**Kaja Kowalczewska**

# Computer network operations in the light of "Ius in bello"

Kultura Bezpieczeństwa. Nauka-Praktyka-Refleksje nr 15, 135-142

2014

**Kaja Kowalczewska**
Jagiellonian University

# COMPUTER NETWORK OPERATIONS IN THE LIGHT OF *IUS IN BELLO*

**ABSTRACT**
The paper deals with the legal definition of attack under international humanitarian law, analysed in the context of cyber "attacks". The armed nature of cyber operation is distinguished from a violent one and therefore special section is devoted to the indirect consequences of cyber attacks. It is also noted that the incremental resort to automated weapon systems, controlled by computer networks still highly vulnerable to hostile malware and interference, challenges the current state of law. Finally, the author attempts to render the linkage between law and IT, both greatly concerned with cyber security.

**KEYWORDS**
cyber attack, warfare, international humanitarian law, distinction

## Introduction

Cyberwar is no longer just a concept stemming from science fiction novels, on the contrary, the cyber threat wording has for good anchored itself in the language of leaders and policymakers, uttering their fears concerning its impact on the collective security system. The issue of cyber security has raised numerous discussions among security experts but also international lawyers concerned with applicable legal framework and practical troubles resulting from intangibility and anonymity of cyber wrongdoer.

Along with the development of the Internet, it was raised that cyberspace would serve for a new battlefield, ordinary hackers would turn into soldiers and hostile attacks would become non-lethal... Modern armed conflicts have acquired not only the asymmetric nature (when one of the parties military capacity exceeds the opponent's in such a way that from the very beginning of hostilities, it is known that the opponent has virtually no chance of balanced fighting and thus, winning) but also they have become widely robotised[1]. Consequently, the emergence of new, mainly anti-terrorist, measures, means and methods of warfare is shifting the conventional warfare to the second plan.

The end of World War II brought the international community commitment to reduce the use of force to the necessary minimum, otherwise to maintain an essential balance between military necessity and humanity in the conduct of hostilities. Minimizing the suffering of civilians and combatants is still central to international humanitarian law governing armed conflicts, therefore an extensive research on the development of the combat robots, replacing human soldiers, should be accepted with relief. Unfortunately, due to the abusive US policy pioneering in use of unmanned combat platforms, this type of armed forces transformation

[1]See more: SAXON D. (Ed.), International Humanitarian Law and the Changing Technology of War, Martinus Nijhoff Publishers, 2013 and DUNLAP Ch. J., Does Lawfare Need An Apologia?, „43 Case W. Res. J. Int'l L. 457-471" (2010).

raises a number of issues, not rarely concerning rather moral and ethical aspects, than their legality[2]. Concurrently, we are increasingly challenged by the growing use of cyberspace by public administrations and political bodies but also exchange of sensitive information and eventually control of the work of critical national security institutions, such as the army and energy providers.

In the last decade we had the opportunity to witness a number of cyber "attacks" that shook the stability of several countries. The quotation marks are used here for a reason: frequent use of the word "attack" in conjunction with "cyberspace", entails a discussion on "cyber war". However, a legal nature of concepts in question, referred to in everyday language, is at least questionable since not every cyber "attack" is an attack that could legitimize the use of military force in self-defense or constitute an attack under international humanitarian law.

This paper presents the perspective of international humanitarian law applicable in the event of such a cyber "attack" occurring in a situation of armed conflict. Given the absence of binding international law regulating the activities in cyberspace, all reflections are inspired by the opinion of the most eminent specialists expressed in the final work of the team convened under the auspices of NATO, released in March 2013 under the title of *the Tallinn Manual on International Law Applicable to Cyber Warfare*[3]. Finally, the paper focuses on the practical aspects of cyber security, casting a doubt from legal point of view.

**The international humanitarian law perspective**

What seems for us to constitute a cyber "attack" will not necessarily be qualified as an attack under international humanitarian law. The analysis starts with the juxtaposition of two definitions, namely the one that we use in daily life, and the one used by lawyers. The Oxford Dictionnary provides for "an aggressive and violent act against a person or place", while the legal definition provided in article 49 of Protocol Additional to the Geneva Conventions of 12 August 1949 (I PA)[4] indicates that ""attacks" means acts of violence against the adversary, whether in offence or in defence". Clearly the scope of the legal definition is wider and includes offensive as well as defensive operations. Notorious referring to the notion of attack in the context of cyber "attack" can have serious legal consequences since *ius ad bellum* is based on the concept of the use of force, thus also the attack. However, should cyber "attack" be considered as an attack, entitling the declaration of war or an armed response, we shall look at the legal structure of such an argument.

