Cyber Defence Strategic Review

February 12, 2018

Sumário

Introduction – The affirmation of a new ambition for France in cyber defence 7

1 Part I The dangers of the cyber world 10

1.1 Rapidly evolving threats 11

1.1.1 Computer espionage 11

1.1.2 Cybercrime 12

1.1.3 Destabilisation 13

1.1.4 Computer sabotage 15

1.2 The main principles of action and the operating modes of computer attacks 16

1.2.1 The four phases of an attack 17

1.2.2 Attacker's infrastructure 20

1.2.3 Structuring the threat 21

1.3 Evermore vulnerable systems 26

1.3.1 An insufficient state of security 26

1.3.2 Risks associated with digital transformation 27

1.3.3 The existence of a systemic risk 29

1.3.4 The growing cyber threat 30

1.4 How to resist attacks? 31

1.4.1 Integrate cybersecurity issues into organisations at a good level 31

1.4.2 Take security into account throughout the life cycle of information systems 32

1.4.3 Know the technologies and the threat 33

1.4.4 Consider a mastered active defence 34

1.5 International regulation still too nascent 35

1.5.1 International negotiations on the regulation of cyberspace at a turning point 35

1.5.2 Theoretical foundations under construction 37

1.6 Different models of cyber defence organisation around the world 38

1.6.1 In the cyber domain, the powers are few and well-identified 38

1.6.2 Powers of a modest size capable of deploying advanced offensive capabilities 42

2 Part 2. The State, responsible for the nation's cyber defence 43

2.1 The French model of cyber defence 43

2.1.1 The origins of the French cyber defence model 43

2.1.2 The principles of the French cyber defence model 45

2.1.3 The legal framework of French cyber defence 46

2.1.4 The six missions of French cyber defence 48

2.2 Consolidating the organisation of cyber defence 52

2.2.1 Create four operational chains to conduct cyber defence missions 52

2.2.2 Modernizing the governance of cyber defence 54

2.3 Improving the protection of sensitive activities 55

2.3.1 Securing State information systems 56

2.3.2 Protection of operators of vital importance (OIV) 59

2.3.3 Protection of essential activities 62

2.3.4 Protection of local authorities 65

2.4 Strengthen the fight against cybercrime. 67

2.4.1 Finely assess the extent of cybercrime 69

2.4.2 Strengthen the effectiveness of the judicial response to improve the fight against cybercrime 71

2.4.3 Develop an international network of collaboration between magistrates and investigators 73

2.5 France's international action in the cyber field 75

2.5.1 Strengthen dialogue and cooperation with our allies and partners to prevent cyber crises 75

2.5.2 Guaranteeing European security and strategic autonomy in the digital space 77

2.5.3 Define a doctrine of action 79

2.5.4 Regulating cyberspace 84

3 Part 3. The State, the guarantor of society's cybersecurity 93

3.1 Digital sovereignty, an essential component of national sovereignty 93

3.1.1 Sovereign activities 93

3.1.2 Three technologies, among others, whose mastery is essential to our digital sovereignty 96

3.1.3 Harnessing the full potential of artificial intelligence techniques for cybersecurity 100

3.1.4 For cloud computing, invent a regulation and data protection strategy 102

3.1.5 Regulating the production and export of arms and cyber offensive activities 104

3.2 Cybersecurity regulation 107

3.2.1 The normative role of the ANSSI 108

3.2.2 Improve the certification framework to improve product security 111

3.2.3 Responsibility by environment: involving all sectoral players to raise our level of cybersecurity 112

3.2.4 Trusted providers: developing a range of cyber defence services 114

3.2.5 Developing the qualification of secure digital service providers 116

3.2.6 The establishment of a certification framework harmonised at European level 117

3.3 The cybersecurity economy 118

3.3.1 The national industrial base 119

3.3.2 Define an industrial cybersecurity policy and build a European cybersecurity industrial base 120

3.3.3 Having efficient and certified products 121

3.3.4 The cybersecurity rating and compliance issues 124

3.3.5 The establishment of a virtuous circle for securing systems through a relevant insurance mechanism 125

3.4 Human challenges 126

3.4.1 Educate cybersecurity issues from an early age 127

3.4.2 Raising awareness among the general public through educational actions 129

3.4.3 Spreading the culture of digital security within businesses and public administrations 130

3.4.4 Develop the professional training offer on cybersecurity challenges 131

3.4.5 Perfecting skills management in the state's cyber defence services: retaining and attracting our talents 133

Conclusion 135

4 Priority recommendations 137

5 Annexe 5 – Glossary 146
6 Annexe 6 – the four phases of the information system life cycle 148
6.1 Design a secure information system 148
6.2 Check security 149
6.3 Manage security over time 149
6.4 Respond to attacks 150
7 Annexe 7 – options for responding to computer attacks 152
7.1 Preventing and managing crises through international cooperation 152
7.1.1 Objective 1: prevent crises and discourage aggression 152
7.1.2 Objective 2: Contribute internationally to the treatment of an attack 152
7.1.3 Objective 3: Participate in the resolution of the crisis 153
7.2 Using retaliatory measures 154
7.2.1 At the national level 154
7.2.2 At European Union level 155
7.3 Adopting countermeasures 155
7.4 Other response options 155
8 Annexe 8 – French operational support for initiatives responding to the growing need for cooperation in the face of attacks on a European scale 157
8.1 Axis 1: Maintain a clear position with regard to the distribution of powers and the preservation of national sovereignty in terms of operational response 157
8.2 Axis 2: Promote the strengthening of national cyber capabilities on the human and technical levels, in particular via increased EU support to States 157
8.3 Axis 3: Encouraging the development of operational cooperation within the EU 157
8.4 Axis 4: Promote an appropriate model of assistance to States in the event of an incident, in particular by supporting the development of a trusted European private sector providing cybersecurity services that can be mobilised in the event of a crisis 158
9 Annexe 9 – Operational description of the cyber measures included in the military programming bill 159

Introduction – The affirmation of a new ambition for France in cyber defence

At a time when computer attacks are likely to seriously damage the interests of the Nation at any time, our country must adapt its cyber defence posture with the ambition of better exercising its digital sovereignty.

With cyberattacks increasing in number, intensity and sophistication, it is advisable to oppose a national apparatus of protection and computer defence. This requires the mobilisation of diverse capabilities and skills, within the state but also at the heart of society.

Better integrate our cyber defence means

Faced with digital threats, the degree of resistance of a Nation and its aptitude for resilience depend as much on the means as on the organisation of its cyber defence. This presupposes good coordination of the various State services concerned, their cooperation with operators of vital[1] importance and essential services, the dissemination of good practices and adopted measures to economic actors and in the population.

However, compared to the four other countries which share specific international responsibilities with it (the United States, Russia, China and the United Kingdom[2]), France still shows, despite a recently accentuated effort, a deficit when it comes to digital security.

This is why the cyber defence strategic review proposes to better structure and develop our national protection apparatus. To this end, it recommends developing a specific programme of public resources devoted to cyber defence.

Strengthening the resilience of France's vital systems

Our country must have as its primary objective the hardening of its cyber protection apparatus and the strengthening of the resilience of state networks and operators of vital importance and essential services. Above all, we must be able to guarantee the continuity of essential functions.

[1] In France, under the name of operators of vital importance (OIV) are grouped 249 organisations essential to the life of the Nation.

[2] All permanent members of the United Nations Security Council and officially endowed nuclear states within the meaning of the Non-Proliferation Treaty (NPT).

Like the human body which, under stress, first preserves its vital organs, the functions and missions essential to the survival of the Nation must be able to withstand a massive cyber shock. This impact resistance depends on the level of protection, redundancy and resilience of certain functions and the territorial continuity of communication networks.

At the top of the list of priorities, alongside national defence imperatives, is the protection of the electronic communications and electrical energy supply sectors. While these sectors provide essential services, a cyberattack against them can have repercussions for all vital activities and potentially catastrophic effects on the nation's resilience.

It is necessary to guarantee the functioning, in degraded mode if necessary, of the services in charge for civil protection, public security, medical emergencies and hospitals[3].

Besides, it is necessary to be able to restore the functioning of the main transport infrastructures as quickly as possible, which a computer incident, even on a limited scale, can disrupt massively[4]. Our transport infrastructure must also be protected against possible computer attacks carried out for sabotage purposes.

Finally, several activities are essential for the proper functioning of large institutions which are the pillars of our democracy such as the Parliament, the Constitutional Council or the judicial authority must, therefore, be considered as of the utmost importance. Securing our electoral processes and the public service of audio-visual communication also requires special attention.

Work internationally for the stability of cyberspace

In order to fully contribute to the stabilisation of cyberspace, France's international action should aim at three objectives:

[3] In 2015, in mainland France and the DROMs, 723 emergency services located in 644 health establishments treated 20.3 million acts. Alongside hospital emergency structures, 104 SAMUs and 410 SMURs provide orientation, prehospital care and patient transport (DRESS, Health establishments, 2017 edition, http://dress.solidarites-sante.gouv.com / IMG / pdf / 28-2.pdf).

[4] For example, the breakdown of a single railway signalling station in the summer of 2017 affected more than 50,000 SNCF users. With regard to air transport, our country must be able to guarantee the maintenance of a minimum flow of domestic and international traffic following a computer attack. This presupposes having the capacity to restore, quickly and under conditions acceptable in terms of flight security, l; activity of at least one of the two Parisian airport platforms, which alone represent more than half of the national traffic.

- work on the regulation of cyberspace, through the respect and implementation of existing international law and agreed standards of behaviour, as well as through the adoption, if necessary, of new standards applicable to the behaviour of States as well as to that of private actors in cyberspace. It is a model of concerted regulation of cyberspace on a European and international scale which should be sought;

- prevent computer attacks by strengthening our technical, organic and operational cooperation with our allies and partners, in particular within the European Union and the North Atlantic Treaty Organisation (NATO);

- be able to manage an international crisis linked to a cyberattack against it or one of its allies or partners, by defining reaction methods which would take full account of the politico-diplomatic and international aspects of it.

Seven principles for an enhanced cyber defence ambition

Cyberspace appears today as a catalyst for progress but also a place of confrontation, domination and all kinds of traffic. This development is neither inevitable nor irreversible. What was doubtless illusory or too idealistic was to believe that such a territory, offered to human activity, could self-regulate, resist the economic and political forces monopolizing it, remain without law and judge.

This is why the object of this strategic review, once presented the state of the threat and our vulnerabilities, is to describe a robust cyber defence strategy and to expose the proposals that France could make for the international regulation of the cyberspace. It proposes, in this logic, to place at the heart of the French ambition in matters of cyber defence, seven main principles:

1. give priority to the protection of our information systems
2. adopt an active posture of discouraging of attacks and coordinated reaction
3. fully exercise our digital sovereignty;
4. provide an effective criminal response to cybercrime
5. promote a shared culture of IT security
6. contribute to a confident and secure digital Europe;
7. act internationally in favour of collective and controlled governance of cyberspace.

To follow the progress of the various recommendations, the cyber defence strategic review recommends setting up a semi-annual progress and implementation report at the expense of the SGDSN, sent to the cyber steering committee.

1 Part I The dangers of the cyber world

As the 2013 white paper on defence and national security underlined, "information systems are now a constitutive element of our societies"[5] Therefore, it is imperative that cyberspace remains a space of trust for public actors, businesses and individuals. If the digital space is a place of communication and exchanges favourable to progress, it has also become a place of confrontation. Offensive actions against state IT systems, critical infrastructures or large companies are daily, and we cannot always grasp their origin and understand the motivations, or even distinguish with certainty who, state or non-state actors, are the sponsors and perpetrators.

It is clear that most internal or international crises and inter or intra-state conflicts now have a cyber dimension. The growing exposure of our increasingly digital and interconnected societies to the risk of major cyber crises resulting from massive attacks or produced by systemic contaminations is obvious.

To date, there have been few analyses of the cyber threat emanating from public sources. States, including France, are in fact reluctant to openly establish a diagnosis which would reveal their cyber defence capabilities in part. On the other hand, several private companies, notably publishers of antivirus solutions, have a great deal of data on their activity and the state of the cyber threat, and have produced relevant assessments. If these evaluations must be taken with caution insofar as they can serve commercial interests, once "objectified" they prove to be useful for forming an opinion and understanding certain concepts commonly disseminated. It will be referred to as necessary in the rest of the strategic review to understand, illustrate and better understand the dangers of the cyber world.

The characteristics, the mode of propagation, the evolutions and the intensification of the cyber threat are factors whose understanding is indeed essential to build an effective national computer protection and defence apparatus and to consolidate a relevant cybersecurity model for society.

Of state origin or name, with or without universal aim, emanating from organisations or simple individuals, the main characteristic of the cyber threat is its polymorphic character, It can attack in a determined way an entire country in the purpose of seriously harming it, as it can cause harm to everyone – users of computers, connected objects – indistinctly and with limited harmfulness. This is why this strategic review necessarily makes distinctions, focusing primarily on threats that can absolutely affect our defence and national security and those that can cause systemic effects on the functioning of our society.

[5] National Defence and Security White Paper, 2013 (http://www.livreblancdefenceetsecurite.gouv.fr/).

1.1 Rapidly evolving threats

The fact is known and shared: the threat of cyber origin continues to grow in its forms and its intensity. Computer attackers pursue four types of objectives, which are not mutually exclusive: espionage, illicit trafficking, destabilisation and sabotage.

In pursuit of these objectives, computer attackers can be led to conduct both highly targeted operations and massive and indiscriminate actions. With various objectives, attacks also have very variable effects: they can be invisible – during a discrete exfiltration of data for example – or conversely completely paralyze the activity of the targeted entity; any damage caused may be easily reversible or, on the contrary, require lengthy reconstruction work.

1.1.1 Computer espionage

Penetrating the heart of the information systems they target, computer attacks have the dual advantage of being particularly effective for massively stealing data and being very difficult to attribute, which limits the risks of judicial prosecution.

The objective of computer espionage is first of all within reach of the intelligence services of technically advanced countries which, for more than half a century, have developed communication interception systems for the purpose of economic, technological or political espionage. Computer espionage is only a transposition into the digital world of traditional intelligence activities. This form of espionage is, however, no longer the exclusive preserve of specialised services of States due to the diffusion of technologies and operational skills.

The digital transformation of intelligence accelerated in the 2000s with the awareness by the public authorities, but also by certain companies, of the frighteningly effective performance of computer attacks in an increasingly digital society. Many countries have thus developed cyber offensive capabilities to gather, by means of computer attacks, information which has become more difficult to obtain by traditional means. The first large-scale cyberattacks revealed were in the United States and were aimed at looting industrial knowledge and skills. Besides the Atlantic, they were regularly attributed to China. Publicly unveiled in January 2010, Operation Aurora affected at least thirty American companies, including GOOGLE, MICROSOFT, YAHOO and ADOBE. In 2013, the American computer security company MANDIANT revealed an even more massive attack campaign that is attributed to a group of identified Chinese attackers. This group has penetrated more than 150 institutions and manufacturers in Western countries for almost ten years.

Today, computer attacks carried out for espionage purposes remain a major problem. Increasingly sophisticated, they constitute the largest number of major offensives that have affected our country in recent years. They are also in France at the origin of the main cyber defence operations led by the National Agency for Information Systems Security (ANSSI) to counter them.

1.1.2 Cybercrime

Until the mid-1990s, cybercrime was reduced to one-off actions by isolated hackers, for whom technical prowess itself, beyond any political or financial motivation, was often an end in itself. If these actions could involve intrusions into sensitive information systems, public or private, their effects remained very limited. The links between hackers and certain political regimes were then anecdotal, and their actions were mainly limited to "clearing" campaigns of Internet sites.

During the 2000s, cybercrime networks gradually developed and became more professional. The appearance in 2010 of Bitcoin and then of other virtual currencies, associated with the establishment of the Tor anonymisation network, created the conditions conducive to a veritable explosion of cybercrime. If there are few precise statistics due to the low rate of reporting of cybercrimes, the multiplication of the number of computer attack tools on sale on the dark web (see glossary) testifies to this contagion.

Cybercriminals now manage to capture very large sums of money. To do this, they use two main methods, real transpositions in the digital world of traditional criminal practices. The first consists in stealing money or sensitive information directly from businesses, banks or individuals, via the Internet, for example by stealing bank information, making fraudulent transfers, or by exfiltrating and then reselling precious information on the dark web. Data from companies and individuals represent a real financial windfall. Cybercriminal groups thus engage in major thefts such as that of the data of several billion accounts of the company YAHOO in 2013. The second method used by cybercriminals is to ransom their victims, either by threatening them to reveal information that they have previously exfiltrated from their information system, or by paralyzing their activity. If the denial of service technique, which allows a website to be temporarily unavailable, has long been used for this purpose, we are now seeing increasing use of ransomware (see glossary). Finally, beyond computer attacks, digital space is also used to anonymously conduct criminal activities (Internet sales of illegal products, dissemination of illegal content, etc.).

In recent years, there has also been a gradual blurring of the line between the fight against cybercrime and the objectives of cyber defence, due either to the ambiguous nature of certain attacks or to the magnitude of their effects. We observe indeed the appearance of computer attacks carried out for the purposes of cybercrime but which, by their indiscriminate nature and their significant propagation capabilities, are likely to paralyze critical activities and therefore constitute a threat in terms of national security. In addition, the border between cybercriminal groups and states is increasingly difficult to establish, in particular due to the increasing use by cybercriminals of tools developed by intelligence agencies and then disclosed on the Internet following computer hacks. The black market for computer vulnerabilities interests both the intelligence services and cybercriminal groups.

1.1.3 Destabilisation

The third type of objective pursued by computer attackers is destabilisation. Recently observed, especially during the last American and French presidential elections, but already identified in propaganda or disfigurement actions (see glossary) of political sites during conflicts or crises, this type of operation is linked to the internet and social media development. For a long time, the development of the internet and online services was seen as a factor favouring freedom of expression as well as the dissemination of knowledge and information. These new means of communication, a priori escaping from the control of the States and overcoming borders, were to favour the freedom of opinion. This vision is not wrong. The Internet thus played an undeniable role in the "Arab Spring" and, in some cases, it enabled whistle-blowers to usefully report certain abuses.

New space of expression, the digital space is also exploited in a logic of political propaganda and propagation of ideologies with very questionable contents. Many extremist groups have appropriated not only the social media space but also the tools implemented by search engines or certain applications, with the aim of widely disseminating their ideas and reaching new targets. Online in March 2016, the experience of artificial intelligence developed by MICROSOFT, in order to learn from the behaviour of internet users how to interact with them on the social network Twitter, was quickly diverted from its goal, moreover questionable. Manipulated, this "artificial intelligence" has contributed to the increasingly frequent dissemination of racist, hateful and negationist messages. If, in this particular case, the cause and the impact of the diversion are measurable, it is not the same for the actions of influence carried out daily with the users of social networks.

Propaganda and influence actions can easily be carried out on social networks, which, unlike traditional media, do not seek to endorse or systematically control the content to which they give access. Unverified facts, even deliberately false, can thus be massively relayed on the Internet, alongside information produced by the traditional media, without one being easily distinguishable from the other. Fake news even spreads much faster than actual facts, in particular because the only criterion for disseminating information on social networks is user engagement, which gives a premium to content that moves, shocks or causes react. Some operators, however, agree to cooperate with public authorities to hinder the dissemination of content relating to child pornography and terrorist propaganda. However, in the name of freedom of expression and their neutrality, if not for convenience, many other digital players give free rein to the dissemination of ideas or messages, even if they are incentives to hatred and crime.

All the classic tools of Internet advertising (targeted dissemination of messages, analysis of data exchanged on social networks, etc.) are very easily returned for propaganda and influence purposes. Basic techniques such as flooding (see glossary), which consists of massively distributing unnecessary information to reduce the visibility of targeted content, can support these operations. In addition to these methods it is also easy to manipulate opinion to fabricate information, to disfigure websites or to usurp social network accounts. The theft of data following a computer intrusion then their publication on the Internet, sometimes accompanied by false information, are increasingly used to sow doubt, to discredit an individual, a company, an organisation, a party, or even to destabilize a political process or a trial.

In this context, some States have developed a cyber-strategy which is not limited to information systems but extends to the whole of the information sphere. Their action can go as far as censoring the content of exchanges in the digital space, or even carrying out influence actions. Thus, many countries have imposed draconian conditions on access providers in order to be able to control messages exchanged on the Internet and social networks and some also act outside their borders to influence public opinion. We are thus witnessing propaganda or destabilisation actions carried out on a large scale, carefully prepared and orchestrated, using various vectors such as the manipulation of social networks, exfiltration and then the massive disclosure of sensitive data on the Internet. Thus, during the 2016 American presidential campaign, the compromise of electronic messaging and the massive disclosure of confidential information concerning members of the Democratic team sufficiently disrupted the electoral process for President Barack OBAMA to openly accuse Russia of orchestrating the attacks targeting the Democratic candidate. FACEBOOK also confirmed to the US Congress in October 2017 that massive advertising campaigns had been bought by Russian actors on this network to influence the electoral debate in the United States, without this practice being deemed to be contrary to the regulations of the platform.

The problem of digital propaganda, like propaganda in general, is tricky to deal with exhaustively and goes far beyond the scope of a cyber defence strategic review. This is why, in the matter, the present strategic review is interested only in the activities carried out by terrorist groups and foreign powers with the objective of provoking violent or destabilizing actions for our society.

1.1.4 Computer sabotage

Computer attacks, the effects of which were once confined to the digital space, can now have potentially catastrophic impacts in the physical world. The digitisation of production systems and their increasing interconnection indeed expose them more and more to cyber risk. A computer attack is now likely to paralyze the activity of an entity not only by blocking its networks, but also by destroying its most critical equipment. These sabotage actions can have permanent or reversible, local or systemic consequences, and offer attackers an extremely wide range of effects. Recent attacks, some of which have served as tests, reveal a disturbing development, in particular by the nature of the targets targeted (industrial sites and critical infrastructures).

The computer attack suffered by Estonia in April 2007 precipitated an awareness of this type of risk. This attack effectively paralyzed activities essential to the functioning of this country for several weeks: relying on the technique of distributed denial of service (DDOS, see glossary), the offensive blocked government websites as well as the media, political parties and banking activities; emergency numbers were even unavailable for short periods. The Estonian government then accused Russia of being behind the attack. The year 2010 and the revelations concerning the Stuxnet software, deployed to obstruct the Iranian uranium enrichment programme, constituted a turning point in the appreciation of the possible uses and the effectiveness of the cyberweapon. The first “computer worm” used to halt an industrial system, Stuxnet did not however use new techniques but a unique and extremely sophisticated combination of several techniques, including the exploitation of multiple zero-day vulnerabilities and the use of infection. This attack was based on careful preparation and precise knowledge of the industrial processes implemented in the Iranian nuclear programme. Less destructive and above all less explicit, but nonetheless highly demonstrative, the computer sabotage attack on the television channel TV5 Monde in April 2015 was the first action of this nature affecting French interests[6]. The restoration of the system, which justified an emergency intervention by the ANSSI, cost several million euros and took several days. Likewise, the NotPetya attack, which paralyzed many companies with interests in Ukraine in 2017, was particularly swift and violent. The attackers took control of the servers of the company that designs the M.E.doc software to insert a backdoor (see glossary) more than two but before launching this lightning attack. This software, which equips 80% of Ukrainian companies, allowed the attackers, through an update carrying destructive malicious software, to simultaneously contaminate many companies present in Ukraine and thus to paralyze their activity. Its spread to France, fortunately little affected, by business networks with Ukrainian subsidiaries, shows the danger of this type of massive and indiscriminate attacks which, in turn, are likely to paralyze essential activities of our country without that it is directly targeted.

[6] The channel’s website and social media accounts were broadcasting jihadist propaganda, its image production system was unusable, and broadcasting was interrupted. TV5 Monde, which broadcasts in two hundred countries for fifty million viewers, had a black screen.

Computer sabotage, with destructive consequences in the physical world, is today a reality. It represents the most worrying threat, whether it is aimed directly at our country as in the case of TV5 Monde, or whether we suffer the collateral effects of it[7]. In addition, the possible collusion of terrorist groups and actors with strong capabilities techniques in this area, makes fear that one day a computer sabotage perpetrated by such movements is possible. These actions could be carried out entirely from abroad while ensuring greater protection for their authors. This hypothesis further highlights the need to strengthen cyber of the most critical infrastructures.

