http://dx.doi.org/10.5007/1677-2954.2014v13n1p27

JUSTICE IN CYBERWAR

JUSTIÇA NA GUERRA CIBERNÉTICA

KLAUS-GERD GIESEN[1]

(Université d'Auvergne, France)

ABSTRACT

The text aims at providing an ethical framework for cyber warfare. The latter is changing our understanding of war (and peace) as well as the relationship between the human being and the machine. Rejecting Heidegger's fatalistic stance towards technology it is argued that norms of international justice should be formulated in order to attempt to regulate this new military dimension. The potentially considerable destructive force of cyberweapon systems for civilian infrastructure is emphasized, especially as far as the "Internet of Things" (all physical objects connected to the Internet) is concerned. In a foreseeable future cyberwar operations may kill many civilians. After defining the concept of cyberwar and explainig why it is a new and important moral issue, the paper heavily relies on just war ethics in order to reach norms for justice in cyberwar. It is shown that Immanuel Kant has not just been a philosopher of (perpetual) peace, but (in the Metaphysics of Morals) also a just war theorist who developed his normative framework in a fruitful dialog with Aquinas (against Vitoria and Suarez). His norms for *jus ad bellum* and *jus in bello* are carefully and critically applied to cyberwar. However, Kant's major innovation in just war theory has been the concept of *jus post bellum*. The paper demonstrates how important this dimension of justice is in cyberwar, and how to apply it, including through recommendations for a treaty in international law.
Keywords: Cyberwar. International law. Internet. Justice. Kant. Peace.

I. Introduction

Over the last few years the world has obviously changed considerably. Among other things, new technology has deeply transformed our reality, our everyday life, our communications, and also the way war is waged. Smart phones, war drones, genetic therapy and cloning, and above all the spectacular rise of the Internet, to mention but a few, challenge our traditional views about justice and how to apply it to society.

Even more, the sudden appearance of new technologies has caused quite some confusion among people, which results in a moral crisis (for instance in bioethics or as far as the use of drones in military operations is concerned), and in a crisis of intelligibility. The new technologies explode, so to speak, our traditional categories of thinking, and the way we conceptualize the human being, communication between the humans, the relationship between humans and the machine as well as with the rest of the planet earth, the dichotomy war-peace.

Philosophy is precisely the main academic field in which urgently needed new conceptualizations may take place. For sure, we have to continue to study the "classical dead white men" for the sake of understanding them. However, it seems also highly interesting, and actually more challenging, to try to carefully use their writings in order to better understand the problems and issues induced by technology, to make sense of our new realities. And that is what will be attempted in this text.[2]

As far as justice related issues are concerned two fundamental stances about "dangerous" new technologies can be adopted: either a fatalistic one, or a "responsible" one. The first stance has been proposed, among others, by Martin Heidegger. In his *Letter on Humanism* to Jean Beaufret, published in 1949*,* Heidegger wrote the following obscure sentence: "Technology is by its nature a destiny - within the history of Being - the truth of Being as it rests in the oblivion." (Heidegger 1949: 32) Five years later, in *Die Frage nach der Technik* [*The Question of Technology*], he makes it more explicit: "The essence of modern technology is revealed in what we call the *Gestell* [frame]." (Heidegger 1954: 27) The *Gestell*, which is actually much wider a concept than simple technology, leads us to "the extreme edge of the abyss". (Heidegger 1954: 30) He declares: "The threat to the human being does not come first from machines and technical equipment [...]. The real threat has already reached the human being in its essence. The domination of the *Gestell* threats us by its ability to deny human access to a more original revelation and hence to a more original truth. And therefore, where there is *Gestell*, there is *danger*, in its strongest meaning. However, where there is danger, also rises what can save us. Let us carefully take into consideration the words of Hölderlin. [...] Thus, it has to be [...] the true essence of technology which contains in itself the rise of what will save." (Heidegger 1954: 32)

According to Heidegger, the rescue from the technological catastrophe can only be performed by non-philosophical thought (*Denken*) which gradually may discover the truth of Being, when the danger of technology is increasing. The bigger is the danger to mankind and the closer it comes to the abyss, the greater are also its chances of being rescued by the revelation of the truth of Being. Hence, we can see a sort of automatism in Heidegger's approach: technology, under the domination of *Gestell,* being more and more dangerous, will almost automatically bring us closer to the truth of Being, and therefore dictate our conduct in relation to it, provided that one pays attention to it, particularly through art and poetry.

In other words, the *Gestell* challenges us by the development of modern technology. However, we notice the challenge only if we pay full attention to the gradual arrival of the

truth of Being, beyond any ontology and any ethics. The technology will remain out of human control as long as mankind does not have access to the Being, and thus to the *Gestell* which "frames" technology. The progressive loss of control of technology is therefore programmed; for the time being it remains beyond the human will. We cannot reach - and therefore slow down or regulate - the development of technology and its dangers, until the truth of the mysterious truth of being is revealed to us, and thus explained to us what is actually the *Gestell*.

Martin Heidegger's approach is, politically and ethically speaking, demobilizing and leading to apathy, since philosophy, the social sciences and even politics can't contribute to "tame" technology. Only the arts and poetry can… once we are getting close enough to the abyss. It is, thus, sheer fatalism. Heidegger's former student Hans Jonas has opposed this stance in his book of 1979 *Das Prinzip Verantwortung [The Imperative of Responsibility]*, which carries the subtitle "An Ethic for the Technological Civilization". Jonas pleads for an active ethics of technology limiting its possibly negative consequences. Instead of just fatalistically waiting and doing nothing, until "something" saves us from Prometheus unchained, Jonas proposes a Kantian inspired categorical imperative which goes as follows: "Act in a way that the effects of your action are compatible with the permanence of genuine human life on earth." (Jonas 1979: 36) It's a future oriented, normative approach of technology leading to a theory of justice for future generations.

