JICLT
Journal of International Commercial Law and Technology
Vol. 8, No.3 (2013)

Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective

Titiriga Remus*

Assistant professor
Inha Law School,
100 Inharo, Nam-gu Incheon
402-751, Korea
titiriga_r@yahoo.com

Abstract: This article highlights legal problems of cyber attacks from a 'jus ad bellum' perspective (international dispositions regarding the justification for entering a war). Since no international instrument whatsoever cover the cyber attacks the analogies with current international solutions are largely employed. We illustrate also the developments with relevant examples taken from main powers' doctrine and practice (US, Russia and China). The starting points are the provisions regarding the use of (armed)"force" under Article 2(4) and "armed attack" under Article 51 of United Nations Charter. The qualification of a cyber attack as use of "armed force" or "armed attack" is based a multi criteria threshold developed by Schmitt. Other developments focus the capacity of present International law concepts (direct and indirect armed attack, identification of the aggressor state, pertinence of pre-emptive or interceptive self defense vis-à-vis cyber 'armed attack', etc.) to answer cyber warfare's structures and challenges.

1. Cyber Means and Legal Perspectives

Computer attacks originate in the world of hackers, major actors in information revolution which began in the 50s and achieved its momentum in the following decades.

This 'milieu' developed, for the sake of it, for ideological proposes or for clear criminal aims a number of 'malware' techniques. The first step of the evolution was the advent of 'viruses' and 'Trojan horses' which allowed hackers to take control of someone else's computer in order to steal, alter or destroy information. The later spreading of the Internet allowed the upgrading of these techniques through 'viruses' and computer 'worms' that can multiply and spread throughout networks. In the meantime new 'network malicious techniques' (such as denial-of-service-DOS, distributed denial-of-service –DDOS or 'botnets') came into being.

By the end of the 80s the American Department of Defense became aware of the new threats. However the real menaces were considered the attacks committed outside the crime domain and perpetrated at international level (by a State, on behalf of a State by terrorists, etc.). The US military doctrine characterized[1] them as Computer Networks Operations (CNO) under three different branches:

- Computer Network Attacks (CNA) were defined as operations to disrupt, deny, degrade, or destroy information resident in computers, computer networks, or the computers and networks themselves.
- Computer Network Defences (CND) were defined as defensive measures to protect and defend information, computers, and networks from disruption, denial, degradation or destruction. They used security measures that seek to keep the enemy from learning about own military capabilities and intentions.2

[1] *Information operation* Joint publication J-13, 13 February 2006, available from: *www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf*.
[2] NSPD 16 [Guidelines for Offensive Cyber-War Fare] (2002) (C) DOD, available from: *www.information-warfare.info/*.

- Computer Network Exploitations (CNE) covered the collecting and monitoring of enemy's information. Usually they involve espionage performed with tools that penetrate systems and return information or copies of files enabling the military to gain an advantage over the enemy.

If the US made the first steps in the field they were soon followed by Russia and China.[3]Russia considers the cyber means an asymmetric method for challenging US warfare supremacy, as part of a total warfare approach.[4]

The Chinese military doctrine is similar. For example Wang Pufeng, general of the People's Liberation Army, considers that "our war strategies must adapt to the needs of the war information. We must make multiple uses of force and, especially, of non-linear war and methods of multiple information warfare".[5]

1.1 International Legal Framework for Analyzing Cyber Attacks

Cyber-attacks are mostly perpetrated by hackers who are private citizens. These kinds of actions entail penal or civil-law remedies at national level. If there are some transnational dimensions, specific remedies may be found at international level. In this respect the Convention on Cybercrime[6] is the first international treaty seeking to address computer and internet crimes by harmonizing national laws, by improving investigative techniques or by increasing cooperation among nations.

However our aim is to study cyber means from the international point of view: cyber-attacks perpetrated by States or, generally, on behalf of States. This point of view relates to International Law of armed conflicts. A choice should be made here between 'jus ad bellum', (body of international law governing the resort to force as instrument of national policy) and 'jus in bello' (body of international law regarding State's conduct during a war). We have decided to analyze cyber means from the perspective of 'jus ad bellum' since such developments remain, at least by now, less speculative.

The evolution of the International law of armed conflict demonstrates a slide from 'jus ad bellum' – the law governing the recourse to force – to a real 'jus contra belum', the coming out of rules prohibiting the resort to war. In this respect the Kellogg-Briand Pact of 1928, [7]was the first comprehensive prohibition of resort to war. After WWII the UN Charter extended the condemnation of war to a general prohibition for the threat or use of force, in its Article 2(4). Contrary to Kellogg-Briand Pact, the UN Charter incorporates an express exception regarding the right of self-defense and defines the circumstances of this right.

