The necessity of redesigning the international laws on the ethical approach to war due to the Information Revolution

Edoardo Saputelli
Politecnico di Milano
edoardo.saputelli@mail.polimi.it

February 7, 2022

Abstract

The phenomenon of the Information Revolution has brought a large number of technological advancements to society but, at the same time, it raised likewise issues in several environments.

The military context is one of the most involved in the consequences of this revolution, since it saw the rise of a completely new way of waging war: the Information Warfare. Introducing a substantially different approach to war, the spread of Information Warfare shook up the conventions established during the XX century with the aim to make war as ethical as possible.

The goal of this paper consists in the analysis of the upheaval that the war environment has to face, evaluating the dissimilarities of Information Warfare with respect to the traditional approach to war. This will be done with the aim to accurately outline the ethical conventions which could still be applied to Information Warfare and which ones, instead, are fundamental to redesign.

Section 1: Introduction

In order to completely understand the reasons behind the spread of Information Warfare, it is necessary to introduce the specific historical and social context in which it flourished.

Around the last decades of the XX century the most developed countries of the world have seen their entrance in the Information Age, thanks to their advancements in digital technologies. Indeed, due to the capillary dissemination of ICTs (Information and Communication Technologies), the society started to experience relevant changes, from people's daily life to wider contexts such as political aspects within and between states.

This could appear as a peculiar event, but it can be seen as a recurring pattern in history. Indeed, technological breakthroughs have often brought to economic and social revolutions, for example during the Industrial Revolution. However, despite all the positive advances, society has always dealt also with the thorny side effects that technological developments bring, since these often entail social changes that are quite complex to face.

Considering nowadays everyday life, it is easy to notice how much the Information Revolution has influenced the way people manage their communications or deal with their daily practices, from the most simple ones like shopping or listening to music, to the most relevant ones, such as working. From this, it can be said that this revolution has changed the way people perceive and understand reality, and these transformations obviously bring to the need of a philosophical examination.

This paper focuses its attention on the issues, raised by the Information Revolution, which overturned the military background.

Despite the fact that this context has already been analysed through the establishment of ad-hoc laws after the bloody wars of XX century, the Information Revolution has raised the need to readapt them to the contemporary context.

This paper is divided into three parts: firstly, Information Warfare will be introduced and defined. This part will also include a comparison to traditional forms of warfare to highlight the main similarities and differences. This will be important to highlight the main challenges that need to be faced. Afterwards, the current state of international law will be thoroughly described, to understand which attempts have been made at making war ethical. Finally, the problems posed by IW to international law will be detailed.

Section 2: the spread of Information Warfare

In line with the diffusion of other phenomena like e-commerce or social networks, Information Warfare too has seen its growth in the context of the shift to the non-physical domain caused by the Information Revolution. It can even be said that it is one of the most relevant instances of it. Indeed, despite the previous existence of other non-physical powers like economic and diplomatic ones, IW gets a substantial role due to its capacity to stand by itself without needing any kind of support (e.g.

diplomatic power lies on the recognition of other forces of a state, while informational powers are independent from any other power) (Taddeo 2011).

As a consequence of the Information Revolution, society increased its dependency on digital infrastructures. This for sure eased complex bureaucratic and political processes but, on the other hand, it paved the way for new types of attacks: the cyberspace-based ones.
Their raise, in addition to the other already existing kinds of attacks (land, sea, air and space), laid the foundation of a new way of waging war: Information Warfare. IW takes advantages of ICTs in different manners: from the employment of cyber-attacks to the deployment of robotic weapons, but also for the management of communications among military units. Despite the branches of IW seem to be different, they have a relevant property in common: exploiting ICTs with an always disruptive intent. Because of this, Information Warfare could be defined in broad terms as "the use of ICTs with either offensive or defensive purpose to immediately intrude, disrupt or control the opponent's resources" (Taddeo 2011, 109)

Section 3: Waging war through Information Warfare

Describing in a more accurate way Information Warfare, it is easy to understand the reasons why it became one of the main forms of war.
First of all, IW needs ICTs to be widely adopted. Nevertheless, this is usually not a limiting factor, since their use grew rapidly for the whole society in the last decades, because of their efficiency and affordability.