In this text the second stance is adopted. To let it just go (before "something" saves us) may ultimately lead either to the potential collapse of the biosphere (for instance through nuclear war, or genetics applied to humans, animals and plants), or at least to immense human suffering, even if there were an ultimate heroic creature or event which saved us from total disaster. In addition, intuitively I just lack the "faith" in the very possibility of such an event. Thus, let us better attempt to *regulate* the use of technology before it's too late. In each case the main question is: how far can we go? How can we use new technologies to improve our life conditions (alleviate poverty, raise comfort, reduce stress, etc.)? And what should be *absolutely* prohibited (nuclear war? human reproductive cloning? state surveillance of private space?)? If, technically speaking, anything goes, there should still be moral limits imposed by theories of justice, and possibly enshrined in legal norms.

In the following I would like to explore justice in a technological realm which has emerged very recently: cyberwar. And I would like to apply the theory of justice of one dead white man – Immanuel Kant – in order to modestly give some hints about how to *regulate* the rapidly developing cyber warfare.

II. Why is cyberwar an important moral issue?

The philosophy of war exists since Heraclitus. That is because the dichotomy of war and peace structures our lives. Almost all major philosophers have outlined a philosophy of war and peace, including the most recent: Lévinas, Rawls, Derrida, Habermas. They outline attempts to grasp the very nature of war and/or peace, as well as to define justice in relation to this domain.

I would like to argue that cyberwar is changing our understanding of what war (and peace) actually is, as well as the relationship between the human being and the machine. At the same time it introduces a completely new military dimension for which the philosophers have the duty to establish an ethical framework (in the Jonasian perspective), as it otherwise remains a state of nature in which the strongest actor rules without limitation.

Cyberwarfare is a new warfare domain; national and international norms have yet to be established. Globalization and the Internet have given individuals, organizations, and nations incredible new power, based on constantly developing networking technology. For everyone – ordinary citizen, scholars, soldiers, spies, propagandists, hackers, and terrorists – information gathering, communications, fund-raising, and public relations have been digitized and revolutionized.

We are now in the beginning of the Information Revolution. The computer is the new steam engine, so to speak. It dramatically facilitates the acquisition and validation of knowledge and information through the rise of the "cyberspace". Nowadays more than one billion computers are directly connected to the Internet, and there are over 1.5 billion Internet users on Earth. As a consequence, all political and military conflicts now have a cyber dimension, the size and impact of which are still difficult to grasp, and the battles fought in cyberspace can in the future be more important than events taking place in the physical world. In cyber conflict, the terrestrial distance between adversaries is almost irrelevant because everyone is a next-door neighbor in cyberspace: with optical fiber and satellite transmissions computer signals travel almost at the speed of light. The most powerful weapons are not based on physical strength, but logic and innovation. Cyber warfare is definitely unlike traditional warfare, but it shares some characteristics with the historical role of aerial bombardment, submarine warfare, and special operations forces. Specifically, it can inflict painful,

asymmetric damage on an adversary from a distance or by exploiting the element of surprise. (Geers 2011) And cyberwar is comparatively very cheap.

The interconnectivity of the Internet poses an enormous threat to civilian infrastructure. Indeed, most military networks rely on civilian, mainly commercial, computer infrastructure, such as undersea fiber optic cables, satellites, routers, or nodes; conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems relying on global positioning system (GPS) satellites, which are also used by the military. Thus, it is to a large extent impossible to differentiate between purely civilian and purely military computer infrastructure. This poses a serious challenge to the principle of distinction between military and civilian objects (see below). Interconnectivity means that the effects of an attack on a military target may not be confined to this target. Indeed, a cyber attack may have repercussions on various other systems, including civilian systems and networks, for instance by spreading malware (malicious software), such as viruses or worms, if these are uncontrollable (Droege 2012).

Therefore, because of its increasingly ubiquitous reliance on computer systems, civilian infrastructure is highly vulnerable to computer network attacks. In particular, a number of critical installations, such as power plants, nuclear plants, dams, water treatment and distribution systems, oil refineries, gas and oil pipelines, banking systems (including cash machines), stock exchanges and all the rest of the financial world, hospital systems, railroads, and air traffic control rely on information technology. These systems, which constitute the link between the digital and the physical worlds, are extremely vulnerable to outside interference by almost any attacker. That is what is labeled the *Internet of Things*, i.e. all objects directly connected to the Internet.

In May 2009, President Obama made a dramatic announcement: “Cyber intruders have probed our electrical grid ... in other countries, cyber attacks have plunged entire cities into darkness.” Investigative journalists subsequently concluded that these attacks took place in Brazil, affecting millions of civilians in the state of Espirito Santo in 2005 and in Rio de Janeiro in 2007, and that the source of the attacks is still unknown. (The White House – Office of the Press Secretary 2009). Richard Clarke, the former special adviser to President George W. Bush on cybersecurity said later : “Given the degree of seriousness that the Obama administration is applying to cybersecurity and the smart grid, we can look forward to the kind of things happening here that happened to Brazil, where hackers successfully brought down the power.” (Mylrea 2009) The claim has been dismissed by the Brazilian government. Whatever the truth may be, Brazil is still today one of the most cyber-attacked nations in the

world.

National security planners should consider that electricity has no substitute, and all other infrastructures, including computer networks, depend on it. The manipulation of electrical grid management systems is probably the greatest threat at present (Mele 2010). In addition, distribution networks for food, water, money, goods (supply chain management) and energy rely on IT at every stage, as do transportation, health care, and financial services. Potentially catastrophic scenarios, such as collisions between aircrafts, the release of radiation from nuclear plants, the release of toxic chemicals from chemical plants, or the disruption of vital infrastructure and services such as electricity or water networks, cannot be discarded.