The legal structure built around United Nations Charter (the interdiction for use of force and the subsequent exception of self-defense) will provide the basics for our analysis. Without any precedents or any specific sources of International law regarding cyber-attacks as warfare, the research should be based on analogies with existing phenomena (the classic use of armed force or armed attacks, the classic use of self-defense, etc.).

Since cyber instruments have a number of particularities[8]vis-à-vis classic warfare tools, the accuracy of analogy should be weighted each time very carefully. The analysis will focus the cyber-attacks as

[3] Attention will be focused on these countries as they seem to be real competitors in international cyber - arena.

[4] ."We are approaching a stage of development when no one is a soldier anymore but everyone is a participant in combat action. The task now is not to inflict losses in men and materiel but to thwart in enemy's plans, demoralize it, undermine its worldview, and destroy its intrinsic values." Cf. Maj. Gen. G.A. Berezkin Deputy Head of the Russian Federation Defense Ministry Center of Military-Technical Information Studies, Military Thought (May 1, 2003).

[5] "China Military Science" Spring 1995.

[6] The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it has entered into force on 1 July 2004. Significantly, Russia and China never sign it.

[7]. Q. Wright, 'The meaning of the Pact of Paris', *(1933), 27 A.J.I.L.* 39-61, 42-43.

[8] It is very important to understand that cyber means are dual-use tools since they can be used either offensively or defensively - depending on the intention of the user (CNA and CND and CNE are differentiated according to function and not to their structure). The cyber means are easy to use with high degrees of anonymity and with plausible deniability, making them suited for covert operations and for instigating conflict between other parties. The cyber means are also uncertain of the outcomes they produce, making difficult to estimates the deliberate and the collateral damage.

offensive cyber means[9]but will take in consideration, where appropriate, other types of information operations (IO).

2. Computer Attacks as Warfare: ' Rationae Materriae' Criteria

2.1 'Ratione Materiae' Feature: Computer Attacks Qualifying as "Armed Force"

Article 2(4) of UN Charter, declares 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" [emphasis added].

This prohibition, as a customary rule of *jus cogens*, is applicable to all States, whether or not members of the UN.

The scope of Article 2(4) may be discovered through its *travaux preparatoires*. During the negotiations of the Charter, the Brazilian delegation proposed a reference to 'armed and economic force', but this proposal was later rejected. [10]Today it is a general agreement in doctrine that the "use of force" covers "armed force" and not economic or psychological pressure. [11]On the basis of the above explanation we can proceed to derive the first legal characteristics of cyber warfare.

If cyber means in their direct appearance could be assimilated to armed force, any further discussion would be superfluous, since Article 2(4) undeniably encompasses "armed force".[12]

An example might be the operation Orchard, an Israeli air strike on a supposed nuclear facility at Deir ez-Zor in Syria, carried out on September 6th 2007. [13]According to *Aviation Week and Space Technology*, U.S. industry and military sources speculated that the Israelis may have used a technology similar to America's Suter airborne network attack system to let their planes pass undetected by radar into Syria. Suter is a military computer program developed by BAE Systems for attacking computer networks and communication structures belonging to enemies. Three generations of Suter have been developed. The last one, Suter 3, tested in summer of 2006, enables the invasion of links to time-critical targets such as battlefield ballistic missile launchers or mobile surface-to-air missile launchers. It seems that high-energy beams act as universal 'back doors' [14]for entering enemy's military networks.

The above situation could have been easily qualified as cyber 'armed force' if the Israeli attack would have been an expression of 'jus ad belum" (if it was the first blow of a new war). That was not the case, since the two countries never concluded a peace treaty after Yom Kippur's war of 1973.

Beside these situations of cyber-attacks covered by "armed force" characterization, there are some problems regarding the cyber means not entering these classical definitions.The doctrines proposed different solutions to handle such circumstances:

i) Textual limitation ('armed attack' limited to classical military instruments)

One approach, popular in academic circles, followed the logic of the Charter to its literal conclusion: anything other than an "armed force" will be allowed. In other terms, the quantity of force is less important than its quality. Military coercion might be discouraged while diplomatic, economic, and political coercion should be tolerated as peaceful alternatives to a full blown war. Therefore the cyber-attacks that are not clearly "armed force" should be permitted by 'jus ad bellum' (even if they can be banned by other provisions of international law).

[9] We may use the term 'cyber attack' to designate 'computer network attack' (CNA). We may also use 'cyber exploitation' to designate CNE and 'cyber defense' to designate CND.

