleases", (Lauterpacht 1952, p. 202). In this respect, the revolution determined by IW also has philosophical implications, beside the military and political ones, for the changes that it determines concern the very *concept* of war other than the way war is waged.

[8] 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

The choice to undertake a (classic) war usually involves a substantial commitment, as it has heavy economical and political costs, borne mainly by the civil society. These features of war have been radically changed by the advent of IW, which provides the means to carry out war in a completely different manner. In this scenario, the changes determined by IW are of astounding importance as they concern both the way the military and politicians consider waging war, and the way war is perceived in the civil society. Like traditional warfare, IW is very powerful and potentially highly disruptive. However, unlike traditional warfare, IW is potentially *bloodless*, *cost effective,* and *is not a military specific* phenomenon.

Let us analyse these three aspects in greater detail. IW is virtually bloodless for the forces that deploy ICTs, as it does not require physical commitment. IW can be fought using tele-operated robots or launching a cyber attack, disrupting the enemy's resources (both human and non-human) without risking any casualties for the army that deploys such technologies. IW is cost effective for two reasons; first, it increases the effectiveness of each fighting unit by providing powerful communication tools. C4ISR, for example, provides greater autonomy to the units on the battlefields and allows for establishing direct links in real time between strategic level and tactical level, reducing time and bureaucracy and, hence, costs. Second, the deployment of robotic weapons, like drones for example, and the use of cyber attacks are both much cheaper than using traditional aerial vehicles and attacks, and can be more efficient. Finally, the technologies and skills required to fight in an IW scenario are not military specific, as they are also *largely* used by civilians, and may be deployed by them for disruptive purposes.

It would be a mistake to consider IW simply as a non-sanguinary, cheap and less military-based version of classic warfare; IW can be as bloody and violent as traditional warfare, as it may determine damages and casualties comparable to traditional warfare. Nevertheless, the deployment of ICTs gives rise to a completely new form of warfare, whose main peculiarity is that of being *transversal*. IW is transversal with respect to the *environment* in which it can be waged, the *kinds of agents* involved in it, and the *modes* of combat. Such transversality represents the ultimate difference between IW and classic war, and it is the aspect of IW from which policy-related and ethical problems arise.

Let us consider the environmental transversality of IW. In section two, it has been argued that with the Information revolution the environment in which we act is

extended to include both the physical and non-physical domains. IW may originate in and affect both domains. The case of Stuxnet will help to clarify this aspect. Stuxnet is a computer-worm, first discovered in Belarus in 2010. It became famous during the same year for being tracked in the Iranian nuclear power plant of Bushehr, damaging a number of centrifuges.[9] This computer-worm targets systems that are not connected to the Internet, like the industrial ones. The worm is spread via USB key and infects Windows systems. Once it has infected a machine, it seeks a specific configuration of industrial control software. Once hijacked, the code can reprogram the programmable logic control software and controls the infected industrial machinery. In this way it is possible, for example, to turn on and off motors, in the case of the centrifuges to manipulate temperature and turn on coolers. The disruptive potential that originates from this computer-worm is quite high.

The case of Stuxnet provides a good example of the environmental transversality of IW, as it is a digital (non-physical) weapon able to affect, and possibly disrupt, objects in the physical domain. It illustrates how attacks originating in cyberspace, like a worm, may quite easily affect physical objects or individuals, and that IW can easily be used for this purpose, and not only to disrupt informational targets.

The transversality of IW also has a bearing on the kind of agents involved in the warfare scenario. In this respect, two issues need to be highlighted: the *ontological* and the *social* status of the combatants. The ontological status ranges over a quite large spectrum, as combat actions undertaken under the umbrella of IW are performed both by artificial agents, such as viruses, drones and robots for example, and human agents. The heterogeneous nature of combating agents is an important aspect to consider, for it poses policy-related and ethical issues. In relation to policy, the questions concern how to deploy and cause interaction between different *kinds* of agents in a warfare scenario. Typical problems are, for example, the definition of the chain of command and the rules of engagement. When it comes to ethics, the issues become even more pressing, because they concern the ethical responsibility of the actions performed by these agents. In IW artificial agents, such as drones, robots and viruses, and human agents may have the same role in achieving a given goal, their actions are equally relevant and important, despite their ontological differences.

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

Therefore it is of paramount importance to define criteria for establishing the responsibilities in combat actions.