Moreover, concretely analysing IW, it results different from the traditional forms of war in many aspects and this is the reason why it should be accurately examined. Certainly, IW is very powerful and highly disruptive as well as traditional warfare, but on the other hand it has the power to be bloodless and cost-effective.
IW is bloodless because it doesn't require the deployment of physical forces, being adequately effective through tele-operated robots or cyber-attacks. This avoids the risk of damages to the attacking armies, while at the same time leading to highly disruptive effects, affecting wide areas but keeping very low levels of losses of life. Military troops are able to reach these goals thanks to the possibility to separate the life of the operator from the mission and to the possibility to hit massively interconnected infrastructures such as traffic grids and electric grids, enabling the disruption of areas wider than ever before. It is true that the employment of drones and tele-operated robots may appear bloodless only for the attacking side, but frequently it is the same for the defending side too. Indeed, even if these technologies are sometimes used in order to strike at the enemies' armies, a lot of times they are just employed for intelligence, reconnaissance and

surveillance missions. Moreover, it is cost-effective because it is able to reduce the amount of the resources employed on the battlefield thanks to the use of powerful communication tools able to increase the effectiveness of the deployed fighting units. Another advantage is the use of cyber-attacks and robotic weapons, which are cheaper and usually more efficient than the deployment of traditional vehicles and attacks. (Taddeo 2011)

In addition, IW could be considered both as a form of close-support for military forces during active operations and as a more direct manner to strike at the logistical infrastructures of an enemy. Even though the strategy of not focusing on the enemies' armed forces could resemble the role of airpowers during 1920s and 1930s, the above-mentioned typical features of IW outline the main differences between it and conventional air power. Indeed, although they are sometimes used towards the same goal, conventional air power is usually focused on destruction of strategic facilities with the additional consequences of copious civilian losses, while information attacks are able to complete the mission and disrupt enemy forces without bringing the same level of material destruction and civilian losses. (Arquilla 1999)

Section 4: current laws and conventions for war

From ancient times, attempts have been made to craft a more ethical approach to war. For instance, the Greeks were already not extraneous from this concept: Strabo, a Greek geographer, narrating about the Lelantine War (c. 700 BC), observed that both parties agreed to ban the use of projectile missiles, considering them unethical weapons. (Ober 1994)

In more recent times, in order to make war less brutal and atrocious as possible, countries have made improvements with a series of pacts signed during the XX century.

Significative advances were carried out firstly at the end of World War I with the Treaty of Versailles (1919) and then with the Kellogg-Briand Pact (1928). However, the real turning point is represented by the establishment of the Charter of the United Nations (1945) which, for the first time, introduced new approaches to war in order to reach a state of international peace and security and to guarantee higher standards of living for the citizens of the member states, promoting a correct respect and observance of human rights and fundamental freedoms.

Two key concepts of the Charter of the United Nations about the notion of "just war" are the *jus ad bellum* and the *jus in bello*. They determine the ethical rules that states must follow during, respectively, the engaging phase and the fighting phase of a war.

Jus ad bellum is focused on avoiding the wage of useless wars, since their only consequence would be harming the citizens of the involved countries.
For example, it demands justifiable reasons to start a war. However, actions like pre-emption (i.e. striking in anticipation of an oncoming attack) and self-defence (evaluated as an "inherent right" by the Article 51 of the Charter) are admitted by the treaty.
Moreover, recalling Thomas Aquinas concepts, it doesn't consider "just" a war if the decision to fight was not taken by a duly constituted authority.
In addition, *jus ad bellum* allows war just as a "last resort" operation. This means that states have the duty to try all the possible non-violent ways (like sanctions or diplomatic actions) before engaging war.

On the other hand, *jus in bello* concerns the principles to follow in order to fight more ethically as possible when war is unavoidable.
For example, it demands non-combatant immunity: soldiers have to avoid harming whoever is not fighting against them, like civilians or surrendered enemy troops.
Moreover, an important concept of *jus in bello* is proportionality, meaning that states have the duty to try avoiding the deployment of excessive military forces.
Finally, it considers necessary for a war that wants to be considered "just" to cause more good than harm. It is a concept taken from the Thomist paradigm that requires calculations of the net good entailed by the use of particular forces.

Section 5: ethical issues raised by IW

The above-descripted principles about the ethical approach to war were considered effective and applicable for a lot of time.
However, the upheaval of the society caused by the Information Revolution has seriously challenged the rules defined in the XX century.
As a matter of fact, some characteristics of Information Warfare brought to light issues that were never questioned before.

The most relevant ethical issues arise because of the property of transversality that belongs to Information Warfare, which is the most important difference with respect to traditional war.

Transversality consists in the ability of a digital (so a non-physical) weapon to influence (and possibly disrupt) objects in the physical domain.

In this context, a delicate point concerns the establishment of the criteria needed to manage the heterogenous nature of combating agents, since they can both be artificial agents (like viruses, worms, drone and robots) or human agents. This poses two major issues: the first one regards the importance of managing in a correct way the interactions between the two types of agents, while the second one is focused on the ethical responsibility of the actions performed by them, considering their different nature and every consequence that derives from it.