[10] A. Randelzhofer, "'Article 2(4)", in B. Simma et al. (eds.), *The Charter of the United Nations: a commentary* (Oxford: OUP) (2002; 2e ed.), pp. 107-128, 112-113.

[11] . Y. Dinstein, *War, aggression and Self-defense* (Cambridge: CUP) (4th ed.: 2005), 86.

[12] The cyber-attacks qualifying as "armed force" might resemble to hacker's techniques already examined but with a more direct military impact. A cyber-attack may deliver a 'weapon' via the host country's Internet or "beam" the weapon to a target directly from an aircraft (by manipulating the power system or by using high-energy radio frequencies).

[13] John Leyden "Israel suspected of 'hacking' Syrian air defenses", Posted in Enterprise Security, 4th October 2007 15:17 GMT, available from: *www.theregister.co.uk/2007/10/04/radar_hack_raid/*.

[14] A backdoor of a computer system is a method of bypassing normal authentication, and secure remote access to a computer while attempting to remain undetected.

This approach, despite the advantage of a certain academic purity, fails to address the newly destructive capacities of cyber-attacks.

ii) Destructive outcome as touchstone

A different idea tried to apply the legal regime of classic warfare to cyber-attacks by ignoring the means of attack and by focusing only the amount of damage. It must be irrelevant whether a factory was destroyed by a bomb or by a malicious code. What really matters is the scale of destruction left after such an attack.

In this respect Sharp [15]proposed a simple rule: ″Any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce the effects of an armed attack prompting the right of self-defense".

Facing the problem of determining whether the term "destructive" means only physical destruction or includes economic harm, Sharp suggests that, in some circumstances, it may cover the latter.

He considered that Article 2(4), while not including all coercive economic and political sanctions intended to influence another State policy or actions, envelops coercive political and economic sanctions threatening the territorial integrity or independence of another State.[16] Therefore a non-physical destructive effect (such as a disruption of financial markets) should be considered force under Article 2(4) if it is sufficiently serious to threaten the target State's territorial integrity or independence.

This conclusion weakens the whole idea and seems incompatible with the weight of legal authority or the international doctrine.

iii) Schmitt's answer: characteristics of "armed force" are the touchstone

The standstill was overcome by Schmitt [17] who proposed a particular solution. He suggested that the analysis of cyber-attacks must fit into traditional instrument/consequence frame of reference, by verifying whether a cyber-attack meets the criteria that distinguish armed force from political or economic coercion.

Schmitt recognized that within the existing structure of international law, cyber-attacks will be considered 2(4) "force" only when they sufficiently resemble "armed force". He observed that traditional notions of force are instrument-based: the Article 2(4) prohibition of using a particular instrument, namely military force, against another State is coupled with the high degree of connection between its use and consequences, primarily physical destruction and injury. That explained why armed force, which almost always results in physical destruction or injuries, was prohibited, whereas economic or political coercion, whose link to expected physical destruction or injury is weak, was not.

Schmitt gathered a number of criteria to verify whether cyber-attacks are more or less close to 'armed force'. These criteria, he suggested, are: *severity*-the higher threat of physical injury or property damage associated with armed force; *immediacy*-the comparative speed of harm arising from armed force, as compared with other forms of coercion; *directness*-the relatively direct connection between armed force and negative consequences, as compared with other forms of coercion; *invasiveness*-the fact that in case of armed force the act causing harm generally crosses into the territory of the target State whereas measures of economic or political coercion normally do not; *measurability*-the greater ease and certainty of evaluating the consequences of armed force as compared with other forms of coercion; and *presumptive illegitimacy*-the fact that violence is presumptively illegal under domestic and international law, while most (or at least many) techniques of economic and political coercion are presumptively legal.

By applying a quantitative scale to each of these factors, any cyber operation may be described as being closer to one end of a spectrum or to another (armed force versus economic or political force)[18].

[15] Walter Gary Sharp, sr., *Cyberspace and the use of force*, Falls Church, Va, 88-91 (1999).

[16] Walter Gary Sharp, sr., idem, p 89-91.

[17] Michael N. Schmitt "Computer network attack and the use of force in international law: thoughts on a normative framework", *Columbia Journal of Transnational Law* 37, 1999, 885.

[18] Schmitt compared two hypothetical uses of cyber-attack (CNA). In the first case CNA is used to disable an air traffic control system, causing airplanes to crash. According to Schmitt, this meets his criteria and qualifies as 'force'. In the second example, the attacker destroys a university computer network for purposes of disrupting military research being conducted on campus. That does not meet the test and does not qualify as 'force'. Schmitt suggests that there should be a different result for the attack on the university because the desired outcome, diminished capacity on the battlefield, is too remote from the CNA and too dependent on indeterminate factors.