Violation of the UN Charter, giving the right to self-defense or raising responsibility of the state, is centered around the concept of "aggression" (legally binding definition was adopted at a conference in Kampala in 2010, and refers only to the cases of "armed attack" (as bombing, armed invasion or blockade[5]). Therefore, it seems extremely difficult, due to the lack of armed nature, to argue now that a cyber "attack" constitutes an act of aggression. According to the current state of law, it is clear that a declaration of war cannot result only from a cyber "attack" since the threshold is not met. Consequently, this article agglomerates the notion of

[2]ZENKO M., *Reforming U.S. Drone Strike Policies,* Council Special Report No. 65, January 2013 and R. Radhakrishnan, *UN urges transparency over US drone deaths*, „Aljazeera", http://www.aljazeera.com/news/americas/2013/10/un-urges-transparency-over-us-drone-deaths-201310189472317752 8.html (06.11.2013).

[3]*The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press 2013, April 2013.

[4]Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (I AP), 8 June 1977.

[5] The Coalition for the International Criminal Court (CICC), *The Crime of Aggression,* http://www.iccnow.org/?mod=aggression (06.11.2013).

attack in the context of *ius in bello*. Thus, since the use of cyberspace takes place in the time of armed conflict, the armed nature of an attack is no longer required from the legal point of view[6].

I AP states that its provisions are "relating to the protection of civilians and civilian objects on land, at sea or in the air against the effects of hostilities"[7]. There is no specification of cyberspace due to a very prosaic reason – non existance of such in 1977, the year of I AP elaboration. Following the modern US military doctrine it can be assumed that the provisions of international humanitarian law are applicable in five areas of conduct of hostilities, namely: land, air, water, space and cyberspace[8]. It is also consistent with the assumption of art. 36 I AP, which provides for the obligation to carry out a legal review in order to determine whether the employment of new weapons would be prohibited by any rule of international law. Therefore, it is clearly stated that the existing international legal framework is applicable to the cyber technology used as a mean or method of warfare.

**The regular perception of cyber "attack"**

The adoption of legal approach to the cyberspace is brought along once again since this section deals with common use of the notion of cyber "attack" which will be subsequently set together with its legal definition.

In order to conduct a coherent legal analysis of cyber "attacks", the exact understanding of this term (which the author reckons on deepening), should be clarified. According to the classification developed by the US Department of Defense, the following actions are distinguished: Computer Network Operations – CNO, Computer Network Attack – CNA, Computer Network Defence - CND and Computer Network Exploitation – CNE[9]. These operations consist of directing data stream in a manner to achieve military goals, previously acquired by means of kinetic energy. Therefore, DDOS attacks and the development of malware are some of the most popular methods of cyber "attacks".

One of the major dilemmas associated with the use of cyber "attacks" is the hardship of accurate prediction and control of the operation's consequences. According to David Turns, the most serious criticism is directed to the secondary effects of CNA which indirect nature spread much more further than it could has been foreseen[10]. We are dealing with a very complex chain of causality affected not only by human reactions, but also uncontrolled alteration of the software and released data.

Despite the rapid development of technology, it is still difficult to imagine that the CNO will soon form the only military actions conducted in ongoing armed conflict. Much more realistic is to see them through the prism of auxiliary, pre-emptive operations associated with traditional methods of conduct of hostilities resorting to the kinetic energy[11]. The cyber

[6]DROEGE C., *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians*, "International Review of the Red Cross", No. 886/2013, p.559.

[7]Art.49.3. I AP „3. The provisions of this Section apply to any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land. They further apply to all attacks from the sea or from the air against objectives on land but do not otherwise affect the rules of international law applicable in armed conflict at sea or in the air."

[8] US Department of Defense, Defense Review Report, February 2010, http://www.defense.gov/qdr/qdr%20as%20of%2026jan10%200700.pdf (06.11.2013), p. 37.

[9]*Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms,* 15 August 2012, p.66.

[10]TURNS D., *Cyber War and the Concept of „Attack" in International Humanitarian Law*, [in:] D. SAXON (red.), *International Humanitarian Law and the Changing Technology of War*, Martinus Nijhoff Publishers, 2013, p. 212.

[11]BOOTHBY W., private, to be published.

technology may be used for the benefit of the military in following manner: to disrupt reception of enemy chain of command, to disrupt the control devices, to interfere the communications, to suppress enemy air defence, to take over the control of weapons and weapons systems and finally to distrupt or destroy the infrastructure of the enemy responsible for the proper conduct of hostilities. At first glance, it appears that the above enumeration encompasses only military objects, therefore legitimate targets under international humanitarian law.

