Use of Force in Self-Defense Against Cyber-Attacks and the Shockwaves in the Legal Community: One more Reason for Holistic Legal Approach to Cyberspace

Dr. Metodi Hadji-Janev

Assistant professor of law, metodi.hadzi-janev@ugd.edu.mk

Dr. Stevan Aleksoski

Full professor stevan.aleksoski@ugd.edu.mk

Doi:10.5901/mjss.2013.v4n14p115

Abstract

Technological advance is a double edge sword. Computer systems that monitor and control industrial infrastructure brings efficiency but at the same time security challenges too. Urged by this complexity some countries have considered to use military force in response to cyber-attacks. Such possibilities have created shockwaves inside the legal community. While some negate the applicability of Ius ad bellum others believe that its principles, standards and norms provide framework for use of force in self-defense. Giving the influence that legal community has in policy making the article offers legal analyses with these regards and use them to provide some incentives for legal alternatives. The overall argument of the article is that division inside the legal community is one more reason for international community to reconsider international legal reforms. These reforms must be based on holistic approach.

Keywords: *Ius ad bellum, cyber-attacks, self-defense, legal reforms*

1. Understanding the Complexity of Cyberspace in the Context of Use of Military Force Against Cyber-Attacks as an Introduction

Progress in information and communication technologies has affected our way of living in a unique way. The effects of cyber-based technologies on the population as a whole are huge and not limited just to information. There are emotional, societal, economic, psychological, and political effects in addition to easy access and sharing of information. Today computer systems that monitor and control industrial, infrastructure, or facility-based processes (widely known as *supervisory control and data acquisition*-SCADA) reduce labor costs, improve systems performance and reliability. Nevertheless, security challenges from cyberspace to these infrastructures make them critical for our safety and security.

The growing asymmetry is a game changer. Non-state actors or smaller nations can take on much bigger powers in cyberspace, and through it, in the physical world, as well. Cyber-attacks on critical infrastructure such as electricity and water supplies could be similar to those that would be caused by weapons of mass destruction. At the same time SCADA systems have been developed in security vacuum which creates "paradox of modernity". As a result the more technologically advanced the state is the more vulnerable to cyber threats is.

Cyber-attacks in Estonia (2007), Georgia (2008), Iran (2010), Burma (2010), USA (2011), Middle East (2012), confirm experts views that cyber security range *"… from the utility (or futility) of network monitoring, to the possibility (or impossibility) of universal trustworthy cyber authentication, to the potential from emerging defensive, offensive, and preemptive cyber operations, to proposed clean-slate designs of future Internet architectures, to the role of the military and intelligence agencies in securing public and private networks, to the role and rules of international law concerning cyber warfare, to the role of cyber security education, among others".*[1]

Urged by this complexity some countries and organizations such as U.S. and NATO have considered radical measures to confront upcoming threats from cyber-attacks. In its first formal cyber strategy U.S. concluded that computer

[1] *Report of the New England Faculty Summit on Cyber Security held at Boston University on June 28, (2011), http://www.bu.edu/hic/files/2011/07/CyberSecuritySummitReport.pdf*

sabotage coming from another country can constitute an act of war.[2] Seeing itself as the world's premier collective defense entity, NATO believes that has a responsibility to take adequate measures to protect itself and its members from cyber threats.[3]

These official statements and arguably potential behavior raise serious legal concerns. The official U.S. cyber security strategy for the first time opens the door for the state to respond to cyber-attack using traditional military force. The lack of international cyber legal framework; the complexity of cyber-attacks due to operational and legal difficulties in deterring and identifying them; as well as the asymmetric and modernity paradigm discussed above; pose without a doubt, great pressure to academic and operational environment. Both operational and legal community is highly divided over the applicability of international principles, standards and norms to cyberspace and cyber-attacks specifically. The importance of the question whether cyber-attacks could trigger use of military force rises in the light of the fact that the U.S. and NATO are not the only victims to cyber – attacks. Widely accused as having aggressive power projection policy and as a country that supports terrorist activities Iran has also suffered from cyber-attacks. Other countries have suffered as well.[4] At the same time it is well known that leading figures from these communities are highly influential when it comes to policy and decision making. Hence this growing dependence on cyberspace must be matched by parallel focus on legislation.

Focusing on the above mentioned issue (potential use of force in case of cyber attack-applicability of the *ius ad bellum* standards, principles and norms) the article will elaborate the burden that legal community is facing and try to build the argument that cyber-security deserves global, holistic and concrete joined measures. These measures should take in to account legal, technical and policy considerations. To achieve this we will confront opposing scholar positions and try to draw conclusions about the applicability of International law regarding the use of force to cyber-attacks. This analysis will help us to understand the shock-waves that these issues brings to the legal community, see what other bodies of law could apply and how or what if necessary needs to be done in order to find appropriate legal framework to address cyber-attacks. We will first address the part of the International law that regulates the use of force.

2. Cyber Attacks and the Use of Force under International Law?

Determination about the legality of use of military force under the international law must be made under norms, principles and standards that constitute the *jus ad bellum*. Norms and procedures that build this body of International law dictate when entity may – and may not - legitimately use force as an instrument of dispute resolutions.[5] Although UN Charter contains norms that regulate this body of law there are other standards and principles that shape the use of force under International law.