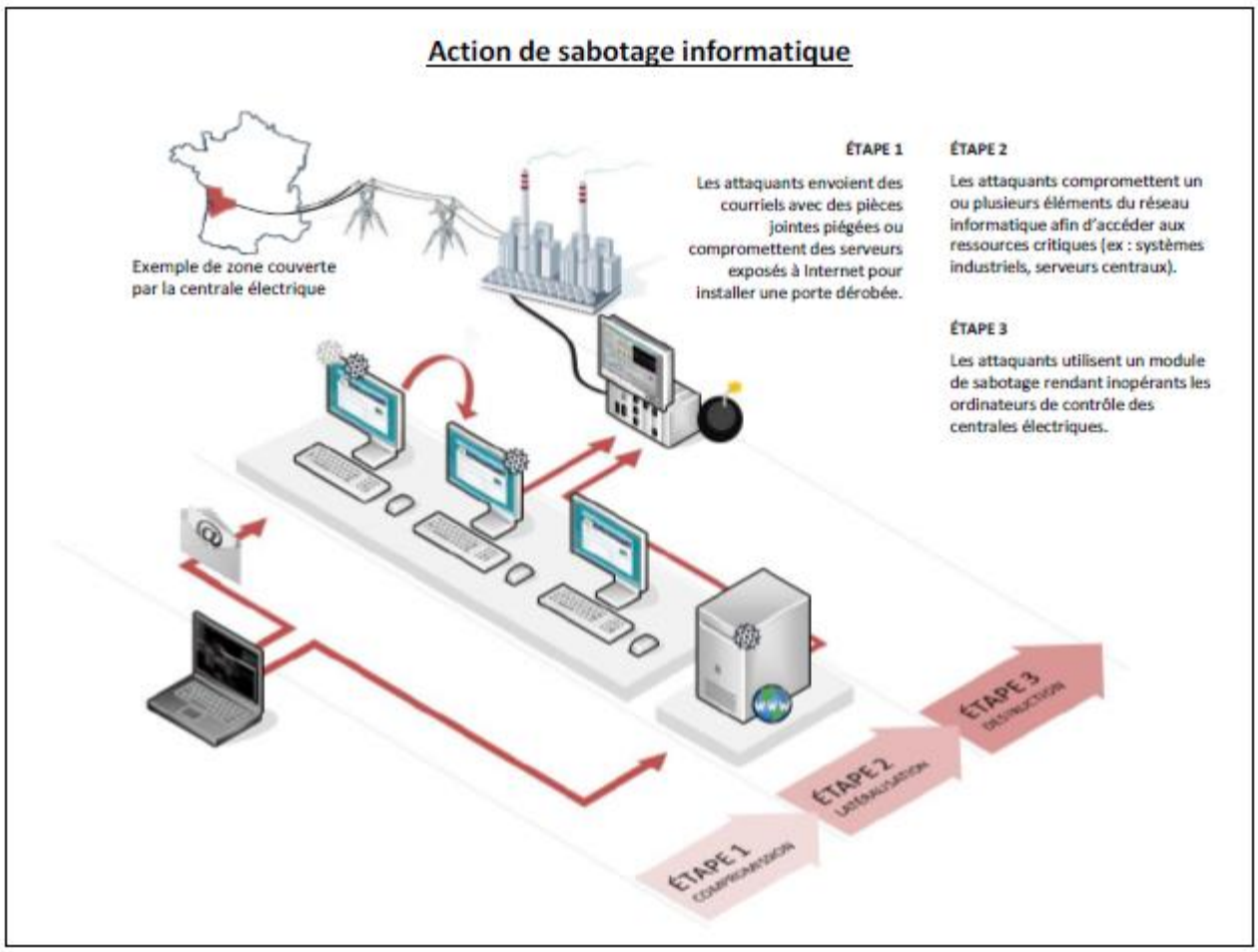


Figure 1: Cyber sabotage action

1.2 The main principles of action and the operating modes of computer attacks

Most computer attacks follow general principles of action. The process followed by a computer attacker was modelled in 2011 by academic work sponsored by Lockheed Martin[8] and then referred to as the "cyber kill chain". If these first works deserve today to be deepened, understanding this process remains essential to apprehend the modes of action of the attackers and to propose parades.

Schematically, a computer attack has four successive phases. It presupposes the development of a

[7] Saint-Gobain was the victim in 2017 of the NotPetya ransomware which targeted the Ukraine.

[8] Intelligence driven Computer Network Defence Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, by Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, of Lockheed Martin Corp.

whole range of tools which will be used to penetrate the target system, to establish itself durably on its networks and to carry out all the necessary technical operations. It also relies on management and operating infrastructures using various compromised IT equipment, purchased or rented, which constitute a real IT complex.

1.2.1 The four phases of an attack

The development of a computer attack is articulated in four phases likely to be repeated as many times as necessary to achieve the desired objective.

The first step is that of target recognition. It consists of a fingerprint that allows understanding the organisation of the victim's computer systems, identifying the technologies that the victim uses to better penetrate his system. This preparatory work can be done using data available in open source, for example on social networks such as LinkedIn. Intelligence services have more intrusive means to retrieve useful information, whether by human espionage or by interception techniques. Another way to collect this useful information is to perform a "port scan". This technique consists in sending a precise message to a targeted machine and observing the response made by this machine. This automatic response can indeed provide the attacker with valuable information on its configuration. Attackers can perform these port scans themselves, but also use databases of scans available on the Internet. If such databases are legitimately used by companies selling connected objects (which can be as varied as connected cameras or refrigerators) to obtain information on the use of their products, they can thus be hijacked by attackers to select targets.

After the impression is taken, the attacker will try to break into the target system. To this end, it will seek to exploit certain vulnerabilities of this system. To attack a computer system, an attacker can do this in several ways. It often relies on this for a user that it leads to provide, for lack of vigilance, access to the targeted information system, for example by opening a trapped attachment, by clicking on a malicious link or by connecting an infected USB key. These phishing actions (see glossary) can be particularly effective. However, there are other more advanced intrusion techniques that require no user error and are done without their knowledge. This is the case, for example, of intrusions using trapped updates of legitimate software (case of the NotPetya attack) or cases where the attacker is able to modify the electronic communications exchanged between his target and the Internet, for example taking control of a router.

CVE vulnerabilities and zero-day vulnerabilities

CVE vulnerabilities are vulnerabilities highlighted in computer programmes for which there are means of detection or even remediation (see glossary) developed by the editors of the product. They are identified by the year of their publication and a unique identifier number and allow, through a database maintained by the American association MITRE[9], to know the impacted product, a description of the vulnerability and its consequences. This de facto standard makes it possible, for example, to make the link between a vulnerability and a patch or a security update.

The zero-day vulnerabilities, unknown to the product publisher, are, however, formidable because they seem unstoppable for the victim. They are the subject of a fight between defenders and attackers concerning who will discover them first. In order to prevent their malicious exploitation, bonuses are provided, for example, during "bug bounty", that is to say competitions organised with the support of the publisher, for finding these "zero-day" vulnerabilities. And financially reward their discoverers. Attackers also engage in internal research or source from more or less legal platforms that act as intermediaries. This "uberisation" of the detection of security breaches is a phenomenon of significant magnitude because of the profits made by the sale of "zero-days". The latter now reach several hundred thousand dollars today, according to Zerodium's[10] critical flaw specialist platform. The discovery of computer vulnerabilities does not always, far from it, lead to their correction.

From the moment they are known, “zero-day” vulnerabilities are designated as “one-day” or CVE vulnerabilities. These known vulnerabilities are often still present on systems after their disclosure. The company EdgeScan, in its 2016 report, points out that the vulnerabilities on the systems are corrected on average two months after their disclosure, but not systematically. For older systems, some weaknesses may persist, especially if the system is no longer maintained by the publisher.

[9] https://cve.mitre.org/

[10] Zerodium.com. This platform was founded by businessman Chaouki Bekrar.

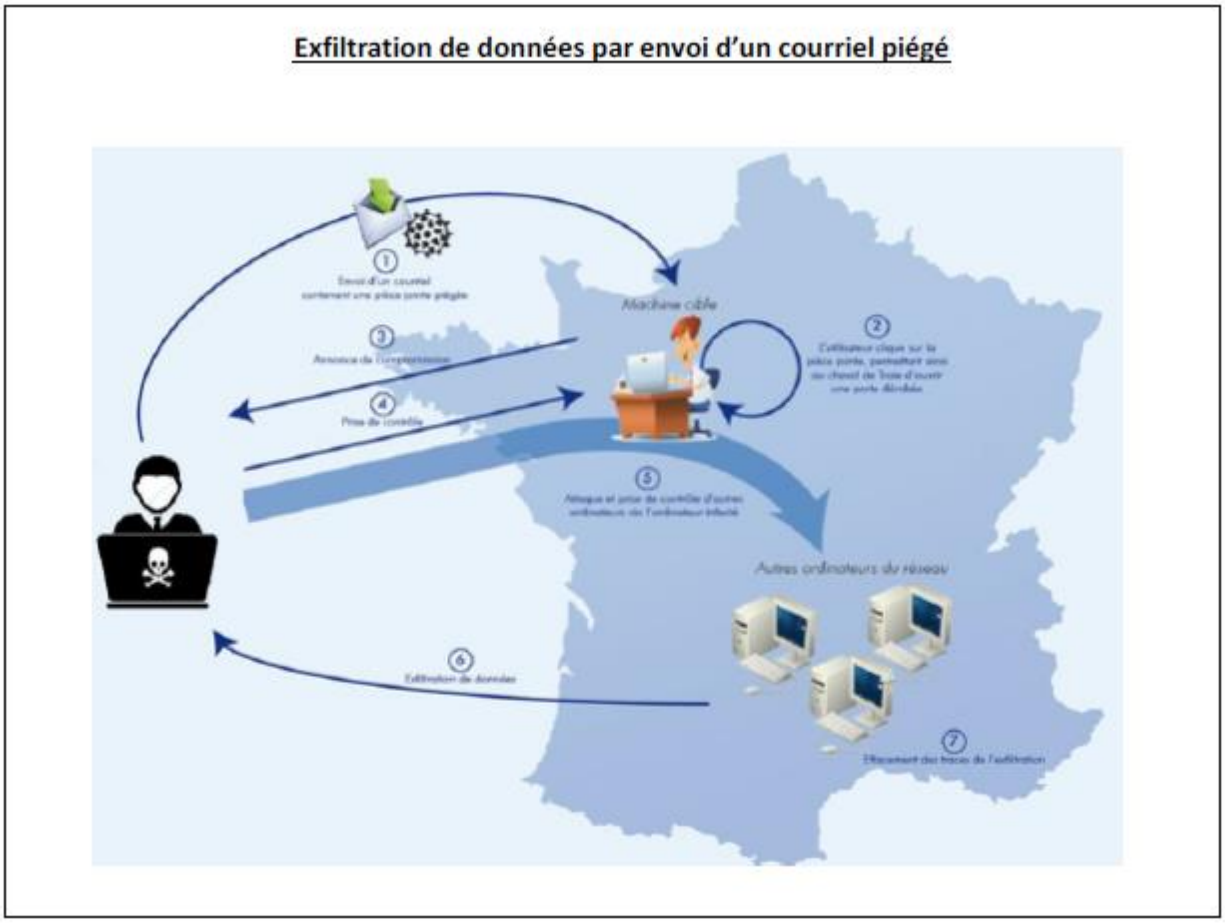


Figure 2: Data exfiltration by sending a trapped email

Once the intrusion has been completed, the attacker will install implants (see glossary) on the compromised machine to control it remotely. For this purpose, it will establish one or more connections to its attack infrastructure. He will try to be as discreet and stealthy as possible, often by encrypting his communications and camouflaging them in legitimate flows in order to remain undetectable. He will also be able to take control of the compromised equipment in order to maintain access despite reboots or updates to the system. At this advanced stage of its attack, the intruder can further extend its hold on the network and the databases of its target. This process, which corresponds to the third phase of an attack, is often called lateralisation (see glossary). It will allow the attacker to master the infiltrated system durably and to definitively take possession of it.

The final phase of an attack consists of the exploitation of the compromised system, that is to say the triggering of the effects sought by the attacker. It can last a few seconds in the case of a punctual exfiltration of data or computer sabotage or conversely extend for several years for intelligence operations. It can be more or less automated. The attacker can also, during this particularly sensitive stage, monitor if it is not detected and, in case of doubt, erase the most visible parts of its intrusion to return later.

It should be noted that sophisticated computer attacks require a fairly long preparation phase, often several months, to trigger effects which are almost instantaneous. The intrusion phase requires time, both to understand the architecture of the target system and to take complete control of it, including the backup network. The offensive against TV5 Monde in 2015 is a textbook case. It took place over three months, from the infiltration of networks to the blocking of emissions, in early April 2015.

1.2.2 Attacker's infrastructure

Carrying out a computer attack requires the possession of certain technical capabilities and infrastructures

- a "cyberweapon" (fault detectors, implants, communication channels and piloting tools);
- a command-control infrastructure, grouping together all of the servers controlled by the attacker and used to control its malware;
- an operating infrastructure to exfiltrate and analyse data.

To be able to be used consistently during a computer attack, the various malware used must be integrated, for example within a specific attack tool for a specific purpose.

With the advent of the web in the late 1990s, attack tools that could be used by non-specialists, known as “script kiddies” (see glossary), appeared. These tools, whose ancestors are called AOHell, Metasploit or even MPack, are mainly of American, Russian or Chinese origin. Their proliferation has favoured the proliferation of good level cyberattacks. Particularly well designed and modular, they make it very easy to integrate new functionalities or exploit new vulnerabilities. More advanced versions of these tools have been sold on the market for a few years under the guise of "security testing" which increases their level of performance and their harmfulness.

The use of this malware requires an IT infrastructure allowing it to be managed in a discreet manner: the attacker's command-control infrastructure. The attacker can, for example, rely on “zombie machines” which he has taken control of or compromise poorly secured servers to use them as relays. Anonymisation networks like Tor can allow it to discreetly create a logical link between its equipment and that of its targets. By choosing the geographic locations of the relays he uses well, the attacker can ensure that it will be very difficult to go back to him. In the most complex cases, this infrastructure can consist of thousands of compromised devices which can be used alternately or simultaneously. The infrastructure of the Mirai attack, which paralyzed several Internet services in 2016 for a few hours, relied on a network of several hundred thousand IP cameras to carry out a massive denial of service attack.

In addition to the command-control capabilities, the attacker can use a different operating infrastructure to exfiltrate and process data, or to collect ransoms. This infrastructure must be discreet and guarantee the transmission rates necessary for the volume of information extracted. Attackers can use exploitation means similar to those implemented for command-control infrastructures. Other solutions are possible. Cybercriminals frequently use financial conversion chains in various cryptocurrencies, making traceability of ransoms almost impossible. All of these methods, alternately or simultaneously used, make it very difficult to investigate cyberattacks and even more problematic attribution in the light of the only technical elements available.

1.2.3 Structuring the threat

During the 1990s, many hackers or groups of American, German and Russian hackers made themselves known by their exploits or when they were arrested. However, this form of activism remained the concern of some specialists. From the 2000s, the somewhat "romantic" vision of the solitary hacker will give way to the observation of a global structuring of the threat around certain groups of attackers who will both specialize and capitalize on their skills, their tools and their operating modes. This is how, in 2010, the concept of Advanced Persistent Threat (APT – see glossary[11]) appeared to characterize a set of tools and techniques used by a structured group, whether state or private.

State involvement is also profoundly transforming the nature of the cyber threat. This is now embodied by powerful and structured public and private organisations which replace the small groups of experts from the beginning. Certain countries, seeking to anonymize their actions in cyberspace, delegate the task of carrying them out to private entities. For example, many anti-virus publishers today publicly link around 20 to China:

- APT1, the first group known by this name Since 2006, this group is at the origin of the compromise of computer systems in more than 140 companies in many industrial sectors aiming to steal sensitive data, whether acts on patents for manufacturing processes, commercial strategies or even contracts content. After having methodically penetrated the computer networks of these companies, sometimes lurking there for several years, this group has managed to regularly exfiltrate considerable masses of information. To achieve this, APT1 used a thousand servers, industrializing both the intrusion phases but above all the operating phases. Several hundred people would be employed to maintain this infrastructure and to guide the search for documents, their translations and their exploitation.

- The attacks on TV5 Monde (APT28[12]) and NotPetya are another illustration of the structuring of groups of attackers under the impetus of a State. The APT28 group, which has been raging since 2008, is said to have successively attacked institutions in Georgia and eastern Europe, as well as NATO and armaments fairs like Eurosatory. Oriented towards data theft at first, APT28 then specialised in influence thanks to the publication of exfiltrated data. The United States has attributed to the APT28 group the exfiltration of data from the Democratic Party during the 2016 American elections. Likewise, the World Anti-Doping Agency linked to this group the theft in 2016 of data relating to high-performance athletes who 'she owned.

[11] Designation introduced by the Mandiant Company.

[12] Also known as Fancy Bear or Pawn Storm.

The Lazarus group, linked by many security actors to North Korea, has been carrying out large-scale operations since 2009. After targeting infrastructure in South Korea, it became famous for attacking the security systems. information from the company SONY where he had access to films not yet broadcast but above all to the personal data of all employees. Later, this APT seems to have been directed towards financial institutions, casinos and cryptocurrency systems in order to steal as much money as possible. The link made between the Wannacry ransomware and this group, notably by the English government and then by the American, Canadian and Australian governments, only confirms the new directions of this APT: recovering cash on behalf of the North Korean government. Difficult under these conditions to make a distinction between this APT, supposedly governmental and whose motivations seem only financial, and the group of cybercriminals named Carbanak who, between 2013 and today, is suspected of having stolen no less than 'a billion dollars by attacking more than a hundred banks in more than 30 countries.

The table below presents a non-exhaustive history of attacks attributed to APTs. For its part, France has chosen not to make the elements available to its public.

Name	Type of attack	Effect of attack	Target	Period
Titan Rain	Espionage	Extraction of a lot of information	American and British administrations and companies	2003 to 2006
Shady Rat	Espionage	Data extraction targeting more than 72 entities mainly in the United States	Governments or associations	2006 to 2009
Comment Crew	Espionage	Extraction of sensitive information from more than 141 high-tech companies	Global companies	2006 to 2013
Bronze Night	Sabotage	DDOS on many Estonian government and industrial websites	Estonia	April 27, 2007
DarkHotel	Espionage	Passwords stolen from luxury hotel customers in Asia	Luxury hotels in Asia	2007 to 2014
Operation Aurora	Espionage	Looting for two years of sensitive information	American web companies	2009 to mid-2010
Stuxnet	Sabotage	Malfunctions and premature wear of the centrifuges at the Iranian uranium enrichment plant in Natanz	Iran	June 23, 2009, to May 13, 2010
Shamoon	Sabotage	Erasing more than 30,000 computer hard drives with a file containing an image of a burning American flag	National Saudi Company Hydrocarbons (SAUDI ARAMCO)	August 15, 2012, to September 1, 2012

Name	Type of attack	Effect of attack	Target	Period
Yahoo	Cybercrime or espionage	The attackers, who first entered YAHOO's systems in 2013 and then in 2014, stole information from 3 billion users. Two first sales of this data were detected in August 2017, but the motivations of the group or groups are not clearly identified.	YAHOO	2013 and 2014
Carbanak	Cybercrime	By taking control of many banks and financial institutions (more than a hundred), the attackers managed to steal up to US$ 1 billion by fraudulently making transfers and cash withdrawals from distributors	banks	2013 to 2014
Sony Picture Entertainment	Destabilisation	Theft of numerous data and disclosure of films not yet released and confidential data	Sony Picture Entertainment	November 2014
TV5 Monde	Sabotage	Paralysis of all the broadcasting means of the TV5 Monde channel for 2 days.	TV5 World	April 8 to 9, 2015
Democratic Party	Destabilisation	Theft and disclosure of numerous emails from the Democratic Party (20,000 emails) and attempt to destabilize the Democratic candidate in the 2016 US presidential elections	American Democratic Party	Summer 2015 to July 2016
Bank of Bangladesh	Cybercrime	Theft, through fraudulent transfers, of US$ 81 million.	Bank of Bangladesh	February 2016
Dyn	Sabotage	The attack via a DDOS blocked the services of the company DYN, making the internet unavailable for a few hours.	Internet	October 21, 2016
WannaCry	Cybercrime	Encryption of over 300,000 computers and ransom demand for data recovery	Not targeted	May 12 to 15, 2017

Name	Type of attack	Effect of attack	Target	Period
NotPetya	Sabotage	Destruction of many computer systems using Ukrainian accounting softwareME.DOC	Ukraine	June 27, 2017

Figure 3: History of attacks attributed to PTAs

1.3 Evermore vulnerable systems

The increase in the general level of the threat is only slightly compensated today by the improvement in the level of security of the systems. Faced with the explosion in the number of attacks, awareness of IT risk remains very insufficient today. In a context marked by the massive digitisation of data and the growing interconnectivity of networks, securing computer systems is becoming an imperative and a crucial issue for our societies, which are now exposed to real systemic risks.

1.3.1 An insufficient state of security

The first malware closely followed the creation, in 1969, of the Arpanet (American military network, ancestor of the Internet). The Creeper software, from 1971, is thus the first programme to be replicated from server to server with no more malicious intention than displaying on the screen a parasitic message "I'm the creeper, catch me if you can ".

During the 1980s, the development of home computing, with Apple II computers and the first PCs running MS-DOS, encouraged the proliferation of malware, which however was not yet a real danger. The damage caused was limited and often unintentional. Like the denial of service caused by the Morris worm (cf. glossary), from the name of its inventor who was also the first condemned under the American law "Computer Fraud and Abuse Act" adopted by the Congress in 1986[13]. It was also in the late 1980s that the first antiviruses appeared. The companies that developed them at the time – McAfee, Symantec, TrendMicro and Kaspersky – are still the leaders in the field today (see Annex 6).

It was at the turn of the 1990s and 2000s, with the rise of the web, that really toxic software appeared, such as the Iloveyou worm created by two Filipino students or the Klez malware which infected computers by the millions by spreading via the Internet messaging for their victims. In response to these large-scale attacks, the Clinton administration took a series of measures to strengthen the computer security of the United States administration and launched a US$ 1.5 billion plan to better ensure the security of federal agencies. In parallel, the first Snort detection probe was proposed as an “open source” project by Martin Roesch. The latter then founded, on the basis of this project, the company SourceFire, which became the first global company in the field to be acquired by Cisco in 2013.

Since then, we have been witnessing a race between the invention of malware and antivirus, between the deployment of increasingly sophisticated attacks and the hardening of protections for computer systems. Often behind the advances of the attackers, computer defences remain too weak. Few companies or administrations today have robust and secure "state of the art" information systems. There are three main reasons for this: the often-insufficient initial level of protection of IT equipment and software offered for sale, the lack of security updates for older products and, finally, the insufficient consideration by cybersecurity companies as a strategic component of their digital transformation.

[13] In France, the Godfrain Law of January 5, 1988 was the first law relating to computer fraud and computer intrusion (Law n. 88-19). This law notably introduced the concept of an Automated Data Processing System (STAD).

1.3.2 Risks associated with digital transformation

The computerisation of systems is not a recent phenomenon. The first industrial programmable logic controllers appeared in the late 1970s to meet the needs of car manufacturers to modernize and automate their production chains. This equipment made it possible to make the link between the digital world and the analogue world. This is why they have imposed themselves in all production chains, in modern buildings to manage, for example, air conditioning systems, or on-board aircraft and ships in propulsion or navigation functions. Mass deployment of on-board computing devices began in 1980 when GENERAL MOTORS was the first automaker to use a processor with 50,000 lines of code to improve engine performance. It was quickly imitated by its competitors and, today, there are commonly found on motor vehicles between 20 and 100 processors running several million lines of code.

Having become ubiquitous in all systems, IT products are no exception to the laws of the market. However, these tend to replace, in a logic of cost control, specific products for more versatile products whose customisation is easy but which include, sui generis, many superfluous functions. It is therefore not surprising to find services such as a "web server" in industrial machines used in an environment that is completely isolated, simply because the generic component used included this functionality. This trend is also reflected in a technological convergence which tends to place the same computer components in systems, however very different. This kind of situation results in increased vulnerability of the systems because potential attackers can have easy access on the market to the computer components in question to prepare their misdeeds.

The other notable evolution of our systems is the increasing interconnection of which they are the object. Like what can be observed with the installation of smart electric meters, many systems present in everyday life are now interconnected via the Internet or specific connections in order to facilitate and reduce the cost of their operation and allow new services. The functioning of certain systems is even sometimes dependent on their good connection with an external server. Interrupting it is therefore enough to render the system inoperative. Their interconnection is a new source of vulnerability[14] which offers a potential attacker two opportunities to exploit:

[14] For this reason, solid work to secure ENEDIS electric meters has, for example, been carried out in close collaboration with ANSSI.

- it offers an infrastructure, or "botnet"[15] (cf. glossary), allowing to carry out massive attacks like that operated by the Mirai malware which, by taking control of a set of video cameras connected to the Internet, has achieved a massive denial of service on part of the web;

- it exposes the systems to a risk of computer attack via their connection to an external network. For example, American researchers succeeded in 2015 in taking control of a vehicle from a smartphone and the CIA was able to spy on targets using cameras and microphones incorporated into televisions.

If it makes it possible to envisage an improvement in the living conditions of the populations and a better management of resources, the prospect of the establishment of smart cities and territories in which will be superimposed and will be interconnected the energy grids, electronic communications, transport, water and waste management will significantly increase the opportunities available to attackers. In this regard, the ambitious choice to make the French capital a digital city in 2024 on the occasion of the Olympic Games must be accompanied by a fundamental reflection on the security of information systems that will support the digital transition in Paris and event management. Substrate for these future deployments, the clouds that will allow the collection of data from these connected cities will constitute potential targets, as will the algorithms that will process this data.

The number of connected objects will be in the tens of billions by 2020 (estimates of this number will vary from 26 to 212 billion[16]). These objects will facilitate everyday life while bringing new functionalities at reduced costs. The "Internet of Things" that they will constitute may, however, be the target of computer attacks with consequences going as far as the loss of human lives when, for example, connected objects used in the health field are targeted. This risk is compounded by the fact that many manufacturers do not secure their connected objects in order to reduce the development cost and speed up their commercialisation. If the current development dynamic is maintained, "botnets" of connected objects will thus massively supplement the traditional "botnets" of already existing computers, further weakening the level of security in the digital space.

An awareness of these dangers appears necessary. It should then quickly lead to the implementation of a real strategy for the development of connected objects with a minimum level of security. Otherwise, user confidence will deteriorate, and the future of digital will become more uncertain. The cyber defence strategic review presents several avenues in this in its third part.

[15] Networks of compromised robots that are in the hands of a group of attackers to conduct their attacks.