In 2010, the Stuxnet computer worm, likely an American-Israeli joint venture, accomplished what five years of United Nations Security Council resolutions could not: disrupt Iran's pursuit of a nuclear bomb. A half-megabyte of computer code quietly substituted for air strikes by the Israeli Air Force. Moreover, Stuxnet may have been more effective than a conventional military attack and may have avoided a major international crisis over (human) collateral damage. To some degree, the vulnerability – even without any direct connection to the Internet! - to such spectacular attacks will provide a strong temptation for nation-states to take advantage of computer hacking's perceived high return-on-investment.

Military forces are, of course, no exception. IT is used to manage military forces – for example, especially for command and control and for logistics. Already today it is technically feasible that a foreign state takes fully or partly control of its enemy's army IT infrastructure and manipulates it in order to fire weapons, such as missiles, including nuclear devices, at its *own* cities and population.

All things considered, the current balance of cyber power favors the attacker. This stands in contrast to our historical understanding of warfare, in which the defender has traditionally enjoyed a home field advantage. Therefore, many governments may conclude that, for the foreseeable future, the best cyber defense is a good offense.

Today cyber attacks can target political leadership, military systems, and average citizens anywhere in the world, during peacetime or war, in many cases with the added benefit of attacker anonymity. In addition, the rapid proliferation of Internet technologies, including hacker tools and tactics, makes it impossible for any organization, including national armies, to be familiar with all of them. Frequent software updates and network reconfiguration change the Internet geography unpredictably and without warning. Cyber

attacks are more flexible than any other weapon system the world has ever seen. They can be used for propaganda, espionage, and the destruction of critical infrastructure as well as of large populations. For the time being, there are few moral inhibitions to cyber warfare because it relates primarily to the use and exploitation of information in the form of computer code and data packets; so far, there is little perceived human suffering. (Geers 2011). But that may change rather soon.

III. How to conceptualize cyberwar?

From the (Jonasian) ethical viewpoint it is important to differentiate between an act of cyberwar and an act which may be wrong, but does not fall under the category of war. Unlike many other authors (Einzinger, 2011; Micewski, 2011) it seems appropriate to plead for a rather restrictive definition in order not to overload the concept.[1] One of the problems lies in the fact that intrusions on the national territory are not done by soldiers or objects (tanks, aircrafts, etc.). In this respect, some misconceptions should be put into perspective.

Cyberwar as such can only take place directly between two or more states. However, contrary to what believes Sean Watts (2012), strict state affiliation should not be the sole criterion for combatant status, that is the otherwise restrictive definition should also include non-state actors which are subordinated to the will of a state, as for instance non-governmental groups of so-called 'patriotic hackers' in Russia, China, Israel and elsewhere, which work closely together with the national armies and which are actually controlled by them (Ventre, 2011). As Michael Schmitt emphasizes, the existing international law provides some interesting analogies to be applied (the Tadić case of the International Criminal for the Former Yugoslavia, the Iranian hostage crisis in 1979, the Hezbollah case in 2066, etc.) (Schmitt, 2011, p.579). The definition excludes also non-state territorial units, such as the Turkish Republic of Northern Cyprus, Palestine, Transnistria.

Unlike Marie Stella (2003), it seems that the principle of territoriality, as an essential attribute of sovereignty, should be an integral part of the definition, despite the fact that, due to the decentralized nature of the Internet, any malware can actually cross many borders within a fraction of a second before finding its target (Hare 2009). What matters here are the *effects* of any cyberattack on a national territory.

The principle of *armed* aggression required to justify any entry into war (art. 51 of the UN Charter) should be maintained, except that the meaning of what can legitimately be

[1] Section 2 partially stems from Giesen 2013.

considered as a weapon must evolve. A targeted, powerful and destructive computer worm can perfectly match the definition of a weapon (Delbasis 2009: 97). Here again, it all depends on the effect. After all, a plane can also be used to transport food or to bomb cities. Cyberwar requires information technologies to be used for destructive purposes.

The specialized literature celebrates the resurgence of asymmetric warfare in cyberspace (Schröfl 2011): facing a state with a powerful cyberarmy, such as the United States, Israel, China or Russia, all other countries may have, to different degrees, some offensive or defensive cybercapacities and may be tempted to harass them. However, the balance of power leaves for the moment no doubt about the outcome of such an asymmetric conflict. It must nevertheless be admitted that neither total victory nor total defeat are likely in cyberspace.

One of the peculiarities of cyberwarfare is the possibility of a *sub rosa* conflict. In this case neither the attacker nor even the defender wishes to make public, including in the eyes of their own people, the existence of a cyberclash – either in order not to lose face in the event of defeat (for the attacked state), or out for fear of the international public opinion (for the aggressor state), or (for both) to avoid an escalating conflict by a spillover effect on other military spheres (conventional or nuclear warfare), or to avoid the panic of populations (Libicki 2009: 128-129). The *sub rosa* conflict poses the dilemma of democratic legitimacy of any major military decision versus technocratic efficiency by experts. It is clear that from the standpoint of international justice the greatest possible transparency must be required. Thereby, waging a *sub rosa* cyberwar should at least be discussed and authorized behind closed doors by the relevant parliamentary defense committees.

Following these prerequisites one can quickly dismiss:

• *Cybercrime*, even by non-state groups, such as the Russian mafia. The Council of Europe is the only international organization to have regulated cybercrime activities.

• *Cyberpropaganda* and *hacktivism*, even if they may include DDoS attacks against government websites.