The UN Charter set up the legal framework over the use of force based on prohibition and exclusion from that prohibition. In its Article 2(4) the Charter prohibits "*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"*. Then in order to accomplish its purpose to *maintain peace and security* the Charter made "exclusive exceptions" from the general prohibition of use of force. Under the Article 39 and *accordance with* Articles 41 and 42 The Security Council *shall decide what measures shall be taken …to maintain or restore international peace and security…*Second exception from general prohibition of use of force is located in Article 51 of the Charter which regulate the rights of state to use force in individual or collective self-defense.[6]

Beside these two exceptions there are other the so-called "extra-Charter exceptions" of use of force resulting from state practice, customary principles or case law. Although self-defense is regulated under the Article 51 of the Charter, lately many Western scholars have emphasized the existence of customary right of self-defense in order to survive in International arena. This however, has also been recognized by the International Court of Justice (ICJ) in "Nicaragua

[2] *Siobhan Gorman and Julian E. Barnes: Cyber Combat : Act of War, The Wall Street Journal, (May 30, 2011), http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html*

[3] *Sverre Myrli: NATO and Cyber Defense, NATO Parliamentary Assembly available at: http://www.nato-pa.int/default.Asp?shortcut=1782.*

[4] *Marco Roscini: World Wide Warfare, in: A. von Bogandi, R.Wolfrum, Max Plank Yearbook of United Nations Law, Vol.14, 2010, 85-130, (2010) 89*

[5] *John Norton Moore: Development of the International Law of Conflict Management, in: John Norton Moore & Robert F. Turner eds. National Security Law 29, 2d ed. (2005) 29*

[6] *Charter of The United Nations, art.39, 41, 42 an 51, available at: http://www.un.org/en/documents/charter/*

case".[7] The so-called "United for Peace" procedure adopted by the General Assembly as political response to meet a presumed non-functioning of the Council is one of these exceptions.[8] Another "extra-Charter" exception is the use of force to realize the right to self-determination, which is articulated in numerous instruments, most notably the 1966 International Covenant on Civil and Political Rights.[9] The doctrine of humanitarian intervention is also cited as extra-Charter use of force. Although there are divided opinions about considering the use of force to protect nationals' abroad or counter-terrorist operations as an extra-Charter use of force, there is no state practice, customary law tradition or case law examples regarding the use of force against a cyber attack.

Absence of legal norms, customary principles or state practice in International law usually pushes scholars to pursue answers based on analogies. This however is problematic for two reasons. First direct analogy is not always easy to complete especially if one needs to compare different nature approaches (traditional with modern and technologically advanced). Second pundits and operators disagree over the analogy. Disagreements are over the body of law to which analogy is being made and over the sufficiency of exiting legal norms, principles and standards to confront challenges from cyber-attacks. For the purpose of drawing conclusions in the light of the above raised questions (regarding applicability of the law of use force if cyber attack occurs) we will proceed with widely accepted analogy among the academics, i.e. the *Ius ad bellum* test to use force under International law.

So far it became clear that the use of force against cyber-attacks could be possible in two cases. First force can be used as an authorization of The United Nations Security Council (UNSC). Second, state(s) could use force in individual or collective self-defense. Since the UNSC mandates binding resolutions the decision to use force against entity that had conducted cyber-attack under the Charter will be legal. However, having in mind that threat perceptions in the context of cyber attacks among member state will differ from state to state and that according to recent Security Council's practice in such situations Council will fail to respond in a timely manner, it seems valid to assume that a state(s) will choose to respond with cyber attacks by exercising it/their right(s) to self-defense (individually or collectively).

3. Self-Defense Against Cyber-Attack(s)?

The use of force by a victim state of a cyber attack(s) lawfully in self-defense would be possible only if: (1) cyber attack(s) meets the standards of an armed attack, (2) cyber-attack is attributable to the state where the self-defense is being carried out and (3) the use of force carried in self-defense is "necessary" and "proportional". Legal analogy based debates among the scholars in the context of applicability of international legal standards and principles to cyber-attacks have stimulated numerous debates in the light of these conditions too. Precisely disagreements steam from the absence of the definition of what constitutes an armed attack under international law; challenges to attribute cyber-attack(s) to a state; and applicability of customary rules of self-defense along with the provisions under the UN Charter and interpretation.

