International judicial aspects of cyberdefense : first views.

Barbara LOUIS-SIDNEY[♣], *Oriane BARAT-GINIES*[♦], *Cécile DOUTRIAUX*[♠], *EVE TOURNY*[♥], *Eric POMES*[*], *Jean-Yann MARIE-ROSE*[#]

October 2013 – Article n°III.11

Summary: *Like any other space, cyberspace, born in the interconnection of computer networks, is a field for conflicts. This fifth conflict field, characterized by its multiple dimensions, increases threats and hostile modi operandi, by renewing them. Now, these cyberattacks*[1] *do not have a normative definition yet. This absence of definition and the newness of these attacks bring us to consider their qualifications with regards both to jus in bello and jus in bello.*

Cyberspace was created by the growth in interconnections between global computer networks. Some see in it a new territory, a new space in the geographical sense. Its importance is such that it would now have become the 5th battlefield, after land, sea, air and space. Despite obvious reality, cyberspace creates problems for lawyers. No normative definition has been agreed upon, for the moment, in an international law instrument.

Attempt to qualify cyberspace

Before setting a definition, defining its composition seems wise. Cyberspace would not be a single environment but a space, composed of several dimensions.

The first dimension, often neglected, is physical. It encompasses the structures of the network of networks, which is the Internet (root servers, databases, satellites, submarine cables, optic fibers, cables and hard drives…). These infrastructures are often critical. Then comes the logical dimension. This one gathers the network's software and protocols. It is the main target of computer attacks. Finally, one finds the cognitive dimension, which is composed of

♣ Doctor in law
♦ Doctor in law.
♠ Lawyer, citizen reserve's officer for the gendarmerie and above all chair member of the cyberdefense chair of the St-Cyr schools.
♥ Doctor in law.
* Doctor in law, Institut Catholique d'Etudes Supérieures, associate director at the CERDES, EA n°3180, Nice Sophia Antipolis university and at the CREC Saint Cyr.
# Army officer, in charge of Armed conflicts law and new technologies research, Army legal affairs.

[1]. The workgroup will refer to cybernetic operations, or non-kinetic operations. The expression cyberattack has been used excessively, thus making it dull. But above all, the term reflects simultaneously the means (a virus…). It therefore makes sense to separate means and action. Additionally, it holds no legal reality: lawyers use the term armed aggression (in *jus ad bellum*) and attack (in *jus in bello*)

all of the data, information, and contents circulating within the network. These three dimensions make cyberspace a multifaceted entity, complex to assess.

For the needs of the study, the definition of cyberspace offered by the National Agency for Information System Security (ANSSI) could be retained, as it synthesizes these three axes. The Cyberspace is defined as « *a communication space embodied by the worldwide interconnection of automated digital data management devices* ».
As a communication and generalized exchange space, cyberspace is the playground or target of many hostile and/or illicit actions perpetrated by states, groups or individuals. How does the law deal with these actions? The reflection will hinge mainly on the cyberdefense subject and, more to the point, the definition of cyberattacks[2]. Cyberwar, a notion which is not used in international law, constitutes, after the economic struggle and the war on terrorism, the new avatar of modern conflicts. All of these terms, however, suffer from the same absence of normative definition.

Cyberspace and resorting to force

However, scientific literature[3], like the media, give to think that such actions are common. Cybernetic attacks can be broken down into three groups, according to their form. First, there are attacks targeting digital data, their processing, their extraction, their deletion, or their corruption, such as the sending of a corrupt file designed to collect important data or destroying the directories of a hard drive. Then there are the attacks targeting information and communication systems, to identify them and detect the breaches which may be used within an attack, thus disrupting their running, temporarily or definitively. Finally, there are attacks which target, through cyberspace, devices, infrastructures, and critical installations which are out of cyberspace, with the intent of disrupting their running or destroying them. This risk is upped by the rising and generalization of use of the Internet, on an international scale (Internet-penetration levels rising, efforts to reduce the digital gap, multiplication of mobile uses and connected objects, but also connection the Internet –voluntary or not – of sensitive installations, omnipresence of computer vulnerabilities, dematerialization, etc.). « Attacks » led, via the *Stuxnet*, *Flame and Shamoon* viruses have shown how these actions rely on « virtual » or digital means can have repercussions in the real world. They also pose real threats to states (and their military actions) and on private individuals (legal or physical), both in times of peace and conflict.

