Is There a Sheriff for the Chaos of Cyber-Far-West?

Alexis Deprau

Lawyer, Doctor of Law

University Paris II – Panthéon Assas

Holder of the CAPA

Author of Le droit face à la terreur *(éditions du Cerf, 2021) and*
Le contrôle parlementaire du renseignement *(Berger-Levrault, 2022)*

Abstract

One of the main peculiarities of cyberspace is the absence of defined borders which would be similar to borders linked to the geography of States. Thus, cyberspace is difficult to regulate, and the regulatory norms that would be necessary for a safer use of cyberspace do not seem to emerge—therefore making cyberspace a lawless zone similar to a "Wild West without Sheriff." The present article explores both the various threats that persist within this "cyber Wild West," and the avenues for legal and technological improvements to deal with them—at both national and international level.

Keywords: Cyberspace, cyberthreats, cyberattacks, viruses, cyber Wild West, regulation, norms, defense, security, international law

¿Hay sheriff para el caos del Cyber salvaje oeste?

Resumen

Una de las principales peculiaridades del ciberespacio es la ausencia de fronteras definidas que serían similares a las fronteras vinculadas a la geografía de los Estados. Por lo tanto, el ciberespacio es difícil de regular y las normas regulatorias que serían necesarias para un uso más seguro del ciberespacio no parecen emerger, lo que convierte al ciberespacio en una zona sin ley similar a un "Salvaje Oeste sin Sheriff". El presente artículo explora tanto las diversas amenazas que persisten dentro de este "cibersalvaje oeste" como las vías para las mejoras legales y tecnológicas para enfrentarlas, tanto a nivel nacional como internacional.

Palabras clave: Ciberespacio, ciberamenazas, ciberataques, virus, ciber Lejano Oeste, regulación, normas, defensa, seguridad, derecho internacional

doi: 10.18278/ijc.10.1.5

是否有负责应对网络蛮荒地带混乱的治安官？

摘要

网络空间的主要特点之一是没有明确的边界，后者类似于与国家地理相关的边界。因此，网络空间难以监管，而为了更安全地使用网络空间一事所必需的监管规范似乎并未出现——因此，网络空间成为一个法外之地，类似于“没有治安官的蛮荒地带。”本文从国家层面和国际层面上探究了在该“网络蛮荒地带”中持续存在的不同威胁，以及一系列法律和技术改进途径，以应对此类威胁。

关键词：网络空间，网络威胁，网络攻击，病毒，网络蛮荒地带，监管，规范，国防，安全，国际法

"*In the next fifteen years, the number of attempted attacks by non-state actors, hackers, activists or criminal organizations will certainly increase. Some of these attacks could even happen on a large scale.*"[1] Here we are in 2023, fifteen years after these words were taken from the 2008 *White Paper on Defense and National Security*, fifteen years marked by a flood of all kinds of cyberattacks, which have always been devastating for the victims (public institutions, private structures, and individuals).

A recent example in the field of healthcare is Corbeil-Essonnes' hospital (Val d'Oise), which was the victim of a ransomware attack on August 21, 2022: a cybercriminal action in which the attacker asked for a ransom in exchange for the decryption password. This example is not isolated: a ransomware cyber-attack targeted the Castel Luccio hospital in Ajaccio (Corse-du-Sud) towards the end of March; it was also the case in Arles' hospital in August 2021. In 2019 alone, the National Agency for Information Systems Security (ANSSI) listed 18 of these attacks in the health sector.[2]

No state is spared in this regard: in the first half of 2021, 235 healthcare facilities were attacked by the cybercriminal group Ryuk, for ransoms of approximately $100 million. In essence, "Central *Europe tops the list of regions affected by the spike in attacks on healthcare facilities, with a 145% increase in November [2020], followed by East Asia, which experienced a 137% increase, and Latin America with 112%. Europe and North America saw increases of 67% and 37%, respectively..*"[3]

However, these computer attacks do not only target the health sector but all sectors and by any means within the reach of cyber-attackers, depending on their purposes. This is why the threat, well identified in the 2008 *White Paper on Security and Defense*, is again recalled in the 2013 *White Paper on Security and*

Defense. First describing the terrorist threat, considering that the question "*is no longer whether an attack will be committed on national territory, but when,*"[4] the 2013 *White Paper* also emphasizes "*the frequency and potential impact of the threat posed by cyberattacks on our information systems, training.*"[5]

Cyberspace, the modern Wild West

"Despite *attempts, notably in France, to regulate the use of the new military capabilities offered by the virtual world, cyberspace remains a Wild West.*"[6]

Like Jérôme Poirot (author of the above comments) and the General Secretariat for Defense and National Security (SGDSN), we believe that the cyberworld should be thought of as a modern Wild West, a lawless place, like those seen in Hollywood movies. In reference to the libertarian California of Silicon Valley[7] and GAFAM, we must not conceive this zone like a strictly speaking lawless zone per se; rather, a lawless zone without the regulation of some cyber sheriff. Hence the result stated by the SGDSN, "we *can choose to have better control of the risks, thanks to a reinforced cyber defense and a more robust hygiene of cybersecurity in our society, or on the contrary to let ourselves drift towards a kind of cyber 'Wild West.'*"[8]