3.1 Cyber attack as an armed attack?

Relevant international organizations guidance, certain international instruments and legal scholar expressing their opinions, had tried to fill the absence of authoritative definition of armed conflict. Today it is well accepted that Jean Pictet's guidance to determine the existence of an international armed conflict under Common Article 2 of the 1949 Geneva Conventions serve as a useful guide for assessing whether a particular use of force could be considered as an act equal to armed attack. According to Pictet's guidance a use of force is considered an armed attack when the force is of "sufficient scope, duration, and intensity."[10] Another useful tool that helps to fill the absence of legal definition of what constitutes armed attack is the U.N. General Assembly's Resolution for "Definition of Aggression". Although the Resolution does not contain definition of armed attack this instrument provides examples of state actions that could be considered as an armed attack. Even more many argue that guidance of this instrument have gained extensive international acceptance.[11]

Some scholars have tried to define armed conflict by explaining the distinction between terms "war" and "armed

[7] *ICJ: Military and Paramilitary Activities in and against Nicaragua, ICJ Cases (1986)*
[8] *Niels Blokker, Nico Schrijver: The SC and the use of force Theory and Reality, Nijhof Publishers, (2005) 37*
[9] *Michel Schmitt: International Law and the use of force: The Jus ad Bellum, The Quarterly Journal, Volume II, No3, September, (2003) 89-97*
[10] *Walter G. Sharp: Cyberspace and the use of force, Aegis Research Corporation, (1999) 60-61*
[11] *The U.N. Documents: Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess. (Dec. 14, 1974)*

conflict".[12] Based on the threshold in ICRC Commentary of the Common Article 2 according to Sharp, *de facto hostilities exists, and consequently the jus in bello applies when any use of force, regardless of its scope, duration, or intensity, occurs between the members of the armed forces of two states*.

Both states and International Court of Justice have frequently applied these guidance and explanations in the context of conventional understanding of use of force. Nevertheless, authors disagree whether these guidance and explanations can be applied to cyber-attacks. While some legal scholars believe that it is intuitive that cyber-attacks can constitute armed attacks, especially in light of their ability to injure or kill, part of the legal community has been reluctant to classify them this way because they do not resemble "classic attack(s) with traditional military force."[13]

Authors that negate the applicability of guidance and explanations of what constitutes an armed attack to cyber attacks are not united. There are authors who in fact disagree over the whole idea of applicability of *Ius ad bellum* to the cyberspace activities. Jeffrey Addicott, for example asserts that "*international laws associated with the use of force are woefully inadequate in terms of addressing the threat of cyberwarfare*"[14]. On the other hand there are authors who disagree only to the applicability limited to guidance and explanations of conventional use of force. For the purpose and space of the given debate, we will focus on general arguments that these authors pose on their behalf in the context of the debate.

Discussing the conditions to meet criteria for use force as response to unlawful armed attack Mary Occonel points that *attempt to apply these conditions to cyber force actions is difficult, if not impossible*. The sort of damage according to this author's views does not meet the condition that an armed attack must be significant to trigger Article 51. To prove her point she offers ICJ case law practice. Using *Nicaragua* case Oconnel emphases Court's views about the importance of "scale and effects" in determination whether or not specific action could be classified as an armed attack.[15]

Peter Singer and Noah *Shachtman* share similar position as *O'connel*. In their argumentation they provide insights from recent state practice. Analyzing the effects of Russian cyber-attacks to Estonia and comparing cyber attacks against Georgian government with the actual Russian missiles and bombs in the accompanying war they tried to point that effects from cyber attacks were incomparable with the effects from actual armed attack.[16] Therefore they believe that it is even inappropriate to apply *Ius ad bellum* rules to cyber domain. Similar explanations come from Duncan Hollis, who asserts that cyber-attack alone will almost never constitute an armed attack for the purposes of Article 51. Hollis' argumentation for this position is that *cyber-attack lacks the physical characteristics traditionally associated with military coercion*".[17] Although there are others who share these views many authors believe that guidance and explanations of what constitutes an armed attack in conventional terms could be also applicable to unconventional use of force including cyber-attacks.

Yoarm Dinstein is among the authors who share the view that cyber attack can constitute armed attack. Accordingly in his analyses based on the "instrument-based approach" Dinstein uses the guidance and explanations of what constitute an armed attack in conventional terms to prove that cyber-attacks can constitute armed attacks. The logic of this approach holds that if cyber-attacks could cause the destruction of a power grid than cyber-attack constitutes an armed attack. This is due to the fact that before development of cyber capabilities such destruction could have been possible only by using kinetic force. Beside that article 3of the "Definition of Aggression" provides implicit support to Dinsteins' approach.[18]

---

[12] Sharp suggests that war refers to a state of de jure hostilities invoked by a formal declaration of one party that creates an international armed conflict as a matter of law. In contrast, any other armed conflict refers to a state of de facto hostilities invoked by the use of force by one party without any declaration of war. He then concludes that determination when any other conflict exists is a factual subjective determination that centers on the use of force between states. Walter G. Sharp, (1999) 74

[13] Thomas Wingfield: When is a Cyberattack an "Armed Attack?": Legal Thresholds for Distinguishing military activities in cyberspace, Cyber Conflict Studies Association, (2006) 6

[14] Jeffrey F. Addicott, "Cyberterrorism: Legal Policy Issues," in Legal Issues in the Struggle against Terrorism, eds. John N. Moore and Robert F. Turner, Durham, NC: Carolina Academic Press, (2010), 550

[15] "…The prohibition of armed attacks may apply to the sending by a state of armed bands to the territory of another state, if such an operation, because of its scale and effects would have been classified as an armed attack rather than a mere frontier incident…" Marry E. O'connell: Cyber Security and International Law, International Law Meeting Summary, Chatham House (2012), 5-7

