Legal borders and sovereignty in Cyber-space?

Maître Cécile Doutriaux
Lawyer and member of the Cyber-Defence and Cyber-Security Chair of the Ecoles de Saint-Cyr Coëtquidan.

January 2015 - Article II.1

Disregarding borders, Cyber-space makes the application of the national legal rules aiming to control it difficult. For the International Court of Justice, the respect of territorial sovereignty is a key foundation of the relationships between States[1] and the simple connection of an infrastructure to the global Cyber-space network cannot be considered as the waiver of territorial sovereignty by a State[2]. Yet infringements on the power of States and extensions of sovereignty are numerous in Cyber-space. The States are trying to construct strategies to address this fact, but are they efficient?

I. Do the concepts of border and territory such as applied to Cyber-space make sense?

Created by geographic, politic, economic, linguistic, ideological and social appropriation, territory is a space which the States must conquer, secure and defend. In order to delimit the space in which the States exercise sovereignty, borders are set and determine the surface on which the State imposes its legislative, executive and judicial authority. National territory defines the perimeter where the right of the State is destined to be applied uniformly, and national jurisdictions must judge all the cyber-conflicts committed on said territory, whoever the authors or the victims may be. The border is therefore a legal reality constituting the limit between the different jurisdictional spaces on which the States exercise their powers to the fullest. However, the border is not an unmoveable and rigid partition[3]. It evolves through time and space and the concepts of territory and borders have lost some of their relevance nowadays. Globalisation and the existence of a world in networks contribute to the construction of spaces with limits which are difficult to precisely define. Cyber-space, a place to exchange and store data, using electronic technologies such as the Internet, telecommunication networks and computer systems, accessible from every place on Earth, has become the symbol of the erosion of borders[4]. Indeed, though sovereignty is defined in physical determined spaces, the Internet links all the territories, without being a territory, and digital technologies are conceived by the circulation of flows and dematerialised data. The information layer of Cyber-space is in perpetual

[1] Corfu Channel Case Affaire du Détroit de Corfou (United Kingdom v Albania), CIJ Compendium 1949, 4, 35
[2] Heintschel von Heinegg «territorial sovereignty in Cyber-space »
[3] Amaël Catturuzza "Preliminary reflections on the concepts of borders and the Internet " p.2
[4] Nils Melzer " Cyberware fare and international law " UNIDIR, Resources 2011 p.4

movement, whereas state sovereignty implies the existence of clearly defined territorial spaces. Therefore, a State can only claim sovereignty if it is capable of controlling all of the informational activities on its territory and outside its borders[5].

The international aspect of digital conflicts is certainly a source of difficulties when trying to determine the applicable law and relevant authority, but faced with the acts perpetrated in Cyber-space, the States use public and private law, national and international law, in order to impose sanctions on the authors of computer conflicts, even if Cyber-space challenges physical borders, its users are quite real, and all located on the territory of a State. Therefore, despite the phenomenons of deterritorialisation and permeability of borders, generated by the globalisation of networks, the concept of territory is still a reference criterion for law. One must thus take into consideration the parties of the action, which is to say the author and the target of the cyber attack, State agent or not, but also the location of the cyber-action, inside and outside the borders of the State.

II. Application of the law to cyber-conflicts inside and outside State borders?

2.1. Inside State borders

On national territory, inside their borders, States have the power to exercise their normative and coercive authority against the authors of cyber-conflicts. The territorial jurisdiction, its capacity to instruct or judge a case, is a concept of public policy, and a State must here exercise its complete and full sovereignty.

