ESIL Reflections
Editorial Board: Samantha Besson, Jean d'Aspremont (Editor-in-Chief), Jan Klabbers and Christian Tams

16 March 2018 Volume 7, Issue 1

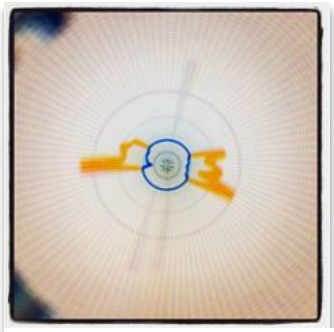

Image by Walter Logeman (cc)

Regulation of Cyberspace by International Law: Reflection on Need and Methods

Emilie Legris and Dimitri Walas
Institut du Droit de la Paix et du Développement Université Côte d'Azur

In recent years, cybernetic news and private codification initiatives, such as the Tallinn Manual,[1] have raised questions regarding the applicable legal framework to cyberspace. While we can count a handful of international specialized conventions that can be applied to this space, there is currently no multilateral convention, such as the Outer Space Treaty of 1967, governing cyberspace in international law. Furthermore, it is also difficult to identify any practice repeated over time that would count as customary law applicable to this space, nor has any specific case-law emerged in the area of cyberspace. In light of the present situation, our contribution argues that the regulation of cyberspace by international law is needed, especially if the peaceful use of this space is to be guaranteed. We will subsequently provide some reflections on the means and methods to determine which legal framework is most relevant and applicable to this space.

The reflection is structured as follows: after a brief presentation of cybernetic news and the issues it raises (I), the alleged intrinsic resistance of the application of international law to cyberspace will be explored (II). Finally, we will suggest, by employing the example of the law of armed conflict, some of the answers regarding the determination of the applicable law and its methodology (III).

[1] The Tallinn Manual is a private codification work, part of the work of the Cooperative Cyber Defense Center of Excellence, which was originally completed in 2013 and a new version was released in 2017. It sets out the international law applicable in case of cyber war, by transposition of customary and conventional law, leading nevertheless some incursions which fall under *lex ferenda.*

I. INTRODUCTORY REMARKS

Contrary to popular belief, “cyberspace” is not synonymous with “the Internet”. According to the Tallinn Manual, cyberspace is defined as an “environment composed of physical and non-physical components, characterized by the use of computer units and electromagnetic spectrum to store, modify and exchange data through a computer network”.[2] Since its evolution, which is essentially impossible to exactly trace, cyberspace has become a new strategic area of interaction between various actors, mainly States and particularly on a military level. The growing importance of such a space, which States must learn to control,[3] makes its regulation by international law necessary.

It is worth mentioning that the first cybernetic[4] questions arose following the invention of the telegraph in the middle of the 19th century. The use of air telegraphy during the Crimean War (1853-1856), and the use of the telegraph for the purposes of coding and guiding artillery fire during the American Civil War (1861-1865)[5] constituted a real breakthrough regarding the operative and tactical plans in war. This lay the foundations for coding, encryption and entrapment procedures that continue to apply to this day. Hence, we can say that since the very beginning there was a convergence between Information and Communication Technologies (ICT) and the conduct of war. Nowadays, military research has become the main vector of technological evolution in the field.

A fundamental change occurred when cybernetics was no longer considered solely a means of communication but transformed into a real weapon that is both operative and autonomous. This shift was made possible by two concomitant phenomena. Firstly, technological evolution, which allowed for the design of robots and drones that are remotely controllable or equipped with an

[2] *Tallinn Manual on the International Law applicable to Cyber Warfare*, Cambridge University Press, 2013, p. 258.

[3] This assertion mainly affects the "technologically advanced States", which are more dependent on the cyberspace because cyber technologies (industry, banks, administration, electronic vote etc.) infuse all spheres of society. Nowadays, developing countries should be more resilient in case of a cyber attack, considering their crude technology.

[4] From a technical point of view, "cybernetics" is a – very specific – scientific area devoted to the artificial intelligence and robotic aspects. As part of our study – and accordance with the legal doctrine – cybernetic means "in relation to cyberspace”.