[16] Peter Singer and Noah Shachtman: The Wrong War, Foreign Policy 21st Century Defense Initiative, Brooking, (2011), http://www.brookings.edu/research/articles/2011/08/15-cybersecurity-singer-shachtman

[17] In other words, because it generally does not use traditional military weapons, Duncan B. Hollis: Why States Need an International Law for Information Operations, 11 Lewis & Clark L. Rev. (2007), 1023-1042

[18] This view has some support in the article 41 of the U.N. Charter as well Yoram Dinstein: Computer Network Attacks and Self-Defense, in: Michael N. Schmitt & Brian T. O'Donnell eds. Computer Network Attack And International Law, (2002), 99

Unlike Dinstein, Walter Sharp also believes that cyber attack could constitute an armed attack. However, Sharp uses guidance and explanations of what constitutes an armed attack in conventional terms and merge them to the target of potential cyber attack. Eric Talbot along with Sharp advocates that cyber attack classifies as an armed attack if it targets a sufficiently important computer system.[19] Baring in mind our previous discussion about the importance of SCADA systems and the complexity of the risks that these systems' failure could cause sound reasonable to agree with these authors' logics. Purposeful cyber-attack to SCADA systems could cause failure of these systems and therefore cascade severe consequences. We could not agree less that in situations like this, cyber-attacks would meet not just the ICRC threshold regarding the "intensity", but also ICJ well established test "scale and effects" for determination whether or not specific action could be classified as an armed attack. Nonetheless the issue with this approach in determination when cyber-attack could constitute an armed attack is that its proponents advocate aggressive response based on the "strict liability". Sean Condron, for example argues that a cyber-attack constitutes an armed attack, and would grant the target the right to use force in self-defense, whenever it penetrates any critical national infrastructure system, regardless of whether it has yet caused any physical destruction or casualties.[20]

Michael Schmitt, former colonel turned professor, uses his own developed model to measure consequences of cyber-attack under the guidance and explanations of what constitutes an armed attack in conventional terms. Schmitt propagates that one needs to consider seven factors before decide if a cyber-attack's effects could be deemed to armed attack. These factors are *severity* (the type and scale of the harm); *immediacy* (how quickly the harm materializes after the attack); *directness* (the length of the causal chain between the attack and the harm); *invasiveness* (the degree to which the attack penetrates the victim state's territory); *measurability* (the degree to which the harm can be quantified); *presumptive legitimacy*, (the weight given to the fact that) and *responsibility* (to be able to attribute the attack).[21] If the cyber-attack, in the field of cyber-activities as a whole, meets these criteria, cyber-attacks constituting an armed attack are the exception rather than the rule. These factors are illuminating, but they call for such a wide-ranging inquiry that they may not provide sufficient guidance to decision makers.[22] Although widely accepted some argue that Schmitt model suffers from some inconsistencies. It could be argued that only small number of cyber-attacks could rise to the level of armed attack.[23] Another issue rises from the ability to foresee the severity of the attack which could be abused since it is highly subjective.

The analyses of two opposing groups of authors further confirm the complexity that cyberspace poses to the society and security in a broader and law in narrow context. In the light of our previous discussion regarding the complexity (growing asymmetry in a cyberspace and the "paradox of modernity") it seems that second group of authors' arguments for now, are more convincing. Just because we have not experienced severe cyber-attack that could cause dead and significant material property damage this does not mean that cyber-attack or series of such attacks could not rise to a level of what is considered to be an armed attack under International law. Precisely, certain cyber-attacks could rise to amount of armed attack that under *Ius ad bellum* principles, standards and norms could justify use of military force. Nevertheless, in order for victim state to be able to use force in self-defense lawfully beside the condition that state needs to be a victim of illegal action that constitutes armed attack the victim state must attribute such illegal attack(s) directly and conclusively to another state or agents under that state's direct control.[24]

3.2 The challenge of attribution

Most of the arguments that build "pro" and "contra" views to use military force against cyber-attacks in the context of requirement to attribute responsibility steam from the premises that we discussed regarding the so call "paradox of modernity". Legal scholars who disagree to apply the analogy of *Ius ad bellum* standards, principles and norms to cyberspace threats generally focus on the difficulties to attribute cyber-attacks directly and conclusively to another state.

---

[19] Walter Sharp, (1999), 129-130

[20] Sean M. Condron: Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harvard J.L. & Tech., (2007), 403, 415-16

[21] Michel Schmitt: Computer Network Attack and the Use of force in International law: The Columbia Journal of Transnational Law, Volume 37, (1999), 885-937

[22] This analytical approach is important for our debate since it seems that it would appear to be the analytical model adopted by the United States. Office Of General Counsel, Department Of Defense: An Assessment Of International Legal Issues In Information Operations, (May 1999)

[23] Daniel B. Silver, Computer Network Attack as a Use of Force Under Article 2(4), 76 Int'l Law Studies 73, (2002) 92–93

[24] Sean M. Condron, (2007), 414

Bret Michael and Thomas Wingfiled propose that the issue of attribution in cyberspace derives from technical challenges… *since the Internet was conceived without a requirement for users' accountability.* The problem according to them is even more complicated since they argue that attribution in cyberspace is "asymmetric".[25]