The transversality of IW with respect to the social status of the combatants follows from the fact that IW does not require military-specific skills and techniques. This aspect has the side effect of allowing skilful civilians to participate in combat actions in IW, for example launching a virus or a DDoS attack. Beside the image of the nerd guy sitting in his room and blowing up a far distant nuclear power plant, this aspect of IW has an important consequence for contemporary society, as it leads to the blurring of the distinction between civil society and military organisation.

The tasks, the skills and the roles, peculiar to the two sectors of society are being completely redefined. In the past, the relation between civil society and military organisations (CMR) were grounded on the normative assumption that civilians' control of the military is preferable to the military's control of the civil infrastructures (Burk 2002; Huntington 1957). The principal problem to solve was to explain how civilian control over the military should be established and maintained. This framework is being eroded by the dynamics developed within IW, and new issues are now emerging such as whether it is acceptable from an ethical and political perspective to allow the distinction to vanish.

This blurring of boundaries may eventually lead to holding civilians responsible for combat actions and to consider civilian public and private infrastructure licit targets in warfare scenarios. So, for example, it may become acceptable to disrupt the civilian supply chain for food and water and to control civilians' private networks and computers.

Finally, the transversality of modes of combat in IW concerns the wide range of techniques that can be deployed, from C4ISR to DDoS or informational viruses, to drones and robots. It also concerns the level of violence of combat actions in IW, which range from 'soft' non-violent actions, such as DDoS attacks, to extremely disruptive and violent attacks, as could be the case of a robotic weapon taking part in an action on the battlefield or a cyber attack that leads to the casualties and physical damage. The transversality here has important consequences. The most important one

is that IW can be unequivocally defined neither as a violent nor as a 'soft' form of warfare.[10]

The analysis presented in this section allows us to refine the definition of IW provided in section two. IW refined definition (RD) is:

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

Note that RD refines the definition of IW provided in section 2 allowing for distinguishing the cases of IW from those of information-activism, crime and terrorism, as it refers to IW as being a state's activity performed through a state's military forces, whereas information-activism, crime and terrorism involve non-state actors.

With this definition of IW in place, we are now ready to turn our attention to the analysis of the application of Just War Theory to the case of IW.

4. Just War Theory and IW

Ethical analyses of war are developed following three main paradigms: Just War Theory, Pacifism or Realism. In the rest of this paper, the analysis will focus only on Just War Theory. This theory is the most influential of the three ethical frameworks, providing the ground for international regulations, such as the United Nations Charter and The Hague and Geneva Conventions, and setting the parameters for both the ethical and the political debates. Therefore it is of paramount importance to understand whether and how the principles of this theory could be applied to the case of IW (Arquilla 1998).

Just War Theory prescribes the principle for states and their political leaders to declare, wage and terminate *just* war. It refers to a classic scenario where war is meant to be 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. Yet, before throwing the baby out with the bathwater, it is worth

[10] See (Wingfield 2000) for a description of the criteria to assess the whether a war action uses economic, diplomatic forces, and other soft measures.

considering whether, despite the differences between classic war and IW, Just War Theory can be endorsed for the ethical analysis of IW. In order to do so, we need to understand where the problems lie, whether it is possible to solve them and, if so, how. In the rest of this paper, attention will focus on the identification of the problems, their solution has been left to another paper.

The first problem has already been partially described in this section - this is that Just War Theory refers to classic warfare scenario. It assumes that governments and their leaders are the only ones who inaugurate wars, by deploying their armed forces, and they are the ones to be held accountable for the actions of war. IW changed this scenario, by fostering a completely new way of declaring and waging war. Just War Theory needs to take into account such changes in order to address the ethical problems that arise with IW. IW has to be considered not simply as a new way of waging war, but as a *new phenomenon*, which engenders radical changes on the modes of conflicts and on the concept of war.

The need to consider IW as a completely different phenomenon from classic warfare, and to take into consideration such difference, becomes evident when considering Just War Theory in more detail. In this respect, there are two problems that deserve attention; they follow from the application of the principles of 'war as last resort' and the one of 'discrimination' to the IW scenario.

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.[11]

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

[11] Note that the problems related to the application of the principle of last resort are not a direct consequence of the informational nature of the possible strike, rather they follow from the fact that cyber attacks may be bloodless. In this respect, the application of the principle becomes problematic in any case where a bloodless first strike could be used to avoid a sanguinary war, independently from the nature of such a strike.