As a result Schmitt's analysis which translate the qualitative charter's paradigm into its quantitative components, provided the best framework for both scholars and practitioners alike.[19]

In practice the Pentagon seems to apply Schmitt's analysis on a day by day basis vis-à-vis cyber-attacks. For example in the summer of 2006, the Pentagon lost most of its telecommunications links to North and Central US. Its analysts were trying to find the cause of this default when, 15 minutes later, they also lost all connections with the Southern central US. It was proved to be an accidental occurrence: a construction crew in Kansas City, Missouri, had dug up a bundle of fiber-optic cables with an earth mover, tearing apart 150 interstate "fat pipes". By coincidence, an unrelated construction crew in Oklahoma City did the same, breaking 400 more large pipes. Together, they cut interstate communications for 36 hours. Using a "Schmitt's analysis" a Pentagon cyber task force had determined that this was probably not a cyber 'armed attack'[20]

2.2 Cyber Means under Concept of "Armed Attack"

The following discussion is linked to a different threshold, this time in relation to self-defense. The UN Charter allows a major exception to the prohibition of '(armed) force' in Article 51, which asserts that "[n]othing in the present Charter shall impair the inherent right of …self-defense if an *armed attack* occurs …" (emphasis added). This disposition is important because once the threshold of "armed attack" is attained it allows the victim-State to respond with legitimacy in military terms.

The choice of words in Article 51 is restrictive. Since Article 2(4) of the Charter forbids the "use of force" while the Article 51 allows self-defense only against an "armed attack," a gap is obvious between the two notions ("[armed] force" vs. "armed attack").

The term 'armed attack', undefined by the Charter, was partially explained by the ICJ in *Nicaragua case*.[21] The Court made clear that armed attacks need to achieve a *minimal level of severity*, by distinguishing the 'gravest' forms in the use of force (those constituting an "armed attack") from other less severe forms [emphasis added].

Additionally, in the same case, the Court distinguished 'armed attacks' from 'mere frontier incidents'.[22] The distinction does not exclude *a priori* that armed confrontations near a border may – alone or cumulatively – reach the level of 'armed attack'. However this seems to imply that incidents without an 'offensive' intent, such as coincidental border incursions, do not trigger recourse to self-defense.[23]

Several other features of 'armed attack' remain controversial. For certain authors an 'armed attack' supposes at least 'a use of force producing…*serious consequences*, epitomized by territorial intrusions, human casualties or considerable destruction of property'[24] [emphasis added]. Consequently the use of force not reaching this high intensity may give rise to non - violent countermeasures, but not to self-defense.

One can adapt these distinctions to cyber-attacks. In order to qualify a cyber-attack as an "armed attack", the only criteria to be retained is the threshold of "severity" and /or "serious consequences" (the criterion of 'offensive intent shown by crossing the border' seem useless here, since the territory and the borders play a minor role in cyber-attacks).

We can go back and observe that this criterion (*serious consequences)* is covered by the *severity* condition in Schmitt's analysis. Therefore the analysis already accomplished in qualifying a computer attack as "armed force" need only an upgrade (to cover a higher 'severity') in order to qualify an "armed attack". All other elements developed for the "armed force"will remain the same. In this way the gap between article 2(4) and article 51 of UN charter will be covered even in case of cyber (computer network) attack.

[19] See James B. Michael & Thomas C. Wingfield & Duminda Wijesekera "Measured Responses to Cyber Attacks Using Schmitt Analysis" *Proc. Twenty-seventh Annual Int. Computer Software and Applications Conf., IEEE* (Dallas, Tex., Nov. 2003).

[20] See for details Paul Marks "Cyber-attack, a clear and present danger", *New Scientist,* 4 March 2009, 18.

[21] "Case concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America)", Judgment of 27 June 1986, *(1986) I.C.J. Rep.* 14, par. 191,195.

[22] Nicaragua case, *loc. cit.,* supra, par. 195.

[23] . C. Gray, *op. cit.,* supra n. 146.

[24] See Dinstein Y., *op. cit.,* supra n. 193.