• A one-time *cybersabotage* by a state: the Stuxnet virus remains thus significantly below the threshold which reasonably defines cyberwar.

• *Cyberespionage*: As a matter of fact, espionage through new technologies is as old as the relations between states. The hacking of government computers, or implants such as the Flame worm, or the theft of data, do not make any exception.

• *Cyberterrorism* and *cyberguerrilla* are the result of non-state groups against one or several states (some scholars believe that the attack on October, 21 2002 against the internet domain name root servers has been perpetuated by Al-Qaeda), and fall therefore not within the category of interstate conflict.

Thus, the dividing lines between different malicious activities taking place on the Internet are actually not so blurred.

IV. Towards a Kantian Theory of Just Cyberwar

We now can turn to the question of the proper basis for an *ethical* approach which could deal with the issue of cyberwar. My preference goes to the just war theory, which historically stems from natural law, precisely because it is an old theory (from Cicero to Walzer). Gradually, over the centuries, the just war theory was able to adapt to all technological revolutions. For instance, Vitoria introduced in the 16th century the important distinction between combatants and civilians, with the concomitant notion of collateral damage, as a result of the emergence of artillery technology on the battlefields. Or in the 1940s and 1950s, John Ford, Paul Ramsey and James Turner Johnson, among others, discussed the highly relevant question if a defensive nuclear war can be just. Just war theory is thus very flexible - almost a casuistry - and adaptable to new technologies of warfare (Giesen 1992: 123-150, 267-277).

However, the classical just war theory will be amended here by reference to Immanuel Kant, in the sense that it seems logical to add to the traditional *jus ad bellum* and *jus in bello* a Kantian *jus post bellum* (Kant 1797: §§58-60). As I have tried to demonstrate elsewhere (Giesen 1997), Immanuel Kant was himself not only a philosopher of peace, renown for his seminal writing on *Perpetual Peace*, but also a philosopher of war who, in the *Metaphysics of Morals*, developed a theory of just war, except that his ultimate philosophical foundation is provided by the subject and not by a metaphysical natural order (as in natural law).

As already in *Perpetual Peace*, but contrary to what he had noticed a few years earlier in his *Idee zu einer Geschichte in allgemeinen weltbürgerlicher Absicht*, Kant states in the *Doctrine of Law* that ultimately "perpetual peace […] is obviously an impossible idea" (Kant 1797: §61), especially because the gradual extension of the *foedus pacificum* to the entire surface of the earth would lead to a (world) government failing to control the situation and, thus, to many civil wars. The problem of the moral status of war remains, therefore, unsolved, since it concerns the conflicting relations of states that are historically still outside the

republican *foedus pacificum*, and of the republican states with one or more non-republican states. Paragraphs 56 to 60 of the *Doctrine of Law* are devoted to define the criteria for determining the justice or injustice of any empirically given war.

From the outset, Kant distinguishes the doctrine of just war from its predecessors. Firstly by the structure of his argument: to the traditional *jus ad bellum* (§§ 56 and 57) and *jus in bello* (§ 57) he adds a surprising *jus post bellum* (§§ 58 and 60). And also by the content of the criteria developed. Here Kant goes back to the criteria used by Aquinas. Indeed, the four Thomistic *jus ad bellum* criteria are found, albeit grouped in a different order than in the *Summa Theologica*, in §§ 56 and 57: 1. The purpose of war is a more perfect peace (Thomas d'Aquin 1985: t.3, II-II, q29, art.2, p. 219) (in the words of Kant's §57: "... conduct war according to the principles that it is still possible to leave the state of nature of states [...] and to enter into a legal state"). 2. The formal declaration of war must be declared by the competent authority (Kant 1797: §55; Thomas d'Aquin: 280). 3. The war must have a just cause, i.e. "it is required that the attack on the enemy is due to some fault" (Thomas d'Aquin: 280) (Kant 1797: §56 specifies that it must be either following a first assault, or a threat, or an offense); 4. "The right intention by those who make war" (Thomas d'Aquin: 280): for Kant this precept refers to a formal prohibition of punitive wars and wars of extermination which may lead the prince to go to war for "impure" reasons (Kant 1797: §56). In Aquinas, as much as in Kant, the other three criteria of the usual catalog of jus ad bellum are missing; they had been added in between the two authors by Vitoria and Suarez, namely: 1. War must be the last resort to resolve a dispute; 2. There must be a reasonable prospect of success before declaring war; 3. There must be some proportionality in the relation of misconduct and punishment.[2]

I will now go through all seven *jus ad bellum* criteria (thus including the three Kant did not include) and try to apply them to cyberwar. The catalog is cumulative, which means that all *adopted* criteria must be met if a given cyberwar is to be considered as a just war.

V: Jus ad bellum

The ultimate aim of war: a more perfect peace (than before the war)[3]

This first criterion is difficult to fulfill, simply because cyberwars tend not to stop, that is to continue almost endlessly, interspersed with more or less long intermissions, possibly at

[2] On these missing criteria: Phillips 1984: 12-134.

[3] Several parts of section V have previously been published in Giesen 2013.

the *sub rosa* level. However, a war can be just only if he there is an end to it and if the plans for the post-war order correct some deficiencies properly identified prior to the conflict. This means that such a cyberwar can only be a response to a kinetic aggression or a cyberassault from another state, and only in the case when it is designed to eradicate the harmful potential of the opponent.

The authority of the prince: the declaration of war

Here we are faced with two challenges: time and attribution. Due to the high speed of cyberwar flows, the formal diplomatic declaration of war must be reduced to the minimum, that is to a computer signal sent a few moments before replying to the aggression, by analogy with the warning shot by an individual in an emergency situation.