This cyber Wild West is permitted, if not facilitated, by the libertarian vision of Internet use. "*Using their giga-servers as "weapons of mass disruption," the lords of Silicon Valley [but not only them] have indeed ravaged, under the blows of their billions, entire industries and institutions: television, music, cinema, advertising, media; not to mention higher education, medicine, and money. And all the while, they were quietly siphoning off Big Data and trampling on the privacy of billions of Internet users on a daily basis.*"[9] Who are we talking about? The GAFAMs (acronym for Google, Apple, Facebook, Amazon and Microsoft), but also the NATUs (for Netflix, Airbnb, Tesla, Uber), or the Chinese equivalents of the GAFAMs, namely the BHATXs (acronym for Baidu, Huawei, Alibaba, Tencent, Xiaomi), not forgetting Russia with the powerful Russian search engine Yandex or the social network VKontakte.

Yes, the "cyber-bazaar" that we observe today is a "cyber Wild West" *that has no borders. Thus, there is no French, American, or Russian cyberspace, the violation of which would constitute a violation in the same way as the violation of land borders, national airspace or territorial sea. To use a military term: there is no front in cyberspace, or else it is a global front. This does not mean that actions carried out in and through cyberspace cannot produce geographically determined or even targeted effects; current events provide almost daily proof of this.*[10]

Types of attacks listed

Given that the Internet is a space that is neither limited by space nor by time, it is summarized by a mesh of all the networks, anonymous, and without necessarily being able to identify the attackers. This is why the computer attacks that are carried out on the Internet can be varied and listed according to three main methods[11]:

- *the "information war,"* which uses the computer vector for the purpose of propaganda, disinformation, or political action, also called destabilization attacks.
- *the "war for information,"* aimed at penetrating networks in order to recover the information that circulates or is stored there, also called cyber-espionage.
- *finally, the "war against information,"* which attacks the integrity of information systems in order to disrupt or interrupt their operation, called sabotage.

These few examples are very circumscribed, and to better understand the various types of attacks listed, a study on this subject would require an in-depth book.

Firstly, the destabilization by denial-of-service *attack (*DOS), the massive sending of data to disrupt access to web pages, Japan was the subject of nearly 450 million (yes million) cyberattacks targeting the Tokyo Olympics, this number of attacks was 2.5 times higher than during the London Olympics in 2012.[12]

Secondly, cyber-espionage, or information warfare, is a method that is both effective and damaging for its victims. It can concern both state espionage and industrial cyberespionage, which is formidable for stealing competitors' industrial or business secrets. For a textbook case, a more powerful virus than Stuxnet (see below) can be observed, one that is dedicated to the field of industrial espionage. This was the Flame virus, "a *very complex type of malware designed to infiltrate a computer without the knowledge of its user in order to take control of it, collect information or delete files*"[13]; precisely this spyware spied on the functioning of the infected system without disturbing it.

Concerning the cyber-espionage of French institutional sites, the Ministry of Economy and Finance suffered two computer intrusions on the evenings of December 30 and 31, 2010, by spyware called "Trojan horses," "*malicious programs [that] open a 'back door' on the infected computer allowing the attackers to connect remotely to the infected computers in order to intercept keystrokes and network communications and, above all, to exfiltrate sensitive documents to remote servers.*"[14] This intrusion on the Ministry of Economy's website was qualified by the French National Agency for Information Systems Security (ANSSI) as "the *first attack against the French State of this magnitude on this scale.*"[15]

Thirdly, the computer threat is also sabotage, or war against information. The Stuxnet virus or worm (which would have weighed between 500 Kb and 1 Mb, equivalent to a digital photograph) was designed to sabotage Iranian nuclear sites in 2010.

Closer to home, the *NotPetya* computer worm massively affected the Ukrainian economy as well as the Chernobyl power plant in 2017. If this virus had the purpose of sabotage, it would appear in the form of ransomware. Through its propagation mechanism and the interconnection of various actors whose subsidiaries were in Ukraine or had business relations there, many collateral victims were affected, "*such as the Danish shipping group Maersk, the French industrial group Saint-Gobain or the British communications and advertising group WPP. NotPetya infected its victims via a booby-trapped update of the MEDoc accounting software used by many Ukrainian companies.*"[16]

Fourth and lastly, we must not forget cybercrime, which, according to General Marc Boget (commander of the Gendarmerie-cyberspace) represented 6,000 to 7,000 billion dollars in 2020 worldwide, with a ransomware attack every 11 seconds. This cost of cybercrime is ten times higher than in 2018. The Center for Strategic and International Studies (CSIS) think tank and the McAfee company had in fact estimated it at 600 billion dollars, as they were unable to have exact figures, "*due to the lack of a clear perimeter of offenses and victims, and because of under-reporting, it seems complex to have stabilized data.*"[17]