3. Specific points where the lega framework is stretched to the limit in dealing with cyber attacks.

3.1 'Ratione Personae' Difficulty for Applying Standard International Framework: Attribution of Cyber "Armed Attack" to a State

Determining through Schmitt's analysis that a cyber-attack (achieving the threshold of 'armed force' or 'armed attack') took place is not enough. The cyber-attacks had to be perpetrated by a State or on behalf of a State-a condition relating to the origin of attack '*ratione personae'*.

i) Indirect attacks

This concept was always broadly interpreted by international doctrine in order to include not only attacks carried out by States, but also attacks perpetrated by private actors for whom States had a responsibility. This second category was described as 'indirect military aggression', as opposed to 'direct' military aggression, carried out by State agents.[25]

The distinction was recently confirmed by the ICJ in *Nicaragua* case, where the Court recognized that 'armed attacks' covered (beside classical definition examined above) also "the sending by or on behalf of a State of armed bands, irregulars or mercenaries carrying out acts of armed force as well as a State's substantial involvement therein, provided the scale and effects of the attacks exceeded those of mere frontier incidents"[26]

These distinctions cover the terrorist acts. Frequently the perpetrators of 'classical' terrorist attack leave no signature. Since States sponsoring terrorists usually try to hide their roles, holding such States responsible for the offenses may be difficult. Prior to determining its options, the victim - State must establish a link between the terrorists and their sponsoring State.

Computer network attacks invite a similar approach since the cyber means are, by nature, easy to use anonymously and with plausible deniability, making them suited for covert operations and for instigating conflict between other parties.

A related interesting experience exists in the US. In the last two decades it was said a lot about cyber terrorism attacks that can break US infrastructures with smallest expenses for the terrorists. It was believed that a group of skilled and determined persons may inflict a blow to military facilities and accomplish a sort of Pearl Harbor in cyber space.

However no attack of this magnitude ever happened. In this respect Virginie Vacca, expert at European Company of Strategic Intelligence, recalls[27] the results of a «Digital Pearl Harbor» exercise organized in 2002 at the US Naval War College. In order to launch a great cyber-attack the pirates (terrorists) would need 200 billion dollars, at least 5 years of preparation and their offensive would not produce huge human losses or any other catastrophic consequences.

Nevertheless these expenses seemed affordable to a foreign power. As a result, if the threshold of "armed force" or "armed attack" is achieved by a terrorist cyber-attack there will be a, at least, a strong presumption of a foreign State implication.

ii) .Passively tolerated terrorist attacks

There is something more. Sometimes a State A, constrained by political or military considerations, would passively tolerate the use of its territory as a base for activities of terrorists against a victim-State B, without actively sponsoring those activities or even encouraging them.

Such a situation will not cover the terrorists with the veil of protection from State B. As in the *Caroline* incident of 1837[28], State B may legitimately invoke self-defense to use counter-force within the territory of State A - targeting armed bands which use that territory as a launch pad for operations against State - when the host government remains inert.

[25] See P.L. Zanardi, 'Indirect military aggression', in A. Cassese (ed.), *The Current Legal Regulation on the Use of Force* (1986), 111-119.

[26] *Nicaragua case, loc.cit.*par.159.

[27] Thevenet Cédric, «Cyberterrorisme: mythe ou réalité?», available from: *www.terrorisme.net/pdf /2006_Thevenet.pdf.*

[28] In 1837 the British attack *Caroline*, a ship used by US citizens to assist Canadian rebels. This ship was anchored in an American port at the time of the British attack.

iii) Identifying the origin of the attack in general

The second problem is to clearly identify the State that launched (directly or indirectly) a cyber-attack. The point from which the attack happened might not be inside the territory of the State that initiated the act (for example the use of proxies or 'botnets' may hide the origin of an attack). And a most effective form of computer network attack is expected to hide even the fact that it ever occurred, leaving the victim - State in doubt as to whether the affected computer network was externally attacked or simply failed for other reasons.

In this situation the result of Schmitt's analysis might be essential. If the attack attained the threshold of "(armed) force" or "armed attack" it should always be (apart from an accidental general failure) the act of a State. Any aggression beginning with a cyber-attack (a "jus ad belum" perspective) should be evaluated by taking in consideration the political interest ('qui prodest?') or the 'casus beli' of the unknown attacker. Such an attack will most obviously happen after an international political crisis. As a result, a political and military analysis may diminish the circle of suspected States.

In the meantime future advances in technology may ease the identification of attackers (in the past, specific technologies enabled, for example, the determination of the source for incoming telephone calls). Therefore the answer to the identification problem lays on technological progress and a careful political analysis of international circumstances.

iv) Some examples

Some interesting illustrations may be found in relation to Russia and China. If details about Russian cyber warfare doctrine seem hard to find, the practice of this great power in the matter seems highly significant.