Nevertheless, as aforementioned, such operations may have indiscriminate effects, thus they may also harm protected objects and civilian population because of blurred lines: the same facilities like servers, fibers, cables and software may be employed likewise for the military and civilian objectives. Without clear distinction, the law of targeting may be called in question. The basic principles of international humanitarian law, it is distinction and discrimination are challenged when the target cannot be attacked due to the assorted cyber reality which is often more complex than already intricate urban space (Droege, 2013). Such unintended and undesired consequences could include: explosion and damage to the central structures of nuclear or chemical facilities, pipelines and refineries, collapse of the system of civil aviation control and public transport (metro, electronically controlled trains), leakage of confidential financial data or disruption of drinking water and electricity supplies. In this combination, the possible consequences of computer network attack appear to be even too perilous.

On the other side, it is clear that the substantial difficulty in predicting the secondary effects of cyber "attacks" is counterbalanced by its low cost and potential non-lethal effect, at least when compared to conventional means and methods of warfare (generally available and relatively easy in use technology).

**Cyber "attack" versus attack**

Having clarified the use of the notion of cyber "attacks", it shall be stated that they presumably rely on control acquisition, false data introduction, intelligence distortion and manipulation, data destruction and computer programs damage. The nature of these activities' consequeneces is essential to the legal analysis of a specific action. Consequently, it may be or not classified as an attack within the meaning of international humanitarian law. If positive, it must be conducted in accordance with the basic principles of distinction, discrimination, proportionality and humanity, which breached may induce perpetrator's responsibility under international law.

How to evaluate the character of an attack in legal terms? The conditions are set in article 49 I AP, which interpreted in the light of article 31 of Vienna Convention on the Law of Treaties, relates to "the ordinary meaning to be given to the term"[12]. Therefore, we need to establish whether the act in question has sparked violent consequences in the form of death, damage or injury among civilians or civilian objects protected by law. This is of great operational and practical significance, since the correct application of the law, allows to diminish collateral damage and better protect victims of armed conflicts.

David Turns, while analyzing the semantics of cyber "attack", refers to the linguistic interpretation methodology and assumes that in order to determine whether the act constitutes an act of violence in cyberspace, we shall examine its intrinsic nature, context of occurrence,

[12]Art.31 „1. A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."

consequences and the intention behind the act[13]. In case of cyber "attack" it is extremely awkward to argue that the mere moment of pushing "enter" button, installing malware or setting a logical bomb is somehow violent *per se*, therefore the sole nature of cyber activity is not very helpful. What is more it is commonly accepted that resort to the chemical or biological weapons consitutes an attack under international law, despite the absence of mere violnce in these actions[14]. Regarding the context, we can presume that currently the majority of cyber "attacks" occur during the peace time, and so called "cyberwars" do not amount to the war in legal terms, therefore international humanitarian law is not applicable. As for the next criterion, we shall consider the type of cyber attacks' consequences. A very interesting, yet complicated issue is to determine whether we can treat a damage done to the stored data (in the cloud, on a hard drive or server) in category of the damage under international humanitarian law, primarily protecting life of civilians. According to the Rule 21 of the Manual on International Law Applicable to Air and Missile Warfare issued by Harvard University[15], prohibition of "attacks directed against civilians or civilian objects, as well as indiscriminate attacks, is confined to air or missile attacks that entail violent effects, namely, acts resulting in death, injury, damage or destruction". Resulting effect-based approach is also supported by the world expert on cyber security – M.N. Schmitt emphasizing the requirement of physical injury as a result of the attack[16]. Therefore, all operations not leading to the physical damage are legitimate and may successfully serve as non-lethal tools of warfare. Such an approach evokes one more time the hardship of confining the extent of consequences: would the isolation of a country from the Internet be associable with possible deat, damage or injury resulting from paralysis of service providers? It seems a bit incongruous to perceive a bomb attack on one house as an attack while cutoff of 1 million houses from the Internet not. Also, it should be stated that such an approach may provoke problems in relation to the accountability under the law of targeting[17]. That is why, while rendering justice, one should also take into account the intention of the attacker which also remains consistent with the principles of international criminal law and the provisions of Articles 51-58 I AP [18]. Consequently, it seems that in order to enable the identification of violent character of an act, especially two guidelines should be maintained: the combination of a perpetrator's intention with the consequences in the form of physical damage, which interpretation will be brought with state practice and further development of cyberoperations.