On the other hand, the problem of attribution lies in the fact that in cyberspace it is highly problematic to identify with certainty the attacker, particularly because of the possible presence of other actors in the virtual battlefield (Wheeler/Larsen 2007), and also because of the likely use of botnets (third-party servers), as it was the case during the attack against Estonia with the diversion of at least one million computers. While absolute certainty is never possible in cyberspace, we can, however, *morally* require a very high probability of 99%. In other words: a probabilistic approach should prevail.

This criterion automatically excludes hackers and private contractors which are not submitted to state authority (for instance by sub-contracting), the *wannabe* states such as Puntland and Abkhazia, the cyberguerrilleros, as well as terrorist groups, unless they are protected by a state which has knowledge of their actions and does not intervene. Here comes into the picture the analogy with the invasion in November 2001 of Afghanistan by the United States and its allies: the Taliban were not aware of the preparation of the September 11 attacks, but subsequently refused to expel Al Qaeda from Afghanistan. Thus, a state which refuses to take action against aggressive non-state actors on its territory may itself become the legitimate target of a cyberresponse by the assaulted state, because it bears indirect responsibility (Tikk 2008: 22).

A just cause

Beyond self-defense against an armed attack (an ethical principle which is legally enshrined in Art. 51 of the UN Charter), which applies *a fortiori* in case of an attack by real-world objects (assuming a first response by cyberweapons against, for example, the occupation of part of the national territory), two other ethically acceptable scenarios seem to

be possible: a humanitarian intervention (to be duly authorized by the UN Security Council), and a preemptive strike in case of a very serious threat from abroad which potentially endangers the survival of a country. In a not too far future the analogy is with Michael Walzer's concept of supreme emergency applied to the Israeli-Arab war which started on 5 June 1967 by a preemptive strike (Walzer 1977: chapter 16).

A right intention

One has to admit that his problem cannot be addressed correctly from a philosophical perspective, because especially in cyberspace any given actor can easily disguise his evil intentions, partly because some actions are not immediately visible to everyone. As a result, we must insist on the greatest possible transparency, and remain attentive to the testimony of outside observers (NGO watchdogs, neutral states, etc.).

The proportionality of fault and punishment

Kant dismissed the criteria, because he wrote his piece at the beginning of the era of mass warfare through the introduction of general conscription (Giesen 1997). However, since cyberwar is exactly the opposite of mass warfare, the criteria will be kept here. It's actually the question of the threshold at which a cyber-response may start. Obviously, a simple DDoS is not enough. It is necessary that the cyberaggression causes human victims (through the Internet of Things) - for example from nuclear radiation or harmful emissions of chemical plants, or through malfunctions in hospitals – or targets *vital* key interests of the state (distribution of electricity and water, stock markets and financial systems, conventional or nuclear defense, social security, aviation system, etc.). In order to reach higher precision – which is not within the scope of this paper – it is very helpful to use the so-called "Schmitt analysis" in law, in which a qualitative one-to-ten scale is applied to seven criteria (Schmitt 1999; Michael 2003: 2; Wingfield 2004: 11-12).

The great advantage of cyberweapons lies in the precision with which the counterattack can be designed at different levels and in various fields (the opposite of mass warfare). Furthermore, since a pure cyberwar - without the involvement of other national armed forces - is rather unlikely above a certain level of aggression, the counterattack can also be made by using the multiplier effect from a close coordination between the cyberarmy and land, air and naval forces. In other words, a gradual build-up of war intensity is quite feasible

through the phasing of the cyberattack with more traditional means of war (Sharma 2010: 63-67).

War as last resort

Immanuel Kant did not adopt this traditional *jus ad bellum* criteria, probably because he found it hypocrite. In cyberwar it doesn't make sense neither. Indeed, after a cyberattack there is insufficient time for real diplomatic negotiations in due form. The moral minimum is, however, to ensure that the aggression did not happen by accident, for example by inadvertently spreading a virus that the attacker himself did not notice. It is therefore necessary to carry out double checks. A first step in this direction was taken in 2011 with the installation, as in the good old days of the Cold War, of a hotline between Washington and Moscow to rule out any 'cyber-misunderstanding'.

A reasonable hope of success

This last criteria was also dismissed by Kant, since it requires a considerable capacity of foresight analysis. In cyberwar the temptation to conduct an asymmetric war - that is to say, a low-level and low frequency harassment - remains strong for weak states vis-à-vis one of the few cyberpowers. Here we can find a compromise between Kant and the late just war theorists: even if all other six criteria of the *jus ad bellum* are met, it requires the abandonment of any response if there is a high risk of failure, or of an even stronger counter-response with negative effects for the civilian population; or if it may contribute to an escalation involving superior kinetic forces of the enemy. Thus, even in cyberspace a minimum symmetry of forces is required. Thus, even if cyberattacked by, say, China, Vietnam has no interest whatsoever to reply. The same applies, for the time being, to Saudi Arabia against Israel. It is the precautionary principle: in these cases it rather seems morally required to bring the case before international organizations, such as the UN Security Council, and/or to ask for assistance and/or protection by a cyberpower.

VI. Jus in bello

In the *Metaphysics of Morals*, Immanuel Kant seems to go back to Aquinas, i.e. to the days before Francisco de Vitoria, to formulate the *jus in bello*. First, he develops in §57 the Thomistic notion of permissive and non-permissive tricks: spies, ambush assassins, poisoners, snipers and rumors are explicitly classified as illegal means, because they destroy the trust

necessary for the development of a future (perpetual) peace (Thomas d'Aquin: 282-283). Second, there is a (weak) criteria of proportionality in the *jus in bello* that states - just as in Aquinas - that looting is prohibited.