It is important to consider also the transversality of the types of violence that follow from IW attacks, since it can range from non-violent actions, just aimed to disrupt the enemy's digital infrastructures (like DDoS attacks), to bloodthirsty strikes and physical damages. (Taddeo 2011)

Section 5.1: detailed issues about Jus ad bellum

Regarding the criteria required by the correct application of *Jus ad bellum*, the spread of IW puts some more under stress than others.

As a matter of fact, the need of a right purpose for waging war doesn't change from a conceptual point of view, but it just needs to be contextualized in the IW environment, i.e. in an approach to war where information weapons replace the traditional ones.

However, because of the possibility of interventions by non-state actors, the criterion that only a duly constituted authority has the right to start a war needs to be redesigned. Indeed, in some IW contexts non-state actors could even assume a key role, since they have the possibility of being employed by states in order to wage war with them or on their behalf. By the fact that the actions of non-state actors have a greater chance of maintaining deniability and ambiguity on their identity, the eventuality of strikes from weaker states to stronger ones is not excluded anymore as it was in classic war, being more difficult to be discovered and, for this reason, to suffer retaliation.

Finally, the concept of war exclusively as a last resort measure needs to be re-evaluated too. Since, concretely speaking, IW brings way less destruction and losses of lives than traditional war, it can be viewed in a similar manner of economic sanctions as a tool of intimidation. For its non-lethal characteristics, IW could even be considered different from an act of war, fading the concept of war as a last resort because of its less destructiveness. (Arquilla 1999)

Section 5.2: detailed issues about *Jus in bello*

Regarding *Jus in bello* criteria, non-combatant immunity gets seriously challenged by the upheaval caused by Information Warfare. Since the goal of IW is to damage the enemy's will to resist in a particular fight, the strategy of striking its transportation, power, communications and financial infrastructures is the most effective. This is in direct contrast to the principle of not targeting non-combatants due to their reduced lethality, also because in traditional war the action of targeting who is not fighting is considered an act of cowardice. In the same way, the precept of proportionality becomes difficult to follow in some contexts. Even though, generally speaking, the possibility to respond to a strike in an accurately calculated and calibrated way is present, two circumstances are particularly problematic. The first one concerns the condition in which an IW attacker strikes at an opponent's critical infrastructure, but there are not infrastructures of similar level on which the attacker could suffer a retaliation. This could encourage a more traditional counterattack like a bloodthirsty strike, violating in this way the concept of proportionality. Another example could be the case where the defender is not in possession of information weaponry with which can respond in a meaningful way, leading again to a lethal retaliation.

Finally, the criterion that requires to do more good than harm results quite difficult to put into practice. However, because of the above-mentioned characteristic of IW that makes it less destructive than classic war, this issue can be considered less problematic with respect to a traditional situation. (Arquilla 1999)

Section 6: Conclusions

The analysis of Information Warfare within the current legislative context makes easier to understand the thesis carried on from this paper. Indeed, even though the great law-making improvements of the XX century were able to make war less atrocious and bloodthirsty, the ethical approach to war is now questioned again. Since, due to the immense power of information weapons, a wrong or malicious employment of them could potentially cause a high level of material damage and losses of life, this issue results as a global priority, also because it involves everyone's safety. Undoubtedly anyone is considered in danger in a world that sees a growing spread in terms of information weapons, especially if there aren't enough rules regulating this kind of conflict.

As already displayed during the paper, it is not the first time that the world is shaken up by technological improvements and it won't probably be the last one. The challenge that the human species has to face consists in being able to take advantage of the latest technological advances, trying at the same time to attenuate as much as possible their side effects. This is, in my opinion, the best way to proceed towards the future, with all its possible challenges and obstacles.

Glossary

- Cyberspace: a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers;
- Cyber-attack: an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information;
- DDoS attack: a category of malicious cyber-attacks that hackers or cybercriminals employ in order to make an online service, network resource or host machine unavailable to its intended users on the Internet.

Bibliography

- Taddeo (2011). "Information Warfare, A Philosophical Perspective", Philosophy & Technology 25: 105-120 (2012), link.springer.com/article/10.1007/s13347-011-0040-9
- Arquilla (1999). "Can information warfare ever be just?", Ethics and Information Technology 1: 203–212 (1999), link.springer.com/article/10.1023/A:1010066528521
- Josiah Ober, "Classical Greek Times," in Michael Howard, Geo. Andreopoulos and Mark R. Shulman, eds., The Laws of War: Constraints on Warfare in the Western World (New Haven: Yale University Press, 1994), pp. 12–26
- https://finabel.org/the-use-of-military-drones-the-impact-on-land-forces-and-legal-implications/
- csrc.nist.gov/glossary/term/cyberspace
- csrc.nist.gov/glossary/term/Cyber_Attack
- www.checkpoint.com/cyber-hub/cyber-security/what-is-ddos/