Without falling into any kind of catastrophic stance, how can law specialists look at these facts? Their nature and their implementation environment give way to two opposite interpretations. The former considers it an evolution which would render existing law inapplicable; creating new norms, adapted to cyberspace, would be necessary. The latter, on the contrary, considers it possible to apply law to these facts (interpreting vision).

The former vision must be rejected because it hinges on a conception of cyberspace, both utopist and false. It considers it to be completely detached from the real world, thus forming a new natural environment, adding to land, sea and air[4]. This being said, cyberspace is not natural, it is a human creation and, in addition, the effects it contains have consequences in physical space[5]. However this vision does have the merit of

[2]. Voir par ex. *Tallinn Manual on the International Law Applicable to Cyber Warfare*.
[3]. S. J. SHACKELFORD, « From Nuclear War to Net War: Analogizing Cyber Attacks in International Law », *Berkley Journal of International Law*, 2008, vol. 25, n° 3, pp. 191-250.
[4]. D. R. JOHNSON, D. G. POST, « Law and Borders - The Rise of Law in Cyberspace », *Stanford Law Review*, 1996, vol. 48, pp. 1367-1402.
[5]. C. ROJINSKY, « Cyberespace et nouvelles régulations technologiques », *D.*, 2001, Chron., p. 844.

Underline the necessity of re-thinking certain cardinal principles of international law : sovereignty, territory principle…

If it is agreed upon that judicial void does not exist, the application of norms, such as they exist, in cyberspace would be a mistake.
Its specificities are its trans-border nature (absence of borders in its logical and cognitive dimensions), its omnipresence on several natural spaces (land, air, sea, extra-atmospheric space), exchange speed and volatility, application duality, etc.
Thus, for example, the regulation of cyberweapons, sometimes broached, couldn't be performed with the simple application of rules which stand for the control of regular weapons. This stems from the dual use of a code: how can one distinguish a hostile code from another conceived for research, when only their use or ends characterizes their possibly "armed" nature?

In the same way, qualifying cyberattacks with regards to international law poses real difficulties, as the notions and institutions involved were designed to deal with kinetic attacks[6].
Several qualifications could therefore be suitable:

- Use of force
- Police measures

Article 2, par. 4 of the United Nations Charter forbids resorting to armed force against another state and article 51 authorizes self-defense only in the case of an armed aggression[7]. Now, in the case of two cybernetic actions, in August of 2012 (the Saudi state-controlled company *Saudi Aramco* (on the 15th) and *Rasgas*, (on the 30th), a Qatari state-controlled company, were the victims of a new virus, *Shamoon*, which targets computers and their hard drives), there was no use of armed force, in the sense of kinetic operations (bombarding …). The action's aim was to destroy the targeted computer companies' computer pools, through the use of a virus, which is to say a program performing operations on the computer it is on (modification or deletion of data). Therefore, there is no use of armed force, but of codes which, in this case, had no real implications within the real world. The action can therefore not be qualified and armed aggression.

Can one therefore definitively come to the conclusion that only physical measures can be deemed armed force[8]? Such an interpretation must be taken with caution, as immaterial measures can potentially cause physical damage, as much as physical ones. The International Court of Justice, in its 1996 ruling *Lawfulness of the threat or use of nuclear weapons*, examining regulations regarding resorting to force, incidentally indicated that "these dispositions [articles 2, paragraph 4, 42 and 51 of the Charter] do not mention specific weapons. They apply to any use of force, independently of the weapons involved" (par. 39). Is deemed a weapon, all things, substances and objects, of physical, chemical or biological nature, used in combat operations, aiming at harming life, physical integrity, the health or, in general, the physiological or mental state of enemy persons, or the physical integrity of the enemy's equipment". In other words, if the "virtual" nature of these attacks could lead to disregarding "codes" as weapons, our reflection does lead us to consider harmful computer programs (and more generally cyberattacks, a cyberattack being possibly performed by a physical act, such as the destruction of a submarine cable) cannot be outright excluded from the scope of