The cyber Wild West would certainly not have been without the promotion of globalization, which is supposed to be beneficial in all respects. This is a statement that has been made for the past ten years at the highest level of government, according to which "*our forces, in conjunction with other government services, must finally have the necessary responsiveness to protect the country and the infrastructures or institutions that are essential to its economic and social life in the face of the risks of globalization (cyber threats, terrorism, acts targeting the security of supplies, and natural, sanitary or technological risks).*"[18]

An evolution of the threat or anarchy in the making

"*Few prospective works exist in the cyber domain, whether they concern future technological evolutions or employment doctrines. (However, it is certain that the threat will worsen in the next decade, resulting in a more dangerous and less stable cyber space, where computer attacks will be commonplace, forcing public institutions, companies, and individuals to protect themselves more strongly than today).*"[19] According to the General Secretariat of Defense and National Security (SGDSN), as familiar as it is to anyone interested in the subject of cyber, the cyber threat is constant and evolving day by day, especially with the advent of new technologies and advances related to it, such as:

- From "cryptojacking," a cybercrime using "*software installed on a system without the owner's knowledge and allowing the computing power of infected machines to be used to perform cryptocurrency mining operations, rewarded by the generation of new cryptocurrency.*"[20]

- The advent of the Internet of Things, which facilitates the interconnection between the Internet and objects, places, and physical environments, for a number of connected objects (often very insecure) estimated at about 30 billion, thus leaving a colossal margin of maneuver to those with malicious intentions…

- The development of 5G and the deployment of software solutions in the Cloud. On this last point, "*in addition to the new potential security flaws linked to the Cloud supporting this virtualization, the growing share taken by the immaterial dimension of the network also exposes it to the need for frequent updates, which have as many windows of risk.*"[21]

- Finally, from what is seen by some as "the scary future of the Internet," and soon to be used by cyber-attackers—to their benefit—artificial intelligence but also and especially quantum computing whose goal is to solve complex problems that cannot be done by classical computers. The other side of the coin: not only can current encryption keys be broken thanks to quantum computing, but quantum computers that manage to be infected by viruses will allow cybercriminals to perform complex calculations and make huge profits. By installing malware to mine crypto-currencies, "*the complex mathematical problems that miners of crypto-currencies such as bitcoin, must solve would be relatively trivial for a network of quantum computers.*"[22]

We can only agree with the fact that the computer threat will evolve as the above elements demonstrate; again, from three factors that are imposed on us: a dangerousness of the threat linked to the multiplication of actors; a more extensive digitalization of our society accentuating the exposure to cyber threats; and an interweaving of cybercrime and national security issues. As proof, "*tools traditionally used for fraud and extortion, can cause damage to the information systems of the State and operators of critical infrastructures, paralyzing the continuity of their activities (e.g., in May 2017, Wannacry ransomware attack that affected Vodafone, Fedex, Renault, Telefonica, Deutsche Bahn and the British health system).*"[23]

A threat legitimately perceived as a strategic priority

Given the importance of the threat to national information systems, as well as to all private information systems whose financial stakes are, strictly speaking, colossal, the cyber threat is logically understood and identified as a strategic priority. It can undermine the protection of the national territory and of French residents, and/or interrupt the continuity of the Nation's essential functions. It was thus placed on the same level as other major threats in the 2013 *White Paper on National Defense and Security*: aggression by another State against the national territory; terrorist attacks; attacks on the Nation's scientific and technical potential; organized crime in its most serious forms; major crises resulting from natural, sanitary, technological, industrial, or accidental risks; and attacks against French nationals abroad.

Beware: the *White Paper on National Defense and Security* remains a white paper, i.e., a document whose aim is to define an overall defense and security strategy for France; an incentive guide devoid of any legal force. For all that, this strategic priority constituted a basis for the elaboration of an offensive public doctrine, whose reflection was officially developed in 2008 within the *White Paper on national defense and security*, on the need to move from a passive defense strategy to an active strategy "*combining intrinsic protection of systems, permanent surveillance, rapid reaction and offensive action, requires a strong governmental impulsion and a change of mentalities.*"[24]

Offensive capabilities are mentioned from the moment when "*it is no longer a question of protecting the system under attack, but of identifying the adversary, uncovering its modus operandi, neutralizing it, or even applying retaliatory measures.*"[25] This offensive posture is not only necessary but can also be implemented (within their competencies and attributions) by the various French services that have cyber as a total or partial competence and should not remain the prerogative of the armed forces (embodied by the Cyber Defense Command, COMCYBER). Thus, in order to neutralize adversary operations centers, offensive public doctrine may also involve intelligence services and police entities fighting cyber threats: the General Secretariat for Defense and National Security (SGDSN); the National Agency for Information Systems Security (ANSSI); the General Directorate for External Security (DGSE); the Directorate for Defense Intelligence and Security (DRSD); the Directorate for Military Intelligence (DRM); the Directorate General of Internal Security (DGSI); the National Directorate of Customs Intelligence and Investigation (DNRED); the Tracfin financial intelligence service; the Central Office for Combating Information and Communication Technology Crime (OCLCTIC); and the Gendarmerie Command in Cyberspace (COMCyberGEND).