**How does it work ?**

Finally, the role of technology in this legal reasoning should be stated loud and clear. Reflections presented in the previous sections remain in the sphere of theoretical discussion, since as we all know, the reality of cyberoperations combined with the realm of international politics preclude us from genuine assessment of what is actually going on. Therefore, it is difficult, if

[13]TURNS D., *Ibid*, p.221.

[14]DROEGE C., *Ibid* , p.543.

[15]Manual on International Law Applicable to Air and Missile Warfare, Harvard University, Bern, 15 May 2009, http://www.ihlresearch.org/amw/manual/ (06.11.2013).

[16]SCHMITT M., *„Attack" as a Term of Art in International Law: The Cyber Operations Context*, [in:] 2012 4th *International Conference on Cyber Conflict*, C. CZOSSECK, R. OTTIS i K. ZIOLKOWSKI (eds.), NATO CCD COE Publications, 2012, p. 283.

[17]DINSTEIN Y., *Concluding Remarks: LOAC and Attempt ti Abuse or Subvert It*, [in :] „International Law and the Changing Character of War, International Law Studies Vol 87", Naval War College, 2011, p. 483.

[18]*Prosecutor v. Dusko Tadic* (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999, : http://www.refworld.org/docid/40277f504.html (06.11.2013).

not impossible to find a case study representing, legally speaking, a cyber attack.

The last decade brought us, at several occasions, illustrations of possible use of cyberspace for military or political purposes. We can recall hacking of public administration websites in Estonia in 2007 (allegedly attributed to Russian secret services), sabotage of ministerial websites during the 2008 war in Georgia (again, alleged Russian initiative), Stuxnet virus damaging Iranian nuclear centrifuges (allegedly joint venture of USA and/or Israel) and many others like Mahdi, Flame and Red October malware[19]. Although only one case could be examined due to its occurrence during an armed conflict (Georgia 2008), it is pretty intelligible that given the absence of physical harm of DDOS attacks and hacking of official websites (nobody got killed or injured at that occasion), it is not possible to classify them as attacks under international humanitarian law.

First of all, in order to hold someone responsible for damages, the basic requirement which in the context of cyberspace arises to the insurmountable challenge, is the ability to identify the perpetrator therefore the factual findings. As to the knowledge of the author, the current technology does not allow to precisely discern the source of the attack. The country of the situation of the server from which the attack was derived is identifiable, however, it is commonly known that perpetrators tend to use the most powerful servers in order to transmit their attack. Therefore the genuine attacker remains undercover. There are also voices raising the issue of availability of high capacity infrustracture which is not rarely limited to the governments, thus a presumption of government's involvement is not excluded.

Secondly, the need of improvement of cyber security is manifest with respect to the execution of the military operation by the means of computer network actions. The growing resort to the unmanned automated weapon systems entails the necessity of high performance of such a technology. Consequently, several issues are to be discussed.

Considering the deployment of artificial intelligence, its ability to implement legal provisions should be revised. Despite the current impossibility of the resort to the fully autonomous weapons, often confused with already employed automated weapons (like Israeli Iron Dome), respective question remains. Is it possible to develop a software that would be able to replace a human being? In a way that its reasoning would remain equally emphatic and flexible to correctly assess the given situation and through legal syllogism, properly undertake the decision? The legal reasoning is far more complex than a binary reasoning of a computer software, however, the limited expertise of the author prevents from providing the desired final answer.

Next, the incremental process of warfare robotisation requires the improvement of cyber security standards because of omnipresence of software which, as previously discussed, becomes a new target in the modern armed conflicts. It is easy to imagine the consequences of hacking into computer network controlling the trajectory of particular weapon, missile or unmanned platform.

Both, the conduct of hostilities and preceding phase of its planning are affected by the software vulnerability. While gathering the intelligence, so crucial for the success of mission, the military personnel needs to know that the collected data is reliable and that the mission carried out on its basis will not entail legal responsibility or endanger civil population. Then, during the conduct of hostilities the operator, in order to properly assess the situation, should receive an instant feedback on all relevant interferences within the computer network, so as to undertake necessary steps to stop, cancel or alter the attack possibly resulting in the death, damage or injury of civilians. On the other hand, such immensity of information and its

[19]TARNOGÓRSKI R., *Prawo konfliktów zbrojnych a cyberprzestrzeń,* „Biuletyn PISM Nr 31 (1007)", 26 March 2013.

uncertainty have already proved to alter in significant way the legal responsibility of a commander[20]. Also, the issue of notifications' relevance remains unsolved.

