APPLYING INTERNATIONAL HUMANITARIAN LAW TO CYBER-ATTACKS

Dan-Iulian VOITAŞEC[*]

Abstract

Technology plays an important role in everyday life. Technological advancement can be found in every field of government including the military. Because of this, new means and methods of conducting hostilities have emerged. Cyber warfare starts to represent the latest challenge at an international level. States and non-state actors have started to implement new security policies and new defences against cyber-attacks but also have embraced using cyber-attacks as a method of conducting hostilities. The question that has to be answered regarding the use of cyber-attacks is what is the legal regime that governs such attacks and if IHL can apply to cyber warfare?

Keywords: *jus ad bellum, jus in bello, cyber-attacks, cyber-warfare, Tallinn Manual.*

1. Introduction

Our world is changing at an increasing rate and this change is caused, mostly, by the rapid advancement of technology. This accelerated technological evolution has led to the development of new means and methods of conducting hostilities. Cyber-attacks represent the latest threat and states and international organizations have begun to develop new defence strategies and new methods to combat these threats. If states and non-state actors resort to using cyber-attacks what is the threshold that these attacks have to reach to trigger a response under article 51 of the UN Charter from the victim state? Also, can a computer attack or a series of computer network attacks trigger the beginning of an armed conflict? International Humanitarian Law (IHL) is a set of rules which seek, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not or are no longer participating in the hostilities and restricts the means and methods of warfare[1]. IHL is a branch of international law and applies only to armed conflict. The question that this article wants to answer is does IHL apply to cyber-attacks? At this moment there is legislation, at a national level, that deals with cybercrimes (cracking, copyright infringement, child pornography, ID theft, fraud, etc.) but there is no international treaty that mentions the applicability of IHL to computer network attacks during situations of armed conflict. As a response to this situation in 2009, the NATO Cooperative Cyber Defence Centre of Excellence[2], invited an independent "International Group of Experts" to produce a manual on the law governing cyber warfare. In April 2013, The Tallinn Manual on the International Law Applicable to Cyber Warfare was published. Even though this is not a binding document it represents a first effort to comprehensively and authoritatively analyse this subject.

2. Content

Conflict is governed by two distinct branches of law, *jus ad bellum* which governs the situations in which states can resort to force as an instrument of their national policy and *jus in bello* which governs the conduct of hostilities. The latter applies only in situations of armed conflict. The term *attack* can be found in both branches of law but its meaning differs.[3] Due to this situation there must be a clear distinction between cyber-attack governed by the norms of jus ad bellum and those governed by jus in bello.

At this moment no definition of cyber-attacks is recognised at an international level. NATO Glossary of Terms and Definitions defines computer network attacks (CNA) as "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself[4]". The Glossary also states that a CNA is a type of cyber-attack.

In the Tallinn Manual, the term cyber operations is used to *define employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace*[5]. Cyber operations are not

[*] PhD Candidate, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: **dan.voitasec@gmail.com**).

[1] International Committee of the Red Cross (ICRC) – "What is International Humanitarian Law?", accesed February 20, 2015. https://www.icrc.org/eng/assets/files/other/what_is_ihl.pdf

[2] International military organisation based in Tallinn, Estonia, and accredited in 2008 by NATO as a 'Centre of Excellence'. NATO CCD COE is neither part of NATO's command or force structure, nor funded by NATO.

However, it is part of a wider framework supporting NATO Command Arrangements.

[3] For more information see Michael N. Schmitt - *"Attack" as a Term of Art in International Law: The Cyber Operations Context, PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283-293* 2012 -https://ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf Accessed on 27.02.2015

[4] NATO Standardization Agency, NATO Glossary of Terms and Definitions (AAP-06) (2013) at 2-C-11.

[5] Tallinn Manual on the International Law Applicable to Cyber Warfare – Cambridge University Press, Cambridge, 2013 – p. 211.

limited to cyber-attacks. While a cyber-attack is defined as a *cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects*[6]. In this case, the term cyber-attacks applies to situations of armed conflict. In this article the terms cyber operations and cyber-attacks will be understood as defined in the Tallinn Manual.

Not all cyber-operation and cyber-attacks are unlawful. There is a threshold that cyber-operations must reach to be considered use of force. Rule 10 of the Tallinn Manual states that "a cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful[7]." This rule references Article 2(4) of the UN Charter which states that "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations." This article is now regarded as a principle of customary international law, thus is binding for all states[8]. A cyber-operation will be considered unlawful when it constitutes a threat or use of force. There are two exceptions from the prohibition set out in art 2(4) of the UN Charter – uses of force authorized by the Security Council under Chapter VII and self-defence in accordance with Article 51 of the UN Charter. The prohibition does not apply to non-state actors, organized groups, individuals and terrorist groups if the actions of the said groups cannot be attributed to a state.