[16] Source: "Cyberattaques. Prévention-réactions : rôle des États et des acteurs privés", Karine Bannelier, Théodore Christakis, in *Les Cahiers de la revue Défense Nationale*, April 2017.

1.3.3 The existence of a systemic risk

Apart from traditional attacks on bank cards, the first major computer attacks on the financial system were carried out by hijacking the Swift[17] system. This system, which allows exchanges between banking establishments by guaranteeing the authenticity of transactions and by archiving them, is one of the pillars necessary for the proper functioning of the international financial system. The attacks carried out by the APT Lazarus Group or Carbanak have enabled them to steal up to a billion dollars, may seem derisory if we compare their earnings to the amount of daily transactions carried out by Swift (every day, more than 8 million transactions totalising billions of dollars). For their authors, they nevertheless turned out to be very lucrative and could give ideas to other criminal groups, even to countries, which could by this means recover financing from carrying out clandestine activities or even make disappear part of the assets. financial of their opponents or opponents. In this context, the confidence placed in the current system of financial transactions by market players could be significantly degraded, and the risk of an entire system collapse cannot be ruled out.

Supply chain attacks, such as the NotPetya malware in 2017, fall under other scenarios that can also produce cascading effects beyond control. These attacks are proving to be very effective since the trap arrives at the target via the usual supply chain or through legitimate system updates, which does not arouse suspicion. If it is effective, this mass trapping presents two major risks:

- that of producing collateral damage which can itself generate a response and an uncontrolled escalation due to an imprecise initial targeting;
- that of seeing another group of attackers discover the vulnerabilities introduced and divert them for their own use, which may be against the user of the device[18].

Serious damage to the credibility of the international financial system, the inability of attackers to circumscribe in time and space the collateral damage of their attacks, constitute the seeds of a major systemic risk for the functioning of the economy and society.

[17] Swift is administered by the company of the same name: Society for Worldwide Interbank Financial Telecommunication.

[18] Thus in 2005, following the sale of the "personal computer" branch of IBM to the Chinese company LENOVO, several Anglo-Saxon intelligence services decided to ban the use of computers from this brand within their organisation fearing their trapping by the Chinese State.

1.3.4 The growing cyber threat

States today are confronted with an evolution of the cyber threat, revolving around three factors:

- the danger of the threat, under the effect of the multiplication of actors, the increase in the offensive capabilities of certain foreign powers, the proliferation of computer weapons and the trivialisation of attack techniques;

- the overlapping of cybercrime and national security issues. The tools traditionally used for fraud and extortion purposes, such as ransomware, can cause damage to the information systems of the State and operators in charge of critical infrastructures, thus paralyzing the continuity of their operations. activities. This has been observed in particular with the effects of the WannaCry attack on the British healthcare system;

- increased exposure of our society to the threat due to its wider digitisation and the large-scale use of connected objects (cf. 1.3.2).

In addition to the countless computer spy operations that are very regularly detected and the well-documented risks of data looting or denial of access, acts of blocking or sabotaging computer systems (which may also be linked to cybercrime), are more and more often noted. It is likely that a computer attack of this nature will one day have lethal consequences.

Our democratic societies are more and more often confronted with the misuse of the Internet and social networks for the purpose of manipulating opinion and institutional destabilisation.

More and more attacks combining different modes of action and seeming to pursue several ends, reveal a work of planning and infiltration upstream led by actors with advanced capabilities.

We are also collectively confronted with the rise of a kind of IT Golem, which, from the manipulation of misappropriated vectors (zombie computers, compromised connected objects, etc.), is likely to trigger unpredictable phenomena of great magnitude., ranging for example from the disclosure of a considerable amount of data to the electric blackout of a city.

Faced with the evolving threat, it is necessary for our country to consolidate and make consistent its objectives and its cyber defence capabilities.

Towards a cybernetic "Far West"?

Few prospective studies exist in the cyber domain, whether they concern future technological developments or employment doctrines. The evolutions imagined at present are often linked to the medium-term appearance of the quantum computer, which could give the states in their possession a significant superiority in the field of security by allowing them to "break" the algorithms. of current cryptography. It is, however, difficult to give a date, even an approximate one, of the entry into service of such computers, which supposes the advent of a real technological revolution, probable but to this day still uncertain. The first copies of these machines existing today are still far from what would be necessary to bring true supremacy.

On the other hand, it is certain that the threat will worsen in the next decade, resulting in a more dangerous and less stable cyberspace, where computer attacks will be commonplace, forcing public institutions, businesses and individuals to protect themselves more strongly than today. This scenario is described by the Center for Long Term cybersecurity at the University of Berkeley as "the new normal." In this context, we can make the choice of greater control of risks, thanks to a reinforced cyber defence and a more robust hygiene of cybersecurity in our society, or on the contrary to let us drift towards a kind of "Far-West" cybernetics.

This future is less conditioned in the immediate future by cyber technology than by the development of new hardened self-defence applications that take security issues more effectively into account. In this respect, the level of protection and control of the Internet of Things and artificial intelligence appears to be a decisive element for the security of our society.

1.4 How to resist attacks?

Under the double effect of an increasing threat of cyber origin and an increased vulnerability of our information systems, the ways and means of ensuring our cyber defence are now essential issues for our society[19].

After having posed the main challenges in terms of governance and risk analysis (1.4.1), this strategic review highlights the need to take security into account throughout the life cycle of systems (1.4.2) and be familiar with the technologies available to deal with the threat (1.4.3), then discusses active defence techniques (1.4.4).

1.4.1 Integrate cybersecurity issues into organisations at a good level

With several years of hindsight, it appears that taking into account cyber threats and implementing appropriate countermeasures within a public or private entity is only truly effective if they fall under the highest level of responsibility. Thus, the level of risk relating to information systems, taking into account the protection measures put in place, must at all times be known and accepted by the management of the entity. To assist in this follow-up, the latter may appoint an information systems security manager, possibly assisted by a group of personnel constituting an SSI functional chain. By virtue of the principle of separation of roles, it is essential that this functional chain is not subject to the hierarchical authority of the management of the entity's information systems. In addition, its role in monitoring the security level of the information system and preparing the related decisions should in no case lead to the disempowerment of the entity's management level.

[19] A mission on artificial intelligence was entrusted to deputy Cédric Villani (see Part 3).

To drive their digital transformation, companies or government departments set up a specific organisation with a manager responsible for driving these developments. These digital directors or “chief digital officer” are often integrated into the management committee and rely on traditional IT departments to lead both the evolution of digital systems in the company, the digitalisation of different business processes, the acculturation of staff to this digitalisation but also to transform the "Business models" of their entity by taking full advantage of the opportunities offered by digital. Also, when such managers exist within a structure, it is essential to also entrust them with the responsibility for the cybersecurity of their project and especially the analysis of the associated risks. The integration of cybersecurity elements from the reflection stages and at a high level makes it possible to assess ab initio the risks of the different options of the digital transition and to considerably improve security, often at negligible additional cost.

1.4.2 Take security into account throughout the life cycle of information systems

Faced with increasingly advanced and evolving attacks, the concept prevailing for many years of a defence based solely on perimeter prevention measures has demonstrated its limits. Thus, whatever the quality of the preventive measures implemented – which remain all their relevance anyway – it is now unrealistic to consider that an information system will remain strictly tight against attacks. On the contrary, it should be taken as an axiom that a motivated attacker will always end up gaining ground within the information system. Adequate defence must, therefore, be extended to the entire information system to be protected, in a defence-in-depth logic, and incorporate a section devoted to detecting and reacting to attacks. this.

More fundamentally, the consideration of security must be effective at all stages of the life cycle of an information system, which can be schematically described according to four phases (cf. appendix 8): design and development phase; system security acceptance and verification phase; operational life phase of the system with, in terms of security, a double challenge of maintaining security and supervising in order to detect attacks; reaction phase to possible attacks.

Failure to take security issues into account in one of these stages greatly impairs the ability to guarantee system security throughout its life. Thus, it is illusory to pretend to achieve a good level of protection by a simple audit and the correction of the vulnerabilities identified on this occasion, if the right technical and organisational choices were not adopted from the design of the system. Likewise, the absence of security oversight of a system, whatever its initial level of security, can only ultimately lead to an illusion of security.

Each phase of the system life cycle calls for specific skills, both technical and methodological, and is associated with a number of good practices. The development of these good practices also requires, at each stage, regularly updated knowledge of available technologies and the state of the threat.

Finally, the sequence of these different phases must be considered as a cycle rather than as a linear sequence, since the reaction to an identified attack must naturally lead to a review of the system design and iterative improvement in its security. This cyclical sequence of stages in the life cycle is all the more justified in the case of development structured according to so-called "agile" methods, which see successive numerous development cycles and the related security stages, including the absence of identified attacks.

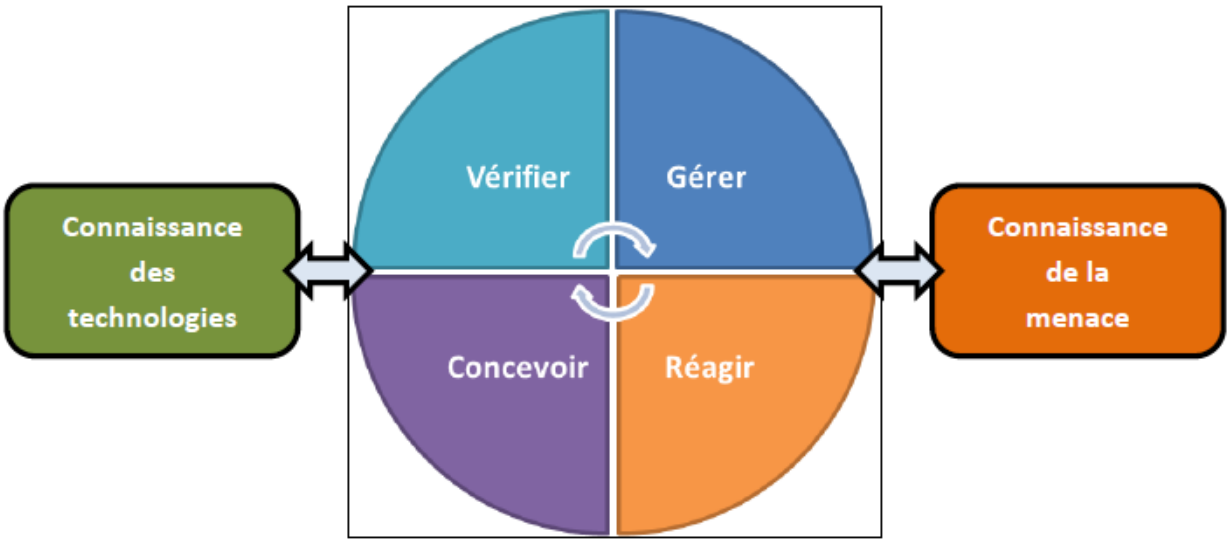


Figure 4: The life-cycle of information system security

1.4.3 Know the technologies and the threat

A security approach can only be effective if it is fuelled, at all stages, by regularly updated knowledge of the technologies and the threat. Maintaining such knowledge requires a significant investment, which is not justified for the majority of entities deploying secure information systems. This knowledge should therefore in most cases be sought from specialised administrations, or from cybersecurity service providers.

Technically, the cumulative integration of feedback from the design and implementation of secure information systems must first be achieved. It is then a matter of having an in-depth knowledge of the available technologies and understanding their security mechanisms, their contributions, their limits and their vulnerabilities. An active watch, covering both the new solutions put on the market as well as the vulnerabilities identified in the existing solutions must be conducted and, if necessary, be supplemented by mock-up and test actions. The early identification of the main technological breakthroughs or changes in uses must also be sought in a logic of anticipation, which requires a close relationship with the field of academic research.

Knowing threats must, for its part, integrate a precise and up-to-date identification of the tools used by attackers in order to deduce therefrom, in particular through the reverse engineering of samples of malicious code, characteristic markers likely to feed the attack detection solutions. It also aims to describe the main adverse operating modes, with a double challenge of identifying the preferred targets of these operating modes, and of understanding for each of them the processes and techniques implemented at each stage of a cyberattack, from the reconnaissance phase to the operational phase. Knowledge of the threat is fed by a capacity to monitor and analyse information available in open sources, by information from the supervision and detection means implemented within the various protected information systems, and by the result of analyses conducted in response to attacks. These elements can be usefully supplemented by comparable reports and analyses made available by third-party organisations. The sustainable development of knowledge requires an ability to carefully capitalize on a vast body of information, the life cycle and rules for sharing with third parties must be carefully managed.

1.4.4 Consider a mastered active defence

To complement current cybersecurity systems, new, more active and aggressive techniques are starting to be implemented in an increasingly systematic manner. Between a purely passive defence and resolutely offensive measures, they are grouped in the category of excessive active defence.

The techniques known as “honey pots” thus aim to attract attackers to fake targets so that they reveal their tools, which will then make it easier to spot them. This technique, which is widely used by researchers, allows them to observe a wide range of malware.

Another technique, known as “sink-holing” (cf. glossary), consists in observing the actions of an attacker by diverting the flows going up towards its command-control infrastructure to a controlled server. This type of operation, often carried out by antivirus publishers, allows them to observe the attacker for several years and to understand the intended targets and the objectives pursued. However, during the time of the observation, the attacker pursues his misdeeds, which questions the attitude of the industrialist who is aware of an offence and decides alone to let it take place to obtain knowledge about attackers which he will then develop for his benefit.

To stop an attack, victims may also be tempted to destroy the attacker's infrastructure by deleting the servers they use for their command-control infrastructure. These actions can be done by judicial means by "seizing" the means complained of. This approach undertaken by MICROSOFT with the support of the FBI has enabled them in recent years to remove many "botnets" from several hundreds of thousands of machines. But other techniques without legal basis are also used to render the infrastructure of an attacker inoperative.

The victim may also be tempted to counterattack using the same techniques as his attacker. This practice, in contradiction with national and international law, called "hackback", can be used to recover stolen data, destroy the attackers' system, or even steal the means at their disposal. This mode of action, which seems to have already been implemented in a few cases, leads to an inevitable escalation, collateral damage being more than probable and the attacker may himself want to retaliate again.

All these techniques raise the need to clarify international law in this area to avoid inextricable situations or uncontrolled escalation.

1.5 International regulation still too nascent

The previously presented picture of an ever more structured threat and of systems made more vulnerable by digitisation and their increasing interconnectivity is part of an international context where no multilateral agreement has yet been found to establish an architecture and rules for common security governing relations between states and between private and public actors in the digital age.

1.5.1 International negotiations on the regulation of cyberspace at a turning point

Cyberspace is not entirely devoid of norms and rules, to the extent that those of international law or the main principles which govern relations between States apply to them. Thus, the negotiations, under the aegis of the United Nations, of the “group of government experts on cybersecurity” (GGE), organised in different formats five times between 2004 and 2017, made it possible to recognize, from 2013, the applicability of international law, and in particular of the Charter of the United Nations, to cyberspace, then to consolidate, in 2015, a base of voluntary commitments of good conduct for States in this field. These “responsible behaviour standards” revolve around several main principles or objectives. In order to facilitate cooperation and reduce the risk of misunderstandings, it is therefore recommended that States show transparency on their organisation and their national posture in terms of cybersecurity and adopt a cooperative attitude towards victim countries attacks from within their own territory, especially when the attack targets critical infrastructure. In order to strengthen the overall resilience of the digital space, each State is also encouraged to strengthen its own cybersecurity at the national level, and in particular that of its most sensitive systems, such as those of critical infrastructures. Another objective is to combat the proliferation of malicious IT tools and to preserve the integrity of the digital supply chain. It may also be recalled that it appeared important for the States participating in these negotiations to undertake, outside the context of military operations, not to damage the critical infrastructure of another State or to deteriorate their capacity to provide their service to the public.

During the last round of GGE negotiations 2016-2017, France made proposals to its partners to deepen this work and clarify all of these standards, in particular on the prohibition of hackback practices (counter-cyberattack see glossary) by private actors or the imposition of export controls for malicious cyber tools. These proposals were generally the subject of a consensus, but negotiations failed on the question– uncorrelated – of the modalities of application of international law to the conduct of States in cyberspace.

This failure of negotiations within the UN GGE is the sign of a fundamental divergence in perception, among the different countries, of the international security architecture that should govern relations between states in the digital age. In the short and medium terms, this incompatibility signals the end of negotiations at the UN on the responsible behaviour of states in cyberspace.

The failure of this last round of negotiations in no way calls into question the standards and principles agreed in previous years. In addition, it must not put an end to the efforts of France and the international community to promote standards of behaviour and confidence-building measures in favour of the stability and international security of cyberspace.

Beyond relations between states alone, a major regulatory effort remains to be carried out in particular around the activities of the private sector. The emergence of digital technology as a new tool and space for confrontation indeed gives this sector, and particularly to certain systemic actors, an unprecedented role and responsibilities in the preservation of peace and international security.

On these various subjects, the States will not be able to create and impose rules alone on all the actors of cyberspace. In recent years, several initiatives aimed at promoting certain visions of international regulation of cyberspace, using a holistic approach integrating actors from the private sector and civil society have also emerged.

Launched in February 2017 by the Minister of Foreign Affairs of the Netherlands, the Global Commission on the Stability of Cyberspace aims to develop original proposals for international standards, with the aim of "encouraging responsible behaviour by state and non-state actors in cyberspace". The Commission is made up of twenty-six commissioners (including a French one) representing a wide variety of geographic regions and stakeholders (governments, industry, technical community, civil society) and chosen according to their legitimacy to express themselves on the issues. different aspects of cyberspace. At the Global Conference on Cyberspace held in New Delhi in November 2017, this Commission called on state and non-state actors to commit to protecting the "public heart of the internet".

In addition, private companies also intend to take part in these debates. MICROSOFT thus, from 2014, proposed to States a set of behavioural standards relating to the various aspects of international cyberspace security (fight against proliferation, responsible management of vulnerabilities, assistance in the event of a crisis) before proposing in 2016 that these standards are included in a “Geneva Digital Convention”. MICROSOFT is also at the origin of a set of behavioural rules for the private sector (the TechAccord).

1.5.2 Theoretical foundations under construction

In this “post-GGE” world in which we now live, where international peace and security in the digital society are still under construction, and the respective roles to be played by States and private actors yet to be defined, the theoretical foundations of cyber defence are still under discussion, both within countries and within various international organisations. Several major trends emerge, however.

The classification of threats and the severity of computer attacks appears, first of all, as a shared necessity. The United States has developed an apprehension grid for cyberattacks which, if it cannot be transposed without adaptation to all countries with regard to the specificities of their cyber defence organisations, constitutes an interesting reference.

In addition, technological advances call into question some of the “state prerogatives”. The extraterritoriality of the data also calls for the structuring of new theoretical foundations.

Finally, the question of the application of the concept of deterrence to cyberspace continues to be the subject of numerous debates at the international level. France reserves, for its part, the term of deterrence in the military nuclear field. As the ultimate guarantee of our sovereignty, deterrence is based on the unique nature of nuclear weapons. The cyberweapon cannot exercise the very specific restraint or deterrent effect observed and maintained with nuclear deterrence because of its profoundly different effects. Finally, the "grammar" of nuclear deterrence is unique and does not apply to cyber actions.

The concept of "cyber deterrence" advanced by some has at least three limits:

- first, any act of deterrence is based on clear and credible rhetoric. However, in terms of cyber, publicly revealing its capabilities amounts to compromising their effectiveness to the extent that this can lead the potential adversary to take the necessary measures to deny any possibility of a cyberattack. Cyber deterrence cannot, therefore, be absolutely effective, since the weapons on which it is based can quickly prove to be ineffective if countermeasures are deployed;

- second, cyber weapons do not have the same deterrent effect as nuclear weapons, the latter having the unique capacity to inflict absolutely unacceptable damage, out of proportion with the benefit of aggression. It is a weapon of another nature, without continuity with conventional and cyber means. The equation is therefore necessarily different for the threat of the use of a cyberweapon;

- nuclear deterrence is based, finally, on a dissuasive dialogue between the endowed states. Today it remains an essential component of international security and stability, particularly in the Euro-Atlantic area. The situation is different with cyberweapons insofar as they can be produced and specially used – for the less sophisticated of them – quite easily by a large number of actors, state or not. Consequently, cyberweapons are not able to create strategic balances that provide stability in the Euro-Atlantic area.

The vocation of deterrence in cyberspace used by our British and American partners actually designates a concept different from ours: it is, by a combination of defensive measures, resilience and response (not necessarily cyber) to "dissuade" (in the American sense) an adversary. It is the reproduction in the cyber domain of a strategic debate which has lasted for 60 years and which has notably already opposed us on the concepts of “conventional deterrence” or “deterrence by denial”.

On the other hand, it is possible, notably at NATO, to manage these old doctrinal differences. The Cyber Defence Pledge, the recognition of cyberspace as a field of operations, the policy of protecting the cyberinfrastructures of the Alliance constitute messages which aim to discourage the adversary and contribute, as such, to reinforce the global posture of deterrence and defence of the Alliance. A form of discouragement of the inclination to assault NATO members in cyberspace is therefore possible and acceptable.

1.6 Different models of cyber defence organisation around the world

1.6.1 In the cyber domain, the powers are few and well-identified

A dozen particularly powerful players in the area of cyber defence dominate the international scene: the community known as the “Five Eyes”, which brings together the United States, the United Kingdom, Canada, Australia and New Zealand, a name that comes from the alliance which brings together the technical intelligence services of these countries since the Second World War, Russia, China, Israel, Germany and France.

Committed since the early 2000s, the French effort in the area of cyber defence is part of a dynamic of capacity development and strategic thinking that can be found in Anglo-American countries (the United States and the United Kingdom), in Germany, as in Russia, China and Israel.

The cyber defence strategies of these countries are however based on distinct models (with on the one hand a model grouping within the intelligence agencies the defensive and offensive aspects and, on the other hand, a model separating these two aspects distinctly), as well only on opposite visions of cyberspace (the Russian and Chinese visions appearing to be fundamentally different from the Western vision).

Furthermore, if the capacity effort is shared, the human and financial resources mobilised by these different countries fall within heterogeneous orders of magnitude. In addition, some countries have adopted or are going to adopt protectionism policies, in particular to fully control the security of their networks.

Cyber, a strategic priority shared by the United States, the United Kingdom, Germany. Russia. China and Israel

Undisputed leader in the field of cyber defence, the United States became aware a step ahead of other world powers, from the end of the 1990s, of the risks weighing on their information and communication systems and their infrastructures. A presidential Decree on the protection of critical infrastructure was signed in 1998, and the Department of Homeland Security was created in 2001 to protect state networks. Legacy of long-standing attention to technical intelligence, the United States has given strategic priority to cyber defence. President OBAMA had made it a priority in his mandate and had appointed, from 2009, to the White House an adviser especially responsible for the subject. Cyber defence has gradually figured prominently in the US national defence and security strategy. appearing among the major axes of the National Security Strategy of 2010, its importance was reaffirmed by that of 2015 and confirmed again in that of 2017. The American cyber defence model differs from the French model, based on the separation of offensive capabilities and defensive. American cyber defence capabilities are, in fact, largely concentrated within the intelligence community. This model, although having the advantage of allowing the pooling of national technical skills within the centre of expertise that constitutes the NSA, nevertheless has drawbacks. It poses the problem of the acceptability by the private sector of State interventions in the area of information systems security, in a context marked by the revelations of Edward SNOWDEN, which highlighted the extent technical information allegedly collected by the NSA.

The British model is close to the American model. The United Kingdom adopted a national information security strategy in 2003; this first strategy emphasised the partnership between the public and private sectors within the National Infrastructure Security Coordination Centre, in particular to ensure the security of networks and computerised industrial control systems. The United Kingdom presented its new National Cyber Security Strategy in November 2016. It constitutes the new framework for action by the British government for the period 2016-2021. The objective is that the United Kingdom can, by 2021, be in a position to be "secure and resilient in the face of cyber threats in order to be prosperous and confident in the digital world".

It was in 2011 that the German federal government adopted its first national cybersecurity strategy. Its version updated in 2016 reflects a vision of cyberspace very close to that of France. Paris and Berlin share common strategic guidelines on many technical subjects, such as cryptography or the certification of security products, but also political ones, such as the promotion of a resolute and dynamic European Union in terms of digital security. This proximity makes Germany a privileged partner of France within the various international fora dealing with these subjects, and gives the Franco-German couple a major impetus role in European projects relating to the security of information systems.

It was in 2006 that the Chinese government's National Development Plan for Science and Technology mentioned for the first time the security challenges of critical information systems. Cyber defence was elevated to the top priority in 2014, with the creation of the Restricted Steering Group for Central Network Security and Computerisation, a strategic body bringing together the country's top political decision-makers. President Xi Jinping then chose to personally preside over this small leading group, sending a strong signal to the country but also to the entire international community. Cybersecurity is given a prominent place in the Chinese White Paper, adopted in May 2015. It constitutes the first public recognition of the existence of cyber-offensive capabilities and introduces an active defence doctrine, ensuring a potentially militarised response, cyber or not, to any action deemed contrary to the interests of Beijing. In December 2016, as an extension of this White Paper, China published for the first time a national cybersecurity strategy, which calls for seeking "peace, security, openness, cooperation, and order in cyberspace "And affirms its ambition to become a cyber superpower". Cyberspace is considered by the Chinese authorities to be both a place and a means of economic development and control of opinion. The Chinese approach to cyberspace is clearly distinguished from the Western approach in that it confers to the State a mission of "information security", which extends far beyond the "security of information systems". This vision, which China shares with Russia, is inherited from the strong attachment of the regimes of these countries to state control of information: the State must not only ensure the integrity of its networks but also control the content of information which pass there. This approach is in fundamental opposition to the Western conception of cyberspace.