These offensive capabilities can—and must—be seen as the armed arm of the strategic priority, the dissuasive role with respect to potential aggressors is not negligible, because "*it is legitimate to draw the consequences, as such a capability can have effects at the tactical, operational and strategic levels.*"[26]

What is the place of law in today's cyber Wild West?

"*The highway code is valid for any vehicle, luxurious or modest: in the same way, only a code of the cyberworld will effectively sanction the predators, marauding financiers, net giants, etc., who today plunder it with impunity or exploit its users.*"[27]

As the law—legitimately—takes a predominant place in our societies, it is not out of the ordinary to consider regulating cyberspace, even though it is, by definition, subject neither to time nor to space. Regulating it is an ambitious but essential mission, given the ravages caused by the computer tools presented above, and with the more than damaging consequences, suffered or observed.

The first question is therefore: can international law have a protective effect? Like international cooperation, which is not the subject of a consensus at present (see above), one cannot help but note the limited place of international law in cyberspace, if only with the principle of self-defense of Article 51 of the United Nations Charter.[28] As proof of this, the 2013 *White Paper on Defense and National Security states* that "*questions that are currently open deserve further national inter-reflection within the United Nations: how to interpret the legitime defense of Article 51 of the UN Charter in the face of cyber-attacks, or in the face of terrorist actions carried out in particular by non-state groups from states that are too weak to effectively control their territory? How can we reconcile the urgency that, in certain situations, attached to the implementation of the responsibility to protect, is the patience that is indispensable for building an international consensus?*"[29] Moreover, Article 51 does not refer to any weapon whatsoever, which could lead to confusion and suggest that cyber weapons might not be considered as weapons as such, although we know today that they are equivalent to weapons of mass destruction in their effects.

In addition to Article 51 of the United Nations Charter, the North Atlantic Treaty Organization (NATO[30]) has a self-defense clause in Article 5 of its treaty. This provision provides that "*the parties agree that an armed attack against one or more of them occurring in Europe or North America shall be considered an attack against all of them, and accordingly they agree that, if such an attack occurs, each of them, in exercise of the right of self-defense individually or collectively, recognized by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in agreement with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.*"

In both the UN Charter and the North Atlantic Treaty, no clarification has been made as to whether cyber weapons could be considered, or whether an armed cyber aggression was indeed considered an armed aggression.

Fortunately, in 2013, a group of experts mandated by NATO drafted the Tallinn Manual, which aims to transpose international law to cyber-conflicts. Even if this document is not binding as it has no legal value, this manual made it possible to develop a reflection on the application of international law to cyber issues.[31] These experts concluded that "*a cyber operation constitutes a use of force when its dimensions and effects are comparable to those of a non-cyber operation reaching the level of a use of force.*"[32] This is why the drafters of the Tallinn Manual proposed to consider—rightly—that cyber-attacks are equivalent to armed aggressions. Specifically, Rule 13 of the Tallinn Manual states that "*a State that is the target of a cyber operation of a level equivalent to an armed attack may exercise its inherent right of self-defense. Whether a cyber operation rises to the level of an armed attack depends on its dimensions and effects.*"[33]

Based on the effects test, the notion of armed cyber aggression is still limited, as most attacks are currently considered below the threshold for the use of force and may qualify as an armed attack, as in the case of Estonia in 2007. "*Which remains probably the most massive attack ever carried out against a State, [and] did not lead to the implementation of Article 5 of the North Atlantic Treaty*"[34] nor to the use of self-defense provided for in Article 51 of the United Nations Charter, nor in Article 42 § 7 of the Treaty on European Union.[35]

In addition to the question of the threshold authorizing the use of force, it is also necessary that the attacker can be fully identified, as the attribution of the attack can be very difficult to establish. Even assuming that the attack has been attributed, the question of self-defense still arises, according to the three criteria that condition it (necessity, proportionality, and immediacy). If individual self-defense does not pose a theoretical problem, what about collective self-defense, which cannot assume the application of the criterion of immediacy? As a practical example, Article 5 of the North Atlantic Treaty, which provides for the automatic mechanism of collective assistance, "*could only be implemented if the States concerned first share the same position on the attribution of a cyber-attack. But if attribution is already a complex process when carried out by a single State, what about a possible "co-attribution" that would have to be shared by some 29 States?*"[36]

In addition to the legal tools provided by the United Nations Charter and the North Atlantic Treaty, the United Nations has had a Group of Governmental Experts (GGE) since 2004, also known as the Consultative Group of Experts (CGE), whose mission is to propose recommendations to strengthen international security in cyberspace. Bringing together some 20 states, the GGE experienced several failures in 2013. Yet a "breakthrough" occurred in 2015, nevertheless a modest one, when it was recognized that "*the principles of the prohibition of the use of force and of the peaceful settlement of disputes and, on the other hand, the principles of the law of armed conflict: jus ad bellum [right to war] and jus in bello [right in war]*"[37] applied to cyberspace. Progress slowed down in 2016 due to the departure of Russia, China, and Cuba from the GGE, resulting in a suspension of the work. However, developments could have been achieved during the 2016-2017 round of GCE negotiations. On that occasion, France proposed to deepen the work and clarify the standards. While most of these proposals were accepted, "*the negotiations failed on the issue of the application of international law to the conduct of States in cyberspace.*"[38]

In the absence of consensus, international regulation and action seem difficult, if not simply impossible, to implement, which does not bode well for joint action to regulate the global cyber Wild West.