However, the major issue in this parallel between Kant and Aquinas lies in the "missing" element of the *jus in bello*: the discrimination between combatants and non-combatants, as well as the concomitant notion of collateral damage. Kant makes no mention of this criterion introduced by Vitoria, which underpins the assumption that he adopts a more traditional doctrine.

The absence of the criterion of discrimination between combatants and noncombatants and collateral damage clearly tells us that Kant had detected something in this concept which he deems inappropriate. Francisco de Vitoria introduced the new criterion in *De Indis*: "By accident, it is sometimes permissible to kill innocent people, even voluntarily, for example when you justly attack a fortress or a city, in which we know that there are many innocent people [...]?" (Vitoria: 140) The reason for the introduction lies in the technical change that occurred in the art of war between Aquinas and Vitoria: "...and when you can use war machines, sending projectiles or burn buildings without also hitting the innocent along with the guilty". (Vitoria: 140) He refers to the massive introduction of artillery on the battlefields of Asia Minor in the 14th and 15th centuries, particularly during the fall of Constantinople in 1453 by Mohammed II. This technology adds a new dimension to weapon systems since it requires the distancing of the hostile combatants from each other, and the absolute anonymity of the opponent, and since it has the inevitable effect of possibly reaching a large number of non-combatants. (Johnson 1981: 175-176) Hence the need felt by Vitoria to clearly distinguish between combatants and non-combatants, while allowing to kill the latter by accident only (collateral damage).

In the *Doctrine of Law*, Kant makes no mention of this important criterion. Our hypothesis is that it does not see the relevance of making such a discrimination, because of a discontinuity in the art of war which he himself witnessed. Indeed, Immanuel Kant has been contemporary to the massification of war. He observes that revolutionary France, as well as in Prussia in the late 18th century, the general mobilization of the population for military purposes has been established. (Corvisier 1995: 162-163) Thus, the philosopher of Königsberg understands that the nature of warfare has changed: it now embraces the entire social sphere. He draws - this is my hypothesis – an important conclusion: why keeping the

criterion of discrimination between combatants and non-combatants of the *jus in bello*, if the entire society is now involved, in one way or the other, in the war effort?

It seems that his silence on this traditionally significant criterion for Vitoria - and therefore his return to the Thomistic doctrine - can be interpreted as if Kant wanted to cancel the discrimination between combatants and non-combatants. Mass warfare makes such a differentiation impractical.

The three mentioned criteria will now be analyzed one after the other[4]:

The authorization of ruses

This is about deceiving the enemy by false appearances. It is already mentioned by Aquinas in his *Summa Theologica*. One could imagine that in order to deter its enemy a state makes in a counter-attack somehow believe that it has far reaching cybernetic abilities, which is not true. Such a behavior seems morally permissible as much as cyberpropaganda in times of cyberwarfare, for example by diverting media aggressor websites for spreading false information, or even cyberespionage.

The proportionality of means

In this context an approach by successive levels is needed. It is important to first define them in a coherent doctrine. For instance, a cyberattack that causes hundreds of deaths by dysfunctioning the civil aviation systems should, of course, cause a less severe response than several nuclear explosions with important radiation effects on a large scale, requiring the evacuation of part of the territory for many years. This criterion is therefore in its structure almost utilitarian: a true calculation of consequences is essential.

The discrimination between combatants and non-combatants

It is even more difficult to operate this distinction in cyberspace than in the conventional battlefield. Fortunately, Vitoria gave us the mentioned casuistic concept *par excellence* : the collateral damage, which is allowed if it is not directly intentioned. This means that the cyberforce general who supervises a response and perfectly knows that it will also affect civilian populations is morally 'clean' if his action is first and foremost aimed at a

[4] The remaining parts of sections VI and VII are revised and considerably enlarged versions of what has been sketched out in Giesen 2103.

military target, such as adverse computer servers or conventional military facilities (for example the communication systems between adverse army units).

This means that "only weaponry (cyber or kinetic) capable of discrimination (i.e., directed against legitimate targets) can be used: However, cyberstrategists should know that legitimate targets can include civilian objects – especially those having cyber aspects – that have dual military and civilian use" (Dunlap 2011: 89). The ethics of just war require both that targeteers 'do everything possible' to ensure the target is a proper military objective. In practice that seems - *for the time being* – technically not be possible. Thus, the Kantian reservation vis-à-vis the concept of collateral damage is – *for the time being* – perfectly acceptable.

VII. Jus post bellum

Just war *ethics* does not need to determine if the ethical norms should be implemented by codified legal norms or by the development of existing provisions of the law of armed conflict, as long as they *can* be implemented correctly. Therefore, new legal agreements are, ethically speaking, not compulsory. The vast legal literature over the last years has shown that *jus ad bellum* and *jus in bello* norms can be applied to the law of armed cyberconflict by drawing legal analogies from the UN Charter and from existing customary law.

However, it seems necessary to amend the traditional just war theory, which is limited to *jus in bello* and *jus ad bellum*, by adding the Kantian *jus post bellum*. And it will be demonstrated that the ethical *jus post bellum* norms must be implemented through a new international treaty.