According to Rule 11 of the Tallinn Manual "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[9] To understand what criteria a cyber operation has to meet to be considered use of force we must look at non-cyber operation that reach the threshold of use of force.

The UN Charter does not provide a definition for the term *use of force* and does not provide the necessary criteria to determine the situations in which actions of a state may be regarded as uses of force. During the 1945 San Francisco Conference, Brazil wanted to include economic coercion as a use of force but the proposition was rejected.[10] Due to this fact cyber-operations aimed at economic coercion will not be considered use of force. The lack of criteria by which to determine when an act could be considered use of force, the International Group of Experts took into consideration the decision of the International Court of Justice (ICJ) in the Nicaragua Judgement. The ICJ stated that the "scale and effects" are to be considered when determining whether a certain action amounts to use of force. The International Group of Experts agreed that "scale and effects" are qualitative and quantitative factors that would apply when determining if a cyber operation qualifies as a use of force. ICJ distinguished between the most grave forms of use of force (armed attack) and other less grave forms[11]. All armed attacks are uses of force and all cyber operations that reach the threshold of armed attack and could be attributed to a state will be considered uses of force. This distinction is important given the fact that an action that amounts to use of force is a violation of Article 2(4) of the UN Charter while an action reaching the threshold of armed attack could trigger an armed response from the victim state under Article 51 of the UN Charter.

Not all cyber operations are uses of force. Because the question of what actions amount to use of force remained unanswered, the International Group of Experts created a series of factors to help states in determining if a certain action reaches the threshold of use of force. These factors are not formal legal criteria[12]:

a) *Severity* – an action, including a cyber operation that causes damage, destruction, injury or loss of life is more likely to be regarded as a use of force.

b) *Immediacy* – there is a higher probability that an operation that produces immediate effects will be considered a use of force.

c) *Directness* – in the case of armed actions, cause and effect are closely related. Cyber operations in which the cause and effects are clearly linked are more likely to be characterized as use of force.

d) *Invasiveness* – refers to the degree to which a cyber operation manages to intrude the computer systems of a State. The higher the security levels of a computer system, the greater the invasiveness of the action. This rule shall not apply to cases of cyber espionage; it will only apply to actions that reach the threshold of use of force.

e) *Measurability of effects* – This factor derives from the greater willingness of States to characterize actions as a use of force when the consequences are apparent.[13]

f) *Military Character* – a link between a cyber operation and a military operation increases the likelihood of being characterized as a use of force

g) *State involvement* - The clearer and closer a nexus between a State and cyber operations, the more

[6] Idem – p. 92.
[7] Idem 5 – p. 45.
[8] Malcolm N. Shaw – International Public Law, Cambridge University Press, 2008, - p. 1123.
[9] Idem 5 – p. 47.
[10] Sergey Sayapin - The Crime of Aggression in International Criminal Law, Asser Press, 2014 – p.80.
[11] International Court of Justice, Case concerning Military and Paramilitary activities in and against Nicaragua (Merits) (1986) para. 191. http://www.icj-cij.org/docket/files/70/6503.pdf. Accessed on 28.02.2015.
[12] Tallinn Manual – p. 49.
[13] Idem p. 51.

likely it is that other States will characterize them as uses of force by that State[14]

h) *Presumptive legality* - International law is generally prohibitive in nature. Acts that are not forbidden are permitted. In the absence of a treaty or a customary rule an act is presumed to be lawful. Thus actions that are not expressly prohibited by a treaty or a customary rule shall not be interpreted by states as use of force.

The conditions in which a state, that is the target of a cyber operation that reaches the threshold of armed attack, can exercise the right of self-defence are defined in Rule 13 of the Tallinn Manual: „A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects."

The right of self-defence is reflected in Article 51 of the UN Charter: "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security."

ICJ, in the Nicaragua Judgement[15], confirmed the customary status of the right of self-defence. The Court held that Article 51 of the UN Charter can only apply if there is a natural[16] or inherent right of States to self-defence and this right has a customary nature. Also, the ICJ noted that a State can resort to armed force in accordance with the right of self-defence only if it was the target of an armed attack[17]. As was the case of actions that reach the threshold of use of force, actions that constitute armed attacks are not defined in any international document. There is a direct link between armed attack and use of force. All actions that reach the threshold of armed attack will be considered uses of force. However, not all uses of force will be qualified as armed attacks. This distinction was made by the ICJ in the Nicaragua and Oil Rigs case.