[5] A. BONNEMAISON, S. DOSSÉ, *Attention: Cyber ! Vers le combat cyber-électronique*, Economica, Coll. Cyberstratégie, 2014, p. 17 et p. 19. In this book, the American Civil War is described as a "proto-form of cyber-electronic combat.

artificial intelligence. Secondly, the growing dependence of developed countries on cyberspace, which can inflict physical damage in the event of a cyber-attack on critical infrastructure management computer systems, such as dams, nuclear or electrical power plants, and hospitals.

Since the mid-2000s, there has been an exponential growth in the number of cybernetic operations, including denial-of-service attacks which is the saturation of networks until they are made completely inaccessible. For example, the attack on Estonia in 2007 caused a total shutdown of domestic communications, including the Internet and telephone. Another example is the attack on South Ossetia in 2008, which completely cut off civilian and military communications during the deployment of Russian troops. Conversely, cybernetic operations can help regenerate and advance communications. This was the case with the creation of the Free Libyana network in 2011, which facilitated mass communication between almost a million individuals in conflict-zones across Libya.[6]

For strategists and jurists, the main case study is the *Stuxnet* case in 2010. This incident concerned the partially successful attempt at paralyzing the Iranian nuclear programme through the contamination of a computer new kind of virus. This new virus was a "worm", which the US and Israeli intelligence services had probably developed, better known as the *Olympic Games Operation*. Once introduced into the host computer system, the worm operated so as to degrade the centrifuges, while emitting false information to Iranian engineers. Estimated at tens of millions of dollars, the research and development costs of such an operation unveils the promises of the 21st century weapon which can be characterized by its ultra-specialized, single-use and largely anonymous nature.

More recently, we witness diplomatic tensions arising between the United States and the Russian Federation, which have been largely fuelled by cyber-attacks on both sides, the most recent–and most publicized–being the hacking of computerized voting during the 2016 American presidential election. As a result of such incidents, the headquarters of Western states have had to continuously adapt their doctrine[7] (and practice) to tackle these issues, to the point that cyberspace is considered "the fourth theater of military operations".[8]

---

[6] *See* M. COKER, C. LEVINSON, ***Rebels Hijack Gadhafi's Phone Network,*** online.wsj.com.

[7] *See,* for instance*, The UK Cybersecurity Strategy : promoting and protecting the UK in a digital world,* November 2011, Cabinet Office, London ; *Canada's Cybersecurity,* October 2011 ; *Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space*, 2011;

It should be noted, however, that for smaller States, or States facing difficulties, the use of cyberspace can serve other objectives. For instance, by applying for (state) membership to the International Union of Communications (UIC) and to the Internet Corporation for Assigned Names and Numbers (ICANN*)* for the attribution of a country top level domain (granted in 1999), Palestine is obviously seeking "recognition" from the main institutions of cyberspace. Moreover, by making it possible to maintain the effectiveness of political power in the Palestinian territories, cyberspace can even be analysed as a precondition for the establishment of a State, especially since Israel banned Gazan's ministers from returning to the West Bank to take up their political positions.

Against this backdrop, the "Islamic State" (ISIS) does not seek any recognition by other States, therefore it does not adopt any "state posture" within the field of cyberspace; in other words, the Islamic State has taken no administrative or "diplomatic" measures that involve international entities such as ICANN or International Telecommunications Union (ITU). There is little evidence to suggest the will of this particular non-state actor to adopt a position or behaviour that is comparable to the position or behaviour of a State. ISIS' activities remain confined to cyber-criminality. Tying in with this, cyberspace is the most appropriate tool allowing a "political dwarf" to become a "media giant" by saturating the cyberspace with information, such as overgrowth of press article, propaganda videos, etc.[9]

These considerations, which briefly present various cybernetic issues, illustrate the need for multilateral regulation of this space. Given the proliferation of cyber activity not only limited to the state level but also non-state level, the question arises as to how to deal with this new development. Since law has stepped in to address a number of issues, it would seem fitting that international law should address the situations already outlined. However, the existing legal framework does not quite cater for the new reality. Because of this apparent legal void, it can be

---

Cybersecurity and Cyberwarfare : Preliminary Assessment of National Doctrine and Organization (Center for Strategic and International Studies, 2011).