As soon as he came to power, Vladimir Putin showed his interest in cyberspace. In 2000, he endowed Russia with its first information security doctrine, which describes information security as an essential component of state security. Russian doctrine expanded in the 2010s with the publication of the military doctrine of the Russian Federation in 2010, and the conceptual views on the activities of the Armed Forces in the information space of 2012. Russia stands out markedly of most of the major Western powers in his conception of cyberspace. Marked by a concern for information control inherited from the Soviet period, the Russian vision is not limited to information systems but extends to the entire information sphere. In contrast to the cyber doctrines of Western states, centred on the protection of containers, Russian doctrine, like Chinese doctrine, is primarily concerned with content. This perception is embodied in the concept of information defence, which is a pillar of Russian doctrine. Moscow thus places influence activities, in particular in their psychological dimension, at the heart of its cyber-strategy. The media are fully integrated as counter-propaganda forces, and numerous trolling agencies pay Internet users to massively relay pro-Russian messages on social networks. The organisation of the Russian cyber defence rests on capabilities in this field largely concentrated within the intelligence community.

Finally, Israel is today at the forefront of cyber defence, thanks to an efficient government apparatus in close collaboration with the army, academia and industry. The Israeli strategy has not yet been the subject of an official document.

Asymmetric capacity efforts

The analysis of these organisations reveals a heterogeneous capacity development, in human and financial terms, of the countries which can be considered as the main cyber powers.

The budget of the United States in the field of cyber defence amounted to 14 billion dollars in 2016 and, in its draft budget for the fiscal year 2017, the Obama administration had requested funding of nearly 19 billion of dollars. In 2016, the Department of Homeland Security (DHS) had 691 agents in the cybersecurity sector and made US$ 818 million in investments in this area, or 2% of its total budget. For its part, the US-CERT has a budget of US$ 98 million for 203 agents. Finally, if the budget allocated to the NSA is classified information, it is estimated to be close to US$ 10 billion, and its workforce exceeds 30,000 agents.

The UK's new National Cyber Security Strategy, presented in November 2016, forecasts budget investment of £1.9 billion over the next five years.

The resources and budget of the German interior ministry allocated to cybersecurity are not known with precision, The BSI employs more than 700 agents, to which should be added 100 new recruits by the end of 2018.

Chinese cyber-offensive capabilities, the exact perimeter of which remains difficult to assess, are mainly concentrated within the People's Liberation Army, which is the spearhead of political and economic espionage actions targeting abroad. The latter is currently undergoing a major reform, one of the objectives of which is the pooling of attack and defence resources within the army.

1.6.2 Powers of a modest size capable of deploying advanced offensive capabilities

Having these few countries positioned themselves early enough on the subject, it would be very surprising if other countries had not already invested heavily in offensive capabilities. Indeed, the disclosure of American tools and the hacking tools available on more or less official markets can allow States, even of small size, to build offensive capabilities as long as they have a workforce. competent. Also, countries like North Korea, Pakistan and Iran or even Japan, South Korea and India, like many European countries, already have capabilities, even if it is difficult to assess.

2 Part 2. The State, responsible for the nation's cyber defence

The power of a state in the cyber domain is not measured only by the possession of offensive and defensive capabilities. It is fundamentally based on the ability and willingness of the latter to use them fully. It depends on the determination to discourage attacks by increasing the difficulty, cost and risk for an attacker. Finally, it presupposes that the State can rely on an industry capable of relaying or expanding its action. It is now up to France to take up this challenge of cyber-power.

France's cyber defence is based on a model of organisation and governance which separates offensive missions and capabilities from defensive missions and capabilities (2.1.). Founded on the establishment of an independent defensive chain, this model guarantees respect for individual freedoms. Today, however, it does not sufficiently take into account the contribution of certain actors to the cyber defence of our country and does not fully reflect the missions of cyber defence. As such, it deserves to evolve (2.2.).

The consolidation of our cyber defence model will allow us to better respond to, or even prevent, computer attacks. It should be accompanied by improved protection against threats from our most critical information systems (2.3.).

The new ambition carried by this strategic review also supposes the improvement of prevention and investigative powers, as well as the reinforcement of the effectiveness of the penal response to cybercrime (2.4.).

Finally, at a time when States' cyber capabilities are evolving considerably, France must act as a benchmark player within the European Union on digital issues. It must deploy a strategy of influence promoting its model and participate actively in the definition of standards regulating cyberspace at European and international levels (2.5.).

2.1 The French model of cyber defence

2.1.1 The origins of the French cyber defence model

France has become fully aware of the new strategic deal that constitutes cyber defence since the mid-2000s, and has reacted continuously to the extremely rapid developments that characterize this sector. Cyber defence is a major strategic issue for national security and the economic development of our country. Meeting the challenge of cyber defence means being able both to create the conditions for operational superiority and to contribute to economic development and to the national and international influence of French solutions in this area.

The 2008 White Paper on Defence and National Security enabled France to take a decisive step in taking into account the cyber threat and in implementing the responses it requires. He announced the creation of a national agency to deal with computer attacks and protect state information systems and critical infrastructure. With the ANSSI, instituted by Decree 2009-834 of July 7, 2009, attached to the secretary-general of national defence, France then set up a model of cyber defence based on the separation of its offensive capabilities and its defensive capabilities. A year later, when an espionage attack on its economic and financial ministries was revealed, France developed its first cybersecurity strategy which it published in early 2011.

In 2013, the new White Paper on Defence and National Security confirmed the threats and risks posed by the widespread expansion of cyberspace. It elevates cyber defence to the rank of strategic priority and affirms the principle of a national doctrine of response to computer attacks integrating two complementary components consisting of the implementation[20]:

- of a robust and resilient posture for protecting state information systems, OIVs and strategic industries, coupled with an operational organisation for the defence of these systems, coordinated under the authority of the Prime Minister;

- of a comprehensive and adjusted capacity for government response to attacks of various kinds and scope, calling first on all diplomatic, legal or police resources, without preventing the gradual use of resources the Ministry of the Armed Forces if national interests are threatened.

The 2013 White Paper identified the possibility of a major computer attack against national information systems in a computer war scenario as a threat of primary importance for France and its European partners. It specifies that such an attack, in view of its conceivable consequences (paralysis of entire sections of the country's activity, triggering of technological or ecological disasters, numerous victims), could "constitute a real act of war".

Drawing on the consequences of this observation, Law 2013-1168 of 18 December 2013 relating to military programming for the years 2014 to 2019 strengthens the IT security of OIVs. This military programming law provides in particular for more than a doubling of the workforce of 3,200 people participating in the cyber mission at the end of the financial year and provides for a tripling of the credits devoted to this mission, with almost 440 million euros committed for the development and acquisition of new cybersecurity solutions over the 2014-2019 period.

Several events have come in recent years to accelerate and strengthen in our country the awareness of the magnitude of the cyber threat. This was the case of the January 2015 attacks which were followed by disfigurements of local government websites which, if they were of no great consequence, highlighted the cyber aspect of the terrorist threat. This was also the case with the computer attack on TV5 Monde, a few months later, which revealed the vulnerability of a television channel participating in France's international influence. Finally, the attack on the e-mail of the members of the team of the political movement "En Marche" in April 2017, followed by the publication of the "MacronLeaks" a few hours before the end of the campaign period, was an attempt to the destabilisation of the French electoral process.

[20] National Defence and Security White Paper, 2013, pages 106-107.

2.1.2 The principles of the French cyber defence model

Our country's cyber defence is based on an organisational and governance model that separates offensive missions and capabilities from defensive missions and capabilities – a distinction that was initially empirical and then enshrined in the 2008 and 2013 white papers on defence and national security. This French model is clearly distinguished from the model chosen by the Anglo-Saxon countries, whose cyber defence capabilities are concentrated within the intelligence community[21].

The French model has undeniable advantages. By distinguishing the missions and resources dedicated to cyber protection from those whose objective is intelligence and offensive actions, it facilitates the acceptance of State interventions in the area of information systems security, both in administration than in the economic sphere. It is considered to respect individual freedoms and the protection of privacy and allows the development of relationships of trust between private actors and the state services responsible for cyber protection. It is the strict separation of the areas of intervention, and its status as an inter-ministerial agency, which allow the ANSSI to be mobilised with efficiency and responsiveness, outside its traditional field of action, to deal with several recent crises, even if these attacks have, at the same time, highlighted the need to strengthen coordination mechanisms. This was the case, in 2015, for the benefit of TV5 Monde, victim of the first computer attack for the purpose of sabotage perpetrated in France and, in 2017, for the benefit of Saint-Gobain society or to contribute to the security of electoral campaigns. For these reasons, other countries, such as Germany, have adopted a model almost similar to the French model.

However, if it is not compensated by a very strong coordination between its defensive and offensive poles, the French model can present, in terms of efficiency, the disadvantage of a bipolarity too strongly assumed. Notwithstanding the advantages it presents, our model still lacks confirmation of its basic principles, a precise description of its governance, a clarification of its operational organisation, as well as a better consideration of objectives related to intelligence missions and legal actions. Finally, to be more effective and consistent, it requires greater fluidity of exchanges within the cyber defence community.

[21] This is particularly the case in intelligence agencies such as the NSA in the United States and the Government Communications Headquarters (GCHQ) in the United Kingdom (see above).

2.1.3 The legal framework of French cyber defence

The legal framework on which the French model of cyber defence is based is essentially polarised on the description and supervision of the defensive component of cyber defence since the creation of the ANSSI in 2009 by Decree 2009-834 of July 7, 2009, taken in the continuity of the recommendations of the 2008 White Paper on Defence and National Security. Law 2013-1168 of December 18, 2013, relating to military programming for the years 2014 to 2019 (LPM 2014-2019) and containing various provisions concerning the defence and national security made it possible to clarify the definition of this legal framework.

Under Article 21 of the LPM 2014-2019, the Prime Minister defines the policy and coordinates government action in the area of security and defence of information systems (Article L. 2321-1 of the Defence Code). The Secretary-General of Defence and National Security, in accordance with Article R. 1132-3 of the same code which defines his attributions, proposes to the Prime Minister and implements the policy of the Government as it regards to the security of the information systems. To this end, it has the ANSSI, a department with national jurisdiction attached to it, and whose missions are described by its creation Decree (see above).

Article 22 of the LPM 2014-2019 set up the appropriate apparatus to protect activities of vital importance for the normal functioning of the Nation, which the 2013 White Paper called for. According with Articles L. 1332-6-1 *et seq.* of the Defence Code, OIVs are now required to implement the security rules necessary for the protection of their information systems, to submit to checks intended to ensure compliance with these rules and to report incidents affecting the operation of their systems.

This law also made it possible to define the framework for the State's response to computer attacks targeting information systems affecting the war or economic potential, security or the ability of the Nation to survive. Article L. 2321-2 of the Defence Code thus provides services acting under the authority of the Prime Minister with the necessary legal tools to enable them to defend vital infrastructure against computer attacks.

At the inter-ministerial level, the defensive capabilities of the State are steered by the ANSSI. National authority for security and defence of information systems, attached to the SGDSN, it was created in particular to ensure the following missions:

- as an inter-ministerial agency serving all administrations, it coordinates inter-ministerial work on the security of information systems;

- it prescribes preventive security rules for administrations and OIVs, controls their application and, in the event of a major crisis, can impose reactive measures on them;

- it coordinates government action in defence of information systems and can respond, by technical measures, to attacks targeting administrations and OIVs, if necessary, by neutralizing the effects of the attacks.

The ANSSI can also provide technical support to the Ministry of the Interior and the judicial authority with a view to characterizing the attacks, in particular by helping to determine the operating procedures and identifying the perpetrators of cyberattacks.

On the perimeter of the armies and in accordance with Article D. 3121-14-1 of the Defence Code, the commander of cyber defence (COMCYBER) is responsible for the defence of the information systems of the operational networks of the Ministry of the Armed Forces. The COMCYBER, in conjunction with the ANSSI, is at the heart of the detection of attacks that target its perimeter and contributes, by sharing its information, to a good understanding of the threat.

Finally, the DGSE and the DGSI deal with cyber defence within the general framework of their missions, described respectively by Articles D. 1326-1 *et seq.* of the Defence Code and by Decree 2014-445 of April 30, 2014, relating to missions and organisation of the DGSI. When a cyberattack threatens the fundamental interests of the Nation, exhaustively listed in Article L. 811-3 of the code of internal security, the specialised intelligence services, acting within the framework of their missions of counter-interference, counter-espionage and counter-terrorism, can request the implementation of an intelligence technique to supplement the information they have at the national or international level, due to the action of their agents or by their partners. Cyberattacks are indeed a means of action increasingly mobilised by enemies or hostile groups, for the purpose of destabilisation, economic and political damage or the compromise and manipulation of agents. The Intelligence Act thus recognizes the action which falls to the intelligence services in the field of cyberattacks.

The implementation of intelligence techniques to anticipate, characterize and assign is done within the strict framework of the law of July 24, 2015, relating to intelligence, under the a priori and a posteriori control of the CNCTR.

In addition, Article L. 2321-2 of the Defence Code offers services acting under the authority of the Prime Minister the essential legal tools to enable them to defend vital infrastructure against computer attacks without risking to enter the field of incriminations envisaged in Articles 323-1 to 323-3 of the Penal Code. It is implemented under the conditions set by the Prime Minister and is only triggered when a computer attack is likely to affect the war or economic potential, the security or the survivability of the Nation.

As defined by the Prime Minister in the classified instruction of March 7, 2016, the conditions for implementing the apparatus provided for in Article L. 2321-2 of the Defence Code provide for coordination of the action of the various departments concerned under the responsibility of the ANSSI which defines, organizes and directs the technical operations necessary for the characterisation of a computer attack. It is up to the SGDSN to carry out, if necessary, the technical operations necessary to neutralize the effects of a computer attack, after a prior assessment of the potential consequences of the planned technical operations.

By derogation from these principles, when the computer attack exclusively targets operational capabilities of armies or defence chains of command, the competent authority is the operational command of the cyber defence of the general staff of the armies, in liaison with ANSSI.

The drafting of this Article, which the Council of State considered that it did not encounter any constitutional obstacle[22], offers the competent services the legal framework necessary to respond to major computer attacks. Although the law does not require it, the organisation scheme of the services in the implementation of the operations authorised by the law could, however, be reinforced, with a constant perimeter of responsibilities, by the adoption of a regulatory act higher than instruction.

Consequently, to consolidate the apparatus for responding to computer attacks, it could be proposed to define by regulatory text, with a constant scope of responsibilities, the conditions for implementing the provisions of Article L. 2321-2 of the code of defence. This text could take the form of a published Decree approving the classified instruction of March 7, 2016, the provisions of which must remain covered by national defence secrecy.

2.1.4 The six missions of French cyber defence

Before detailing the evolutions necessary for the consolidation of the French model of cyber defence, this strategic review proposes a classification of the missions of cyber defence in six categories:

- prevention;
- anticipation;
- protection;
- detection;
- allocation;
- reaction (remediation, repression of offences and military actions)

[22] Opinion 387788 of July 25, 2013 “the authorisation given by law to the State services, to respond to such a computer attack, to hold materials allowing intrusion into an information system, and deletion, modification or alteration of the data or its functioning in order to carry out the operations strictly necessary for the characterisation of the attack and the neutralisation of its effects did not come up against any constitutional obstacle ”.

Prevention

The level of awareness of digital risks remains very different from one user to another. While OIVs and, in the near future, operators of essential services are legally bound to respect a certain number of cybersecurity rules, a good number of actors and a fortiori individuals remain very vulnerable and often react only after having been victims of a cyberattack. Small and medium-sized enterprises (SMEs) like local authorities are struggling to free up resources for their cybersecurity.

However, given the threats that cyberattacks represent for business and individuals, all players must be made aware at a high level. While budgetary and financial constraints are real for small structures, there are, however, good practices in computer hygiene and in designing systems that are inexpensive and easy to implement, with particular emphasis on the risks linked to the human factor[23].

This prevention and awareness-raising mission is inter-ministerial in nature. In accordance with the guidelines of the National Strategy for Digital Security adopted by the Prime Minister in 2015, it is based locally on the action of prefects and state services. The ANSSI territorial network, the regional delegates for economic intelligence and the departments of the Ministry of the Interior responsible for economic security, and the digital transition network also participate in this mission. Chambers of commerce and industry, chambers of trades and more broadly all professional networks are also called upon[24].

Anticipation

In addition to awareness-raising actions for potential victims, attacks can be anticipated (prevented, mitigated or neutralised in their effects) through better knowledge of groups of attackers. ANSSI estimates that there are around sixty different operating methods currently used by groups of attackers likely to harm interests in the field of national security. These attack procedures (MOA) can be schematically classified into three categories:

- Strategic MOA: operating mode used by attackers with very advanced capabilities (exploitation of non-public vulnerabilities, codes with a high level of stealth and persistence, sustained operational rhythm) and known to engage in large-scale critical infrastructure sabotage activities, destabilisation or espionage likely to jeopardize national sovereignty.

[23] See third part of this strategic review.

[24] National digital security strategy, 2015, p. 21-22.

- Active MOA: operating mode used by attackers who do not fall into the first category but are known to have already reached French targets or suspected of currently targeting French interests (institutions, government departments, OIV).

- Other MOAs: old MOAs belonging to the first two categories on which the ANSSI has little information, or new MOAs which have recently been the subject of reports by security solution publishers or intelligence services.

The anticipation phase is conducted by ANSSI and all of the intelligence services under the guidance of C4 TECHOPS (see page 55).

Protection

The protection of information systems is the essential brick to resist computer attacks. Whether it is the State or the OIV, the protection apparatus must be reinforced and be able to greatly complicate the task of the attackers, while facilitating detection by the competent services. This effort, which must translate into the perimeter and intrinsic securing of systems, is the only option to obtain resilient and secure information systems in the medium term.

If the strategy of strengthening the resilience of vital information systems, and more generally of all systems, led by ANSSI, is absolutely necessary, the beneficial effects of this strategy will only be obtained in the middle term. In the meantime, France must develop a more assertive strategy with regard to cyber threats[25].

Computer attacks targeting our country or our allies should be detected and attributed and, if necessary, neutralised their effects.

Detection

Detecting computer attacks is an essential task in the fight against cyber threats. The detection of an attack which can occur, as we saw in the first part, several years after the start of it, is linked to the observation of the effects of the attack or to the identification of technical elements related to the attacker's operating mode. These elements, which can come from private companies of foreign partners, intelligence services or the administration, are centralised at ANSSI. ANSSI must also ensure the proper coordination of different entities. In addition to this consolidation and coordination work, ANSSI is in charge of detecting attacks on the administration's systems. The COMCYBER, by delegation from ANSSI, ensures this detection on the perimeter of the armies.

The deployment of encryption techniques in the civil sphere, including for individuals, greatly complicates the task of detection tools which, unless deciphering all of the flows observed, only easily access metadata. This generalisation of cryptography invites to develop new detection strategies by deploying sensors within systems.

[25] Annex 10 (page 166) describes the measures included in the military planning bill and their consequences.

Intelligence services play an important role in this detection apparatus. They are likely to obtain information demonstrating an intrusion. They can, acting within the framework of their missions of counter-interference, counter-espionage and counter-terrorism, request the implementation of an intelligence technique to supplement the detection information which they have at the national or international level, due to the action of their agents or by their partners.

Attribution

After detecting an attack, it is essential to be able to go back to the instigator in order to be able to launch legal proceedings against it or prepare an appropriate response. The attribution of the attacks, if it remains a political decision, is based first of all on the clues collected during the detection of the attack and the investigation that follows. This work carried out by a private company, the police and gendarmerie services or the ANSSI is often not sufficient to obtain factual elements.

To complete the first technical elements, the specialised intelligence services may request, as in the context of their detection mission, the implementation of an intelligence technique to perfect the allocation. The Intelligence Act recognizes the action of intelligence services in relation to cyberattacks.

The implementation of intelligence techniques for the purpose of attributing cyberattacks is done within the strict framework of the law of 24 July 2015 relating to intelligence, under the a priori and a posteriori control of the CNCTR. The necessary information obtained by this means, as by any other means, is brought, when necessary, to the knowledge of the ANSSI and the COMCYBER for the exercise of their missions.

Reaction (remediation, repression of offences and military actions)

Responding to an attack requires quickly putting the attacked system back into working condition while ensuring that the attacker cannot easily get back on the system. This work, also called remediation, is led by the system manager who can benefit from the advice of the ANSSI to ensure that the new system is healthy and will remain so. It is up to the system manager to assume the compromise between a rapid functional restoration of the system and the assurance of ultimately having a healthy and robust system.

In addition, a computer attack can trigger a judicial investigation. While cybercrime is exploding and requires appropriate punishment, traditional crime is also increasingly based on IT resources. The encryption techniques and the precautions implemented by criminals require the establishment of new means for investigations. These cyber means, allowing the recovery of evidence on the equipment of a suspect, will multiply, in particular the remote collection of computer data. Other means, such as the pseudonym inquiry, will have to be extended. This development must obviously take place under conditions which make it possible to preserve the incontestable legal character of digital evidence and the means of obtaining it (see below 2.4.).

Finally, the significant development on a global scale of digital presents a real opportunity for the use of cyber actions in support of military operations. Some countries are already massively using cyber means to carry out intelligence operations or support special operations. "Cyberweapon" is a tool that can be particularly selective and whose effects can be reversible. Used to guarantee superiority in cyberspace, cyber capabilities also allow armies to conduct their traditional operations more efficiently and less costly. France has already invested in this area and cyber capacity is now integrated into all military operations.

2.2 Consolidating the organisation of cyber defence

Organised around its two poles responsible, for one, active computer fight (AU) and, for the other, defensive computer fight (DU), our cyber defence model presents, as we have emphasised, undeniable advantages. However, as we have shown, it takes insufficiently into account the contribution of certain national players to cyber defence and currently does not fully reflect the different purposes of cyber defence that we have just described. This is why this strategic review proposes to clarify the organisation of cyber defence by formalizing it around four operational chains (2.2.1) and strengthening its governance and technical consistency mechanisms (2.2.2). It then recommends optimizing the capacity approach (2.2.3) and setting up an operational process for managing cyber crises (2.2.4).

2.2.1 Create four operational chains to conduct cyber defence missions

Without questioning the principles on which the French model is based, the cyber defence strategic review proposes an organisation of state action in the area of cyber defence according to four operational chains, each contributing to one or more of the six cyber defence missions previously exposed: “protection” chain, “military action” chain, “intelligence” chain and “judicial investigation” chain. Each operational chain aims to have, in appropriate ways, ad hoc management and control procedures, which preserve the distinction between the different cyber defence missions.

The “Protection” operational chain

Under the Prime Minister's responsibility, the “protection” chain covers the perimeter of the defensive computer fight and aims to ensure national security in the event of a cyberattack. Prevention, anticipation and protection missions are carried out there.

In accordance with the laws and regulations governing cyber defence in France, the SGDSN runs this channel. Responsibility for the conduct of operations is entrusted to the Director-General of the ANSSI. In connection with the ANSSI, the COMCYBER is responsible for operations carried out on the perimeter of the Ministry of the Armed Forces.

The "Military Action" operational chain

Under the authority of the President of the Republic, head of the armed forces, the "military action" chain uses computerised combat and must allow the conduct of national defence operations.

The “Intelligence” operational chain

Under the authority of the government, the "intelligence" chain covers all of the actions undertaken for the purpose of intelligence and in particular with a view to attribution.

Today, the intelligence laws of July 24 and November 30, 2015, regulate the faculties of collecting data for intelligence purposes for the intelligence services. The employment authorities are the directors of the departments concerned, under the authority of their supervisory minister.

The CNRLT promotes, between departments, the sharing of information of cyber interest. It can occasionally rely on the inspection of intelligence services to ensure a role of advice and capacity control.

The Prime Minister authorizes operations for intelligence purposes carried out on the national territory, after the opinion of the CNCTR, which are carried out in compliance with the Intelligence Act, in particular concerning the duration of data storage and legal purposes.

The “Judicial Investigation” operational chain

The chain “judicial investigation” covers the action of the police and gendarmerie and justice services.

According to the investigation frameworks, the police and gendarmerie services work under the control of the judicial authority (public prosecutor, liberty and detention judge or investigating judge).

Different services are responsible for providing investigative services, specialised or not, with modern investigative tools and techniques. For example, the DGSI is responsible for the implementation of operational data collection capabilities; the Inter-ministerial Technical Assistance Service (SIAT) implements infiltration techniques; the National Agency for Digital Judicial Investigation Techniques (ANTENJ) via the National Platform for Judicial Interceptions (PNIJ) provides a judicial interception service.

2.2.2 Modernizing the governance of cyber defence

The cyber steering committee

The guidelines and directives in the field of cyber defence are taken by the National Defence and Security Council (CDSN).

The Cyber Defence Management Committee (known as the Cyber Steering Committee) is responsible for monitoring the implementation of decisions taken in matters of development and general organisation of the field. In particular, it oversees the smooth development of the system's capacity in the technical field (investment in human and financial resources, technological coherence base) and good functional coordination between the four operational chains described above.

The cyber steering committee has an organic role and does not intervene in the conduct of operations.

Responsible for preparing and instructing decisions at the level of the President of the Republic, it is co-chaired by the Chief of the General Staff of the President of the Republic (CEMP), the National Coordinator for Intelligence and the Fight Against Terrorism (CNRLT) and the Director of the Prime Minister's Office. It brings together all the ministries and services involved in the field of cyber defence.

The secretariat of the cyber steering committee is provided by the Secretary-General for Defence and National Security (SGDSN).