This is why it seems more reasonable to focus on individual actions taken by States on their territory to hope for regulation and the effective implementation and application of a "cyber highway code." With regard specifically to our national law, this regulation is done on a case-by-case basis, in order to set up protection systems for operators of vital importance, cryptology, surveillance (infiltration) or criminal responses. Laws are used for specific cases: recently, the proposed law on the security certification of digital platforms. French legislation has known many legislative provisions, but the first one must be mentioned, the law n°88–19 of January 15, 1988, relative to computer fraud (known as the Godfrain law) which initiated the fight against cybercrime. Without elaborating, let us not forget the law n°2004–204 of March 9, 2004, adapting justice to the evolution of crime (Perben II law), or the important military programming laws, the law n°2013–1168 of December 18, 2013, relating to the military programming for 2014 to 2019, and the law n°2018–607 of July 13, 2018, relating to the military programming for 2019–2025. These laws have been of major interest—in their field—to progressively carry out an efficient fight, whether in cyber-security or cyber-defense.

It is also through the law that the strategic priority has a legal basis justifying both defensive and offensive actions. It covers three themes. First, the defense of the fundamental interests of the Nation as defined in Article 410-1 of the Criminal Code. This includes its independence, the integrity of its territory, its security, the republican form of its institutions, the means of its defense and diplomacy, the protection of its population in France and abroad, the balance of its natural environment and the essential elements of its scientific and economic potential and its cultural heritage.

The second theme complements the first, as a consubstantial element in the protection of the Nation, national security. Article L. 1111-1 paragraph 1er of the Defense Code stipulates that "the purpose of the national security strategy is to identify all the threats and risks likely to affect the life of the Nation, particularly with regard to the protection of the population, the integrity of the territory and the permanence of the institutions of the Republic, and to determine the responses that the public authorities must provide." All public policies contribute to national security.

Finally, the third theme is that of intelligence, set out in the important intelligence law of 24 July 2015, which highlighted the link—quasi-umbilical—between intelligence and national security, with article L. 811-1 of the Code of Internal Security, noting that "*public intelligence policy contributes to the national security strategy as well as to the defense and promotion of the fundamental interests of the Nation. It falls within the exclusive competence of the State*."

At first glance, the legislative and regulatory framework seems complete—but improvements are still needed, hence the modest focus on cyber security in the Ministry of the Interior's draft orientation and programming law (LOPMI), since it only deals with cyber-patrollers or the fight against ransomware. Granted, a Cyber Security Code may have been developed. But when will there be a "cyber law" which, like the orientation and programming laws adopted for defense or interior, would aim at the global theme of cyber defense, cybersecurity, and offensive public doctrine, or even more? Of course, many legislative and regulatory evolutions have been noted, and additions have been made in reaction to situations, actions, and misdeeds with heavy, even disastrous consequences. This is not an isolated case, as it is the same with terrorism where the legislative reaction is made after the fact, after an attack or a mass murder. Here again, as in the case of anti-terrorist legislation in its early days, the lack of anticipation and of a proactive posture predominates today, leaving room for circumstantial measures.

Avenues to consider

As indicated above, effective regulation is needed for cyberspace, all the more so in the absence of an international consensus or because of gaps that need to be filled, in order to have a body of effective tools and real effectiveness. To fill these gaps, two avenues can be seriously considered:

1 - the most feasible as it stands is to focus on research, innovation, and industrial policy. For example, the companies that have entered the field of cyber security, such as Thales, or the recent creation of the cyber campus at La Défense. Efforts are certainly made by the State, with the cyber security plan launched in 2021 (176 million euros for the purchase of French technologies and 515 million for research and development). 110 billion committed between 2010 and 2030 by the PIA (Programme d'Investissements d'avenir). The question is therefore not so much about the resources invested as about the related issues: installing a real innovation strategy, then reindustrializing through innovation and reinforcing this innovation culture, making tax changes to support innovative industrial companies, or bringing out new industrial champions. In fact, in addition to supporting innovation, it is clear that "*priority must be given to mobilizing all possible levers in terms of industrial policy*."[39]

2 - the implementation of digital sovereignty. But which one, European or national? In his work *Contribution à la théorie générale de l'*État, Professor Carré de Malberg observes three conditions for sovereignty: sovereignty-capacity, which is linked to independence; sovereignty-power, which is linked to competences; and sovereignty-authority, which is linked to the sovereign. Sovereignty cannot therefore suffer from any lack of those mentioned.

A European digital sovereignty, then? Some argue that it is necessary to establish European sovereignty,[40] even if there is already a lack of consensus on other important issues (Brexit, European defense, the position of certain states during the Russian-Ukrainian conflict). An even more obvious lack of consensus in the digital domain, with a "*lasting inability of the Union to fight against the predatory practices of certain Member States that take advantage of their national competence to develop 'accommodating tax measures' (tax advantages granted by certain States* *to GAFAMs)*,"[41] without forgetting an economic history that stems from three traditions: the first, colbertist and interventionist; the second, ordo-liberal, encouraging reasoned competition; and the third, Anglo-American, with deregulated liberalism. From this, and from Carré de Malberg's definition of sovereignty, a European sovereignty is a challenge, so a European digital sovereignty...