[8] The other three theatres are land, sea and air.

[9] See E. LEGRIS, D. WALAS, « La reconnaissance de l'Etat de Palestine dans le cyberespace », *in* GARCIA T (Dir.), *La Palestine : d'un Etat non membre de l'Organisation des Nations Unies à un Etat souverain,* Paris, Pedone, 2016, p. 155-171 and E. LEGRIS, D. WALAS, « La reconnaissance de la qualité d'Etat à *Daesh* dans le cyberespace », *in* GARCIA T (Dir.), *La reconnaissance du statut d'Etat à des entités contestées : approches de droit international, régional et interne*, to be published (Paris, Pedone).

argued that cyberspace demonstrates an intrinsic resistance to the application of international law (II).

II. CYBERSPACE'S ONTOLOGICAL RESISTANCE TO INTERNATIONAL LAW?

As noted previously, to date there is no multilateral convention governing cyberspace. This situation contrasts to other spaces, such as the *Outer Space Treaty* which imposes a use of this space "in accordance with international law". There are a few specialized conventions adopted in the area of cyber; for example, the Council of Europe Conventions: Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (1981) et Convention sur la cybercriminalité (2001). In 2011 and 2015, the draft framework-conventions on the adoption of "cybernetic confidence-building measures" and on the respect of international law by States in their use of ICTS, elaborated by the UN Group of Governmental Experts, were considered inconclusive[10]. The scarcity of codified law applicable to cyberspace has led to private codification initiatives, some of which enjoy a certain degree of authority, such as the Tallinn Manual. Others are simply in a draft form.[11]. All these documents are certainly of great help on definitional and technical issues but they are non-binding legal instruments and have no application in actual practice.

Can this apparent legal void as to the regulation of cyberspace be explained by the very nature of this space? Indeed, cyberspace is a peculiar space. Unlike other *global commons*, such as outer-space or the high seas, which are tangible, cyberspace is entirely *artificial*, conceptualized and manufactured by man. Except for its physical infrastructures, all that belongs to cyberspace is entirely *intangible*. It is also *changeable*, since within it, any programme, tool, or user can change its location, its functions, and even its identity, thus generating anonymity. Another particularity of cyberspace centres around question of its *accessibility*: cyberspace has become truly universal.

However, the specificity of cyberspace does not justify its exemption from the law. From a historical point of view, whenever man has been able to expand his ability to conquer new

[10] *See* UNGA Resolutions 65/41 (2011) and 70/174 (2015).
[11] *See* proposals for an « *International Convention on the Peaceful Use of Cyberspace* » from Edward M. Roche & Michael J. Blaine (2013), and for a « *Geneva Digital Convention* » from Brad Smith (2015).

spaces (airspace, outer space, Antarctic, and so forth), international law has thus found application. Borrowing from the law of the sea for the purpose of illustration, it would be appropriate to evoke a form of “creeping jurisdiction”, which is especially evident in the law of armed conflict. Moreover, jurists, the military and strategists seem to share the intuition that "*there is no law void in cyberspace*".[12]

To provide some methodological reflections on the regulation of such a space by international law, while also noting the limitations due to this study’s brevity, we will concentrate on the law of armed conflicts. This branch of law seemingly constitutes a privileged site of study, regarding the issues presented earlier and highlights the close relationship between technological evolution and its use for military purposes, the Internet being the result of military research. Finally, an objective that clearly emerges from the work of private codification is an effort to guarantee the peaceful use of cyberspace (III).

III. The Means and Methods on Determining the Applicable Law

Even for this branch of law, the regulatory process of cyberspace remains complex. To presume an "automatic" application of public international law is *a priori* methodologically adventurous. The Law of The Hague and the Law of Geneva developed long before the emergence of cyberspace and was at a time when cyber existence was wholly inconceivable. Moreover, *jus in bello* is formally imbued with spatial criteria, which are largely ineffective in cyberspace; for example, the Hague Conventions of 1907 is applicable to “war *on earth*” (IV), “bombardement by *naval forces* in time of war” (IX); the Geneva Conventions of 1949 is applicable to “armies *in the fields*” (I) or to the “wounded, sick or shipwrecked armed forces *at sea*” (II).