The Cyber Defence Steering Committee

The work of the Cyber Steering Committee is prepared by a steering committee, under the direction of the Prime Minister's office.

The Cyber Crisis Coordination Centre (C4)

If today the State is well organised to face a major crisis of cyber origin (with the inter-ministerial crisis cell – CIC), recent operational experience has shown that the organisation of crisis management of lesser scope was perfectible. For cyber crises that do not require the implementation of government plans, as well as in the event of the publication of major vulnerabilities likely to be exploited in the short term, it seems essential to set up a permanent interdepartmental mechanism for analysing the threat, preparation and coordination, bringing together all the ministries affected by the crisis.

It is proposed that this mechanism take the form of a Cyber Crisis Coordination Centre (C4), called upon by the ministries involved in the cyber defence mission. Responsible for the supervision of cyber defence, this C4 will be structured in three distinct levels: a strategic C4 (C4 STRAT), a technical C4 (C4 TECH) and a permanent and technical restricted C4 (C4 TECHOPS).

❖ *Strategic C4 (C4 STRAT)*

The C4 STRAT will bring together, monthly and as often as necessary, all the actors concerned beyond the technical sphere alone. Its mission will be to ensure the exchange of information and analyses relating to computer attacks and to facilitate the preparation of the State's response options, both on the technical, diplomatic and even judicial aspects, without prejudice to political and operational responsibilities supervisory bodies and ministries and the judicial authority.

As such, the C4 STRAT will encourage, by comparing the expertise of its members, the preparation of response options brought by the ministries and actors concerned during crises in the cyber field which do not require the activation of the CIC. To this end, it will promote in particular the technical elements from C4 TECH and will ensure the consistency of technical measures with non-cyber actors in crisis management.

❖ *Technical C4 (C4 TECH)*

The Technical C4 is hosted at the ANSSI and chaired by the Director-General of the ANSSI or his representative. It oversees the use of resources relating to the resolution of smaller cyber crises. In particular, its missions are to:

- structure the dialogue between the representatives of the various actors to establish a technical assessment of the current crisis;
- ensuring the consistency of the technical decisions of the State services;
- ensure the consistency of technical measures with non-cyber actors in crisis management.

In the event of a major crisis, and whatever its field, the C4 TECH places itself in support of the CIC as soon as it is activated to provide the authorities with a state of the cyber situation and provide an advisory role.

❖ *The permanent and technical restricted C4 (C4 TECHOPS)*

The C4 TECHOPS is a permanent body, with a technical-operational vocation, allowing a shared analysis between the competent services, of the threat, the modes of action and threatening actors, as well as the anticipation of responses in the short and medium terms, whose work is covered by the secret of national defence.

2.3 Improving the protection of sensitive activities

Consolidating the national cyber defence model proposed by this strategic review would make it possible to react better, or even prevent computer attacks. It must go hand in hand with improving the protection of our most critical systems against threats. In this regard, five fields appear to be priorities: securing state information systems (2.3.1), protecting vital organisations (2.3.2), protecting essential activities (2.3.3), the protection of local authorities (2.3.4) and the protection of democratic life (2.3.5).

2.3.1 Securing State information systems

The security of state networks is one of the priorities of the French cyber defence strategy. Beyond the most sensitive networks, which must benefit from uncompromising security, all of the State's networks must be given special attention. This constitutes the historic mission of the ANSSI, which, since its creation in 2009, has provided IT security expertise for the benefit of all government departments and, as such, provides technical support to many sensitive IT projects. As the national authority for the security and defence of information systems, the agency also deploys attack detection apparatus for the benefit of ministries, develops computer security rules that apply to state services and performs security inspections of departmental information systems.

If we take better account of cybersecurity issues by public actors, in particular by the authorities, this remains insufficient. The real level of security of State information systems remains uneven and often too low, which exposes them to computer attacks, including those not targeted or carried out by attackers with limited technical skills. Several areas for improvement can, however, help to overcome these weaknesses: perfecting cybersecurity governance, optimizing the use of the state's inter-ministerial network for cyber defence purposes, strengthening cybersecurity supervision State services and the adaptation of the State purchasing policy to IT security issues.

Perfecting cybersecurity governance

The attachment of the ANSSI to the Secretary-General of Defence and National Security, which places it closest to the Prime Minister, facilitates decision-making processes and enables it to fulfil its role as an inter-ministerial centre of expertise. However, the visibility of the ANSSI and its power of control over the digital initiatives of the State are not enough to enable it to ensure that security is taken into account. San expertise is often called upon at too advanced stages of departmental IT projects, which then generates significant additional costs and makes it difficult to ultimately achieve a level of security adapted to the risks. This is why this strategic review recommends that the largest and most sensitive IT projects in the State be submitted, from their launching phase, to the ANSSI for opinion. Regarding projects of an operational nature from the Ministry of the Armed Forces, it is up to the COMCYBER to be contacted for advice and to request the ANSSI as much as necessary. This approach should be articulated with the existing apparatus for supervising IT projects by the DINSIC.

Within the ministries, the governance of information systems security must be strengthened so that cybersecurity is better taken into account in state IT projects. First, the departmental Information Systems Directorates (DSI) are insufficiently trained and have little responsibility in this area. Their work processes rarely include an information systems security component, and cyber risk is therefore often poorly taken into account in many departmental digital projects. This is why the strategic review recommends making departmental CIOs responsible for taking cybersecurity into account in the IT projects they lead, and strengthening their training in information system security.

With regard to the security needs associated with business IT projects, we can see that the dialogue between the business departments and the departmental CIOs can be improved. If the responsibility for the security of the computer base common to the whole of a ministry – including for example office automation or electronic messaging – raised by the DSI of the ministry, it is on the other hand up to the business departments themselves to fix the needs in the security of digital tools and applications developed for the benefit of their business, sometimes without significant involvement from DSI. They alone have the knowledge necessary to qualify the impacts of a possible computer attack on the data and processes specific to their activity and can, therefore, assess the risk and their cybersecurity needs. For this, they must be able to rely on staff with business skills and trained in cybersecurity. This mission must be carried out by security referents, from business expertise centres and trained in digital security. The responsibility of directors of administration with regard to the security of business information systems thus appears essential, as well as the appointment and training of digital security referents within the business departments of the ministries.

Optimizing the use of the Interdepartmental State Network (RIE) for cyber defence purposes

The Interdepartmental State Network (RIE) is the unified electronic communications network connecting the state administrations. Its management and operational operations are entrusted to a service with national jurisdiction created in 2012 and placed within the Prime Minister's office. Its missions are to streamline inter-ministerial exchanges and optimize the costs linked to the State's IT infrastructures, but also to strengthen the security of the State's information system. The state's interdepartmental network is notably based on a unified Internet access platform that offers centralised security services. These security functions allow an effective reaction in the event of a computer attack, for example by implementing measures to block malicious traffic.

This common Internet access platform is nevertheless insufficiently used by certain ministries, and moreover often used without its security functions, which reduces the State's cyber defence capabilities. San widespread use to all departments would also allow ANSSI to significantly strengthen its computer attack detection service. Beyond the aspects relating to the security of the network itself, it is therefore advisable to optimize the use of the RIE to improve the capabilities of State cyber defence. This involves encouraging departments to join the Internet access platform of the RIE and to make full use of the services it offers. More generally, departments should be encouraged to resort almost systematically to the security services offered by RIE.

Furthermore, the exploitation of the metadata of the inter-ministerial network of the State could be reinforced, the service with national competence responsible for managing this network not having the resources and skills necessary to ensure their collection and their exploitation for cybersecurity purposes. However, these data are likely to strengthen the national capacity for detecting attacks, in particular by making it possible to search after the fact for traces of compromise in the State's information system. Entrusting the ANSSI with the detection of attacks on this network would constitute an appropriate response to this situation, it is up to the ANSSI to inform the ministries of the discoveries of attacks for decision by the qualified authority SSI (AQSSI) and possible action.

Strengthen the supervision of cybersecurity of State services

Since its creation, the ANSSI has operated an inter-ministerial security supervision service, which relies in particular on probes for detecting computer attacks, positioned on the networks of the ministries and on the RIE. The current model, however, faces several limitations.

First, several administrations are still not subject to security oversight, which effectively limits the national capacity to detect attacks. This situation is explained by an insufficient investment of the teams of certain ministries in the support which they must bring to the deployment of detection probes. It should nevertheless be noted that the gradual connection of the ministries to the RIE should make it possible to extend the national detection apparatus to actors currently not covered.

In addition, this security supervision apparatus is not applicable to state services hosted by external providers, since these private companies do not fall within the competence of the ANSSI. The trend towards outsourcing business applications is therefore likely, as a matter of law, to question the national capacity for detecting computer attacks. This is why this strategic review recommends imposing complete coverage of IT services used by the State through a security supervision apparatus, including in cases where these services are outsourced.

Adapt State purchasing policy to IT security issues

The use of cybersecurity products and services labelled by the ANSSI constitutes an important lever for ensuring the security of State networks. However, its implementation faces several obstacles, including the incompatibility of departmental and interdepartmental purchasing frameworks with the acquisition of such solutions and the inadequacy of departmental budgets in this area. In addition, the acquisition of security solutions by the State is still fragmented and, therefore, sub-optimal from an economic point of view.

Several approaches implemented punctually in recent years have demonstrated their ability to remove some of these obstacles, while generating beneficial effects for the industrial suppliers of the solutions concerned. Thus, the registration of certain solutions labelled by the ANSSI in the existing frameworks for the acquisition of IT solutions has greatly facilitated their implementation by the administrations, and the acquisition by the ANSSI, in 2015, of a license a comprehensive release for Prim'X's labelled software solutions has also been successful, enabling the deployment of more than 600,000 robust encryption software licences within the administration.

An inventory of the needs of administrations for secure solutions and the development of an inter-ministerial framework for the acquisition of such solutions, including according to the logic of release licenses, with a double objective of optimizing public expenditure and facilitation of the deployment of these solutions, could be entrusted to the State purchasing department, with the support of the ANSSI.

Beyond the acquisition of specialised security solutions, the more general procedures for purchasing IT solutions by the State should also be the subject of particular attention to security, in order to guarantee at least the respect of basic good IT security practices by any new digital tool acquired by the State.

The principle of opinion of the ANSSI on the IT projects of the State is not enough to achieve this objective, insofar as a significant part of the public order in digital matter does not come from major IT projects, but from current acquisitions or other projects – such as, for example, the installation of a video surveillance system as part of a real estate project. This is why the strategic review recommends developing standard contractual clauses grouping together good security practices applicable in the acquisition of an IT solution and strongly encouraging departments to systematize the inclusion of these clauses in their public contracts comprising a digital component.

2.3.2 Protection of operators of vital importance (OIV)

Pillars of state resilience, critical infrastructure includes public and private entities that provide goods or services essential to the Nation or can present a serious danger to the population. Although the definition of critical infrastructure varies from country to country, it generally covers at least energy supply, electronic communications, transport systems, financial services, public health, water management and services. essential audiences. In 2006, France thus defined twelve "sectors of activity of vital importance" and identified more than 200 "operators of vital importance" (OIV), public and private. These constitute the hardcore of French critical infrastructures. The security system for activities of vital importance, inserted in the Defence Code, constitutes the legislative and regulatory framework allowing the association of OIVs with the national apparatus of protection against terrorism, sabotage and malicious acts. It formalizes the permanent dialogue between the State and these operators in order to ensure their security.

Since its creation, ANSSI has gradually strengthened its role with OIVs. Until 2013, with the exception of the electronic communications sector, ANSSI's missions were limited to the dissemination of technical advice by the development of guides and recommendations or the performance of security audits, only to their request. Faced with a growing IT threat and an increasingly high risk of computer sabotage, the level of security of these actors remained insufficient, exposing them, and then the Nation, to a major cyber risk. France, therefore, chose in 2013[26] to impose, by legislative means, IT security requirements on OIVs, thus becoming one of the first countries to legislate in the field of cybersecurity of critical infrastructures. The cyber provisions of the military programming law of 2013 have entrusted ANSSI with new missions in this area: they provide that these operators apply the computer security measures set by the ANSSI and notify it of security incidents affecting their systems. of information. These measures, which were the subject of consultations with operators, are today fixed by Decrees of the Prime Minister and are therefore of a binding nature. ANSSI supports OIVs on a technical level in the implementation of application texts. In parallel with this approach, the DGSI, through its territorial network, carries out essential work in the area of internal security and economic protection covering, in particular, OIVs.

This new apparatus is a major step in strengthening the cybersecurity of critical infrastructures. It has already made it possible to identify the nation's most sensitive information systems, sensitize OIV leaders to cyber risk and has led to significant investments in cybersecurity. However, the level of maturity remains uneven between the various business sectors, and many operators do not currently have sufficient resources and adequate organisation to effectively manage the security of their information systems. Certain basic IT security rules are sometimes not applied to critical systems, some of which are still flawed and exploitable by low-level attackers. In addition, the base of rules set by the current apparatus does not allow optimal consideration of the particularities of certain business systems. It is important, in parallel with the preparation of these new rules, to make a financial assessment of the measures already in place in order to assess their cost-effectiveness.

It is therefore advisable to develop the model to adapt it more to the constraints of the sectors and to the evolution of the cyber threat, in five directions: the adaptation of IT security rules to the trades; strengthening cybersecurity for "supercritical" operators; the extension of the regulatory apparatus to handling incidents; taking into account the particularities of digital service companies; and the development of private cybersecurity technical assistance.

[26] Articles L. 1332-6-1 to L. 1332-6-7 of the Defence Code.

The implementation of the proposals made in this part of the strategic review will be subject to a detailed impact study, which will have to confirm their economic feasibility (cost for economic actors and for the State), technical, legal and conclude with the no-risk for companies' business processes.

Adapt IT security rules to trades

In order to be able to establish security rules adapted to the different trades, it was decided to include them in sectoral Decrees. However, the requirements set by these implementing texts are today very close from one sector to another. In fact, preliminary work carried out with operators revealed a very heterogeneous level of maturity in cybersecurity, including within the same sector. This observation led the ANSSI, in agreement with the ministries concerned and the OIVs, to adopt a two-step strategy: firstly impose on all operators a common foundation of elementary security rules and then, secondly, adapt them more precisely to the trades and, if necessary, strengthen their level of requirement. The Decrees published to date embody this first step, the objective of which is to make all operators cross the first threshold in terms of digital security.

The application of this set of rules will protect the most critical information systems against the vast majority of cyberattacks, in particular against indiscriminate attack campaigns such as those carried out by ransomware in spring 2017. However, it does not allow to secure, according to state-of-the-art, all of the business information systems, certain specificities of which cannot be taken into account by a body of generic rules. For example, it does not optimally cover the security of the information systems of digital infrastructure operators (Internet exchange points, DNS service providers, etc.), for which it is necessary to develop specific rules, allowing in particular to take into account their strong interconnection with public networks. This generic model is also not suitable for the particularities of industrial and embedded systems.

In view of the impacts that an attack against such systems is likely to have on the Nation and the increasing level of sophistication of computer attacks targeting critical infrastructures, it is now necessary to initiate fine adaptation work rules for trades. Work aimed at adapting security rules applicable to VLVs to the specific business characteristics of each sector could thus be initiated, under the guidance of the ANSSI and in close collaboration with the public and private players concerned.

Reinforce cybersecurity for “supercritical” operators

Because of their role as service providers to other OIVs, the electronic communications and electrical power supply industries can be described as "supercritical". A computer attack against one of these actors is likely to have repercussions on activities of vital importance, and therefore potentially catastrophic effects on the resilience of the whole Nation.

In addition, the potential rapprochement between terrorist groups and actors with strong technical capabilities that they would be ready to monetize suggests the possibility of acts of computer sabotage perpetrated for terrorist purposes. The transport sector, which would then be a privileged target, could in the future be described as "supercritical" and require reinforced security measures.

Develop the private offer of technical assistance in cybersecurity

If the ANSSI has an important role to play with OIVs, in particular in terms of technical support and support for handling serious incidents, it cannot alone ensure the implementation of this apparatus and must be able to rely on a large ecosystem of cybersecurity service providers that are both technically competent and trusted. The qualification by ANSSI of incident detection, security audit and incident response providers, provided for by the regulatory framework and being implemented, largely meets this need.

However, this qualification appartus does not currently meet the need for operators to have labelled providers able to support them on a daily basis in taking cybersecurity into account in their IT projects. The absence of a clear definition of cybersecurity technical assistance missions constitutes a clear obstacle to the development of an ecosystem. A new standard relating to the cybersecurity technical assistance profession, and the extension of the ANSSI labelling to this field, could prove to be very useful. A reflection could also be conducted on the implementation of a financial incentive measure aimed at promoting the labelling by the ANSSI and taking security into account.

2.3.3 Protection of essential activities

Beyond the OIV, which constitute the pillars of the nation's resilience, other actors provide essential services for the daily functioning of the economy and society. As such, they also fall into the category of critical infrastructure.

Despite growing awareness, many of these remain very vulnerable to computer attacks that can permanently paralyze their activity. The recent worldwide waves of cyberattacks have shown the extreme fragility and the lack of preparation of entities essential to the daily life of the Nation. The spread in May 2017 of the WannaCry ransomware, for example, made many services of various kinds permanently unavailable around the world[27]. Despite the existence of recommendations, guides and awareness campaigns, the level of cybersecurity of these actors is progressing too slowly in relation to the threat. The lack of good IT security practices, often linked to a lack of human and financial resources allocated to cybersecurity, exposes them to computer attacks likely to strongly affect their activities.

[27] WannaCry has affected production plants, including Renault plants in France, ATMs, hospitals, station billboards, etc. In the UK, more than 20% of regional health management organisations have been affected, which has led affected hospitals to postpone certain medical procedures.

It is, therefore, necessary to impose a minimum base of cybersecurity requirements on these sensitive actors for whom a cyberattack is likely to have major consequences on the daily life of the Nation.

Transpose the "NIS Directive"

Directive (EU) 2016/1148 of 6 July 2016, known as the "NIS Directive", which relates to measures intended to ensure a high common level of security of networks and information systems in the European Union, has, in particular, the purpose of strengthening the level of IT security of operators providing services essential to the functioning of the economy and society. The first comprehensive legislative initiative of the European Union in the field of cybersecurity, this directive is part of a European strategy aimed at strengthening cyber-resilience at European level. In particular, it seeks to increase national capabilities in the area of cyber defence and to increase coordination in the event of incidents affecting several Member States.

The NIS Directive sets a minimum list of critical activities to be subject to these new obligations. It also protects a range of activities which, if they were affected by a cyberattack, could have major repercussions on the life of the nation. Such an apparatus would also generate a ripple effect on the digital ecosystem by reaching a critical mass of companies using secure solutions. The actors in charge of health, social benefits or even the preservation of the national digital heritage are intended, for example, to be included in the transposition of this directive, in particular to be able to respond to a systemic criminal attack which would aim to massively paralyze and which unfortunately will not fail to happen.

Define a common foundation of proportional security rules

If it would be disproportional to impose on these essential service providers rules as demanding as those which apply to OIVs, it is necessary that the State establishes a common foundation of proportional elementary security rules making it possible to protect these actors. Indeed, if the paralysis of one of these operators would have less impact than the shutdown of a critical infrastructure, a massive cyberattack affecting a significant number of these actors would be likely to have a serious impact on the life of the Nation. The application of basic IT security rules will protect these actors against the majority of threats, in particular against the waves of massive and indiscriminate attacks, such as ransomware, which spread in spring 2017.

Promote progressive European harmonisation

If the security of OIVs is a sovereign prerogative of the States, the security of companies essential for the economy and for society is part of the competences of the European Union. Article 114 of the Treaty on the Functioning of the European Union indeed provides that the European Union is empowered to adopt measures intended to establish or ensure the functioning of the internal market. The essential role played by information systems in support of this functioning justifies the implementation at European level of common cybersecurity systems.

In addition, a large share of these players is made up of multinational companies which provide essential services to several Member States, and whose information networks and systems are deployed in several countries. This situation justifies the search at European level for the harmonisation of cybersecurity rules applying to these operators in the different Member States of the Union.

This harmonisation must however be gradual and take into account the different levels of maturity of each country in this area. Strengthening the capabilities of each member state must therefore be a priority, and France must ensure that the harmonisation process is not carried out at the expense of the level of security requirements, so as not to weaken the security of French players.

Strengthening the role of electronic communications operators

Electronic communications operators who, through their networks, connect their customers' information systems to the global network, and see all the flows passing through their networks, have a key role to play in the cyber defence of essential operators to the economy and to society.

Cyberattacks targeting their customers' systems can indeed be detected, blocked, analysed and processed at the level of the networks of electronic communications operators. In addition, these actors are able to identify and alert the owners of vulnerable information systems – for example, from technical data provided by the ANSSI, which can drastically limit the effects of a wave. computer attacks. Electronic communications operators must therefore be major partners of the State in the fight against cyber threats.

In this perspective, the ANSSI has woven many partnership links with these operators to improve the level of cybersecurity of their networks, in particular through technical advice and audits. However, given the development of the cyber threat, a strengthening of State cooperation with electronic communications operators in order to strengthen the use of their networks for the purposes of detecting and blocking attacks, preventing incidents and alerting victims, possibly framed by a new legislative framework, would significantly improve cybersecurity for all stakeholders.

2.3.4 Protection of local authorities

Local authorities are self-governing. The State cannot decide on the governance of their information systems, let alone impose supervision by its services. Because of this autonomy, combined with the diversity of their sizes and their physiognomies, the communities organize and manage themselves in very different ways. Their level of maturity and sensitivity to digital security issues is therefore very variable, depending on economic, cultural and, a fortiori, digital contexts.

However, they remain particularly vulnerable to cyber threats.

Given the weight of local authorities in the public sphere, the number of their constituents, their responsibilities in the processing of personal and sensitive data or the pre-eminence of their economic role, as far as the regions are concerned, their cybersecurity calls for support, even indirect, from State services. The work carried out in the concerted development programme of the DcANT territorial administration should, therefore, continue to take into account cybersecurity challenges and suggest avenues to help them.

Encourage the pooling of resources from local authorities

Local authorities have already committed to pooling their resources.

Whether they are Public Establishments for Inter-municipal Cooperation (EPCI), mixed unions or, more generally, all forms of inter-municipal co-operation, the structures which assume the function of DSI, for example for the benefit of each municipality of a department, have demonstrated the effectiveness of the approach. Where such entities exist, awareness and support actions are simpler to set up and better accepted by members. However, the entire territory is not covered by these dedicated structures and experience shows that skills are relatively scarce and poorly distributed.

More recently, several elected officials have announced their intention to quickly set up and finance dedicated structures themselves which must ensure, in particular at the regional level, the functions of awareness-raising and training, and even supervision of systems, and incident response. Some even plan to play the role of certification centres.

These initiatives will allow the pooling of skills in information systems security and will aim to support local authorities in the implementation of their digital projects, safely and in a relationship of trust. Such groups of skills could also serve as an observatory concerning the maturity of digital protection and awareness-raising, on the basis of precise and shared regional indicators. They can be immediately identified as the regional benchmark for digital security.

However, initiatives aimed at developing certification activities for security products or services within these regional coordination bodies should be discouraged, insofar as they would not be consistent with the approach to European harmonisation of certification advocated by France, and would in fact lead to a counterproductive fragmentation of this apparatus.

With this last exception, State services must support this movement, in particular so that the security rules applied or promoted are those recommended by the ANSSI, instead of being shaped by the sole offer of service providers.

It is therefore recommended to support the creation, by the local authorities themselves, of a coordination of cybersecurity resources.

Foster communication in digital security with local authorities

The information systems of local authorities are the targets of numerous and very diverse digital attacks. The response to these attacks, and more generally to security incidents, is very often made delicate by the absence, at least in the smallest communities, of contact points for their interlocutors in digital security, in particular the services of the State. In addition, even if these contact points can be clearly identified, it is rare for them to be able to communicate effectively with specialised structures, failing to master a common language. The escalation of the security incidents which affect the communities cannot thus, in the state, to operate in a fluid way.

Furthermore, even if they are carried out by local players, awareness-raising actions carried out for the benefit of smaller communities, and in particular the majority of municipalities, lose much of their effectiveness in the absence of an internal relay able to master the challenges of cybersecurity.

It is therefore recommended to encourage and help each local authority, in particular the smallest, to designate and train a "referent" in digital security, a privileged interlocutor for cybersecurity actors and relay of awareness and training actions.

Foster the development of an adapted range of products and services

All communities set up services for citizens which require them to turn to outsourced turnkey solutions, in particular cloud computing, without worrying about the level of security or the trust that can be placed in them. When digital security is taken into account, it is only rarely integrated from the start of digital transformation operations. In practice, particularly in the absence of ad hoc benchmarks, few local authorities have the capacity to draw up precise specifications themselves or to choose the specialised companies likely to meet very specific regulatory needs and requirements. specific. Training courses organised by local authorities for the benefit of their agents are generally provided by private operators, on the basis of existing modules intended for businesses.

Experience shows that, even if the adequacy between the supply of products and services qualified by the ANSSI and the needs of local authorities has never been formally analysed, it seems to be improving. It is therefore recommended to improve the integration of needs and constraints specific to local authorities in the ANSSI standards and in its catalogues of qualified products and services, by carrying out an inventory of these needs and analysis of the associated industrial market. This approach must be accompanied by the establishment of appropriate dialogue bodies, for example with certain inter-municipal players, in order to encourage the communication of these needs to ANSSI over time.