In the case of cyber operations the International Group of Experts concluded that certain action could reach the threshold of armed attack. The Group of Experts' opinion is based on the ICJ's view in the Legality of Nuclear Weapons Advisory Opinion "that the choice of means of attack is immaterial to the issue of whether an operation qualifies as an armed attack[18]". To reach the threshold of an armed attack, a cyber operation has to cause damage, destruction, injury or loss of life. Cyber espionage operations, information theft and cyber operation causing short term disruption of non-essential services will not be qualified as armed attacks. If a cyber operation reaches the threshold of armed attack then the victim state can exercises its inherent right of self-defence. The International Group of Experts believes that a state can exercise its right of self-defence if it is the victim of a cyber-operation that can be qualified as an armed attack, launched by a rebel or terrorist group. This view is based on the response of the international community to the situation that occurred on the territory of the United States of America on September 11, 2001. The action launched by the terrorist organization Al Qaeda was characterised as an armed attack triggering the right of self-defence of the United States.

International Humanitarian law[19] applies to all situations of armed conflict regardless of a formal declaration of war and irrespective of whether the parties involved recognise the state of armed conflict. None of the rules that form IHL explicitly deal with cyber operations. For situations of international conflict, common Article 2 of the 1949 Geneva Conventions states that the provisions of the Conventions shall apply in full "to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them" and "to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance." Additional Protocol I to the Conventions states that its provisions shall apply to all situations stated in common Article 2 and to situations of "armed conflicts in which peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination". Common Article 3 to the Geneva Conventions deals with situations of non-international armed conflict stating that the hostilities take place on the territory of one of the high contracting power. Additional Protocol II (AP II) to the Geneva Conventions, in Article 1 includes additional rules for application such as control of a territory by an organized armed group, under responsible command that can carry sustained and concerted military operations. AP II differentiates between situations of internal disturbance and tensions such as riots, isolated and sporadic acts of violence and armed conflicts. The

[14] Ibid.
[15] Nicaragua Judgment – para. 176.
[16] Article 51 of the UN Charter – *droit naturel*
[17] ICJ - Case Concerning Armed Activities on the Territory of The Congo (2005): "Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these parameters. Other means are available to a concerned State, including, in particular, recourse to the Security Council.
[18] Tallinn Manual – p. 54.
[19] Laws of Armed Conflict (LOAC) in some Manuals.

term armed conflict was not defined in the Geneva Conventions or in the Additional Protocols. A definition of armed conflict was given by the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia in the Tadic case: "An armed conflict exists wherever there is resort to armed force between states or protracted armed violence between government authorities and organised armed groups or between such groups with a state. International humanitarian law applies from the initiation of such armed conflicts and extends beyond the cessation of hostilities until a general conclusion of peace is reached; or, in the case of internal conflicts, a peaceful settlement is achieved. Until that moment, international humanitarian law continues to apply in the whole territory of the warring States or, in the case of internal conflicts, the whole territory under the control of a party, whether or not actual combat takes place there.[20]" According to the definition given in the Tadic case, resort to armed force is a requirement to be in a situation of international or non-international armed conflict. Will IHL apply if a cyber operation rises to the threshold of armed force? According to Rule 20 of the Tallinn Manual "cyber operations executed in the context of an armed conflict are subject to the law of armed conflict." The rule states that IHL will apply to cyber operations executed both in international and non-international armed conflicts. In the context of cyber operations launched against Estonia in 2007, IHL does not apply because the situation did not rise to the level of an armed conflict. The only situation were IHL could be applied to cyber operations was the 2008 conflict between Russia and Georgia but those operations could not be attributed to any party to the conflict. The International Group of Experts agreed that there must be a nexus between the cyber operation and the armed conflict for IHL to apply to the operation in question but there were two different opinions regarding the nature of that nexus. According to one view, IHL governs any cyber activity conducted by the party to the armed conflict against its opponent while the second view noted that the cyber operations must be undertaken in furtherance of the hostilities[21].

Given the way that Rule 20 was formulated one could say that a cyber operation could not be considered the start of an armed conflict. If we look closely at Rule 22[22] of the Manual that defines: "*An international armed conflict exists whenever there are hostilities, which may include or be limited to cyber operations, occurring between two or more States*" and Rule 23[23] which states that "*a non-international armed conflict exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of one or more armed groups, or between such groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organisation*" we can see that the International Group of Experts addressed the situations in which armed conflicts of international or non-international nature could be limited only to cyber operations, if said operations reached the required threshold. It is safe to note that a cyber operation launched by a state or a rebel group that causes physical damage to life or property could be considered the start of an armed conflict if all the necessary conditions are met.