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 Just War Theory, 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 described in section three, 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 2008a) - which need to be taken in consideration. There are means that can be *justly* endorsed proactively to avoid classic warfare and soft-cases of IW may be among these means (Bok 1978). Nevertheless, the disruptive intent, even when it is not achieved through violent and sanguinary means, must be taken in consideration by any analysis aiming at providing ethical guidelines for IW.

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 Just War Theory 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 Just War Theory 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, Just War Theory would only be able to address 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.

The other consequence is that this approach unveils the need of a flexible framework when considering contemporary war waging. Cyber attacks can be deployed in different circumstances and with different goals, see for example the use of Suter in the Operation Orchard[12] and the 'cap cake attack'.[13] In the first case the cyber attack was part of the military action and should be considered an act of war, in the second case it was a pure act of espionage. Nonetheless, the heterogeneity of the possible uses of cyber attacks should not lead to exclude them from the ethical analysis of IW, it rather shows the need to develop a framework for the analysis of this new kind of warfare able to account for such heterogeneity.

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

In classic warfare, the distinction between combatants and non-combatants reflects the distinction between military and civil society. Hence it forbids targeting not only civilians but also civilian infrastructures, like hospitals or 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). As noted in section three, IW does not require military expertise; civilians can easily undertake a war action. The

[12] In 2007 Israel launched Operation Orchard and carried out an airstrike on Syria. It has been speculated that the Israeli army may have used a computer program, Suter, to interfere with the Syrian air defense system in order for Israeli planes to pass undetected by the Syrian radar.

[13] The 'cup cake attack' was launched by MI6 against Al Qaeda on-line magazine in June 2011. In this case the instructions on how to 'Make a bomb in the Kitchen of your Mom' where changed into the recipes of 'The Best Cupcakes in America'. http://idle.slashdot.org/story/11/06/03/1346209/MI6-Swaps-Bomb-Making-Info-With-Cupcake-Recipe-On-al-Qaeda-Website

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 problem 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.[14] 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.

These problems highlight the pressing need to provide an ethical framework for the regulation of IW. Such regulation needs to be accepted by states and international organisations and to be consistent with the existing ones regarding classic warfare; for this reason, applying Just War Theory to IW is of major importance.

5. Conclusion

IW represents a staggering revolution, which concerns military affairs and has also political and social ramifications for contemporary society. Such a radical revolution leaves a vacuum for both ethical principles and regulations. Ethical guidelines are deemed to be the grounds on which any regulation of IW stands, and for this reason most of the extant literature focuses on the ethical analysis of this form of warfare (Schwartau 1996; Nitzberg 1998).

[14] This problem is part of the 3R problems described in section one.

This paper proposed to take a step back in the analysis of IW, and to focus first on the nature of this phenomenon and *then* to turn attention on its ethical implications, for which the conceptual analysis is meant to provide the groundwork.

Three aspects of IW have been highlighted in this paper, its relation to the Information revolution, and its disruptive and transversal nature. Considering IW in relation to the Information revolution unveiled a fundamental aspect of this phenomenon, that is, the shift toward the non-physical domain. It has been argued that IW represents one of the most compelling cases of such shift, as it shows that political and militaries authorities are investing their resources to establish and maintain power over such domain.

This analysis leads to the consideration of the effects of the dissemination of IW on the concept of war, and showed that this new form of conflict imposes radical changes on the way war is waged and conceived. In particular, IW redefines the concept of war as a phenomenon not necessarily sanguinary and violent, but rather transversal in the way in which it concerns the environment in which it is waged, the way it is waged and the ontological and social status of its agents.

Finally, Just War Theory and the problems arising from its application to IW have been taken in consideration. The analysis of such problems indicates that in order to endorse the principles of Just War Theory to analyse IW, it is necessary to extend the set of the assumptions concerning war scenario on which this theory rests to include the peculiarities of IW scenario.

The analysis presented in this paper examines the nature of IW, and highlights the problems generated by this phenomenon, be they ethical, social or purely philosophical. With such an analysis in place, attention will now be devoted to defining an ethical framework for IW. This task has been left to a future work.

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., & Borer, D. A. (Eds.). (2007). *Information Strategy and Warfare: A Guide to Theory and Practice (Contemporary Security Studies)*. New York, USA: Routledge.