After Estonia relocated a Soviet World War II memorial in April 2007, the country suffered widespread attacks which suddenly disabled websites by overloading the server's bandwidth. Among the servers targeted were those hosting websites of the Estonian president, major Estonian news agencies, government ministries, and two of the country's largest banks·Estonia, as an extremely advanced and informatics-based society, was likewise very insulated from outer networks. Therefore this was an ideal occasion for Russia to test Estonia's and its NATO allies' abilities to resist a cyber-attack[29]

If these attacks would have attained the threshold in Schmitt's analysis, Estonia would have been entitled to act in self-defense (and all other members of the NATO alliance would have had to act through the collective defense mechanism). However that level of 'armed attack' was not reached.

And even if Schmitt's analysis would have qualified these denials of service as "armed attack", the last step, their attribution to a State (Russia), was very difficult to prove. Attempts to track back the origin of attacks revealed that, at least some of them, had Russian origins (were alleged as emanating from Russian state institutions).

Apparently the cybercrime seems to be developed in Russia. The relations between Russian security forces and the movements and networks of cyber mobs or patriotic 'hacktivists' may be based on a tacit pact of non-aggression and, eventually, 'ad hoc' cooperation. For example, an activist within a pro-Kremlin youth group recently recognized that he and his friends were behind the electronic attack on Estonia that paralyzed the NATO Internet network.[30] The creation of this youth group was attributed to Kremlin officials and its activists have met former President Vladimir Putin. This cyber crowd seems to act as a 'reserve army' which can be mobilized to a full blown cyber-attack if needed· [31]. Nevertheless the state implication is very difficult to prove and therefore is still a highly controversial topic.

[29] The attack was more than just an inconvenience for the Estonian population: the emergency number, used to call for ambulances and the fire service, was unavailable for more than an hour. No State or terrorist group claimed responsibility after the attack, but analysts believed the complexity of the attack required the cooperation of a State and/or several large telecom firms.

[30] The group is called Nashis and stages regular protests outside the embassies of Western States with which the Kremlin has disagreements. More details available from: *en.wikipedia.org*/wiki/Nashi(youth_movement).

[31] The next occurrence of a Russian cyber-attack was linked to the Russian-Georgian conflict in August 2008. It seems that forces within Russia launched a coordinated cyber-attack against Georgian web sites that coincided with ordinary military operations. The solution to incoming attacks was found when Google had provided to Georgia its network facilities and bandwidth. Google had such a tremendous network power that all efforts to isolate Georgia with over saturation were drowned in a bandwidth 'ocean'. More details available from: en.wikipedia.org/wiki/2008_South_Ossetia_war.

Finally it was almost impossible (and equally politically sensitive) to prove the indirect implication of Russia. [32]And even if this implication would have been proved it would have been very dangerous to act in self-defense through classical or cyber means since any escalation could have produced immeasurable consequences.

In China the situation is similar. If the Communist Party is unforgiving about protests and political dissent, it is less strict against cyber-crime. Hacker associations which involve thousands of members-like the Red Hacker Alliance's or the China Union Eagle - regularly target sites pro-Tibetans, pro-Uighurs, and pro-Falun Gong and frequently attack Taiwanese, Indian, European and American government's servers.

If ordinary criminals are doing it for money, these hack-tivists or cyber military pirates ('corsairs') may do it for glory. All these groups are suspected of being used by Chinese Army and may act, as in Russia, as a 'reserve army' very useful in a non-linear (or asymmetric) war.

In both situations if these hack-tivists would lance a cyber-armed attack satisfying the threshold in Schmitt's criteria – an almost impossible feat, as we already saw- these countries should be considered responsible and may suffer the consequences of a legitimate military self-defense. If these cyber-attacks do not achieve the threshold of 'armed attack' they must be considered as raising problems of International law (state responsibility) or International criminal law.

One can see that technical, legal or political analyses should be always balanced with strategic choices in this highly sensitive matter.

3.2 'Ratione Temporis' Conditions for a Cyber "Armed Attack" Triggering Legitimate Defense

The analysis will focus here just the self-defense. In this respect the timing for a self-defense triggered by an "armed attack" is a different critical element. A self-defense can be triggered at different moments "vis- à- vis" an "armed attack":

i) Anticipatory self defense

First it is necessary to examine whether a computer attack must already have occurred in order to trigger the right of self-defense (whether the self-defense may be or not *anticipatory*). For classical armed attack this question is the source of a controversy between two groups of scholars.

The first and the largest group has traditionally rejected anticipatory self-defense by a literal interpretation of the phrase 'if an armed attack occurs' and on the ground of the fact that, as exception to a general prohibition of force use, Article 51 of the UN Charter should be interpreted narrowly.

The opposing side argues that the reference to 'inherent' right of self-defense preserves ancient customary law, which allowed the anticipatory action.[33] Proponents of a broad reading of self-defense invoke the 1837 *Caroline* incident and suggest that in the nuclear era States cannot be expected to wait for a 'first strike'.