It shall be emphasised that such solutions may disguise a double blade denouement. Indeed, international humanitarian law allows resort to the ruses of war simultaneously distinguishing and prohibiting acts of perfidy. As stated in article 21 I AP, the use or abuse of good faith of the opponent plays here a crucial role. If the action is conducted in such a manner that the opponent remains convinced of the legality of the attack, and accordingly causes death, damage or injury to civilians or civilian objects, such an action constitutes a breach of law. Still, the problem to assign a particular interference to the other side of the conflict, remains relevant. Of course, the whole process is taking place only if the manipulated party becomes aware of the act of perfidy, which is not recurrent.

Therefore, with the increasing use of computer network as the battlefield, it is imperative to strengthen its protection against any interference from the outside, and simultaneously develop an efficient warning system, informing the operator of possible intrusion and enabling him to take an immediate and adequate decision to stop the attack or possibly reduce the foreseeable damage.

**Conclusions**

In conclusion it must be assumed that the widespread use of cyber "attack" in everyday language do not coincide with the definition of attack adopted under the regime of international humanitarian law. The current legal framework along with lack of state practise, do not allow to refer to the cyber “attack” as a sufficient premise legitimising the resort to the use of force. Contrary to *ius ad bellum*, *ius in bello* deals with an ongoing armed conflict and embraces a lower standard of act's nature, therefore a violent act resulting in death, injury or damage of civilians or civilian objects, also derived from cyberspace, may be classified as an attack. Otherwise, in absence of such effects, it is rather appropriate to perceive it from the perspective of sabotage or ruse of war.

A computer network interference, abusing the good faith of the opponent and consequently resulting in death, injury or damage of civilians or civil objects, may be regarded as a perfidy constituting the infringement of law and entailing legal responsibility. Nevertheless, the identification of a cyber perpetrator remains still a primary and considerable challenge, bringing the efficiency of justice close to zero. Finally, whilst modern armies are increasingly eager to employ automated combat systems, the military operations in cyberspace abiding to international humanitarian law, feel even more uneasy. The fortification of software controlling weapon systems along with the effective interference warning system, are laudable and will provide for enhanced respect of basic principles of conduct of hostilities as distinction, discrimination, proportionality and humanity. Notably, since we all are present in this new dimension of battlefield.

[20]See more: GARRAWAY Ch., *The Application of Superior Responsibility in an Era of Unlimited Information*, [in:] SAXON D. (red.), International Humanitarian Law and the Changing Technology of War, Martinus Nijhoff Publishers, 2013.

## References

1. DINSTEIN Y., "Concluding Remarks: LOAC and Attempt ti Abuse or Subvert It" in *International Law and the Changing Character of War*, International Law Studies Vol 87., Naval War College, 2011.
2. DROEGE C., *Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians,* "International Review of the Red Cross", No. 886, 2013.
3. DUNLAP Ch. J., *Does Lawfare Need An Apologia?*, „43 Case W. Res. J. Int'l L. 457-471", 2010.
4. GARRAWAY Ch., The Application of Superior Responsibility in an Era of Unlimited Information, [in:] D.Saxon (red.), *International Humanitarian Law and the Changing Technology of War*, Martinus Nijhoff Publishers, 2013.
5. Harvard University, *Manual on International Law Applicable to Air and Missile Warfare*, http://www.ihlresearch.org/amw/manual/, *2009.*
6. *Prosecutor v. Du*sko Tadic (Appeal Judgement), IT-94-1-A,International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999.
7. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (I AP), 8 June 1977.
8. SAXON D. (Ed.), International Huma*nitarian Law and the Changing Technology of War*, Martinus Nijhoff Publishers, 2013.
9. SCHMITT M. (Ed.), (2013), *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, 2013.
10. SCHMITT M., *„Attack" as a Term of Art in International Law: The Cyber Operations Context*, in Czosseck, C., Ottis, R. and Ziolkowski, K. (Ed.), *4th International Conference on Cyber Conflict*, NATO CCD COE Publications, 2012.
11. TARNOGÓRSKI R., *Prawo konfliktów zbrojnych a cyberprzestrzeń,* „Biuletyn PISM Nr 31 (1007)", 26 March 2013.
12. TURNS D., *Cyber War and the Concept of „Attack" in International Humanitarian Law* in Saxon, D. (Ed.), *International Humanitarian Law and the Changing Technology of War*, Martinus Nijhoff Publishers, 2013.
13. US Department of Defense, *Quadrennial Defense Review Report*, February 2010.
14. US Department of Defense, *Joint Publication JP 1-02 Department of Defense Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf, 2012.*
15. Vienna Convention on the Law of Treaties, 22 May 1969, the United Nations.
16. ZENKO M., R*eforming U.S. Drone Strike Policies,* Council Special Report No. 65, 2013.