Discussing the challenge of attribution in cyberspace Eric Jensen concludes similarly to Michael and Wingfield, that tracing cyber-attacks can be exceptionally long process. The problem with accuracy however never ends since as he asserts even if the server is located to "…*identify the entity or individual directing the attack* is extremely hard. Nevertheless he advocates for changing approach.[26] The issue with cyber terrorists and cybercriminals *modus operandi* discussed by Davis Brown seems to echoes Jensens' analyses. Cyber-terrorists and cybercriminals often hijack innocent systems and use them as "zombies" to initiate their cyber-attacks. While victim-states must try to penetrate such guises, current technology may not always allow them to do so in a timely manner.[27] O'connel offers state practice to point that as a source of International law it also requires for attribution to be made with clear and convincing evidence. Nevertheless much similar as previously cited authors she concludes that in the case of cyber-attack such convincing evidence is hard to find.

Since legal requirements for conclusive attribution is hard to apply in case of cyber-attacks some have suggested that states could legally employ cross-border cyber attacks and therefore not use military force. Using the transnational criminal approach Michael and Wingfiled see this approach promising. They do believe in potentials to establish international jurisdiction where individuals and groups may be investigated and prosecuted under another countries' domestic law.[28]

Authors who advocate that cyber-attacks could trigger use of force in self-defense lawfully under the International law in response to "attribution challenge" offer different proposals. Mainly they build their argumentation based on the same issues proposed by the authors who disagree with their positions i.e. the complexity to directly and conclusively attribute the cyber-attack(s).

Some recognizes that attribution stubbornly permeates every aspect of cyber operations however they consider this as a technical issue, not a legal one. Therefore they advocate that the identity of the attacker may well determine if a state of war exists.[29] Others have tried to materialize their argumentation emphasizing the risks that cyber-attacks pose to the states. Sean Cordon explains that if states are about to follow traditional procedures to attribute responsibility regarding the nature of cyber-attacks than they need to be ready to experience risks that cyber attack could pose. This according to him could create dilemma for the states. [30]Similar views have echoed that such situations could put states in the limbo position between its safety traditional legislation and imperfect reality. [31]

From all of the above it is clear that direct and concessive attribution to cyber attack is not easy to achieve. Difficulty to locate the entity responsible for cyber- attack(s) is stubborn impediment that questions lawful response in self-defense. On the other hand neither cyber-attacks are traditional nor the traditional test for state responsibility aloud victim state to exercise inherent right of self-defense appropriately. Legal scholars' disagreements over applicability of self-defense under international law to cyber-attacks culminate in the context of necessity, proportionality and anticipatory self-defense.

3.3 Necessity and proportionality against cyber-attacks

Necessity and proportionality are founding principles of appropriate self-defense. [32] As well as other elements that build the threshold of lawful self-defense against cyber-attacks these principles considered in the context of cyber-attacks are highly disputed among the legal scholars. If under the given evidences state cannot achieve a reasonable settlement of a dispute through peaceful means self-defense against cyber-attack will meet the requirement of necessity. Self-defense

---

[25] Bret Michael and Thomas Wingfiled: International Legal Reform Could Make States Liable for Cyber Abuse, Per Concoridiam, Journal of European Security and Defense Issues, Vol.2 Issue 2, (2011), 40-41

[26] Eric Jensen: Computer Attacks on Critical National Infrastructure: AUse of Force Invoking the Right of Self-Defense, 38 Stanford Journal of International Law, (2002) 207

[27] Davis Brown: A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, 47 Harvard International Law Journal (2006) 181-183

[28] Bret Michael and Thomas Wingfiled, (2011), 41

[29] Charles Dunlap: Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Study Quarterly, Spring, (2011), 88

[30] Sean Condron, (2007), 414-415

[31] Duncan B. Hollis, (2007), 1026

[32] Thomas Wingfield: The Law of Information conflict: National Security Law in Cyberspace (2000) 42

against cyber-attack is proportional if victim state limits it actions to the amount of force required to defeat an ongoing cyber-attack or to deter a future cyber-attacks.[33] Compliance with the principles of necessity and proportionality is difficult and fact-intensive even for conventional attacks, and therefore cyber-attacks present new hard challenges.

Authors who disagree with the overall applicability of *Ius ad bellum* to cyber-attacks believe that necessity and proportionality are difficult conditions to meet. Building on the previous discussions this part of the legal community considers that difficulties come from the complexity of cyber-attacks and as a consequence the amount of the time needed to attribute the attack. Evidences from recent cases like Estonia or Iran confirm these considerations. In both situations attacks came from different locations. Therefore the biggest concern regarding the international legal requirements for lawful self-defense against cyber-attack is the defensive response. Technical challenge also raises considerations toward these directions. In fact the defending state would need time to consider the effects that counter measures could cause. Nevertheless, putted in to the light of analytical models previously described in determining whether cyber-attacks could constitute lawful armed attack, such evidences are not convincing. If for example one considers effect based-approach to determine if cyber-attacks qualify as an armed attack necessity is highly dependable of the effects caused by the cyber-attack(s). If victim state suffers severely and there are reasonable doubts that aggressor is preparing further cyber-attacks than the threshold of necessity change. In fact the imminence of danger aloud for victim state to respond before it is too late. At the same time proportional-limited military response to disrupt or destroy the base or the system that has caused or is about to cause further cyber-attacks sounds logically and acceptable under the recent *Ius ad bellum practice*.