However the majority of scholars reject the precedent value of the *Caroline* incident based on the fact that it precedes the actual interdiction for the use of force. [34]They warn of the risk of escalation that results from accepting anticipatory actions.

We think that the latter reason should prevail in the case of cyber-attack and as such, anticipatory self-defense should be clearly banned.

ii) Interceptive self defense

If an armed attack is incipient or is on the verge of beginning, the intended victim may not wait powerlessly for the inevitable blow. The attack can be legitimately intercepted. In fact interceptive (different from anticipatory) self-defense seems to be acceptable under the Charter.[35]

[32] See Jurich, Jon P "Cyber war "Customary International Law: The Potential of a 'Bottom-up' Approach to an International Law of Information Operations", *Chicago Journal of International Law*, available from: *http://www.allbusiness.com/technology/software-services-applications-internet-social/11461870-1.html*.

[33] Bowett D.W., *Self-defense in international law* (Manchester: Manchester University Press) (1958), 188-192.

[34] See Brownlie I., *Principles of Public International Law* (Oxford: OUP) (2003; 6e ed.), 701-702.

[35] Dinstein Yoram "Computer Network Attacks and Self-Defense", *International law studies [Symposium on Computer Network Attacks and international law (1999 Naval War College)]*, vol. 76, 2002, 99.

The theme of interceptive self-defense is pertinent to a computer attack when the intrusion into a computer network has been discovered, although it is not yet lethal to persons or destructive of property (using Schmitt’s analysis). The issue is to determine whether the intrusion may reasonably be seen as a first step of an unavoidable and developing ‘armed attack’. This is a very difficult matter of evaluating and interpreting information available at the time of action (including warnings, intelligence reports and other data).

4. New Horizons and Challenges

In the following section we will lance a debate about possible use of cyber means as self-defense or over the boundaries of the classical international paradigm (armed force or armed attack). There are numerous theoretical and practical challenges to be relived in this exploratory topic.

4.1 Computer Attacks as Means of Self Defense

If a preceding armed attack (or a computer attack qualified as ‘armed attack’ –according to Schmitt’s analysis) occurred, the possibility to use the computer attacks as legitimate defense seem obvious (legitimate defense allows the use of all military means against an aggression therefore the cyber means should be included).

However there are two substantive constraints for the right of self-defense: the criteria of *necessity* and *proportionality*. In the *Nicaragua case*, the International Court of Justice acknowledged the ‘inherent’ right of self-defense as part of customary law. The Court recognized the two criteria, ‘necessity’ and ‘proportionality’, as additional requirements under Article 51.[36]

i) ‘Necessity’

‘Necessity’ means that no alternative way of redress may be available and the target should be a military one, in agreement with the rules of International humanitarian law (“jus in bello”). Likewise, ‘necessity’ requires that the timing between the armed attack and the recourse to self-defense to be reasonably short, taking into account the need to carry out investigations and/or negotiations, or to make military preparations (this is an upper time limit while the above discussed interceptive self-defense concerned the lower time limit).

ii) ‘Proportionality’

‘Proportionality’, on the other hand, supposes that the use of self-defense will be weighed against initial armed attack(s), not only in terms of gravity/intensity, but also in terms of duration, location, and range of selected targets.

And here lays a real problem for cyber-attack qualifying as self-defense. Computer attacks are naturally uncertain as to the outcome they produce, making difficult to estimate deliberate and collateral damage. In fact the consequences of a cyber-attack may be both direct and indirect, and in some cases the indirect consequences can be higher than direct consequences.[37]

As result it is very difficult to fulfill the criteria of proportionality in case of a self-defense by way of cyber-attacks. The risk of escalation should prevent this use of cyber-attacks in the present international framework. An eventual solution may be revealed by technological breakthroughs that will allow controlling the outcome of cyber-attacks. But this kind of technological evolution is far from being assured yet.

[36] These criteria originated in the diplomatic exchange of letters following the British attack of 1837 on the *Caroline*. The Secretary of State Webster requested his British counterpart to “show a necessity of self-defense, instant, overwhelming, leaving no choice of means, and no moment for deliberation”. This standard, which was agreed upon by the United Kingdom, became known as the *Caroline* doctrine

[37] During the first war on Irak in 1991 U.S. and the coalition forces did not used computer network attacks against Iraqi systems. U.S. forces may have rejected launching a planned cyber-attack against Iraqi financial computers because Iraq’s banking network was connected to financial networks located in Europe. A cyber-attack directed at

4.2 Difficulties on the Boundaries of Classical Paradigm: Cyber Means Not Qualifying as "Armed Force" or "Armed Attack"

Much more appealing might be an analysis of the use of cyber-attacks in response to an initial act (a computer network attack) not achieving the threshold of "armed attack" (Schmitt's criteria).

i) Computer network attacks not achieving the threshold of "armed attack"

If an initial (cyber) attack does not reach the threshold of an"armed attack" there is no right of self-defense. We should examine the case of a computer attack used in retaliation short of the right to self-defense. This situation is not purely hypothetical since there are plans to use computer attacks as counter offensive instruments.