Regulating the use of a specific weapon constitutes the classical way in modern humanitarian law; examples include the Convention on Bacteriological Weapons (1972), the Convention on Certain Conventional Weapons (1980), and the Convention on Anti-Personnel Mines (1997). However, owing to the mutability of cyberspace—the capacity within it for any weapon or programme to mutate and to change its location, its functions and its own nature—this makes it difficult to adopt conventional rules that are specifically designed to regulate the detention or the use of a specific weapon.

[12] C. Droege, *Pas de vide juridique dans le cyberespace*, CICR, 16 août 2011.

Accessibility and anonymity are also a particularity of this space. In cyberspace, the amalgam is absolute between the civilian and the military, and the State and the individual. Although the army and the government have specific servers, more or less independent of the public network, cyber-attacks transit through the same accesses (submarine cables, satellites, antennas, etc.) and the same means (computers) as peaceful connections. By favouring the invisibility of the actors, cyberspace goes against another general trend observable in public international law: the multiplication of legal subjects, divided into clearly identified categories, such as States, international organizations, and individuals as "functional subjects". Technically, it is not so much the origin of the cyber-attack that is difficult to trace but rather the attribution to a specific author. Put differently, a major obstacle in regulating cyberspace is the question of accountability. More than in any other space, the distinction between a regular fighter, a mercenary, a spy, a private military contractor or an isolated hacker proves a challenge to establish, especially when false identities or "*zombie units*"[13] are recruited from the civilian population.

It is therefore possible that the specificity of cyberspace requires the adoption of new rules, which take into account its *sui generis* nature. However, there are many existing rules of law, whose applicability does not depend on the nature of the space in question, and which may, *mutatis mutandis*, govern cyberspace. For example, in the context of humanitarian law, the Martens clause imposes respect for "basic considerations of humanity" in any situation, thus avoiding any legal void.[14]

Among the norms which can possibly govern any situation independently of spatial considerations are also the principles of the prohibition on the use of force in international relations (*jus ad bellum*), and all those which, in humanitarian law, are sufficiently abstract to be applicable in any situation. Foremost among these principles governing the use of force are

[13] Also called "*zombie machines*", these are computer units partially controlled by hackers remotely, without their true owners (often individuals) knowing. The Russian antivirus provider *Kaspersky*, estimates the number of infected computers in the world to several hundred thousand units. On the issue, *see* https://blog.kaspersky.com/computer-a-zombie-verify/4435/+&cd=2&hl=en&ct=clnk&gl=fr.

[14] Included in the Hague Convention (II) of 1988, this article stipulates that "in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity and the requirements of the public conscience". Nowadays, this article has an indubitable customary value, and plays a major role in all new situations.

necessity[15], humanity[16] and distinction.[17] The United States seems to have made the same argument after declaring that it will respond in the event of a cyber-attack by Russia in 2016. The United States considers a cyber-attack to be an "attack" in the sense of *jus ad bellum*.

These arguments are also supported by some authors who believe that "the interpretation of existing international law is sufficient to frame [cyberspace]"[18]. Such views were expressed, for example, at the 2011 London Conference on Cyberspace.[19] Similarly the group of experts drafting the resolution on Developments in the field of information and telecommunications in the context of international security stated “international law and, in particular, the Charter of the United Nations are applicable and essential to the maintenance of peace and stability, as well as to the promotion of an open, secure, stable, accessible and peaceful environment for information technologies and of communication".[20]

In clear cases where the current rule cannot be applied to cyberspace, the question arises as to the application of international law by employing he method of analogy. This method is also widely used in private codification efforts. For the purpose of this study, analogy is understood as the possibility for an existing rule (conventional or customary) to apply to a situation unforeseen at the moment of its creation, provided that it fulfils two conditions: firstly, the existence of a similar situation (the objective condition), and secondly, the legal conviction that the existing rule is appropriate to govern the new situation (the subjective condition). However, the extension of an existing rule to a new situation should be based on real similarities between situations.[21] As already discussed, cyberspace has *sui generis* characteristics.