What then of a national digital sovereignty? The summary of the report of the commission of inquiry that led to the report of October 1, 2019, on digital sovereignty expressly mentions the "duty of digital sovereignty" in the face of challenges from digital giants, more precisely "*threats to our sovereignty and resulting in the challenge of the economic order, the legal order, and the fiscal and monetary system*."[42] National digital sovereignty is essential to establish a mechanism for protection and action against cyber threats. While some people call for European digital sovereignty, it is illusory without national digital sovereignty. Let's remember that "*the European Union will not be able to defend us for a long time. It doesn't know how to do it for borders. How could it do so on a subject as complicated as this, where the economic stakes are so high? We saw it during the pandemic: some EU countries (not France) were ready to sell their citizens' health data on Covid-19 to one of the GAFAMs. We must therefore avoid the trap of the slogan: "We are weak because there is not enough Europe." Let's not wait until it can defend us: it will be too late!*"[43]

The purpose of digital sovereignty is to serve national sovereignty. Because there is national sovereignty, there can also be digital sovereignty. One is exclusive to the other. Linked to the protection of the State and its population, national sovereignty implies the legitimate use of regalian prerogatives. In other words, "*the goal of digital sovereignty is to be able to exercise its own norm(s) to ensure the security of its economic, scientific and technical, and informational potential, which is necessary for the development of the country's activities, especially with regard to the digital market in cyberspace*."[44] If there is to be sovereignty, it can only be national digital sovereignty (which is appropriate, because we now have a Ministry of Economy, Finance, and Industrial and Digital Sovereignty).

To conclude, since 2008—and in considering this threat by the *White Paper on Security and Defense*—the technological means of defense against cyber threats have evolved, in order to respond as well as possible to devastating attacks, which persist and evolve, without us having a really effective response. A century ago, the historian Jacques Bainville already wrote that "*what is curious is not so much that everything has been said, but that everything has been said in vain, so that everything is always to be said again*." Thus, it is necessary to act quickly, even if we have been hearing these words for the past fifteen years. Let's not forget that the 2013 *White Paper on Defense and National Security* already discussed the slowness with which the system for fighting cyber threats was taking hold: "*How can such emergency action be combined with a longer-term political strategy aimed at establishing* *the authority of a State, the only legitimate and lasting guarantor of the protection of populations? The answer to these questions emerges too slowly in the crises where these principles are tested. The international consensus that could accompany and channel the necessary changes remains insufficient, while unprecedented situations are rapidly transforming the strategic landscape and or widening the range of possibilities.*"[45]

Appendix: Cyberattacks with a geopolitical background

Today, cyber threats are unfortunately diverse, and always have a definite impact on victims. Above all, cyber-attacks are virtual theatres of operations between states, supplanting traditional conflicts. If the great powers are not spared, cyber-attacks also affect the geopolitical area. Without having a clear answer on the identity of the aggressor, doubts or strong suspicions can appear.

Among all the publicly revealed cases, let us not forget that cyber-terrorism actions can be carried out, such as those mounted by the military branch of Hamas from a secret base in Turkey, created without the knowledge of the Turkish authorities (the headquarters of Hamas being in Istanbul).[46]

Target States	Attacks
United States	December 2020, the U.S. Department of Energy confirmed that it was the victim of a cyberattack, suspecting that hackers linked to the Russian government were connected to the case. January 2021, the FBI, and NSA, DNI, and the U.S. Cyber Security Agency confirmed that Russia had massively hacked the government to gather information through cyber espionage. The Departments of State, Defense, Homeland Security, Commerce and Treasury were among the victims of these attacks. In February 2021, a computer attack was foiled *in extremis*. It was aimed at poisoning the water supply of a Florida city.[47] May 2021, the U.S. Colonial Pipeline (distributing gasoline and other fuels) suffered a ransomware attack (*ransomware*). Without confirming the Russian government's involvement in the attack, the U.S. accused a Russian-based hacker group called Darkside of being behind the attack. Because it transports 378.5 million liters of fuel per day on the U.S. East Coast (about 45% of the fuel consumed by the region), a state of emergency had to be declared in 17 U.S. states due to the failure of one of the largest oil pipelines in the United States. The same group of hackers, Darkside, also claims to be behind the cyber-attack (ransomware) that targeted several European subsidiaries of the Toshiba group, including the one located in France.[48]

(Table cont'd.)