As far as I know, nobody has yet tempted to adapt the Kantian *jus post bellum* to cyberwar. Most authors using the just war theory either do it in law (Denning 2007; Roscini 2010, Dipert 2010) and/or entirely ignore the Kantian *jus post bellum*. The very few authors who deal with it (DiMeglio 2005; Ohrend 2000; Ohrend 2005) actually get mixed up with two *jus ad bellum* provisions (the ultimate aim of war, and the proportionality of fault and punishment) which they mistakenly take for *jus post bellum* norms. They are exclusively concerned by the way war is terminated and how the transition from war to peace is to be organized. Some even write mistakenly that "although he recognized the need to identify and discuss *jus post bellum*, Kant did not specify criteria for the category" (DiMeglio 2005: 133). Kant was not concerned with war termination or the transition from war to peace, except as

prospective *jus ad bellum* provisions. Otherwise it was not his problem as a philosopher. His concern was rather on a more abstract level about the consequences of a particular war act for *all* or most countries of the international system of his time. We can draw two criteria:

Firstly, Kant is very much concerned by the "violation of [international] public agreements, which presumably are of interest to all peoples, since their freedom is threatened" (Kant 1797: §60). Applied to cyberspace this disposition can be interpreted in the following way: the 'bombing' and decommissioning of all thirteen root servers, meaning the implosion of the entire internet for at least some time, constitutes a breach of the agreement that connects all nations of the world to ICANN. Although the latter is formally a private firm in California, its role is to ensure the free movement of data through the constant and real-time update of the single global registry of domain names. The implosion of the internet (including the web and email), even for only a few days, would cause such economic and social damage, that it seems justified to morally ban it.

Secondly, Kant provides us with a second *jus post bellum* norm: an unjust enemy is "one whose publicly expressed will [...] reflects a maxim according to which, if it were a universal rule, no peace is possible between peoples, while on the contrary the state of nature becomes eternal" (Kant 1797: §60). Here we recognize easily one form of the categorical imperative.

Such a return to the (political) state of nature seems possible in one case scenario: a malware which destroys in a very short time and permanently all or most artifacts connected to cyberspace: computers, mobile phones, tablets, servers, satellite systems, GPS, TV, digital radio, etc. with unimaginable consequences on the global economy, the relations between states, and the internal cohesion of societies. For sure, in Malawi or Kiribati the consequences would be relatively minor, but most developed states would experience shocks on an unprecedented scale, so that at least for a while no stable peace would be possible, and a return to a sort of state of nature would appear as inevitable. Our societies have become just too dependent on cyberspace.

The two Kantian *jus post bellum* criteria of §60 of the *Metaphysics of Morals* may raise concern about a sort of virtual Armageddon in which the existing electromagnetic spectrum is used to destroy many parts of the cyberspace as such and many objects linked to the Internet of Things. Despite the fact that both are artifacts they can nowadays be labeled as *global commons*. At least the most developed and emerging countries of the world heavily rely on them each single minute. The cyberspace and the Internet of Things have actually become the center of gravity for the globalized world (Schreier 2012: 13). By analogy with

the biosphere one may call it the infosphere, and it almost total informational entropy can morally be considered to be the ultimate evil in cyberconflict (Taddeo 2011).

It is the common duty of all nations to prevent and to outlaw any actor who may try to interrupt the peaceful flow of data in the international system and to bring the world back to a pre-cyber age. Especially the vulnerable developed countries should fear such a debilitation equally. Unfortunately, it cannot be totally ruled out that a rogue state – such as North Korea – launches one day an attack against the entire cyberspace and/or the Internet of Things. In addition, transnational actors – such as jihadist groups – may acquire sufficient technical competence to destroy at least part of the Internet. We don't know what will be technically possible in, say, ten years.

Therefore, it seems of outmost ethical importance to demonstrate a common, universal (or almost universal) consensus on these issues. Experts of international law should be mandated, if possible by the UN Security Council, to find law provisions which clearly outlaw any attempt to destroy the cyberspace and the Internet of Things. Possibly they could qualify it even as a crime against humanity, because it targets one of the global commons as such. Any international treaty may be fostered against the will of the United States of America which are reluctant because America has the most advanced cyberwar capability and any new agreement or norm would likely oblige it "to accept deep constraints on its use of cyber weapons and techniques" (Gjelten 2010).

VIII. Conclusion

In the foregoing it has been attempted to superficially clear the ground. All the different just war criteria deserve considerably deeper discussion. It was important to clarify several provisions, especially of the *jus ad bellum*, as some of them are frequently mixed up with the Kantian *jus post bellum*.

The main conclusions are: 1. The Kantian *jus post bellum* has by far not attracted enough attention as far as cyberwar is concerned; 2. While the Kantian *jus ad bellum* and *jus in bello* can be implemented by adopting and developing the existing UN Charter and customary law, this seems not to be possible for the *jus post bellum*. Here an international treaty is needed, for the simple reason that any other legal solution may only arrive when it is already much too late. It is morally required to implement as soon as possible an universal

treaty banning once for all any attempt to destroy entire parts of the cyberspace and of the Internet of Things.

Notes:

[1] Université d'Auvergne, Clermont-Ferrand, France. E-mail: klaus@giesen.fr

[2] The text is the revised version of the opening lecture of the 6th International Symposium on Justice which took place in Porto Alegre, Brazil, in August 2013. Its oral character was preserved as much as possible. I would like to thank the organizers and participants for their helpful comments and questions.

References:

Corvisier, A. 1995. *La guerre. Essais historiques*, Paris: Presses Universitaires de France.

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

Delbasis, D. 2009. "Information Warfare Concept of Operations Within The Individual Self-Defense". In: *Cyber Conflict and Global Politics,* edited by Karatzgianni, A. Abingdon, Routledge.

Denning, D. 2007. "The Ethics of Cyber Conflict", *Draft of March* 27.

DiMeglio, R. 2005. "The Evolution of the Just War Tradition: Defining Jus Post Bellum". *Military Law Review*, 186: 116-163.

Dipert, R. 2010. "The Ethics of Cyberwarfare". *Journal of Military Ethics*, 9(4): 384-410.

Droege C. 2012. "Get Off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians" *International Review of the Red Cross*, 94(866): 515-531.

Einzinger, K. 2011. "Cyber Warfare 2.0 – The Undertow of the Internet". In: *Hybrid and Cyber War as Consequences of the Asymmetry,* edited by Schröfl J. et al. Frankfurt, Peter Lang.