For example Col. Charles W. Williamson [38] argued that an Air Force-controlled 'botnet' could be a cost-effective mean to protect military networks. He envisioned collecting computers that would otherwise be discarded and remove their hard drives by making them available to launch attacks against foreign-based computers targeting American military facilities. To prevent collateral damage this 'botnet' would have built-in filters preventing US military and government computers from being targeted.

We think that Schmitt's threshold of an "armed attack" by cyber means (and the corresponding right to self-defense) is not attained in the example above. At this point we are considering a non-military 'retaliation'. However this kind of action brings up tremendous risks for cyber escalation linked to the obvious indiscriminate nature of computer attacks. All those affected by this computer retaliation may react with devastating (deliberate and collateral) effects to networks. This outcome could, by aggregation and escalation, finally trigger a classical armed conflict.

The dangers are too high to consider this kind of action.

i) The exception of espionage and the challenge of multi-purpose nature of cyber means

If there is no destructive outcome (lacking the threshold in Schmitt's analysis) the cyber means could be covered by the espionage exception in interstate relations. These are harmful actions (not illegal from the point of view of armed conflict) that each state use constantly.

Nevertheless some problems related to the nature of cyber means remain unclear. Cyber means are by nature multi-purpose tools ('weapons'). The methods used for computer network exploitation are similar to those used for computer network attack, but configured for different objectives.

For example the Wall Street Journal claimed [39] that some agents from China and Russia, along with several other countries, had infiltrated computer systems charged with managing electricity in the US. They left behind software which could be used to control or disable electric grids of the country. Security experts stated that while the incident showed gaps in the US security infrastructure in time of conflict, such an attack could have catastrophic effects. In this case, a cyber-activity (intelligence-gathering) can easily become, if undetected, the ground for a future cyber-attack.

In situations like this, the only solution for the offended State is to use its own cyber exploitation or cyber defense instruments while the use of computer attacks in retaliation would be the least reasonable choice (even less reasonable than in the above example of cyber retaliation to a previous computer attack not qualifying as "armed attack").

This is another example where classical armed conflict framework seems unable to cover certain cyber means characteristics.

5. Conclusion

The main pillars of legal analysis were the provisions regarding the use of "force" under Article 2(4) and "armed attack" under Article 51 of United Nations Charter. The characterization of a cyber-attack as "armed force" or "armed attack" was based on a multi criteria threshold developed by Schmitt and

Iraq's facilities could have brought down banks and systems located in allied countries. The same situation happened in the case of NATO vs. Serbia conflict of 1998 or in the second war on Irak of 2003.

[38] Dan Goodin, "Enemies reduced to 'hunks of metal and plastic'", *San Francisco Posted in Government*, available from: http://www.theregister.co.uk.

[39] Shaun Nichols, "The Chinese government is denying any involvement in the reported infiltration of US electric grid systems", in *San Francisco, vnunet.com*, 10 Apr 2009.

grounded on its 'destructiveness'. Some other challenging aspects were also explored (the proof of state implication, the preemptive or interceptive self-defense, etc). We uncovered the inherent difficulties for characterizing cyber-attack under the actual framework of armed conflict.

On empirical side, major nation-states with significant capabilities of kinetic and cyber-attack at their disposal (as the US, Russia and China) are aware of international stability. The evolution of real cyber-attacks shows these States acting hidden behind private actors (in the case of Russia or China) or using highly specialized military forces (in the case of the US). Nobody is willing to escalate computer network attack to match the "armed attack" standard (according to Schmitt's criteria) and to risk triggering a legitimate defense and eventually a full blown war. Therefore one may qualify all these uses of cyber means as "cyber warfare" only as metaphor. Under the actual international normative framework most cyber acts that can be (loosely) linked to a State belong to cyber exploitation. This is in fact a new secret terrain that increases the reach of States.

One can reasonably hope that States with cyber facilities will achieve by these new means their political aims and will stop riskier developments toward a real 'cyber warfare'.

.* * * * *

Cite as: Remus. Titiriga. Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective.*Journal of International Commercial Law and Technology,* Vol.8 No.3 (July, 2013)