2.1.1. About Cyber-conflicts between private players.

For Cyber-conflicts between private players, acting on the principle of territoriality, national law applies whenever a constituting act occurs on the territory[6]. The victim can then file an application either in the place where the offender lives or in the place where the prejudice was suffered. Thus access in France to illegal contents is enough to allocate national jurisdictional competence, even if the perpetrators are outside of the territory. The location of the servers does not matter when the crime has an effect on national territory. This means in theory that almost all the crimes committed with the support of cyber networks falls within the competence of the national judge. Thus, in a decision made on December 9, 2003[7], the Cour de Cassation judged that when the crime is committed on the Internet, every country is potentially targeted, "since the sites in issue are accessible from every country and that the alleged prejudice, by the simple fact of this broadcasting, is neither virtual nor potential". This could suggest that all online activities are potentially subject to the concurrent legislations of all the States' legal systems from which the site is accessible. However, a certain number of connecting links between the site in question and the territory have been required afterwards, and the judges indicated in a decision made on January11, 2005, that the audience targeted had to be considered (taking into account the currency, the language and the delivery place) so that the action may be successful[8]. It is therefore mandatory to characterise a sufficient connection, substantial or significant between the facts committed on the Internet and the alleged prejudiced on national territory. In a decision made on March 29, 2011, the Cour de Cassation recalled that the sole criterion of accessibility of a website in France is not enough to fall within the jurisdiction of French law[9]. On

[5] Leïla Bouchera, " Informational sovereignty: between utopia and project" Le Monde 1er février 1996
[6] A.113-2 of the Code Pénal Français
[7] Société Castellblanch / Société Champagne Louis Roederer, Cour de Cassation 1ère Chambre Civile
[8] Cour de Cassation, Decision of January 11, 2005, Hugo Boss / Reemtsma Cigarettenfabriken
[9] Cour de Cassation, Decision of March 29, 2011, Ebay Europe and others/ Maceo and others

October 3, 2013[10], the Court of Justice of the European Union confirmed again that though a legal action can be claimed on the territory on which the illegal content is accessible, the litigious content must also be intended for the audience of that State. In any event, simple accessibility of the website on the national territory is not enough anymore to establish the State in question's jurisdiction, which limits the capacity of the States to impose sanctions for the illicit activities committed in Cyber-space.

2.1.2. About Cyber-conflicts between States.

When Cyber-conflicts do not involve private Cyber-space players, but States, armed forces, organised armed groups; in international armed conflicts, other law rules are applicable, but the concept of territory such as applied to Cyber-space remains central. Thus, in the case of the Tallinn Manual[11], though no State can rule on Cyber-space, it remains nonetheless sovereign on its own territory. The digital infrastructures located on the State territory are submitted to the State's territorial jurisdictional law and competence, which can "regulate, restrict or forbid the access to the digital infrastructure located on its territory"[12]. Furthermore; an attack against the Cyber-infrastructure of a country could be interpreted as a violation of sovereignty if the cyber-operation is simultaneous with an attack threatening the territorial integrity of the nation and of a sufficient level of intensity[13], namely when a State is under the obligation of modifying the key components of its policy, its cultural or socio-economic system.

2.2. Outside the State's national borders

While exercising the State's legal power is in principle limited to its national territory, under general international law, connecting factors such as domicile and nationality are accepted and enable the States to exercise jurisdiction beyond their national borders. Hence the concept of extra-territoriality makes it possible to consider that a national law is applicable to any crime or felony punishable by imprisonment committed by a Frenchman or a foreigner, to a victim with French nationality[14]. However, the right only retains its role to regulate the infringements which occurred outside its territory if the cyber-attacks are also punished by the law in the country where they were committed, according to the principle of double jeopardy[15].

Insofar as networks and the Internet cover areas which fall within different cultural, moral, social, economic and sociologic concepts, it is obvious those national rules are not enough and that the solution must necessarily be found at an international level, in order to ensure the prosecution and the sentencing of the authors of cyber-conflicts. This is why accelerating the harmonisation of the national laws governing digital conflicts is necessary. To this day, eighty-two countries have signed or ratified several binding conventions relative to cyber-criminality, such as the Council of Europe Budapest Convention, the League of Arab States Convention on the war against information technology-related offences, the Agreements of the Independent States in the fight against cyber-offences, and the Shanghai Organisation Agreement for cooperation in the area of international information security. The legal instruments make it easier to repress cyber-attacks issued outside the
'States' national borders; but the States remain obviously free to join the Convention or not.