Target States	**Attacks**
Israel	May 2020, a large-scale cyberattack was reportedly foiled by researchers at Tal Aviv University: "*a massive informatic denial-of-service (DDOS) attack [dubbed NXNSAttack (non-existent domain name server attack)], which could have proved 800 more destructive than the one that crippled part of the U.S. East Coast Internet in 2016*,"[49] an attack that had rendered unavailable on a temporary basis, Amazon, Reddit, Spotify and Slack sites for users on the East Coast. Doubts are also emerging about Iran, which, through the hacker group, named Charming Kitten. Above all, Israel has been the victim of numerous cyberattacks carried out in particular by Iranian hackers: - May 2020, attack of hydraulic installations; - July 2020, new computer attacks against Israeli water infrastructures targeting a water pump in the Upper Galilee region and a facility south of Quds, claimed by a group of hackers called the Cyber Avengers; - November 2020, the impersonation of a former head of the Israeli military intelligence service; - May 2021, hacking of the computer system of the clothing company H&M Israel by the Iranian hacker group, identified as N3tw0rm. This attack is a blackmail on the publication of 110 gigabytes of data belonging to the company, if the latter did not meet the demands (not publicly disclosed) of the hackers.[50]
Iran	While Iran is suspected of being behind many cyberattacks, the country is also the subject of cyberattacks, claiming to be subject to thousands of cyberattacks daily. The Islamic Republic of Iran has confirmed that an Israeli-origin attack targeting the electronic infrastructure of the country's ports failed in July 2021. In October 2021, the fuel distribution system was crippled by a nationwide cyberattack.

(Table cont'd.)

Target States	Attacks
South Korea	South Korea has also not been spared from numerous cyber-attacks that have been rising sharply over the past five years, targeting South Korean defense information systems: 4,000 in 2017, 5,500 in 2018 and 9,533 in 2019. While most of the hackers' IP addresses were found to be in the United States or China, a North Korean cybercrime group was reportedly identified following an attack targeting the South Korean military's domestic computer networks, with an insignificant number of altered military documents. Even more, 1,580,000 is the number of cyber-attack attempts spotted every day in South Korea since the beginning of the year born 2021, an increase of 32% compared to the same period in 2020. Most of the attacks were carried out by North Korean hackers, with the aim of stealing money and cutting-edge technology, as well as obtaining data on vaccines and treatments for Covid-19. According to South Korean experts, hackers linked to North Korea intensified their attacks on South Korean diplomacy, security, and reunification experts during the joint military exercises between Seoul and Washington, D.C. in March 2021. A UN Security Council committee has accused North Korea of stealing an estimated $316 million over the period 2019–2021 to fund their nuclear and missile programs, and with the cooperation of Iran.[51]
Taiwan	Finally, Taiwan has seen an increase in cyber-attacks targeting Taiwanese companies since the year 2020. In December 2020 alone, nearly 100,000 cyberattacks affected Taiwanese government institutions, consisting partly of cybercrime and partly of destabilization of peripheral agencies, which were targeted due to a lack of protection of their systems and software. The island of Formosa is said to have suffered more than two million computer attacks in the first quarter of 2021 alone, attacks touching a large part of the infrastructure of the Internet of Things, shown by the example that the evolution of the threat described above is increasingly affecting so-called "smart" devices.

Endnotes

[1] *Livre blanc sur la défense et la sécurité nationale*, La documentation française, Paris, 2008, p 53.

[2] Olivier CADIC and Rachel MAZUIR, *Information report on the follow-up of the cyber threat during the health crisis*, Senate, n°502, June 10, 2020, p. 12.

[3] Even as this is being written, a cyberattack has just disrupted the United Kingdom's health care system (or NHS), resulting in a full restoration of some benefits that could take several months.

[4] V. Alexis DEPRAU, *Le droit face à la terreur*, éditions du Cerf, September 2021.

[5] *Livre blanc sur la défense et la sécurité nationale*, La documentation française, Paris, 2013, p. 135.

[6] https://www.opinion-internationale.com/2021/10/12/cyberespace-la-troisieme-guerre-mondiale-a-commence_95577.html

[7] We must give credit where credit is due, as GAFAMs did not originate in California alone. Amazon and Microsoft come from Seattle, a place famous in the world today for what concerns technology and digital.

[8] General Secretariat of Defense and National Security, *Strategic Cyber Defense Review*, 2018, p. 31.

[9] Xavier RAUFER, *Cyber-criminology*, CNRS éditions, Paris, 2015, p. 46.

[10] Bastien LACHAUD and Alexandra VALETTA-ARDISSON, *Information report on cyber defense, Assemblée nationale*, No. 1141, July 4, 2018, p. 20.

[11] This distinction was made by Roger ROMANI, *Rapport d'information sur la cyberdéfense*, Sénat, n°449, 8 July 2008, p. 12

[12] https://www.zdnet.fr/actualites/450-millions-de-tentatives-de-cyberattaques-pendant-les-jeux-olympiques-de-tokyo-39931213.htm

[13] Jean-Marie BOCKEL, *Rapport d'information sur la cyberdéfense*, Sénat, n°681, 18 July 2012, p. 16.

[14] Jean-Marie BOCKEL, *op. cit*, July 18, 2012, p. 20.

[15] Ibid., p. 21.

[16] Bastien LACHAUD and Alexandra VALETTA-ARDISSON, *op. cit*, July 4, 2018, p. 37.

[17] Éric BOTHOREL, *Information report on the future of European cybersecurity*, National Assembly, n°2415, November 14, 2019, p. 13.