Since both analytical models "effect based" and "strict liability" model advocated for elements that consider *ex-ante* use of force in the context of our debate it is worth mentioning the issue of anticipatory self-defense.

3.4 Anticipatory self-defense and cyber-attacks

The issue of anticipatory self-defense has been long debated among the legal scholars even in conventional terms. Measures undertaken in anticipatory self-defense are lawful when the "necessity of that self-defense is instant, overwhelming, and leaving no choice of means, and no moment for deliberation."[34] Since the vocabulary that explains what constitutes anticipatory self-defense differs from the course of article 51 of the Charter it is well accepted that anticipatory self-defense is considered as customary self-defense. Contrary to these views significant part of the legal community believes that self- defense should be practiced not outside the Charter.[35] Under these circumstances lawful *ex-ante* use of force (as "strict liability" or to a certain degree "effect based" analytical models suggest) would require victim state to sufficiently demonstrate the imminence of an anticipated attack. In the case of cyber attacks, such a requirement would invariably be difficult to meet, if not impossible.

The overall debate over the applicability of *Ius ad bellum* principles, standards and norms to cyber-attacks unequivocally showed that legal community is not united with these regards. Although under specific conditions cyber-attacks could amount to armed attack(s), it is very hard to attribute such attacks to a state or non-state actors. Additionally necessity and proportionality along with the *ex-ante* attitude (i.e. anticipatory self – defense) are highly disputed among the legal scholars. All of these challenges require for one to reconsider legal alternatives that could provide more appropriate solutions to cyber-attacks and cyber-security.

4. Building a Platform for Lawful Response to Cyber-Attacks

Much has been written about legal alternatives that could help to overcome some of challenges that cyber-attacks poses to our society and way of life. While some have focused on applicability of different bodies of law as a general approach to confront cyber-attacks, others have suggested that existing law is sufficient there those who have suggested that there is need for international legal reform. Nevertheless for analytical purpose in general the article classifies these alternatives in the so called military approach solutions, and non military. Although aware that recommendations which follow are not silver bullet to the complex challenges from cyber-attacks we believe that they could create incentives and give small contribution in the field where everyone is invited.

---

[33] *Yoram Dinstein: War, Aggression and Self-defense (4th ed. 2005) 237*

[34] *Lori Fisler Damrosch et al.: International Law: Cases and Materials 59 5th ed. (2009) 1135*

[35] *In fact, The UN World Summit Outcome Document of 2005 restates the international community's support for strict compliance with the "Charter rules on use of force"*

4.1 Brief overview on some of the military approach alternatives

One of the most disputed issues in applying *ius ad bellum* principles for self-defense as we discussed above is attribution. Several scholars have written on the subject. One of the well elaborated alternatives is the application of the "imputed responsibility".[36] The idea of imputed responsibility is that this it would apply not only to cyber-attacks conducted by a state's own citizens, but to all non-state actors who launch such attacks from within a state's territory. Applying imputed responsibility if cyber-attack occurs would launch two related questions: What is a state's duty to prevent cyber attacks?; and What constitutes a state's violation of this duty? Scholars advocating this alternative provide broad legal support that derives from variety sources of law and relevant institutions. Such as *international instruments* The European Convention on Cybercrime; *growing number of U.N. declarations* that have dealt specifically with cyber-attacks; The attitude of the U.N. General Assembly which has called upon states to criminalize such attacks; to prevent their territories from being used as safe havens from which to launch attacks and to cooperate in the investigation and prosecution of international cyber attacks; Case law (ICJ and ICTY practice) and Documents adopted by the International law commission. [37] Parallel to these views in the legal community there are serious calls for civilian legal approach alternatives to cyber-attacks.

4.2 Brief overview on civilian approach alternatives

Sofaer and Goodman argue that it has been easier to obtain agreement among the nations involved on standards and methods for regulating the civilian (commercial) aspects of a given activity than to obtain agreement on standards and methods for regulating the military (governmental) aspects of the same activity.[38] Additional arguments for civil approach come from the fact that nations under international law standards and principles have agreed on the need to protect some area of international activity such as airline transport, telecommunications or maritime activities. and also on standards for such protection. They may declare certain purposes collectively with regard to a given area of activity on which they agree, often in the form of a multilateral treaty, and then establish consensus-based multilateral institutions (generally referred to as "specialized agencies" composed of experts rather than politicians) to which to delegate (subject to continuous review) the task of implementing those agreed purposes. O'connel argues that "…*in general, international law supports regulating cyberspace as an economic and communications sphere and contains coercive means of responding lawfully to cyber provocations of all types*".[39] Under this logic many scholars argue that approach used to incriminate activities in this area will generally be lawful to use in the case of a cyber-attacks. To ensure safety in civilian aviation and maritime areas states have agreed to criminalize terrorist attacks, and to prosecute or extradite violators. These agreements are far from perfect. However it is common understanding that they are valuable instruments have enhanced security due to the virtually universal support given to protecting these activities from identified threats.