---

[10] CJUE, Decision of October 3,2013 Peter P. / KDG Mediatech AG

[11] Tallinn Manual, Cambridge University Press mars 2013
[12] Tallinn Manual, (article 1 about sovereignty)
[13] J.Combacau and S Sur, Public International Law (Montchrestien, Paris 2012), 266
[14] Article 113-7 Code Pénal
[15] Article113-6 Code Pénal

II. Which sovereignty infringements and extensions of the States in cyber-space?

3.1. The difficulty of sovereignty by the State in cyber-space.

3.1.1. On national territory.

If it is the States' duty to exercise their sovereignty and enforce their laws on their national territory, the States don't always have the means to enforce their regulations inside their borders, when they order Internet Service Providers to block access to illegal sites on their national territory. These technical intermediaries, in accordance with article 8.3 of the 2001/29/CE Directive issued by the European Parliament, can act by using three techniques, which are blocking the "Uniform Resource Locator" (URL) address, the "internet Protocol" (IP) or blocking the domain name ("Domaine Norme System" ou "DNS"). But the implementation of such measures is long, expensive and can prove to be inefficient. In a case judged on October 14, 2011, by the Tribunal de Grande Instance de Paris, the website Copwatch, located in the United-States in order to expose police violence by broadcasting the personal data (name, surname, internet address, phone number, photos) of many law enforcement officials had been blocked by the Internet service providers[16]. A new suit was filed one year later, because an identical version of the site Copwatch was put online and it was deemed legal to forbid access to 34 "mirror sites" to all subscribers on the national territory. But the experts pointed out that the time needed to implement these technical measures would be between six months and a year and would cost an initial investment of 10 million Euros per operator. In a decision made on November 28, 2013[17], the TGI de Paris ordered five Internet service providers to block the sites of the network Allostreaming and three search engines (Google, Microsoft and Yahoo) to stop referencing them in order to stop the illicit representation of films or series, in streaming mode, for French surfers. Here again, the Internet service providers indicated that the targeted sites would bypass these requirements. In this case, it is therefore not the law which is defective, but the impossibility of a State to exercise its full sovereignty on its territory and to enforce the effectiveness of its legal decisions when the servers and the data are located in a foreign country.

3.1.2. During international investigations in order to identify the authors of cyber-attacks

Other forms of encroachment of the sovereignty of the States exist in international criminal investigations. The Sates are generally required to provide the connection data enabling the identification of the author of a cyber-crime located on their territory to the foreign enforcement authorities[18]. In order to be able to access this technical information through the Internet service providers, obtaining prior consent from the State which holds the connection data is mandatory, according to the Permanent Court of International Justice in its decision on the Lotus case[19]. This decision specifies that any exercise of power from a State cannot be exercised outside its territory, except in the case of an existing permissive rule stating the contrary, under customary international law or from a convention.

In theory, only seven countries allow foreign authorities access to connection data (Czech Republic, Lithuania, Germany, Sweden, Turkey, Bosnia and Herzegovina, Hungary, Estonia and the

---

[16] Tribunal de grande instance de Paris Order of the Referee 10 February 2012, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3337

[17] Tribunal de grande instance de Paris Order of the Referee 28 November 2013, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_aricle=3935

[18] Articles 31 et 32 of the Budapest convention from 23 November 2001.

[19] Lotus case (France vs/Turkey ° CPIJ serie A, n°10, p.18 (1927).

Netherlands)[20]. In reality, despite the obligation to obtain consent from the State in question, the enforcement authorities frequently get access to data which is stored abroad by cooperating with private companies, without any demand for mutual assistance being issued to the State where the data is stored. The International Chamber of Commerce has revealed that many companies are subjected to intense pressure from foreign governments who want to obtain connection data, despite the fact that this access without consent is not authorised by the law in their country[21]. Thus many States infringe upon the national sovereignty of other States within international investigations, in an attempt to repress cyber-crime.