[18] *White Paper on Defense and National Security*, *op. cit,* 2013, p. 89.

[19] General Secretariat of Defense and National Security, op. cit, 2018, p. 31.

[20] Éric BOTHOREL, *op. cit*, 14 November 2019, p. 11.

[21] Ibid., p. 16.

[22] https://www.zdnet.fr/actualites/l-avenir-effrayant-d-internet-et-si-le-pire-etait-devant-nous-en-matiere-de-cybersecurite-39947196.htm

[23] Christian CAMBON, *Report on the activities of the Parliamentary Delegation on Intelligence for the year 2019-2020*, National Assembly, n°3087, Senate, n°506, 11 June 2020.

[24] *Livre blanc sur la défense et la sécurité nationale*, La documentation française, Paris, 2008, p. 53.

[25] Jean-Marie BOCKEL, *op. cit*, July 18, 2012, p. 96.

[26] Jean-Marie BOCKEL, op. cit, July 18, 2012, p. 96.

[27] Xavier RAUFER, *op. cit*, 2015, p. 11.

[28] "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations until the Security Council has taken such action as is necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall in no way affect the power and duty of the Council under the present Charter to act at any time in such manner as it deems necessary to maintain or restore international peace and security."

[29] *White Paper on Defense and National Security*, *op. cit.* 2013, p. 32.

[30] As an anecdote, "*NATO was the target of several computer attacks in April 2010, attacks attributed to the Anonymous movement, and even the personal computer of the Secretary General of NATO was hacked," in* Jean-Marie BOCKEL, *op. cit.*, 18 July 2012, p. 59.

[31] For all that, "France is not in favor of creating new legal tools in public international law to adapt to these new challenges," *in* Oriane BARAT-GINIES, "Existe-t-il un droit international du cy berespace?" *Hérodote,* n°152–153, 2014, p. 204.

[32] Tallinn Manual, Rule 11 - Definition of use of force: "A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."

[33] Tallinn Manual, Rule 13: "*A State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and effects.*"

[34] Bastien LACHAUD and Alexandra VALETTA-ARDISSON, *op. cit*, July 4, 2018, p. 30.

[35] "*If a Member State is the object of armed aggression on its territory, the other Member States shall render aid and assistance by all the means in their power, in accordance with*

Article 51 of the Charter of the United Nations. This shall not prejudice the specific character of the security and defence policy of certain Member States."

36 Bastien LACHAUD and Alexandra VALETTA-ARDISSON, *op. cit*, July 4, 2018, p. 30.

37 Ibid., p. 29.

38 General Secretariat of Defense and National Security, *op. cit.* 2018, p. 36.

39 Guillaume TISSIER, "Cybersecurity: does France have the means to achieve its ambitions?" *Conflits*, September-October 2021, p. 52.

40 Industry, politicians, and parliamentarians in particular, see to this effect Éric BOTHOREL, *Information report on the future of European cybersecurity*, National Assembly, n°2415, 14 November 2019; Jean-Luc WARSMANN and Philippe LATOMBE, *Bâtir et promouvoir une souveraineté numérique nationale et européenne*, Assemblée nationale, n°4299, 29 June 2021.

41 Didier DANET, *Conflits*, hors-série, June-July 2022, p. 47.

42 Franck MONTAGNÉ, *Report made on behalf of the commission of inquiry on digital sovereignty*, Senate, n°7, 1er October 2019, p. 16.

43 Le cercle de la donnée, Agora 41, *Souveraineté numérique: essai pour une reconquête*, 2022, p. 78.

44 Ibid.

45 *White Paper on Defense and National Security*, *op. cit/*, 2013, p. 32.

46 https://fr.timesofisrael.com/le-hamas-opererait-en-secret-un-qg-de-contre-espionnage-cybernetique-en-turquie/

47 By breaking into the computer system, the cybercriminal wanted to "significantly increase the amount of sodium hydroxide—caustic soda—discharged into the water. In small doses, this chemical substance prevents corrosion of the pipes that carry water, but in large quantities, it is a poison for the body that can burn the skin and cause, in particular, serious damage to the eyes," *in* https://www.france24.com/fr/%C3%A9co-tech/20210209-l-eau-dans-le-collimateur-des-pirates-informatiques

48 https://investir.lesechos.fr/actions/actualites/une-filiale-francaise-de-toshiba-visee-par-une-cyberattaque-1962812.php

49 https://www.ami-universite-telaviv.com/index.php/recherche/sciences/informatique/1225-les-chercheurs-de-l%E2%80%99universit%C3%A9-de-tel-aviv-r%C3%A9ussissent-%C3%A0-pr%C3%A9venir-une-cyber-attaque-%C3%A0-grande-%C3%A9chelle

50 https://www.i24news.tv/fr/actu/israel/1619975074-des-hackers-iraniens-auraient-pirate-les-donnees-de-h-m-israel

[51] https://www.lepoint.fr/monde/ces-millions-de-dollars-voles-par-des-hackers-nord-coreens-pour-acheter-des-armes-nucleaires-09-02-2021-2413322_24.php