4.3 Recommendation for military legal alternatives against cyber-attacks

Even though well developed and promising this alternative have some technical and legal shortfalls. Without appropriate *framework* that could measure states agents' activities it would be naïve to believe that one could locate responsibility with ease in the cyberspace. This would reduce legal uncertainties and would frame state agents' activities so that it will established criteria under which could be achievable to locate state responsibility. Such criteria could be oriented to determine state behavior, involvement, attitude-incrimination of activities and investigations or request for international assistance even previous records etc. This recommendation also requires some improvement. Recommendation toward this direction starts with the ability to make *change in the communication standards*. The new standards should allow for information traffic flow monitoring and recording of the source, path and destination of the overall communication package. For this sender and receiver should agree in advance on how to judge the integrity of messages without relying on the path of the message. Legal challenges additionally steam from the core of the principle. The question for example is whether a state exercising all due diligence would be liable if transnational harm results despite the State's best

[36] *David E. Graham: Cyber Threats and the Law of War, Journal of National Security Law & Policy, Vol. 4, (2010) 93*
[37] *Ibid*
[38] *Abraham D. Sofaer and Seymour E. Goodman: A Proposal for an International Convention on Cyber Crime and Terrorism, Center for International Security and Cooperation, Stanford University,(2000)*
[39] *Marry E. O'connell, (2012), 7*

efforts.[40]

Some of the challenging issues could also be confronted by preventing them. Following the concept of this alternative, one could look for solution in the logic of traditional arms control theory. In this context *regulatory regime for cyber-attack* could contribute in reducing the likelihood of such illegal activities, the potential destructiveness and financial costs. International agreements to eschew the use of cyber-attack will reduce the likelihood of kinetic conflict in the context of our previous discussion - use of force in self-defense against cyber-attack. Measures toward this direction could consequently facilitate a more rapid cessation of cyber hostilities. Another benefit of a *formal agreement regarding use of cyber-attack* is that it can help to make explicit many of the concerns that military operators will have (or, at least, should have) in using cyber-attack as an operational weapon. If certain activities are prohibited, questions about whether or not an operator can engage in those practices would be easier to resolve. Signatory would have incentives to take suppressing actions in order to avoid undue and unwanted escalation by privet and non-state actors. Such regime could create space for coordinated unilateral declaratory policies. For example, the NATO states could collectively agree to refrain from using large-scale cyber-attacks against the entire critical infrastructure of an adversary nation as a matter of declaratory policy. Any such agreement (or discussions leading to such an agreement) will inevitably stimulate dialogue and debate regarding the topic of cyber-attack.

The challenges that traditional arms-control regime has are even more likely in the context of cyber-attacks. State might consider that is premature to enter into an agreement given the discrepancy between the state desirability of an agreement and the achieved level of development of technology or doctrine at the time. This is why the article supports the view that part of the legal community advocate, i.e. the civilian approach alternatives.

4.4 Recommendations for civilian legal alternatives against cyber attacks

Self-help under international law has been generally underestimated. The international law literature contains little on countermeasures as the lawful response to cyber-attacks. However, the absence of international police force and compulsory justice are starting point to build on the logic of self-help. Case law provides some incentives for state to employ countermeasures against cyber-attacks.[41]

Fostering ability to apply international jurisdiction sits well along the countermeasures against cyber-attack. Individuals and groups may be investigated and prosecuted under the domestic law of third state if the case meets the territorial principle (substantial effect in territory or actions happened in territory of the state); principle of active and passive nationality (violator or victim are states citizens); protective (severity meets the threshold of national security) and universality (crime is so severe that any nation state could apply jurisdiction - piracy, slavery genocide etc.)

Considering the complexity and interconnectivity additional indirect measures are more than welcome. *Efforts toward creating common culture and discipline* through international cooperation along with applying best practices could be a starter in contributing toward safer cyberspace. This will relax the atmosphere among the legal, policy and technical experts involved in the attribution process by *building a common lexicon* and understanding of issues and solutions. This however will not be achieved without *proper education and mindset among all users*. Precisely although International legal reforms could make states more liable for cyber-attacks at the end of the day our safety depends on the frontline computer and network security measures.