3.2. Extensions of State sovereignty.

3.2.1. The application of national law outside State borders.

Can a national judge apply the law of his State beyond the limits of his territory and thus ignore the sovereignty of the other States? Beyond the technical difficulties, measures aiming to filter and block foreign sites on national territory can also potentially jeopardise the sovereignty of another State. In a legal dispute between Germany and the American company CompuServe[22], the court ordered that the forums should be made inaccessible from German territory, under the German law repressing their contents. This legal decision blocked access to the sites 4 million subscribers from the company CompuServe, in 140 countries. In another case, the Tribunal de Grande Instance de Paris required that the American company Yahoo Inc implement a filtering system designed to identify French cybernauts, in order to block their access to the Nazi objects auction site[23]. The company Yahoo considered that a foreign jurisdiction could not impose their intervention on their servers located in the United States, and that a coercive measure against them could not be applied, as it was in contradiction with the 1st Amendment of their Constitution, guaranteeing all citizens freedom of expression. In this case, the application of national law has impact beyond borders, when it is applied to the users of the network located on other national territories, and the State can obtain increased power, an extension of its sphere of sovereignty; which places the other States into a competition for power.

3.2.2. Guaranteeing the sovereignty of the States by preventing cyber-attacks on its territory.

Lastly, if sovereignty is understood as the right to exercise its prerogatives on its territory, excluding any other State, it also implies the duty of protecting the territory of the other States, in accordance with the principle of sovereign equality of the States as set out in article 2 (1) of the United Nations Charter. Thus, under international law "no State has the right to use or allow the use of its territory in such a way as to cause prejudice on the territory of another State"[24]. In the Corfu Channel case, the International Court of Justice indicated that each State was under the obligation "not to allow the use of its territory for the purpose of acts contrary to the rights of other States"[25]. According to the Tallinn Manual, there is a duty on the States to prevent illegal acts committed in the cyber-space originating from their territory and causing damages to persons or property. But the implementation of the duty of prevention in cyber-space must take into account the actual ability of the States to control the digital infrastructures located on their territory. Indeed, most of the time they belong to private companies, on which the States don't always have much hold.

---

[20] http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/TCY(2012)3F_transborder_repV31public_7Dec12.pdf

[21] ICC Policy Statement: Cross-border law enforcement access to company data – current issues under data protection and privacy law » (February 2012)

[22] Case Munich Public Prosecutor Germany versus CompuServe, judgement 28 May 1998 – 8340, Ds 465

[23] TGI Paris, Order of the Referee 20 November 2000, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm

[24] Case Trail Smelter (United States v Canada) Collection of International Arbitral Awards, Vol. III pp 1905-1982, 1965 (1941)

[25] Corfu Channel, Merits, Judgements, ICJ Reports 1949, p21

Conclusion

The law has proved to be insufficient in guaranteeing the power of a nation to take action against infringements and extensions of sovereignty of other States. Under those conditions, what are the strategies considered by the States in order to recover their digital sovereignty? In effect, the measures taken are more technical than legal. Thus the States wish to regain their independence and develop their own digital networks. For example, Brazil wants to build a fibre optic cable which would link Europe to Latin America. Some States are considering the potential shutting-down of a part of digital infrastructures in order to counter a cyber-incident endangering their essential interests, even if this may affect the cyber networks and systems of the other States. The Prism case alerted the States to the importance of relocating the servers and data on national territory. In France, the decision was made to give priority to national infrastructures in order to safeguard the confidentiality of the data stored on the cloud with Numergy and Cloudwatt. Germany took measures of strategic retreat for the purchasing of hardware and software and called for the creation of a European Internet space, in which personal data would be safeguarded. In order to ensure the safety of the State information systems, the French government requires administrations to use exclusively the national networks and infrastructures, to host sensitive data on the territory and to purchase security services and products accredited by the French Network and Information Security Agency[26]. Without considering China, Russia and Iran's position, who strive for a closed and highly controlled cyber-space, we are witnessing the implementation of a certain form of digital protectionism. Does this necessarily mean that we will witness the breaking-up of the cyber-space into several isolated territories and the fragmentation of the hardware, software and information layers, resulting in a "Balkanisation" of cyber-space? In effect, that is a long way off, though the States, with the support of the companies, wish to offer an alternative to the Asian and American products and software, their strategy cannot be, in the long run, to keep all of their infrastructures and all of their data exclusively on their territory, to guarantee a truly competitive offer in a globalised context. Thus, despite the political will of the States, and their more secured key information systems, the measures taken have relative efficiency nowadays in the aim of recovering their part of sovereignty in cyber-space.

---

[26] See Security Policy for the information systems of the State -ANSSI du 17 juillet 2014