Even though no specific instrument of IHL deals directly with cyber operations, the Martens Clause could be considered. The Clause can be found in Hague Convention IV[24], the 1949 Geneva Conventions[25] and Additional Protocol I[26]. The text in the Hague Convention IV states that: "Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience." The Martens Clause reflects customary international law and ensures that cyber operations launched during an armed conflict are not conducted in a legal vacuum. Opinions stating that IHL should not apply to cyber operations could be dismissed by citing, in addition to the Martens Clause, Article 36 of Additional Protocol I: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."

It is important to remember that the role of IHL is to limit the effects of armed conflict not to prohibit the use of armed force. Jus ad bellum is the body of

---

[20] The Prosecutor v. Dusko Tadic – International Tribunal for the Former Yugoslavia, para. 70 - http://www.icty.org/x/cases/tadic/acdec/en/51002.htm Accessed on 2.03.2015.

[21] Tallinn Manual – p. 69, Rule 22, para.5: "*Consider a cyber operation conducted by State A's Ministry of Trade against a private corporation in enemy State B in order to acquire commercial secrets during an armed conflict. According to the first view, the law of armed conflict would govern that operation because it is being conducted by a party to the armed conflict against a corporation of the enemy State. Those Experts adopting the second view considered that the law of armed conflict does not apply because the link between the activity and the hostilities is insufficient."*

[22] Tallinn Manual – p. 71.

[23] Idem p. 76.

[24] Hague Convention IV, preamble.

[25] Geneva Convention I - art.63; Geneva Convention II, art. 62; Geneva Convention III, art. 14; Geneva Convention IV, art. 158.

[26] Additional Protocol I to the Geneva Conventions, art.1 para. 2.

law that limits the situations in which states may resort to armed force. In the opinion of Professor Yoram Dinstein[27] the usage of International Humanitarian Law as a term designated to incorporate both the Hague Law and Geneva Law, could cause the false impression that the role of IHL is truly humanitarian in nature. The use of armed attacks is permitted under IHL if the fundamental principles of this branch of law are respected. As with conventional attacks, cyber-operations are permitted during situations of armed conflict if the principles of military necessity, proportionality and the humanitarian considerations are respected. Application of IHL rules to cyber operations serves to limit the effects of the operations on the civilian population.

3. Conclusions

International Humanitarian Law applies to cyber operations launched both during situations of international armed conflict and non-international armed conflict. Fortunately, until the present time, no cyber operations reached the threshold necessary to be considered an armed attack but that moment may come sooner than imagined and the international community must be prepared to respond in a timely manner. The horrors of the Second World War should never be repeated and states and international organizations should pay more attention to emerging means and methods of warfare and, if that is the case, create the necessary legislation to protect the civilian population.

References

- Michael N. Schmitt et al., Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge: Cambridge University Press, 2013)
- Heather Harrison Dinniss, Cyber Warfare and the Laws of War *(Cambridge: Cambridge University Press,* 2012*)*
- Yoram Dinstein – The Conduct of Hostilities under the Law of International Armed Conflict *(Cambridge: Cambridge University Press, 20*04*)*
- Raluca Miga-Beșteliu, Drept Internațional Public Volumul I, (Bucharest: C.H.Beck, 2010)
- Raluca Miga-Beșteliu, Drept Internațional Public Volumul II, (Bucharest: C.H.Beck, 2008)
- Beatrice Onica-Jarka , Drept International Umaniar (Bucharest: Universul Juridic, 2010)
- Beatrice Onica-Jarka, Jurisdictii Penale Internationale (Bucharest: C.H.Beck, 2008)
- Malcolm N. Shaw, International Public Law (Cambridge: Cambridge University Press, 2008)
- Sergey Sayapin, The Crime of Aggression in International Criminal Law (The Hague: Asser Press, 2014)
- Michael N. Schmitt - "Attack" as a Term of Art in International Law: The Cyber Operations Context, Proceedings of the 4th International Conference On Cyber Conflict 283-293 2012 - https://ccdcoe.org/publications/2012proceedings/5_2_Schmitt_AttackAsATermOfArt.pdf Accessed on 27.02.2015
- The 1949 Geneva Conventions I-IV and Additional Protocol I & II (1977)
- International Court of Justice, Case concerning Military and Paramilitary activities in and against Nicaragua (Merits) (1986) http://www.icj-cij.org/docket/files/70/6503.pdf. Accessed on 28.02.2015
- International Court of Justice - Case Concerning Armed Activities on the Territory of The Congo (2005)
- The Prosecutor v. Dusko Tadic, International Tribunal for the Former Yugoslavia, http://www.icty.org/x/cases/tadic/acdec/en/51002.htm Accessed on 2.03.2015

[27] Yoram Dinstein – The conduct of Hostilities under the Law of International Armed Conflict, Cambridge University Press (2004) p.13.