5. Conclusion

Progress in information and communication technologies has brought benefits and challenges. *Supervisory control and data acquisition*-SCADA systems provide efficiency and vulnerabilities. Asymmetric threats as a result have increased vulnerabilities to technologically developed societies. Urged by the security challenges some states have opened possibilities to use force in self-defense against cyber-attacks and have thus caused Shockwaves inside the legal community. While some supports the idea that *Ius ad bellum* principles, standards and norms are applicable to cyber-attacks, others offer legal solutions based on alternative bodies of International law. Since the legal community is not alone in disagreement with regards to cyber-attacks responses it is more than clear that International legal reform are needed. This reform must be holistic offering solutions that consider law, policy and technical issues. Changes should lead toward greater international liability providing background for attribution and appropriate technical solutions. Some

[40] *Alexandre Kiss and Dinah Shelton: Strict Liability in International Environmental Law, Tafsir Malick Ndiaye and Rüdiger Wolfrum, editors, The George Washington University Law School, (2007) 1131*

[41] *I.C.J: Gabcikovo-Nagymaros Project (Hung. V. Slovk.), Judgement (September 25 1997)*

indirect measures are welcome as well. Building the culture that would provide for common understanding of issues that have cased shockwaves is a promising alternative as well. Additionally this will encourage focus on appropriate security measures to protect the frontline computers. Although there are no silver bullet solutions and change means sacrifice practice has proven that all stake holders so far have its own "Achille's heel". Long-term and short-term political and economic interests have so far pushed international actors to find generally accepted solutions for their issues.

References

Abraham D. Sofaer and Seymour E. Goodman: A Proposal for an International Convention on Cyber Crime and Terrorism, Center for International Security and Cooperation, Stanford University,(2000)

Alexandre Kiss and Dinah Shelton: Strict Liability in International Environmental Law, Tafsir Malick Ndiaye and Rüdiger Wolfrum, editors, The George Washington University Law School

Bret Michael and Thomas Wingfiled: International Legal Reform Could Make States Liable for Cyber Abuse, Per Concoridiam, Journal of European Security and Defense Issues, Vol.2 Issue 2, (2011)

Charter of The United Nations, art.39, 41, 42 and 51, http://www.un.org/en/documents/charter/

Charles Dunlap: Perspectives for Cyber Strategists on Law for Cyberwar, Strategic Study Quarterly, Spring, (2011),

Daniel B. Silver, Computer Network Attack as a Use of Force Under Article 2(4), 76 Int'l Law Studies 73, (2002)

Davis Brown: A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict, 47 Harvard International Law Journal (2006)

David E. Graham: Cyber Threats and the Law of War, Journal of National Security Law & Policy, Vol. 4, (2010)

Definition of Aggression, G.A. Res. 3314, U.N. GAOR, 29th Sess., U.N. Doc. A/RES/3314 (Dec. 14, 1974)

Duncan B. Hollis: Why States Need an International Law for Information Operations, 11 Lewis & Clark L. Rev. (2007)

Eric Jensen: Computer Attacks on Critical National Infrastructure: AUse of Force Invoking the Right of Self-Defense, 38 Stanford Journal of International Law, (2002)

ICJ: Gabcikovo-Nagymaros Project (Hung. V. Slovk.), Judgement (September 25 1997)

ICJ: Military and Paramilitary Activities in and against Nicaragua, ICJ Cases (1986)

Jeffrey F. Addicott, "Cyberterrorism: Legal Policy Issues," in *Legal Issues in the Struggle against Terrorism*, eds. John N. Moore and Robert F. Turner, Durham, NC: Carolina Academic Press, (2010)

John Norton Moore: Development of the International Law of Conflict Management, in: John Norton Moore & Robert F. Turner eds. National Security Law 29, 2d ed. (2005)

Lori Fisler Damrosch et al.: International Law: Cases and Materials 59 5th ed. (2009)

Marco Roscini: World Wide Warfare, in: A. von Bogandi, R.Wolfrum, Max Plank Yearbook of United Nations Law, Vol.14, 2010

Marry E. O'connell: Cyber Security and International Law, International Law Meeting Summary, Chatham House (2012)

Michel Schmitt: Computer Network Attack and the Use of force in International law: The Columbia Journal of Transnational Law, Volume 37, (1999)

Michel Schmitt: International Law and the use of force: *The Jus ad Bellum*, The Quarterly Journal, Volume II, No3, September, (2003)

Niels Blokker, Nico Schrijver: The SC and the use of force Theory and Reality, Nijhof Publishers, (2005)

Office Of General Counsel, Department Of Defense: An Assessment Of International Legal Issues In Information Operations, (May 1999)

Peter Singer and Noah Shachtman: The Wrong War, Foreign Policy 21st Century Defense Initiative, Brooking, (2011)

Report of the New England Faculty Summit on Cyber Security held at Boston University on June 28, (2011)

Sean M. Condron: Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 Harvard J.L. & Tech., (2007)

Siobhan Gorman and Julian E. Barnes: Cyber Combat : Act of War, The Wall Street Journal, (May 30, 2011)

Sverre Myrli: NATO and Cyber Defense, NATO Parliamentary Assembly

Thomas Wingfield: The Law of Information conflict: National Security Law in Cyberspace (2000)

Thomas Wingfield: When is a Cyberattack an "Armed Attack?": Legal Thresholds for Distinguishing military activities in cyberspace, Cyber Conflict Studies Association, (2006)

Walter G. Sharp: Cyberspace and the use of force, Aegis Research Corporation, (1999)

Yoram Dinstein: Computer Network Attacks and Self-Defense, in: Michael N. Schmitt & Brian T. O'Donnell eds. Computer Network Attack And International Law, (2002), 99

Yoram Dinstein: War, Aggression and Self-defense (4th ed. 2005)