2.4 Strengthen the fight against cybercrime.

As the opening remarks of the report "Protecting Internet users: report on cybercrime"[28] already made clear in 2014, there is no legal definition of cybercrime to date. The first recommendation of this report consisted in the formulation of a very encompassing definition of the term: "Cybercrime includes all criminal offences attempted or committed against or by means of an information and communication system, mainly the Internet". The preamble to the 2001 Budapest Convention (see box below), while it does not define what cybercrime is, mentions three types of activities that the convention intends to cover: attacks on integrity, availability or confidentiality of an information system; the use of electronic networks and electronic information to commit criminal offences; data breaches.

The text of the Budapest Convention provides an outline of an operational approach to what the fight against cybercrime represents. Thus, cyber defence measures are implemented and legal proceedings possibly triggered when an act undermines the availability, integrity or confidentiality of an information system and if it involves the defence or national security (act of war, espionage, sabotage), the life of populations (terrorism), the functioning of the economy (denial of service, massive compromises or wide dissemination of ransomware) or of society (obstacles to democratic life, massive theft of personal or health data). When, on the other hand, the act does not have one of the consequences mentioned above, or when the information system is only used as a vector (phishing, internet sales of illegal products, dissemination of illegal content on the Internet, etc.), it does not entail the implementation of cyber defence measures.

[28] www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf

Conventional statistical tools do not make it easy to draw up a precise inventory of cybercrime, these crimes falling into different categories of ordinary crimes without explicit reference to the use of the computer techniques used. Complementary to the expected statistical results of the anti-cyberbullying[29] platform set up in 2017, the work undertaken within the Ministry of the Interior by the Ministerial Statistical Security Service (SSMSI) must therefore continue to improve knowledge of cybercrime. It has nonetheless been established that, in a context of increased digitisation of society, the multiplication and increasing sophistication of the means available to cyber criminals (anonymisation networks such as the Tor network, attack tools available on the Internet, etc.) complicate access to digital evidence and create the conditions for an explosion in cybercrime.

As highlighted in the report published in 2016 by EUROPOL[30], there are five trends in cybercrime:

- the development of ransomware, which today constitutes the main threat among malware;
- the interest shown by certain criminal groups in contactless payment technologies;
- the rise of denial of service attacks, in particular thanks to “botnets” of connected objects;
- the use of cryptocurrencies, in particular Bitcoin, as the preferred means for financial exchanges between criminals;
- the use of encryption technologies to protect communications between offenders or to store information.

These developments constitute an important challenge for the investigation services and a major challenge for the judicial actors who have to face a protean litigation sometimes requiring a real specialisation.

The analysis conducted as part of this strategic review has also highlighted a movement of convergence between cyber defence and the fight against cybercrime. Computer attacks likely to harm the fundamental interests of the Nation and, more particularly, the information systems of operators of vital importance (espionage, theft or modification of data, sabotage hindrance, etc.) constitute offences passible of punishment since the Godfrain Law of 1988.[31]

[29] www.cybermalveillance.gouv.fr

[30] https://www.eouropol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

[31] Law 88-19 of January 5, 1988 relating to computer fraud.

Budapest Convention

The Budapest Convention on Cybercrime was drawn up under the aegis of the Council of Europe. Signed on November 23, 2001, in Budapest – hence its common name "Budapest Convention" – this convention is the first – and to date the only – international text dealing exclusively with the fight against cybercrime.

By the end of 2017, the convention had been ratified by 56 states (four states have signed but not ratified), some of which are not members of the Council of Europe such as Australia, the United States, Israel, Japan, Morocco or Senegal. The only member of the Council of Europe who has not signed the convention is the Russian Federation.

The objective of the convention is to promote the harmonisation of national laws targeting criminal offences committed via the Internet and other computer networks. The text deals with both computer offences (illegal access, illegal interceptions, attacks on the integrity of data or systems, network security) and offences relating to content (child pornography, copyright infringement).

The agreement also contains a series of procedural powers, such as the search of computer networks (preservation of evidence, production order, etc.) and interception. The convention also aims to facilitate international cooperation between law enforcement agencies and the judiciaries of States parties.

2.4.1 Finely assess the extent of cybercrime

The fight against cybercrime is first and foremost based on the fairest possible perception of criminal acts committed in the digital space. Four sources now allow the judiciary to learn about cyber incidents and offences:

- the citizen, whether a simple Internet user reporting acts of cybercrime[32] or a victim;
- police and gendarmerie services carrying out proactive search operations with open sources;

[32] The Internet user confronted with illegal content or behaviour on the Internet has the possibility of sending a report on the PHAROS platform of the Central Directorate of the Judicial Police. The latter receives nearly 200,000 reports per year, mainly concerning scams and child pornography content, incitement to hatred or praising terrorism.

- trusted partners, aggregators or information relays;
- network operators and electronic communication service providers.

The assessment of the extent of cybercrime is today affected by two factors. First of all, when it comes from an IT security solution publisher, whose economic viability is closely linked to the level of the threat, it is legitimate to question its objectivity. Then, the police and the gendarmerie are not able to identify the totality of the cybercrime facts because the infringements noted cover only a part of the cyber malevolence, some of them being not detected and all the victims not being made to know.[33]

A better assessment of the extent of cybercrime should however become available in the national police. The PERCEV@L project of the national gendarmerie and THESEE of the national police. The PERCEV@L project initially provides for an online reporting process for card payment[34] related offences, followed by an extension to the online complaint process. The THESEE project concerns five modes of Internet scams (mailbox hacking, Romance Scam and classified ad fraud, webcam blackmail, fraud linked to fake sales sites and Ransomware). Its purpose is to allow the filing of complaints online, to improve the quality of procedures and to develop the ability to analyse phenomena.

The government platform "cybermalveillance.gouv.fr" (see box), of which this child is not the main object, also plays a role of sensor of digital risks for the Ministry of the Interior and ANSSI in order to refine the global knowledge of cybercrime.

The government platform "cybermalveillance.gouv.fr"

The government platform "cybermelveillance.gouv.fr" now plays a role in raising awareness, prevention and support in terms of digital security for the French population. It supports individuals, companies and local authorities who think they are victims of an act of cyber-malfunctioning for the establishment of a precise diagnosis of their situation, the contact with specialists and competent organisations close to their home (1,123 service providers referenced by the end of 2017) and the provision of tools and publications providing a lot of practical advice.

[33] In this regard, it is regularly observed a lack of reporting or filing of complaints by companies who fear that this approach will result in unnecessary publicity on their vulnerability and damage to their image.

[34] Just over 4.5 million fraudulent bank card transactions in France in 2016 for a total amount of € 400 million according to the Observatory for the security of means of payment.

This national assistance apparatus, led by the Public Interest Group (GIP) *Action Contre la Cybermalveillance* (ACYMA) and supported by an inter-ministerial approach associating ANSSI, the Ministry of the Interior and the State Secretariat in charge of digital, is accessible since October 2017 for all regions of France. Between May and October 2017, the testing of the apparatus enabled more than 700 connections between cybersecurity providers and victims[35].

The platform also constitutes a lever helping to reference and federate more broadly all the tools and awareness campaigns relating to cyber vis-à-vis the general public under the same signage.

The platform also constitutes for the Interior Ministry and ANSSI the opportunity to refine the knowledge of the threat targeting information systems, through an observatory of digital risks.

2.4.2 Strengthen the effectiveness of the judicial response to improve the fight against cybercrime

In a context of blurring the border between cyber defence and the fight against cybercrime, on the one hand, and the transposition of traditional crime to the digital world, on the other hand, strengthening the effectiveness of the criminal response is a priority.

Beyond the necessary adaptation of techniques for collecting criminal evidence to this new context, it is the conditions for preserving digital data that must be rethought today. Data retention and access is indeed the first issue for judicial police services.

Adapting criminal policy in the fight against cybercrime

The democratisation of anonymisation and encryption techniques, the development of parallel markets on Darknets and technological developments make it more difficult to identify cybercriminals and oblige to rethink the way of conducting investigations, in particular in view of the principle of fair trial.

Consideration may first be given to the relevance of investigating in a more systematic manner, including in the absence of a complaint, when the information gathered suggests the probable existence of criminal offences.

Then, it seems useful to initiate an assessment of the ways and means likely to reduce the feeling of impunity which animates a certain number of cybercriminals. Arresting and convicting those of them who have an established reputation and targeting the most popular criminal platforms could thus constitute areas of effort. In this regard, the recent operations carried out against the sites selling narcotic products Alphabay[36] and Hansa by EUROPOL and the American and Dutch authorities are an example to follow.

[35] 83% of cyber malware incidents were declared as viruses, but 44% of them were in fact attacks by Ransomware.

[36] Online drug and weapons supermarket in the Darkweb which, according to EUROPOL, has been brewing since 2014 for more than a billion dollars in criminal transactions.

France could also step up its international efforts by playing a key role in Joint Investigation Teams (JITs) at the EUROJUST level. The example of the JIT mobilised in the NotPetya case should be commended and reproduced.

To achieve this adaptation of the penal policy in the fight against cybercrime, a strengthening of human resources (magistrates and specialised investigators) appears essential. Increased material resources are also necessary both at the level of specialised investigation services and at the level of digital proof processing units. Efforts should be made to install monitoring tools adapted to the various open sources, enhanced decryption capabilities and remote data collection tools. Beyond this material aspect, an appropriate legal framework is still sometimes lacking, such as for example in the area of storage of data collected in open source outside of a purely judicial framework.

Improving the judicial response

The judicial process must be fully used in the general mobilisation of State services in the face of cybercrime. As such, strengthening the resources currently deployed within the judicial chain appears necessary.

The creation in 2014 of the section of the Paris public prosecutor's office specializing in cybercrime[37], as well as the centralisation in 2016, at the level of the *Tribunal de Grande Instance* (TGI) of Paris, of the jurisdiction in matters of attacks on computerised data systems go in the meaning of better coordination of the judicial response to cybercrime. However, it appears necessary to reinforce the staff of the Public Prosecutor's Office and the TGI of Paris, as well as those of the TGI of Nanterre and Pontoise which will probably be impacted by the THESEE and PERCEV@L projects.

Bringing together the players in the fight against cybercrime and those in cyber defence

The adaptation of criminal policy to the challenges of cybercrime must go hand in hand with an effort in cyber training for the benefit of the prosecutors, judges and investigators involved. In particular, it seems essential to raise awareness, within the framework of their initial and continuous training, of magistrates and investigators of the needs of the cyber chain. Conversely, better information for the staff of this channel on the challenges of the fight against cybercriminals and on the interactions to be maintained with judicial actors is also necessary.

[37] This section is armed by two magistrates and a specialised assistant.

More generally, it seems necessary to develop exchanges between judicial actors and specialists in the cyber field. A reflection could thus be launched on the counter-establishment of a legal framework authorizing the reciprocal sharing of certain information collected by the judicial authorities or the services specialised in cyber defence.

The present strategic review thus recommends allowing a transfer of the technical elements recovered in the judicial investigations towards the ANSSI in a logic of capitalisation of technical data on the threats, and from the ANSSI towards the operational services to facilitate the technical acts of investigation and to understand the threat.

Make territorial interventions more effective

In the context of economic intelligence, coordination between the various government departments concerned is now carried out at the decentralised level under the aegis of the regional prefects. The Regional Economic and Territorial Intelligence Committees (CRIET) thus distribute risk awareness actions – including cyber risk awareness actions – carried out for the benefit of economic actors. Better planning of the interventions carried out in the areas of the fight against cybercrime and cybersecurity enabled the CRIETs to become more efficient.

This point joining the already identified need to group skills to secure the systems of territorial actors, the strategic review recommends that the creation of regional cyber defence entities be studied.

2.4.3 Develop an international network of collaboration between magistrates and investigators

Cybercrime does not recognize the borders between States, it is not enough that France alone is well prepared to deal with it. Data useful for guiding investigations are in fact held by foreign actors. France must, therefore, endeavour to perfect, with its partners, the mechanisms for mutual legal assistance in the fight against cybercrime and to continue the exchange of experience and technology in this area.

In this logic, it seems essential to encourage an effective and constructive dialogue, in particular with the big American operators of the Internet[38], and to maintain an international network of police and judicial collaborations.

The permanent contact group, which brings together investigators and the Chancellery with the major Internet players, provides a first response to this requirement by allowing a technical-operational dialogue. In matters of police and judicial cooperation, bilateral contacts, in particular with the source countries of cybercrime, and exchanges with the competent services of the various States within European or international bodies (EUROPOL, EUROJUST, INTERPOL) exist and regularly demonstrate their interest. But, in addition to sharing information, the objective is also the definition of shared, if not common, approaches and solutions. This is the case, for example, of European work carried out in the area of availability and access to digital evidence. Access to digital evidence today represents a challenge which must be met thanks to better cooperation with the major internet operators but also with the national authorities concerned. The decisions taken in defining the location of the data will be decisive in this regard.

[38] The dialogue does not exclude when necessary, considering legislative constraints - European or national.

Contacts with net companies at the national level or in an international framework (European Union, G7, UN) must allow companies to better take into account our needs in terms of removal of illegal content and in particular the contents of apology of terrorism. Our sector partners must also be mobilised regarding the use of new technologies for terrorist financing.

The resolutely technical and cross-border nature of cybercrime implies a mobilisation and a constant effort in order to give actors in the criminal chain all the means useful for the development of investigations, the identification and the arrest of perpetrators, even if outside the national territory. Cross-border access to digital evidence – very often held by foreign operators – is therefore an essential issue for the proper development of criminal investigations. This access must be improved in order to allow the obtaining in a few hours of technical data and in a few days of content data (against respectively several days and sometimes several but currently).

Finally, France must continue to promote international cooperation in the fight against cybercrime by providing demonstrative and training support to the so-called Budapest Convention. In this perspective, this strategic review recommends modernizing the transposition of the Budapest Convention with regard to cooperation measures, in particular to make them possible when no judicial inquiry is opened in France. In particular, the transposition into French law of Articles 29 and 30 of the convention, relating to digital data freezes, is not adequate; freezing requests do not fall within the legal framework (data freezing is not framed in French law), they cannot be the subject of requisitions as provided for by the French text. It also recommends identifying the provisions of the Budapest Convention that may be brought into international law, beyond the criminal policy objectives pursued by the convention. France is opposed to the negotiation of a new international legal instrument.

2.5 France's international action in the cyber field

At a time when the cyber capabilities of States vary considerably, France must position itself as a benchmark player, leader within the European Union. This strategy of influence must lead to promoting the French model and to actively participate in the definition of cyber standards at European and international level. This strategy must be carried out within the European Union, the Atlantic Alliance, the United Nations and in the various multilateral bodies attached to them, but also through privileged bilateral cooperation. This approach of influence supposes in return for agreeing to provide assistance to a close ally victim of a large-scale cyberattack. This support must in particular be able to be offered to our European partners without France taking the place of the prerogatives and responsibilities of the rescued states. Through its public positions, France can express its desire to contribute to the strategic stability of a cyberspace of peace and prosperity.

This strategic review first recommends strengthening our dialogue and cooperation with our allies and partners to prevent cyber crises (2.5.1). It then presents several proposals aimed at better guaranteeing European security and strategic autonomy in the digital space (2.5.2). It proposes the adoption of a classification scheme for computer attacks and an action doctrine (2.5.3). Finally, it analyses the conditions for better regulation of cyberspace (2.5.4).

2.5.1 Strengthen dialogue and cooperation with our allies and partners to prevent cyber crises

Strengthening the protection, resilience and cooperation of all cyberspace actors directly contributes to strengthening our national security. France must today increase its international efforts and continue to develop its bilateral dialogues on these issues with a view to consolidating the stability of cyberspace and the resilience of all States in the face of cyber crises.

France must establish bilateral strategic relations and develop the channels for a frank and open dialogue with the main players in cyberspace. These exchanges offer both the opportunity to monitor and organize work of common interest at the strategic level as well as to improve understanding of the organisation and strategy of these countries, to clarify French positions on major subjects. cyber and share information about possible incidents.

These contacts, and more broadly, our bilateral strategic relationships in the cyber field, respond to imperative traits:

- the frankness of the dialogue, including with regard to the threat emanating, if need be, from our interlocutor;

- the establishment of dedicated exchange channels, which will in particular allow escalation control in the event of a crisis;

- mutual acceptance of limits not to be crossed bilaterally, such as, for example, prohibiting certain practices identified as harmful by the two interlocutors.

France is already conducting, under the coordination of the Ministry of Europe and Foreign Affairs, a certain number of bilateral dialogues on cybersecurity issues (with the United States, China, India, Brazil and Japan in particular). These exchanges must obviously be continued and, if necessary, deepened.

As regards our structural, technical and operational cooperation, they are strategic instruments which contribute directly and indirectly to consolidate our national security and our influence. These cooperations are an asset for several reasons. First of all, they raise the general level of cyberspace security and strengthen its stability by improving the capabilities and resilience of allied and partner countries, as well as the international organisations to which we belong. They also contribute to improving our capacity to face a cyber crisis of international dimension, which would affect France or one of our partners. Finally, they are an effective vector to promote the French offer and expertise in cybersecurity, to publicise our national organisation and to keep us at state of the art by confronting our peers and learning from them. These cooperations thus participate in the dissemination of our political-diplomatic and legal vision concerning the responsible regulation and behaviour of actors in cyberspace.

In the cyber domain, France's geographic priorities largely depend on the type of cooperation envisaged (operational, technical, structural, etc.) and on the institutional actor who will be called upon to implement it (ANSSI, Ministry of Interior, Ministry of the Armed Forces, Ministry of Europe and Foreign Affairs, etc.). Of course, our European and Western partners, with whom exchanges and cooperation are now deepened and regular, remain privileged partners. Certain areas are also priority such as sub-Saharan Africa, in particular the French-speaking countries, North Africa, as well as certain countries of the Middle East and South and East Asia.

It is important that the cooperation maintained by the various government entities be coordinated and consistent with their respective areas of responsibility. In addition, the various actions carried out must be complementary in order to be able to offer some of our partners a French offer of global cooperation.

In addition to the work carried out with our partners and state allies, France must contribute to strengthening the cybersecurity of the international organisations of which it is a member, in particular those which have to deal with information essential to our strategic autonomy, foremost among which the European Union and NATO.

These cooperative actions, in particular when they are operational, require the mobilisation of scarce and limited public resources with regard to human, technical and financial needs. To overcome this obstacle, several avenues can now be explored, in particular the mobilisation of reservists, the solicitation of trusted non-state actors (operators, universities, private sector, etc.) and, finally, favouring the "training of trainers" action.

The national school with a regional vocation on cyber challenges in Dakar

France will support, in partnership with Senegal, the opening in Dakar, by the end of 2018, of a national school with a regional vocation (ENVR) on cyber issues. This project will be built in close collaboration with our Senegalese partner, as well as with the countries of the region, in order to define together the specific needs of West Africa in this area. It will be a school of a new kind. Our field of expertise could be very broad, ranging from governance and international regulation of digital technology, to more practical, even operational, aspects covering the needs of public and private decision-makers. The flexible organisation of its courses should make it possible to meet the training needs, both long and short, in a sector where knowledge evolves very quickly. Drawing on the experience of the Directorate of Security and Defence Cooperation (DCSD) of the Ministry of Europe and Foreign Affairs in the creation of regional schools whose teaching quality is recognised, this school must finally be able to deliver a certified education which will lead to combining, in the initial round table, royal, university or even private partners.

2.5.2 Guaranteeing European security and strategic autonomy in the digital space

Within the European Union, France seeks to promote the best balance between European strategic autonomy for digital security and the maintenance of its sovereign prerogatives in this area, in a logic of subsidiarity and respect for the powers of States in matters of national security.

The objective of European strategic autonomy is the pledge of our collective capacity for initiative and action. As the cohesion of the European Union is weakened and questions have been raised about the credibility of the alliances, awareness of shared security interests is growing, as is the ambition to have more autonomous means of action.

This objective fully applies to the security challenges within digital Europe and is declined between axes.

The first axis is technological and will be detailed in the third part of this strategic review. European Union industrial policy is an important vector for supporting cutting-edge research and development capabilities in order to encourage the deployment of trusted digital security technologies and services, the reliability of which must be able to be assessed. Integrating security into all digital components will also give European offers a competitive advantage.

The second axis is regulatory. Through its external policy, the European Union must seek to maintain its capacity to define regulations which take into account the requirements of competitiveness and the digital potential but which remain protective of citizens, businesses and member states, in accordance with our common values (right to privacy and protection of personal data, protection of critical infrastructure).

The third axis, finally, is capacity. The European Union has an essential role in promoting and supporting the development of cyber defence capabilities of public and private entities within the member states, drawing on European know-how. This need also concerns the European institutions themselves (Commission, Parliament, etc.) which have to protect themselves from possible attacks.

In this context, France must continue to defend the reinforcement of cyber-resilience in the European area (implementation of the NIS directive, cooperation for the treatment of large-scale cyber crises, cybersecurity of institutions and agencies of the European Union, etc.) and to promote a European industrial policy in this area (public-private partnership for cybersecurity, new investments in digital technologies for the future, so-called "breakthrough", etc.). It is also essential to work to take better account of cyber defence within the common security and defence policy (projects of the European Defence Agency, joint training courses, procedures and means to integrate the fact cyber operations of the European Union, etc.). France must, finally, implement means of diplomatic response to cyber crises on a European scale.

Beyond these different dimensions, it now seems necessary to strengthen operational cooperation between the 28 member states of the European Union. Indeed, if the Cyber Europe exercises, organised by ENISA (the European agency responsible for network and information security) since 2010, have enabled member states to test their collaboration in the event of cyber crises, cooperation operational in the event of incidents remains embryonic. However, it has been gradually structured since the launch of the European network of Computer Security Incident Response Teams (CSIRTs) in 2017.

Many Member States, which are experiencing difficulties in developing their own capabilities, want the European Union to play an increased role in support of States victims of cyberattacks. The European Commission, as well as ENISA and certain sectoral agencies which could be called upon to intervene in this field, are particularly receptive to these expectations.

This context could lead to a strengthening of the obligations of the Member States in terms of information sharing and the establishment of a supranational operational capacity within the European Union.

These proposals must continue to be subject to particular vigilance, taking into account the associated sovereignty issues. France, at this stage and taking into account the principles of sovereignty and subsidiarity, considers that in this area operational exchanges must be made on the basis of voluntary cooperation and wishes to avoid the emergence of an autonomous, redundant and competent European capacity to intervene within member states in response to incidents. However, it promotes the deepening of voluntary cooperation between member states, in particular through the European network of CSIRTs. France must fully associate itself and provide support for all initiatives that could help meet this growing need for cooperation in the face of attacks on a European scale, while respecting the competence of States.

This approach must be based on four principles:

- maintaining a clear posture on the distribution of powers and the preservation of national sovereignty in operational matters
- strengthening the cyber capabilities of States;
- the development of operational cooperation within the European Union
- the promotion of an adapted model of assistance to States in the event of an incident, which notably supports a trusted European private sector providing cybersecurity services that can be mobilised in the event of a crisis.

A variation of this approach in operational actions is proposed in appendix 9.

2.5.3 Define a doctrine of action

This strategic review recommends the establishment of a policy of action. Response options to a cyberattack must be prepared in advance to allow the authorities to react in the tempo of the crisis. Questioning the relevance of adopting a doctrine of action, however, first requires strengthening our capacity to discriminate against incidents and attacks in the light of our national interests.

Adopt a classification scheme for computer attacks

Today, in fact, there is no classification scheme for incidents and attacks that can be used at the national level and even less in a manner recognised by all at the international level.

However, to make a political decision, the authorities must be able to rely on a classification scheme for computer attacks which must in no way become the trigger for an automatic response. In order to be able to react appropriately to a cyber incident, any State must first analyse and characterize this event. The effects of computer attacks are complex, varied and cannot be the subject of an exhaustive inventory. To allow an appropriate and proportional response, it is necessary to rely on a rapid understanding of the attack, supplemented by conducting more in-depth analyses of the operating mode and the techniques used.

The United States has made such a classification scheme public, but it is not directly transferable.

Echelle de gravité	*Equivalence avec l'échelle CISS USA*	Caractérisation de l'impact	Caractérisation comme agression armée au sens de l'article 51 de la Charte des Nations-Unies
Niveau 5 - *Situation d'urgence extrême*	*Level 5 Emergency (Black)*	Impact extrême	Probablement possible : à examiner au cas par cas.
Niveau 4 - *Crise majeure*	*Level 4 Severe (Red)*	Impact majeur	Probablement impossible : les actions correspondant à ces niveaux pourraient néanmoins constituer d'autres faits internationaux illicites (intervention, violation de la souveraineté, usage de la force, etc.).
Niveau 3 - *Crise*	*Level 3 High (Orange)*	Impact fort et étendu	
Niveau 2 - *Incident grave*	*Level 2 Medium (Yellow)*	Impact fort et circonscrit	
Niveau 1B - *Incident*	*Level 1 Low (Green)*	Impact significatif et circonscrit	
Niveau 1A - *Evénement significatif*		Impact faible	
Niveau 0 - *Evénement*	*Level 0 Baseline (White)*	Impact négligeable	

National classification scheme for computer attacks

This classification scheme, compatible with the American scheme, integrates national legal standards (Penal Code, Defence Code, etc.) and international standards (general data protection regulations, United Nations Charter, international humanitarian law, etc.). It has four advantages: it makes it possible to share a common and synthetic vision, to accelerate the understanding of the situation generated by the computer attack, to facilitate decision-making with regard to the potential responses to be brought to it and, beyond of its use at the national level, to promote international collaboration in the event of an incident.

It is essentially based on the effects induced by the incident. Among the elements that must be taken into account, we can notably mention the observed negative effects, direct and indirect, produced by the attack, the foreseeable harmful effects of an unfinished attack, a threat or an imminent attack, and the urgency to respond, and, finally, the technical aspects, in particular the innovative nature of the attack vectors.