[6]. P. WALKER, « Rethinking Computer Network 'Attack': Implications for Law and U.S. Doctrine », *Journal of National Security Law & Policy*, 2011, vol. 1, n°1, pp. 33-67.
[7]. M. ROSCINI, « World Wide Warfare - 'Jus Ad Bellum' and the Use of Cyber Force », *Max Planck Yearbook of United Nations Law*, 2010, vol. 14, pp. 85-130.
[8]. M. C. WAXMAN, « Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4) », *Yale Journal of International Law*, 2011, vol. 36, pp. 421-459.

"armed" measures[9]. It therefore seems wise to analyze them through the grid of two criteria[10]. The first is subjective, and consists in asking oneself whether these measures target the state. However, this does not suffice to constitute resorting to armed force. It must therefore be completed by the overstepping of a certain threshold: it is the objective criterion. Before this threshold, these measures could be considered police matters, violating the sovereignty of the state, and could only be justified if the perpetrating state would be able to prove that it lies in circumstances excluding illicitness. Beyond this threshold, these immaterial measures would constitute resorting to armed force, and be justified only if authorized by the Security Council authorizing it, or in the case of self-defense[11]. Also, qualifying the measures either as police measures or as armed force, could rely on the gravity of the consequences these presumed attacks could induce.

But, most of all, the covert nature of most of these actions asks the questions pertaining to the attribution of these actions. How can these actions be substantiated and linked to states or groups?

The judicial responses to these actions depend upon the answers brought to these questions. One reflection path suggests considering not a single qualification but a group of them, according to the type of attack. In such a case, the response would not be identical, and would have to adapt according to the type of attack.

*
* *

Of what precedes come more questions than answers. First and foremost, what is a cyberattack?
Where should a cyberattack be placed, in the array of traditional notions of international armed conflicts[12]? Does such an attack form the first step of an armed conflict or a new way of leading hostilities? How can a cyberattack with only "virtual" effects and no physical ones, be assessed? How can they be replied to, legally? How can they be answered to, appropriately, with the (state) means we have? How can misinterpretations and disproportional retaliations be avoided?
How can the author be identified[13]? This question gains weight with the emergence of "patriotic" computer hackers, claiming to serve their state, or hacktivists[14].
What is to become of state neutrality within cyberspace[15]? What about the states' responsibility? Should sovereignty be re-designed? Should law be re-founded, or simply re-interpreted in the light of the new computer deal and the Internet?

This list, which is non-comprehensive and destined to grow, of questions, is to serve as a draft roadmap for this workgroup, dedicated to judicial aspects of cyberdefense.

[9]. R. KOLB, *Ius contra bellum. Le droit international relatif au maintien de la paix*, Bruxelles, Bruylant, 2003, p. 172.
[10] . O. CORTEN, *Le droit contre la guerre. L'interdiction du recours à la force en droit international contemporain*, Paris, Pédone, 2008, p. 65 et sq, Y. DINSTEIN, « Computer Network attacks and Self-Defense »,
International Law Studies, Naval War College, 2002, vol. 76, pp. 99-120.
[11]. M. HOISINGTON, « Cyberwarfare and the Use of Force Giving Rise to the Right of Self-Defense », *Boston College International and Comparative Law Review*, 2009, vol. 32, pp. 439-454.
[12]. M. N. SCHMITT, « Wired Warfare. Computer Network Attack and jus in bello », *ICRC*, 2002, vol. 84, n° 846, pp. 365-399.
[13]. S. WATTS, « Combatant Status and Computer Network Attack », *Virginia Journal of International Law*, 2010, vol. 50, n° 2, pp. 391-447.
[14] . Hacktivism is the non-violent use of new information and communication, by activists, to spread their political demands.
[15]. E. T. JENSEN, « Sovereignty and Neutrality in Cyber Conflict », *Fordham International Law Journal*, 2012, vol. 35, pp. 815-841.