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

Barnett, R. W. (1998). Information Operations, Deterrence and the Use of Force. *Naval War College Review, 51*(17), 7-19.
Benbow, T. (2004). *The Magic Bullet?: Understanding the Revolution in Military Affairs* London: Brassey.
Blackmore, T. (2005). *War X*. Toronto: University of Toronto Press Incorporated.
Bok, S. (1978). *Lying: Moral Choice in Public and Private*. New York, USA: Pantheon.
Brenner, S. W. (2008). *Cyberthreats*. New York, USA: Oxford University Press.
Burk, J. (2002). Theories of Democratic Civil-Military Relations. *Armed Forces & Society, 29*(1), 7-29.
Campen, A. D., & Dearth, D. H. (1998). *Cyberwar 2.0: Myths, Mysteries and Reality*. Fairfax, Va: AFCEA International Press.
Ciborra, C. (2005). Interpreting e-government and development: Efficiency, transparency or governance at a distance? *Information Technology & People, 18*(3), 260 - 279.
DeGeorge, R. T. (2003). Post-september 11: Computers, ethics and war. *ar. Ethics and Information Technology, 5*(44), 183-190.
Denning, D. (1999). *Information warfare and security*. Boston, USA: Addison-Wesley.
Denning, D. (2007). The Ethics of Cyber Conflict. In K. E. Himma, & H. T. Tavani (Eds.), *Information and Computer Ethics*. Hoboken, USA: Wiley.
Floridi, L. (2008a). 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. (2008b). The Method of Levels of Abstraction. *Minds and Machines, 18*(3), 303-329.
Floridi, L. (2009). The information Society and Its Philosophy. *The Information Society, 25*(3), 153-158.
Gelven, M. (1994). *War and Existence*. Philadelphia, PA: Pennsylvania State University Press.
Huntington, S. P. (1957). *The Soldier and the State; the Theory and Politics of Civil-Military Relations*. Cambridge, USA: Belknap Press of Harvard University Press.
Lauterpacht, H. (Ed.). (1952). *Oppenheim, International Law* (7th ed., Vol. II Disputes, War and Neutrality).
Libicki, M. (1996). *What is Information Warfare?* Washington, D.C, USA: National Defense University Press.
Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology, 6*(3), 175-183.
Nitzberg, S. (1998). *Conflict and the computer: information warfare and related ethical issues.* Paper presented at the 21st National Information Systems Security Conference., Arlington, USA,
Perry, D. L. (1995). Repugnant Philosophy:Ethics, Espionage, and Covert Action. *Journal of Conflict Studies, Spring*.
Powers, T. M. (2004). Real Wrongs in Virtual Communities. *Ethics and Information Technology, 5*(4), 191-198.
Saxena, K. B. C. (2005). Towards excellence in e-governance. *Journal of Public Sector Management, 18*(6), 498 - 513.
Saydjari, O., Tinnel, L., & Farrell, D. Cyberwar Strategy and Tactics: An Analysis of Cyber Goals, Strategies, Tactics, and Techniques. In *2002 IEEE Workshop on*

Information Assurance, United States Military Academy, West Point, NY, USA., 2002

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.

Schwartau, W. (1996). Ethical Conundra of Information Warfare, in Cyberwar: Security, Strategy and Conflict in the Information Age. In A. D. Campen, D. H. Dearth, & R. T. Goodden (Eds.), *Cyberwar: Security, Strategy and Conflict in the Information Age*. Fairfax, USA: AFCEA International Press: Fairfax, USA.

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

Singer, P. W. (2009). Robots at War: The New Battlefield. *Wilson Quarterly, 33*(1), 30-48.

Sparrow, R. (2007). Killer Robots. Journal of Applied Philosophy. *24, 1*(62-77).

Steinhoff, U. (2007a). *On the Ethics of War and Terrorism*: Oxford University Press.

Steinhoff, U. (2007b). *On the Ethics of War and Terrorism*. New York, USA: Oxford University Press.

Toffler, A., & Toffler, H. (1997). Foreword: The New Intangibles. In J. Arquilla, & D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. xii-xxiv). Santa Monica, USA: RAND, MR- 880-OSD/RC.

Wall, D. S. (2000). Introduction cybercrimes, cyberspeech and cyberliberties. *International Review of Law Computers & Technology, 14*(1), 5-9.

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

Walzer, M. (2000). *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (3rd ed.). New York, USA: Basic Books.

Weber, J. (2009). Robotic Warfare, Human Rights & the Rhetorics of Ethical Machines. In R. Capurro, & M. Nagenborg (Eds.), *Ethics and Robotics* (pp. 83-104). Amsterdam: IOS Press.