In order to characterize more precisely the seriousness of any incident, at least five criteria complementary to the induced effects must be taken into account, namely a criterion of intentionality (the intention behind the attack), a criterion of dangerousness (the nature of the targets), an attribution criterion (the nature of the attacker), a massiveness or volumetric criterion (the relationship of the incident to other incidents) and a recurrence criterion (the repetition of an attack).

Finally, the seriousness of the incident must be understood in terms of the attack on four realities:

- the fundamental interests of the Nation, its sovereignty and its democracy (attack on Institutions and democracy, attack on the continuity of State action and government action, attack on the integrity of the national territory, attack on the security of the armed forces, attack on the capabilities of nuclear deterrence, attack on the secrecy of national defence, attack on the capacity to keep international engagements);

- internal and civil security;

- the population and the environment (damage to the health of the population, damage to daily life, damage to essential civil infrastructure, water, electricity distribution networks, etc., damage to the basic needs of the population, damage to public confidence in the capacity of public authorities, damage to the environment);

- the economy.

This plan will constitute both a decision-making aid tool for the authorities, a fundamental element of an action doctrine for France, and support promoting international cooperation. However, such a scheme will never, on its own, make it possible to settle the questions of evaluation and characterisation of a cyberattack, which precede an attribution ultimately falling under a political decision to be taken on a case-by-case basis.

Define options for responding to cyber incidents

France, like any state, has a wide range of possible responses, military or otherwise, to an incident or computer attack. These options, which are sometimes cumulative, can respond to different logics, legal bases and objectives. Some may be carried out in concertation with our partners, others will remain purely national. In all cases, they can only be taken on the basis of a fully sovereign decision, based on a national and independent assessment of the threat or attack to which it is intended to respond.

These measures are of several orders depending on the severity of the event and its legal characterisation. France must, first of all, endeavour to have recourse to mechanisms for international cooperation and the peaceful settlement of disputes. France has a clear, specific and precise vision of the application of international law in cyberspace, presented in the box below.

The application of international law in cyberspace

As the UN group of government experts (GGE) was able to conclude in its report published in 2013, the principles and rules of international law apply to the behaviour of states in cyberspace. If cyberspace has its own specific features (anonymity, the role of private actors), international law nevertheless offers the necessary means to responsibly regulate the behaviour of States in this environment. In this respect, the lack of attribution should not constitute a definitive obstacle to the application of existing international law, all the more since the latter offers neutral means of action with regard to the latter. The principle of sovereignty applies to cyberspace. As such, France reaffirms that it exercises its sovereignty over information systems, people and cyber activities on its territory, within the limits of its obligations under international law. The scope of the measures that France could adopt to react to a computer attack of which it would be a victim depends on the severity of the attack. The more serious the cyberattack, the wider the scope of the measures. A major computer attack targeting France, in view of the serious damage it would cause, could constitute an "armed attack", within the meaning of Article 51 of the Charter of the United Nations, and thus justify the invocation of self-defence. The characterisation of a cyber-attack as “armed aggression”, within the meaning of Article 51 of the Charter of the United Nations, will depend on a political decision on a case-by-case basis. This decision may take into account, in particular, the following parameters:

- Armed aggression is a use of force defined as such because of its gravity and its effects. It is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State.

- The victim State could thus qualify a computer attack as an armed attack, due to substantial loss of life or physical damage to property. In such a case, the State would be the victim of a computer attack causing damage and / or victims similar to those which would result from the use of conventional weapons.

- A second hypothesis could be that of a computer attack targeting a State, which would seem to constitute the first stage of a more classic massive military intervention.

- Furthermore, it cannot be excluded that a series of attacks, each of which taken in isolation would not amount to an armed attack, could be qualified as such, the accumulation of attacks reaching a threshold of severity sufficient to allow qualification of armed aggression.

Below the threshold for armed aggression, which represents the most serious form of the use of force, and above that from which a cyber incident is considered to be an internationally wrongful act, a distinction must be made between different severity thresholds:

- Certain attacks could thus not reach the threshold of the use of force prohibited in Article 2, Paragraph 4 of the Charter of the United Nations. These attacks could nonetheless be contrary to the principle of non-intervention, as well as to other specific rules of international law and thus pave the way for the international responsibility of the State responsible for the attack to be committed and the possibility for the victim State to take peaceful countermeasures or other means of retaliation in response and, in certain cases, to seize the Security Council;

- In the event of attacks reaching the threshold of the use of force within the meaning of Article 2, Paragraph 4 of the Charter, but not reaching the threshold of aggression within the meaning of Article 51 of the Charter, the victim State's response options must remain peaceful, in accordance with the theory of countermeasures. Depending on the gravity of the damage, the victim State is however justified in sanctioning the commissioning State all the more seriously.

The adoption of countermeasures is lawful if the following conditions are met

- The action of the victim State is conducted in response to an initial internationally wrongful act (including the use of force), and has the sole aim of its cessation;

- The action of the victim State is necessary and proportional to this objective, and must remain peaceful (below the threshold of the use of force).

The violation of an international obligation by another State, thereby creating an internationally wrongful act, could manifest itself:

- by “action”: in cases where the State in which the infrastructure from which the attack originates is itself the sponsor. The sponsoring State thereby engages its international responsibility and is exposed to countermeasures. Likewise, a cyber-attack emanating from non-state actors may engage the international responsibility of a State if the State exercises some form of control over the perpetrators of the attack;

- by “omission”: by virtue of the obligation of due diligence, which is a principle of customary international law, every State has “the obligation not to knowingly allow its territory to be used for the purposes of acts contrary to the rights of others States”. A State which has not fulfilled this obligation (means) could thus, in certain cases, engage its responsibility and be the object of countermeasures by the victim State, even if it is not the sponsor. To put this hypothesis into play, it is nevertheless necessary to notify the State beforehand that its infrastructure is used for malicious purposes (knowledge criterion) and to ensure that the State has not fulfilled its obligation (of means) to stop the attack. Such a situation could for example be characterised by the complete silence of a State seized of a request for assistance, or the refusal to cooperate with a view to solving the incident or putting an end to the attack.

Given the specificities of the cyber vector (an attack can be prepared clandestinely and be implemented very quickly; the damage can be considerable on all levels, human, financial, organisational), France cannot exclude the use of exceptional circumstances, to self-defence against an armed attack not yet started but about to be imminent and certain, provided that the potential impact of this attack is sufficiently serious. In the context of armed conflict, the planning and conduct of cyber operations that may be considered as "attacks" within the meaning of jus in Bello (or international humanitarian law) will be subject to it. The main principles of this right are necessity, proportionality, distinction and humanity. Beyond the main general principles, it is a matter of deciding the operational questions which arise on a case by case basis, on the basis of precise and proven facts. In this analysis, the following elements should in particular be taken into account:

- Cyberweapons must be able to be used in a discriminatory manner: the designers of the cyberweapon must ensure that it can be aimed at one or more targets explicitly designated, while taking care to minimize the negative effects on others entities as the designated target. It is a condition for respecting the principles of proportionality and distinction;

- The civilian population and civilian objects must not be attacked, unless civilians participate directly in hostilities, and civilian objects have lost their protection by becoming military objectives

The neutrality of States not party to conflicts must be respected if the simple transit of a cyberattack through the infrastructures of a State not party to the armed conflict seems to be tolerable in international humanitarian law, on the other hand, the use of the infrastructures of this State as attack infrastructure is against international law.

If the situation required, it would then be possible to take retaliatory measures, resort to exceptional self-protection mechanisms and / or adopt peaceful countermeasures. The most serious cases may require a response using force. The main options for responding to cyber incidents are presented in Appendix 8.

2.5.4 Regulating cyberspace

France must take the initiative to promote the strategic stability of cyberspace and its vision of the application of existing international law in this area (law applicable in peacetime and the rights of armed conflict). This approach should be complemented by the identification and promotion of new standards of responsible behaviour by states in cyberspace. It is therefore a question of agreeing on regulatory options or informal international standards, allowing us to preserve our values and our interests by discouraging the most destabilizing offensive IT actions.

France must defend its vision of a secure, free and open digital space within the various fora and international organisations in which it participates as well as with its state partners but also in new formats which remain to be defined, including, where appropriate, the private sector.

We first present the rules and standards applicable to States and possible developments for the latter, before turning to the rules and standards relating to the responsibility of private actors in the security of cyberspace.

Rules and standards applicable to States

The various negotiation cycles conducted within the framework of the United Nations (UN) Governmental Group of Experts (GGE) on cybersecurity have made significant progress in terms of international regulation.

France has also had the opportunity, with several of its partners, to affirm its position in favour of the clear and unequivocal recognition of the lawfulness of the means of responding to a cyberattack, which they involve the use of force (self-defence) or not (countermeasures, retaliatory measures, etc.), and the applicability of international humanitarian law to cyber operations carried out in the context of armed conflicts.

The failure of the GGE's 2016-2017 negotiation cycle will not put an end to France's efforts to promote standards of behaviour and confidence-building measures at the international level in favour of the stability and security of cyberspace.

If negotiations stalled on the question of the applicability of international law to cyberspace, France had nevertheless managed to generate a consensus of all experts on several of its proposed principles for regulating cyberspace. An agreement had notably been reached concerning the control of exports of offensive cyber tools and techniques or the prohibition made on non-state actors, including private companies, from carrying out offensive activities in cyberspace for themselves and on behalf other non-state actors. The proposal to follow up on the implementation of behaviour standards and confidence-building measures already approved had also aroused wide interest among representatives of the GGE.

France will therefore continue to work towards the universalisation of certain standards applicable in cyberspace with a view to strengthening security. This approach revolves around three principles: prevention, cooperation, stability.

- *In order to strengthen resilience in and of the digital space: the principle of prevention*

The uncertainty intrinsically linked to the attribution of a cyberattack should encourage States to focus their efforts on preventive measures, making it possible to reduce their vulnerability.

The defensive pillars on which the French cybersecurity model is based (a national regulatory framework for the protection of critical infrastructures; a high level of requirements in terms of systems and data security; an organic separation between intelligence and cybersecurity) deserve, in view of their stabilizing effect, to be disseminated internationally. States choosing to adopt this model would thus be led in particular to set up an institutional organisation making it possible to responsibly manage the vulnerabilities discovered.

In addition, these states should commit to limiting the proliferation of cyberweapons by controlling the export of offensive cyber tools and techniques (while taking into account the legitimate interests of cybersecurity companies and the academic world) and by supervising the destabilizing practices of private actors (these States should not authorize, within their jurisdiction, the use by non-state actors, in particular of the private sector, of techniques and cyber tools which can have unfavourable consequences on a third party).

- *In order to implement and enforce the standards already approved: the principle of cooperation*

Improving the cooperation of the international community in cyberspace is an effective way to reinforce its stability through mutual knowledge, even trust, deepened between the actors and by the establishment of mechanisms for joint crisis management, communication and de-escalation.

In this perspective, France must in particular work to reach an agreement, at the international level, on the obligations which weigh on a State whose infrastructures would be used for malicious purposes. The objective is to apply, in the cyber field, the principle of due diligence which provides that every State has the obligation "not to allow its territory to be used for the purposes of acts contrary to the rights of other States". This principle of "cyber-diligence" could in particular make it possible to strengthen voluntary operational cooperation between States, essential in order to protect certain critical infrastructures and to respond to major cyberattacks, especially when these transit via a third State.

France will propose to its partners to study the feasibility of a cooperative mechanism for monitoring the implementation of the recommendations agreed during the GGE sessions of 2013 and 2015, or even in other frameworks such as the G7. This intergovernmental apparatus could notably be based on peer review practices, conducted on a voluntary basis, formulating recommendations addressed to States. A directory of identified contact points would also help establish communication channels that facilitate crisis prevention and resolution.

- *To ensure the right of states to defend themselves in a legal and appropriate manner: the principle of stability*

On the basis of the recognition by the GGE in 2013 and in 2015 of the application of existing international law in cyberspace, France must continue to promote the principle of the existence of certain rights allowing States victims of cyberattacks to take action. appropriate measures to preserve international peace and security.

The first of these rights would allow a victim state to seize the Security Council of the United Nations, in the event that the situation is serious enough to be considered a threat to peace and international security. Among other options, the Security Council could then adopt coercive measures on the basis of Chapter VII of the Charter of the United Nations.

The second of these rights is to be able to respond to cyberattacks. If States must seek to settle their differences through cooperation and negotiation, this does not exclude the possibility for a State victim of a cyberattack having reached a critical infrastructure to take the necessary and proportional technical measures in order to neutralize the effects of this attack, in compliance with its obligations under international law.

The third right is, finally, the possibility of considering a cyberattack as an armed attack, in particular if it was carried out against a critical infrastructure, resulting in paralysis or the destruction of vital economic functions and activities, or if it undermined the population.

Rules and standards concerning the responsibility of private actors in cyberspace security

The rise of digital technology as a new tool and space for confrontation has given the private sector, in particular to a certain number of systemic actors (.), a critical role and an unprecedented responsibility in the preservation of international peace and security.

Cyberspace is largely made up of commercial products for the general public, which can serve as a support for large-scale attacks which exploit their manufacturing defects (Windows software flaw for WannaCry and Petya attacks). It is therefore necessary to set international standards aimed at ensuring that products of a systemic nature cannot be diverted from their initial use to conduct computer attacks. The problem is posed in an increasing way with the multiplication of connected objects that can serve as attack vectors.

“Cyberweapons” (intrusive or destructive software) are also partly produced by private companies in a market which is very difficult to regulate due to the dual offensive and defensive purpose inherent in these products. Intrusion software is now included in the list of dual-use goods of the Wassenaar Arrangement, a multilateral regime for the control of conventional weapons and dual-use goods and technologies that France applies. It is necessary to continue regulatory efforts in this direction, including by raising the question of the inclusion of certain cyber tools on the list of war materials. This aspect will be deepened in the third part of this strategic review, taking into account the viability of a national or European offer.

Finally, "mercenary" services are developing and offering offensive cyber counterattack services, according to a logic of private self-defence (Hackback). In order to allow States to maintain the monopoly of legitimate violence in cyberspace, it is necessary to lay down clear rules for businesses with regard to "active" cyber defence.

In this context, interstate regulation alone cannot provide an effective and lasting solution to the security challenges of the digital world. Strengthening the stability and international security of cyberspace therefore requires the definition of new forms of regulation, taking into account the role of the private sector.

Three priority axes for a better regulation of the activities of the private sector need to be addressed: the supervision of offensive action by the private sector in cyberspace, the control of exports of cyber tools, software and techniques, and the responsibility of companies in the design and maintenance of digital products.

- *Supervise the offensive action of the private sector in cyberspace*

The proliferation of attacks and the difficulties encountered in prosecuting them have prompted the private sector to develop cyber defence capabilities. This dynamic can lead to promoting Hackback, that is to say the authorisation for a private actor to carry out cyber offensive actions in response to an attack of which he is the victim.

At the same time, some States plan to entrust private companies with a certain number of cyber offensive actions as part of their military policy, like what exists with private military companies for traditional capabilities.

The use of offensive capabilities by the private sector poses a risk of systemic instability in cyberspace. The conduct of such computer attacks against actors located on the territory of another State, or even directly against a State, would entail a risk of dangerous escalation and would call into question the monopoly of the international use of force by States. In addition, the question of attribution is posed in the same way for the private sector as for States. Indeed, these companies often having multiple international holdings, they could be brought to lead the response from the territory of a third country, different from that having undergone the aggression. This would complicate the attribution.

Faced with the risk of a multiplication of offensive actions in cyberspace, France proposes, on the one hand, to promote the prevention of the use of cyber offensive capabilities by non-state actors and, on the other hand, to support the prohibition, for non-state actors, from carrying out offensive activities in cyberspace for themselves or on behalf of other non-state actors, except in very specific cases and provided that the technical actions possible in this context are strictly framed.

In order to be realistic, such rules must be defined precisely on the technical level in order to draw a clear line, controllable and acceptable to all. The question of a possible exception to the general prohibition on the use of cyber offensive actions by private companies in self-defence will have to be asked at the international level.

❖ *Corporate security responsibility for the design and maintenance of digital products*

Many computer attacks are made possible by the lack of security updates for widely used computer products. This situation raised the question of corporate responsibility for maintaining security conditions. This risk takes on a systemic dimension when the products concerned are used extensively.

It therefore seems relevant to lay down at international level a principle of responsibility for the security of systemic private actors in the design, integration, deployment and maintenance of their digital products and services. This accountability could translate into an obligation for systemic companies to guarantee the long-term security of their digital products, in particular by providing appropriate patches in the event of vulnerability. The level of responsibility must be fixed according to the role and the size of the actor concerned and could be presented as an obligation of means rather than results.

The primary responsibility rests with the producer, who must guarantee progressive security corresponding to the use of his product throughout its lifetime, in accordance with good IT security development practices. This aims both to guarantee a level of security for the product itself but also a minimum level of security vis-à-vis the systems to which this product is connected. The use of security certification, in particular within the framework of the European certification scheme being defined, should be strongly encouraged and even made compulsory for critical components in sensitive sectors.

Given the rapid evolution of state of the art in digital security, it is the producer's responsibility to put in place the necessary apparatus to continuously maintain the security of his products (watch, dedicated teams security reviews, training of development teams, “bug bounty” competitions, etc.). The patches must also be accessible, as widely as possible, even in the absence of a maintenance contract, and within a reasonable time once the vulnerability is brought to the attention of the manufacturer.

The producer's responsibility must extend beyond the end of the product's marketing date and for a period long enough to cover the life of the products concerned. In the event of permanent cessation of maintenance, it is necessary for the producer to make available the necessary technical information (code, documentation) so that its customers can take charge of maintaining the condition in security themselves.

Producers must also be able to provide assistance to their customers in the event of an attack, in particular in order to facilitate the restoration of the functioning of the products concerned. This responsibility relates in particular to supporting public authorities in the event of a breach of a critical system. At a minimum, this would involve communicating the necessary expertise and technical information, as well as providing systems allowing the reconstruction and updating of the product.

Furthermore, the responsibility of distributors and integrators should also be defined. The distribution of products in obsolete or non-updatable versions must be prohibited, as well as the distribution of products known for their insufficient level of security. Indeed, the integration or purchase by customers of such products represents a risk not only for their systems but also for the entire digital space.

In this perspective, France must mobilize the private sector to disseminate good practices and codes of conduct as well as to contribute to taking these issues into account in contractual clauses. However, for the most sensitive products, regulatory initiatives, in particular at European level, could be envisaged.

Negotiation formats

The failure of negotiations in the UN GGE underlines the absence of a common vision, shared by the main cyber powers, as to the international security architecture which must govern relations between states in the digital age. However, this failure in no way signifies the end of diplomatic efforts to regulate this area. France must continue to take an active part in these debates, whatever the negotiation framework chosen: the UN, the G20, the G7 or even regional organisations such as the Organisation for Security and Cooperation in Europe (OSCE).

The failure of the last session of the GGE invites us to rethink the treatment of cybersecurity issues within the United Nations.

The G7, of which France will assume the presidency in 2019, already published, in March 2017, the Lucca Declaration on the responsible behaviour of States in cyberspace. This text, first negotiated within the framework of the Ise-Shima Cyber Group, takes up the standards of behaviour agreed in 2015 by the GGE, while reaffirming and deepening the recognition of the full applicability of international law to cyberspace.

The G20 seems to constitute, for its part, a forum adapted to a subject combining issues of sovereignty, international regulation and private actors. In 2015, the G20 member states agreed to ban the use of cyber means for economic espionage.

The work within the OSCE needs to be further developed. France is continuing its action in favour of the implementation of the 16 confidence-building measures applied to cyberspace, adopted in 2013 and 2016. It will continue to encourage its partners to adopt inter-ministerial procedures which can be mobilised to ensure good communication between states in times of crisis. Such mechanisms could usefully be replicated in other regional fora (African Union, Organisation of American States, ASEAN regional forum, etc.).

In addition to these intergovernmental formats, the so-called "track 2" forums, which bring together States and representatives of civil society, the private world or research such as the Global Commission for the Stability of Cyberspace, the Global Forum on Cyber Expertise, Sino, European Cyber Dialogue, etc. These forums also constitute important frameworks for debate.

This strategic review recommends the creation of a new national (or European) think tank dedicated to cyber defence issues, within which the ideas of France could find a relay.

It also recommends the launch of a French initiative as part of the G20 to regulate the activities of the private sector having an impact on the international security of cyberspace, around three axes:

- the supervision of offensive actions by the private sector in cyberspace
- export control of certain cyber tools, software and techniques
- the security responsibility of systemic companies for the design and maintenance of digital products.

***

France's positions must make it possible to display its desire to build strategic stability in cyberspace, so that it is at peace, prosperous and respectful of freedoms and in which it intends to ensure all its sovereign functions and assert its sovereignty.

The French model, based on the establishment of an independent defensive chain, must be promoted among our partners, in particular through the conduct of strategic dialogues dedicated specifically to cyber issues, and in various European and international forums. France must develop these bilateral dialogues as a priority with a few key countries, with the aim of negotiating frameworks for political agreement that will avoid the most destabilizing or dangerous actions (Russia, China, United States, United Kingdom, etc.).

France must also be a driving force for Europe to become a space conducive to digital development and guaranteeing citizens a cyberspace of trust, secure and protective of individual freedoms. France must have an ambitious vision of the role of the European Union in cybersecurity while reaffirming the responsibility of the Member States and the preservation of their sovereignty in terms of operational response.

France must continue to fully engage in the work devoted to cyber issues within the framework of the Atlantic Alliance, and contribute to it proactively in view of the Brussels Summit (July 2018). It will thus endeavour to continue strengthening the defence capabilities of NATO and the Allies, in particular via the Cyber Defence Pledge, and will ensure that cyber offensive effects are integrated into Alliance operations and missions in accordance with its interests. Public communication is likely to contribute to our own policy of discouraging computer attacks while opposing any hint of collective attribution will be developed.

France must bring to European and international bodies a strategy to promote responsible behaviour by state and non-state systemic actors and to develop confidence-building measures in cyberspace, as well as its vision of the application of existing international law, including international humanitarian law in this area. This posture is all the more essential in the current international context of the failure of the last negotiations conducted within the framework of the group of government experts (GGE). Therefore, France must take the initiative to defend its interests in cyberspace, put forward its model and the ideas it carries in terms of international regulation of cyberspace.

Finally, the development of a serene and secure cyberspace requires an effective fight against the criminals who operate there, including when attacks are launched from abroad. France must therefore continue to promote international cooperation in the fight against cybercrime, in particular by supporting the so-called Budapest Convention. France must endeavour to perfect, with its foreign partners, the mechanisms for mutual legal assistance in the fight against cybercrime and to continue the exchange of experience and technology in this field.

3 Part 3. The State, the guarantor of society's cybersecurity

France's cyber defence, beyond that of the state itself and operators of vital importance, involves raising the overall level of cybersecurity in society. To be effective, it is a question of considering, in a logic of digital sovereignty, a cyber defence-in-depth of our country integrating that of the citizens, the companies and the territorial collectivities.

This is why this third part of the Cyber Defence Strategic Review proposes ambitious advances in terms of both regulation and the economics of cybersecurity. Public action must double that of economic agents, who remain primarily responsible for their IT security. The role of the State is to provide an increased effort in terms of training and skills management in the field of cybersecurity.

3.1 Digital sovereignty, an essential component of national sovereignty

Digital sovereignty can be understood as the capacity of France on the one hand, to act in a sovereign manner in the digital space, while preserving an autonomous capacity of appreciation, decision and action and on the other hand, to preserve the most traditional components of its sovereignty over new threats taking advantage of the increasing digitisation of society. Digital sovereignty therefore does not represent the desire to do everything nationally, which would be synonymous of withdrawal, but rather to retain autonomy and freedom of choice.

The reflections conducted in the context of this strategic review converge on the need for our country to fully exercise its digital sovereignty. To this end, it is proposed to structure an industrial policy in digital matters, based on the mastery of key technologies (for example, IP stream encryption, attack detection probes, professional mobile radio).

The challenges of cloud computing and artificial intelligence are also at the heart of any digital sovereignty strategy.

3.1.1 Sovereign activities

The mastery of certain technologies and services is essential to the exercise of our digital sovereignty. This mastery is largely based on the qualification by the State of a trusted offer of digital technologies and services. In addition, an industrial strategy based on "open source", provided that it is part of a thoughtful commercial approach, can allow French or European manufacturers to gain market share where they are now absent and thereby allowing France and the European Union to regain sovereignty.

Identify the needs necessary to protect digital sovereignty

Identifying the needs necessary to protect the interests of sovereignty is a preliminary step to determining the digital technologies and services whose availability, and even ownership, are essential for our country. These needs arise from the need to ensure the sovereign missions of the State and the critical activities of the OIV on the one hand and, on the other hand, to protect the nation's values, heritage and economic interests.

For each of these families of needs, an analysis must be conducted in order to bring out the key technologies that support these needs. Subsequently, the strategic choices making it possible to respond to these needs must be identified, like the architectures of solutions adopted[39]. Finally, if there is no relevant solution or if technological developments are likely to change these strategic choices[40], it is then necessary to identify the concrete avenues that could make it possible to propose suitable solutions.

Assessing the need, proposing solutions and solution architectures, deciding on a strategy, in particular to own, control or bring to light key technologies, these must be the objectives of a public cybersecurity policy. The conduct of this policy requires dedicating specific resources, in charge of a technological watch and proposing choices. It could be a small inter-ministerial team (positioned with the general management of companies or the ANSSI) mobilizing for these works and its studies all the competent administrations (Ministry of Economy and Finance, Ministry of the Armed Forces, Ministry of Interior, Digital Secretary of State, ANSSI, France Stratégie, etc.) as well as the industrial sector. It could usefully rely on the structures put in place within the framework of the Industrial Security Sector Committee (CoFIS) for regular and updated identification of critical technologies and disruptive technologies.