Geers, K. 2011. *Strategic Cyber Secuity*, Tallinn, CCD COE Publications.

Giesen, K.-G. 1992. *L'éthique des relations internationales*, Brussels, Bruylant.

Giesen, K.-G. 1997 "Kant et la guerre de masse". In: Union scientifique franco-hellénique (ed.), *Droit et vertu chez Kant*, Athens, Société hellénique d'études philosophiques, 331-341.

Giesen, K.-G. 2013. "Towards a Theory of Just Cyberwar." *Journal of Information Warfare*, 12(1): 22-31.

Gjelten, T. 2010. Shadow Wars: Debating Cyber 'Disarmament'. *World Affairs*, November/December, (http:www.worldaffairsjournal.org/article/shadow-wars-debating-cyber-disarmament).

Hare, F. 2009. "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cybersecurity?". In: *The Virtual Battlefield: Perspectives on Cyber Warfare*, *edited by* Czossek, C., Geers, K., Amsterdam, IOS Press, 88-105.

Heidegger, M. 1949. *Über den Humanismus*, Frankfurt: Klostermann [2000].

Heidegger, M. 1954. "Die Frage nach der Technik". In: *Vorträge und Aufsätze*, Stuttgart: Verlag Günther Neske.

Johnson, J.T. 1981. *Just War and the Restreint of War. A Moral and Historical Inquiry*, Princeton: Princeton University Press, 1981.

Jonas, H. 1979. *Das Prinzip Verantwortung. Versuch einer Ethik für die technologische Zivilisation*, Frankfurt: Suhrkamp, 1979.

Kant, I. 1797. *Metaphysik der Sitten*, Berlin, Akademie-Ausgabe.

Libicki, M. 2009. *Cyberdeterrence and Cyberwar*, Santa Monica, RAND.

Lin, H. 2012. "Cyberconflict and International Humanitarian Law". *International Review of the Red Cross*, 94(866): 515-531.

Mele, S. 2010. Cyber warfare and its damaging effects on citizens, September 2010. (http://www.stefanomele.it/public/documenti/185DOC-937.pdf)

Micewski, E. 2011, Cyber Warfare and Strategic Cultures – Information Technology and the Human Factor. In: *Hybrid and Cyber War as Consequences of the Asymmetry,* edited by Schröfl J. et al. Frankfurt, Peter Lang.

Michael, J. et al. 2003. Measured Responses to Cyber Attacks Using Schmitt Analysis: A Case Study of Attack Scenarios for a Software-Intensive System. In: *Proceedings Twenty-seventh Annual International Computer Software and Applications Conference*, Dallas.

Mylrea, M. 2009. Brazil's Next Battlefield: Cyberspace. *Foreign Policy Journal*, 15 (November),(www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/).

Orend, B. 2000. *War and International Justice: A Kantian Perspective.* Waterloo, Wilfried Laurier University Press.

Orend, B. 2005. "War Effective Justice". *Ethics & International Affairs*, **16**(1): 43-56.

Philipps, R. 1984. *War and Justice*. Norman: University of Oklahoma Press.

Roscini, M. 2010. "World Wide Warfare – Jus ad Bellum and the Use of Cyberforce". *Max Planck Yearbook of United Nations Law*, **14**: 85-130.

Schmitt, M. 1999. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, USAF Academy, Institute of Information Technology.

Schmitt, M. 2011. "Cyber Operations and the Jus ad Bellum Revisited". *Villanova Law Review*. **56**(3): 568-605.

Schreier, F. 2012. *On Cyberwarfare*. Geneva, DCAF Horizon 2015 Working Paper No. 7. file:///D:/Meus%20documentos/Downloads/OnCyberwarfare-Schreier.pdf

Schröfl J. et al. 2011. *Hybrid and Cyber War as Consequences of the Asymmetry*. Frankfurt, Peter Lang.

Sharma, A. 2010. "Cyber Wars: A Paradigm Shift from Means to Ends". *Strategic Analysis*, 34(1): 63-67.

Stella, M. 2003. "La menace déterritorialisée et désétatisée: le cyberconflit". *Revue internationale et stratégique*, 49: 165-171.

Taddeo, M. 2011. "Information Warfare: A Philosophical Analysis". *Philosophy and Technology*, 25(1): 105-120.

The White House – Office of the Press Secretary, Remarks By the President On Securing Our Nation's Cyber Infrastructure, May 29, 2009 (www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure)

Thomas d'Aquin. 1985. *Somme théologique*. Paris: Le Cerf.

Tikk, E., Kaska, K. Rünnimeri, Kerti, M., Talihärm, A., and Vihul, L. 2008. *Cyber Attacks Against Georgia: Legal Lessons Identified*, Tallinn, CCDCOE.

Ventre, D. 2011. *Cyberespace et acteurs du cyberconflit*, Paris, Hermes.

Vitoria, F. 1966. *De Indis* [1532], Genève: Droz, 1966.

Walzer, M. 1977. *Just and Unjust Wars*. New York: Basic Books.

Watts, S. (2012) "The Notion of Combatancy in Cyber Warfare". In *4th International Conference on Cyber Conflict*, edited by Czossek, C., Ottis, R., Ziolkowski, K., Tallinn, CCD COE Publications.

Wheeler, D. and Larsen, N. 2007. *Techniques for Cyber Attack Attribution*. Alexandria, Institute for Defense Analysis.

Wingfield, T. et al. 2004. *An Introduction to Legal Aspects of Operations in Cyberspace*. Monterey, Naval Postgraduate School.

Recebido / Received: 02/05/2014
Aprovado / Approved: 12/06/2014