[15] On the prohibition of superfluous and unnecessary damage, see article 23(e) of The Hague Convention (IV) and Article 35 §2 of Protocol I.
[16] According to the *Martens Clause*, the principle of humanity imposes the conciliation of military and human interests in the course of the conflict, thus providing a "*course of action in unforeseen affairs*" ("ligne de conduite dans les affaires imprévues", in the words of Jean Pictet).
[17] This principle articulates both the obligation of distinction of the civil and military targets (prohibition to use terror as well as indiscriminate attacks for example), the proportionality in the attack (human losses or damage to the excessive goods given the expected military advantage) and precaution (verification of objectives, obligation of warning).
[18] O. BARAT-GINIÈS, « Nouvelles formes de conflictualité dans le cyberespace », *Forum International sur la Cybersécurité*, Lille, janvier 2013.
[19] *London Conference on Cyberespace: Chair’s Statement*, 2 November 2011.
[20] 70th Session of the General Assembly, A/C.1/70/L.45.
[21] See *Dissenting opinion by Judge Badawi Pasha* in the *Reparations for Injuries Suffered in the Service of the UN Advisory Opinion Case,* pp. 210-211.

To return to the example of the law of armed conflict, the method of analogy seems possible for most cases of *jus ad bellum*. Indeed, its main principles (the prohibition on the use of force, legitimate defense, etc.), which are also considered tantamount to customary international law, constitute general obligations, not conditioned by the nature of the space under consideration. The question seems more difficult concerning *jus in bello*, where treaties are intended to govern a specific conflict zone or a specific type of weapon, as discussed above. Nevertheless, in this field, the application of the Martens clause and the general principles of humanitarian law also undermines the hypothesis of a legal void.

Irrespective of these general principles of humanitarian law, the question of applicable law arises in a variety of specific situations. For example, how should the obligation for States to assess the legality of any new weapon (Article 36 of Protocol I) be enforced? How to approach the question of international responsibility in a space where the real authors of these acts often remain unknown? What about the protective status of civilians participating in cybernetic conflicts?[22] The question of actors using reasoning by analogy poses a specific challenge. It is therefore necessary to distinguish between situations which they may give it a binding force—be it by States (adopting a new international convention based on reasoning by analogy) or the international judge (settling a dispute based on reasoning by analogy to determine the applicable law)—from cases where the actors using reasoning by analogy do not have creative power of law (or if this one is questionable: article of doctrine, work of private codification). For the latter actors, notwithstanding the quality of their legal arguments, they do not have the capacity to create international law. Their influence is undeniable, but in the absence of inter-state consensus, it must be heavily tempered.

CONCLUSION

It is necessary to dissociate the rules of international law whose transposition poses few theoretical problems from those, which must be handled with greater precaution. If certain principles of law are sufficiently broad enough to apply to cyberspace, there are others, more specific principles, which do not necessarily lend themselves to application by analogy of existing rules, and are waiting to find an answer that is tailored to address such specificities.

[22] Tallinn Manual, Rule 29.

When making a determination on the applicable law, the danger lies in a quasi-systematic recourse to reasoning by analogy. The example here is the Tallinn Manual, which reiterates the work of the San Remo Manual on the Law of the Sea and of the Manual on International Law Applicable to Air and Missile Warfare, which are themselves private codes. These instruments are non-binding and, above all, are not very representative of the various legal systems. It is also worth pointing out that no author of a Latin law system participated in the Tallinn Manual.

In any case, the lack of consensus regarding the adoption of a multilateral treaty can be simply explained. For many developed states, it now appears that cyberspace plays a remedial role, allowing the pursuit of strategic and defense operations in a world that now prohibits the use of force in international relations.

Cite as: Emilie Legris and Dimitri Walas, 'Regulation of Cyberspace by International Law: Reflection on Need and Methods', 7:1 ESIL Reflection (2018).