Qualify an offer of trust

The security of our supplies requires that demand can be satisfied by an offer of confidence and sufficiently diversified. Certain uses or certain functions require minimal control of the condition of the products used (approval, certifications, access to source codes, etc.). Finally, the satisfaction of certain needs calls for the development by a trusted industrialist of specific products according to the specifications of precise specifications. This product must remain completely free to use and for exclusive use and be subject to regular evaluation as to its security level[41].

[39] This description of architecture and key technologies must include an analysis of the degree of control required over the technologies used, over confidentiality, if cryptography is used, this can be broken down into products (IP encryptors) or optionally into a communication offer (messaging, web, etc.).

[40] This presentation must be made in the short and medium terms and specify the time horizons selected.

[41] The level of security must be assessed with regard to the potential risks, whether they are endogenous and linked to product performance (failures / discontinuity of service, lack of performance), or exogenous and linked to different forms of attack (aimed at gaining access information, modify information, take control of systems).

To qualify an offer, the State must be able to identify the manufacturers and the products that are both eligible and available (see box below) for our security and sovereignty needs. Then, a certain number of criteria must be met, five of which are of particular importance:

- control by the company of its industrial developments and processes[42];
- the degree of transparency accepted by the manufacturer on the manufacturing of its products (provision of source code for example);
- the decision-making autonomy enjoyed by the manufacturer (to fix, for example, the roadmaps of its products, its architectures, etc.) which must not be subject to possible interference from undesirable third parties;
- acceptance of controls by the manufacturer. The premises in which its products are developed must in particular be accessible (located in Europe) and its production processes must be subject to audit;
- compliance, by the manufacturer, with rules for the protection of secrecy (process for enabling people and facilities, setting up security rules and restrictive areas, etc.)[43].

Nationality (French or European) is in itself a criterion to be taken into account in order to recognize the quality of a trusted industrialist. However, it is not always enforceable or relevant.

Compliance with these different criteria must be able to be regularly assessed, as well as certain changes relating to the capital development of the company or its strategic choices.

Establish an inventory of the existing supply of digital technologies and services essential to the maintenance of national sovereignty.

For each of the key technologies, the establishment of the inventory of the existing offer is done on the basis of the following questioning scheme:

[42] Any subcontracting should only be carried out on non-critical parts of the products (risk analysis supported). Or via trusted industrialists themselves.

[43] It should be noted that the location of decision centres, research and development units has a direct impact on several of these criteria.

Is an offer of trust necessary?

a) If yes, do we have such an offer? Is it sustainable and capable of adapting to needs?

If so, by what methods, under what conditions and at what cost? What are the requirements for the offer (maintenance of the availability of an open-source offer, competitive intensity and maintenance of several competing offers, adequate positioning in the value chain, substitutability of the product or service, etc.)?

b) If not, is an alternative offer of confidence likely to emerge? Under what conditions and at what cost?

This step must integrate all the technological (in principle in the roadmap of the industrialists concerned) and economic (including the "sovereign", national or export market[44]) dimensions. It must also detail the various possible public actions and their scope (at least in order of magnitude) to be compared with the size of the market. The action can be financial (public support in capital or in subsidy for the manufacturer or its subcontractors, purchasing policy, etc.), regulatory (control of foreign investments) or take the form of aid for the supply of certain components.

3.1.2 Three technologies, among others, whose mastery is essential to our digital sovereignty

Among the key technologies whose mastery is necessary for the exercise of our digital sovereignty, the strategic review has chosen to highlight three. The choice was made on the essential nature of these technologies: encryption of communications, detection of computer attacks and professional mobile radios. The questions of cloud computing and artificial intelligence are also fraught with challenges.

Communication encryption

With the convergence of all digital communication protocols towards IP technology, the encryption of communications has gradually concentrated around encryptors dedicated to this technology (called "IP encryptors"), whether they are hardware equipment or pure software.

The hardware or software developed by several manufacturers is non-interoperable, and none of the suppliers is able to meet all of the needs, which results in a very fragmented and small-scale market which relies almost exclusively on the public order. To avoid obsolescence and loss of competitiveness of products vis-à-vis their foreign competitors, in particular for the EU or NATO markets, but also for certain needs of our companies, it is necessary to revitalize our national offer. The ANSSI has undertaken in this sense, by means of a generic specification, to make the products interoperable, which should ultimately allow to have a complete coverage of the need and to relaunch an area frozen by investment costs on the supplier side and the migration costs on the customer side. For the success of this approach, it is essential that state customers, but also large industrial accounts, require interoperability in their calls for tenders.

[44] Even sensitive security products are exported.

Detecting computer attacks

The capacity to supervise on a large scale the information systems of the infrastructures of the State and the OIV to detect if there are computer attacks constitutes a crucial stake, which supposes product suppliers and service providers of total confidence. The effectiveness of attack detection solutions depends on the integration of software or hardware components in strategic locations of an information system, which accentuates the need to master these components and to have all the guarantees on those who manufacture or implement them.

The market for attack detection tools (probes and agents, see table) is largely dominated by foreign industrial players who do not necessarily meet the necessary confidence criteria. However, work has been undertaken to bring out in 2018 trusted solutions for France in terms of network flow analysis or local agents at IT stations. They are supplemented by specific state developments, reserved for the supervision of administrations. All these solutions (industrial and state-owned) are technologically dependent on critical third-party components for analysis, the confidence or durability of which are not fully acquired, whether they are industrial supplies or free software.

There is also no leading national publisher in the field of fundamental technologies enabling the processing of large volumes of information. Alternative implementations, however, exist in the form of free software and can be integrated by trusted actors or by state teams. The sustainability of these implementations is not necessarily guaranteed and constitutes an important issue.

The situation is similar in the areas of attack detection and malware analysis, where existing solutions rely mainly on foreign players or free software. We nevertheless note the emergence of national offers, the robustness of which remains to be confirmed or which are aimed at specific markets. The expertise associated with these activities, held by specialised teams within the State, is also being structured within a fabric of private service providers, through the qualification by the ANSSI of Providers of Security Incident Detection (PDIS).

The creation and availability of updated and trusted databases of attack markers remain a point of weakness. No national industrialist providing such bases, sovereign detection solutions remain entirely dependent on public bases. The ANSSI has an autonomous capacity for developing markers, the provision of which to trusted private actors is being organised. However, the ability of only state teams to change scale and cover all the needs for markers remains all the more problematic as the current extension of the field of detection to client workstations, servers and the cloud increases the workload.

More generally, the lack of national or European actors in the field of Threat Intelligence reduces our capacity to have massive information on cyber threats. This situation risks over the long-term national capabilities to search for new algorithmic detection solutions. This dropout risks being accentuated by the development of new detection methods based on artificial intelligence. However, responses to this soon expected real technological breakthrough are strongly linked to access to such data sets. The emergence of a benchmark industrial player, national or European, in the field of Threat intelligence and the development of markers, is for these reasons eminently desirable and should be sought.

The essential components of a complete detection solution

A complete detection solution combines several means and capabilities:

- sensors making it possible to observe the activity of an information system in real-time, through network flows (probes) or the operation of computer stations (agents), whether on isolated stations or cloud architectures;

- capabilities for collecting, indexing, processing and storing large volumes of data, from sensors or the collection of operating logs for example;

- methods and algorithms to distinguish normal activities from malicious activities, based on information from sensors. This discrimination can be affected by the recognition of signatures characteristic of attacks and "behavioural" anomalies;

- bases of markers, including signatures of attacks classified because of their sensitivity, and more generally a knowledge of the main adversary operating modes;

- an ability to analyse detected attacks, enabling doubt to be raised and the signature base to be enriched.

These components, in turn, depend on key technologies (high-speed analysis of network packets or files, Big data processing, reverse engineering or secure detonation tools of malicious code, etc.), on the integration capacity of these technologies, and specific expertise.

Professional mobile radios

In twenty-five years of existence, professional mobile radio networks have demonstrated their usefulness for the security forces and rescue units. The needs have however evolved and the current networks are both saturated and technically limited.

The organisation of forces and the concentration of resources on limited geographic areas make the technical limitations of current networks even more manifest (number of group conferences, registration capacity of terminals in the area, etc.) which, combined with expectations of users generate frustration. The performance of the terminals entrusted to them – whose ergonomics are closer to the mobile phones of the 1990s than current smartphones – increasingly leads them to use their professional or private smartphones as a means of communication. Security forces or rescue services also complain of insufficient coverage, both outside and inside buildings[45]. Operational managers criticize the absence of functions now perceived as essential: video, access to the information system, access to public telephone networks, etc.

For the operational reasons mentioned above and with a view to protecting the confidentiality of communications, a new generation of professional mobile radios should be developed for the benefit of the security forces and rescue units. It would be a question of providing a network offer favouring the interoperability and the coordination of the forces and the means engaged on the ground, in particular in situation of operational crisis, without functional regressions compared to the current means (in particular compared to the commercial services mobile phone)[46].

In order to go beyond the limits of current technologies, the future solution should rely on standard equipment and as much as possible on existing operator networks, thus limiting costs and training effort for agents. It should also be able to evolve over time (in particular to ensure the transition to 5G). An opening to operational service with limited coverage in 2022 and across the whole of Paris in the run-up to the Olympic Games in 2024, appears technically possible.

Due to the convergence observed between this field and that of mobility security (telephony, messaging, social networks, etc.), this strategic review recommends conducting a global analysis to see how to pool an infrastructure and products to respond to these two needs. Like the RIE, the DINSIC could provide administrations with mobility services allowing in particular secure and resilient access to RIE data.

[45] The problem is not so much that of the lack of coverage as the differential that exists with commercial mobile telephone networks.

[46] Among the issues of non-regression is the subject of direct mode (direct communication, outside infrastructure, between two terminals).

3.1.3 Harnessing the full potential of artificial intelligence techniques for cybersecurity

The challenges of sovereignty around artificial intelligence (AI) are considerable and push all the major powers to invest massively in research and industrial developments. Following the publication of several reports on the subject (in particular the report "France Artificial Intelligence" and the report "For an artificial intelligence controlled, useful and demystified" of the Parliamentary Office for the Evaluation of Scientific and Technical Choices (OPECST of March 2017[47]), a mission was entrusted on September 8, 2017, by the Government to the deputy Cédric VILLANI, in order to refine, deepen and prioritize the work already carried out on artificial intelligence. The conclusions of this mission could then be broken down into a concrete roadmap laying the foundations for long-term French and European action, pending these[48], only the links between cyber defence and artificial intelligence are analysed in this part of the strategic review.

The first issue already identified in the Paragraphs of this strategic review devoted to memory (see part l) and in the *France Artificial Intelligence* report of March 2017 is that of cybersecurity of artificial intelligence systems. Elon Musk, after an electric vehicle of his brand TESLA was hacked by researchers from the company TENCENT, stressed in this regard, in July 2017 before the American authorities[49], that the future of autonomous vehicles was conditioned by cybersecurity. Whether in learning phases, which may involve taking into account sensitive data in terms of security, or during the use phases, AI systems must be protected in order to prevent an attacker from stealing information or take control of it. For reasons of efficiency and cost, the cybersecurity of AI systems must be thought out *ab initio* and be integrated into their development from the design stage.

[47] Synthesis report France Artificial Intelligence, March 2017: wwrw.economie.gouv.fr/France-IA-intelligence-artificiel. Report for a useful and demystified controlled artificial intelligence, Claude de Ganay, Dominique Gillot, OPECST, March 2017: http://www.senat.fr/fileadmimages/opecst/quatrepages.pdf.

[48] The objective assigned to the mission consists in studying the actions necessary to allow France and Europe to be at the forefront of the economy of artificial intelligence, to describe the best international practices of application of these technologies at the service of the transformation and improvement of public policies, identify priority applications to deploy within the public sphere and open the field to national reflection on the impacts of artificial intelligence, considering its effects on the work the ethical issues it raises (http: //www.villani201Zeu/blog/mission.villani.sur.l.intelligence.artificiel).

[49] Speech by Elon MUSK, July 15, 2017, before the National Governor Association.

Beyond the issue of cybersecurity of AI systems, the application of artificial intelligence techniques to the field of cyber defence offers promising prospects. The IT field lends itself easily to simulation or automation, greatly facilitating experimentation and learning by reinforcement from available and labelled data (malware databases, vulnerability database, network database, …). Artificial intelligence techniques have already been used to detect an attack among network flows or malicious software, but also to recover the PIN code of a smartphone, the key of a smart card or even perform operations of phishing, through tweets adapted to the habits of a target[50]. In 2016, DARPA, the Pentagon's research agency, launched a cyber challenge to test the ability of AI systems to detect and fix software flaws. If the performance of the Mayhem software, winner of this competition, does not match the skills of the vulnerability researchers at the DEFCON 2016 conference[51], it is likely that the machines will exceed the best world experts in a short time.

The mastery of artificial intelligence systems applied to cyber defence is therefore a major issue for France because, used in support of state experts, these machines will considerably increase their efficiency. However, if French research in AI is at the forefront in many fields, it is unfortunately only little mobilised on the objectives related to cybersecurity. In connection with our industry, an effort should therefore be made to correct this situation, particularly in the fields of attack detection, vulnerability search, analysis and categorisation of malware.

Beyond the classic research support actions, access to quality, updated and categorised data sets is a major determinant of research in artificial intelligence. In its application to cyber defence, it is clear that the publicly accessible datasets concerning computer attacks and malicious code are of small size and of poor quality. While certain private players (publishers of antivirus or detection solutions in particular) have high-quality data, these are generally not shared, and the players concerned are mostly non-European. The consolidation of public data sets, and access by researchers, under conditions to be determined, to data sets held by private actors and the State, constitute capital challenges in this respect.

[50] https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-SpearPhishing-On-Twitter.pdf

[51] https://www.computerworld.com/article/3105044/security/mayhem-supercomputer-takes-on-humans-at-defcon.html

3.1.4 For cloud computing, invent a regulation and data protection strategy

Data protection, the real fuel of the digital economy, can only be envisaged at the European level. In particular, it will be necessary to find a fair balance between good data protection and their free movement on European territory, which is likely to encourage the full emergence of a European digital single market. States should be able to maintain access to data, especially the most sensitive, which they should be able to continue to regulate. However, this approach can only be truly relevant with the implementation of a strategy to promote the development of cloud computing trust offers.

For the sole hosting of their data or for the hosting of complete applications, organisations tend to move an increasing part of their information systems to cloud platforms operated by third-party providers. Outsourcing to a cloud is likely to offer proven benefits to the customer, in terms of cost as well as reliability and flexibility. It also provides an attractive response to the growing complexity of IT and the difficulty, for many organisations, of having all the necessary skills.

The development of the cloud is now accelerated by the strategy adopted by the majority of software publishers, which aims to make them evolve from a product marketing model (software installed at the customer) to that of a service provision (client access to software hosted in the publisher's cloud). This trend is tending to become widespread, including for highly specialised and particularly critical software, such as that which provides centralised routing of network flows for electronic communications operators.

For some organisations that do not have sufficient internal skills (SMEs for example), the use of the cloud can prove beneficial to their IT security. It can indeed bring a certain resistance to non-targeted IT attacks of moderate technical level. The use of the cloud nonetheless carries new risks and the strong domination of the cloud market by a small number of foreign players, mainly American and to a lesser extent Chinese (but whose size and number are constantly growing), gives at these risks a dimension of national sovereignty.

First of all, on the legal level, the use of the cloud raises the question of the law applicable to hosted data and applications, as long as the hosting is done outside the national or European territory, or that the nationality of the provider subjects it to constraints legal whose scope may include an extraterritorial character. In addition to the problem of illegitimate access to data that could arise from this, consideration should also be given to the possibility for cloud users to circumvent certain binding provisions of national law, in particular with regard to cybersecurity.

On the technical side, then, the use of the cloud can offer the service provider complete control of the data and software entrusted to it by its customers. A malicious provider could thus, on his initiative or at the request of a State, infringe the confidentiality of data (spying), but also their availability (sabotage). The provider could also be the victim of a computer attack, with the same consequences. This risk is particularly significant when systems hosted in the cloud could, in the event of a malfunction, cause the destabilisation of an economic player, or even of a State.

Finally, economically, outsourcing to the cloud can lead to a risk of increased technological dependence on the service provider. Thus, the marketing of software in the form of a service[52] in the cloud transforms the customer, previously the owner of the software, into a simple tenant, dependent on the pricing imposed by its provider, and often without recourse due to the lack of alternative solutions or reversibility.

The so-called “sovereign” cloud offers, put in place by national operators funded by the state, could have provided an answer to the strategic problem of locating the cloud and trusting its operator. However, these offers are struggling to establish their economic viability. On the other hand, it should be noted that other national cloud operators manage to remain competitive and masters of their technological solution, whether on the general hosting market or on a niche market.

In recent years, several large non-European cloud providers have also established partnerships with European operators, allowing the latter to market the solutions of the former by ensuring their hosting. The agreement between DEUTSCHE TELEKOM (DT) and MICROSOFT is the most emblematic case. Established at the instigation of the German government to respond to security concerns, this agreement enables DT to host MICROSOFT cloud software solutions in its own data centres and to market them, in particular for the benefit of German administrations. In France, OVH is also positioning itself as a host for certain MICROSOFT solutions.

Faced with these findings, this strategic review proposes to implement the following four series of measures.

1. Establish, in connection with the work carried out under the Public Action 2022 programme, a global policy of recourse to Cloud by the State, by combining recourse to Cloud solutions under control of administration and that to Cloud providers benefiting from a qualification by the ANSSI (SecNumCloud).

[52] For example, replacing Microsoft Office software with the Office 365 Cloud service.

2. At the same time, encourage the development of encryption solutions for the cloud. Current encryption techniques only respond to very simple cloud use cases, mainly related to storage, but nevertheless present an undeniable interest, for example for outsourced backup devices. In addition, the development of encryption means that can be extended to other uses, in particular the so-called “homomorphic” encryption techniques, which allow encrypted data to be processed in the cloud, and no longer only at the storage, should remain a priority prospect.

3. Support European strategic autonomy on the subject, both by investing in disruptive technologies in the field likely to bring out the champions of tomorrow, as well as by ensuring tax measures to restore fairness between European players and certain of their competitors who largely escape tax or who are not subject to the same regulations.

4. Establish a global trust framework to enable companies, communities and individuals to assess the risks of use and guide the market by developing the SecNumCloud qualification, including at European level.

3.1.5 Regulating the production and export of arms and cyber offensive activities

The emergence of cybersecurity challenges and the desire of a growing number of countries to have cyber offensive capabilities have led many manufacturers to develop such means. At the same time, the intangible nature of these technologies makes controls difficult, where they exist. Limiting the proliferation of offensive technologies, in particular by maintaining the principle of applicability of arms control and dual-use technologies to the cyber domain therefore represents a key issue for the stability of cyberspace.

In 2013, the category of “intrusion software” was included in the list of dual-use goods of the Wassenaar Arrangement. Three new control entries have been included in this international agreement: systems (hardware), software (software) and technologies enabling the development and use of intrusion software. This development made it possible to lay the first milestones for regulating the global trade in offensive cyber tools. The modification of the Wassenaar list was integrated in 2014 into the list of dual-use goods of the European Union. The implementation of this control allows the national authorities to ascertain the conditions of end-use of the exported capacity and thus to refuse operations which could be considered as risky. Some countries participating in the Wassenaar Arrangement, such as the United States, have not yet transposed or implemented these new controls and plead for a relaxation of these rules.

It is now important to consolidate this development by working to deepen the export control regime in the cyber domain. Two options can be considered in order to continue the work undertaken so far. The first is the promotion of a universal standard of behaviour by which States commit to controlling the export of offensive cyber tools and techniques according to methods to be defined. The implementation of this standard should be adapted to the capacity of the competent national authorities to exercise effective and harmonised control and to respect the legitimate interests of cybersecurity companies and the world of research. The second option is to consider the advisability of adding certain software to the list of war materials, since they are not only designed to be punctually introduced into a system but to last or damage their target, constituting thus a veritable “digital weapon”.

To implement these regulatory mechanisms it is essential to try to categorize these tools. Tools are software or sets of software that can find multiple applications whether to test the security of a system for defensive purposes, to carry out intrusion activities for intelligence, obstruction or even purely for profit to steal money or data which can then be converted into cash. An intrusion tool to extract intelligence can also very easily be enriched with a few lines of code to become a very effective instrument of destruction. Under these conditions, it is difficult to distinguish, among these tools, those which can be qualified as digital weapons and, as such, be controlled as are, for their manufacture and their marketing, weapons of war.

It is however possible to classify cyber defence software into four categories allowing to fix rules relating to their production, their use and their export:

1. The first category includes "security intrusion tools". This software which makes it possible to discreetly penetrate a system and to exfiltrate or modify information is marketed in order to test the robustness of an information system. This type of tool is not intended to integrate codes exploiting zero-day vulnerabilities or loads capable of destroying a system. Designed for relatively limited operations, these tools do not include very advanced functionalities. This type of product nevertheless falls into the class of dual-use goods, insofar as, slightly modified, it can be transformed into destructive software. However, it remains a manual tool for punctual intrusion.

2. A second category is "data capture tools", which make it possible to massively collect individual data, for example from smartphones or personal computers and to process it almost automatically. These tools can include zero-day operating and steering functions. They can be installed over a long time but are not intended to penetrate complex information systems. These tools, deployed within a legal framework, are useful for the police and the justice system. Capturing data at the source makes it possible to overcome certain obstacles encountered by legal interceptions made by operators, especially in the case of encryption of the applications used to communicate. The dangerousness of such tools presupposes close control over their dissemination.

3. The third category corresponds to "targeted computer weapons". These tools, with advanced functionalities, make it possible to take control over a long time of varied but targeted systems, by allowing intelligence exploitation or destruction of the system at the desired time. Their purposes combine those of the first two categories, which in terms of use and effect cannot be obtained by simply superimposing the tools of the first two categories. Much more sophisticated, their creation requires ad hoc developments. They correspond to tools used by the most advanced groups of attackers.

4. The last category is made up of “massive computer weapons”, making it possible to take control or destroy a large number of devices. It can be malware that can replicate and propagate independently without precise targeting. These tools are particularly harmful because of the risks of uncontrolled collateral damage that they generate.

Most software and products, falling under these four categories are controlled as dual-use goods in our legislation[53] or regulated as tools that can invade privacy (Articles R226-1 to R226-12 of the Penal Code). The Article of the Penal Code prohibits moreover the possession or the provision of tools allowing to be introduced into an automated system of data processing except for reason of research or data-processing security.

Less by its rigorous nature than by its complexity, these regulations have not encouraged French companies to invest in the development of computer weapons, or even intrusion or data capture tools. However, countries like the United States, Israel or India have set up an industry in this field which is now setting out to conquer the world market. Certain products sold by foreign companies, although not qualified as "trusted", are of definite interest for the intelligence, police or justice services. This software makes it possible to ensure the capture of data with regular updates which adapt them to the evolutions of the terminals marketed. European countries are not left out. English, Italian or German companies have thus created effective capture tools, although not always sufficiently hardened[54]. This European situation should be all the more emphasised since most of the member countries of the European Union, including France, are engaged in the fight against terrorism and major trafficking and have, as such, authorised in their legislation the installation of electronic capture systems for the purpose of spying on criminal and jihadist networks. The European market today appears to be sufficient to make industrialists who manufacture this type of product viable and create competition between players, while preventing these products from being diverted for malicious purposes. Measures to protect these manufacturers from takeovers by foreign capital are also essential.

[53] Decree 2001-1192 of December 13, 2001 relating to export, import and transfer control of dual-use goods and technologies modified by Decree 2010-292 of March 18, 2010

[54] Thus, the two European leaders (the Italian HACKING TEAM and the German-English GAMMA) have recently suffered computer intrusions demonstrating the low level of security of their systems. The attackers stole all of their data and published it on the internet, revealing both the identity of their customers and their expertise.

While the need is not debatable, we face the double risk of using capture products that are insufficiently secure, or that are not considered to be trusted. So, when the tools developed by the Italian company HACKING TEAM were made public following a theft of their source code, it appeared that the company had hidden a trap in all the tools for capturing data from their customers. It therefore seems necessary today to harmonize the manufacture, import and export of these tools, unless we take the risk of delivering this particularly sensitive market to non-European suppliers.

France could promote, particularly within the European Union, a regulatory approach to the production and export of cyber defence software, based on the four categories of products introduced above:

- the treatment of first category tools as dual-use goods raises questions insofar as other States do not apply this control. Adopting it unilaterally would penalize our manufacturers vis-à-vis other actors. These tools could thus be freely manufactured in Europe, respecting a code of ethics, and used by the private sector in a logic restricted to security tests. Their export outside the European Union should be accompanied by rules of use and be able to be checked *a posteriori*;

- second category tools could be manufactured by manufacturers subject to transparency and control obligations, for uses exclusively under government responsibility. The import and export of these products outside the European Union could be prohibited, or at least strictly controlled;

- third category tools could be developed only under state responsibility and used only by the State

- the manufacture and use of fourth category weapons would be prohibited.

3.2 Cybersecurity regulation

Guarantor of society's cybersecurity, the State intervenes in this area as a prescriber, reformer and provider of security solutions. Along with the Parliament which enacts the law, the government plays a normative role in the field of cybersecurity.

Responsible for coordinating and coordinating public policies contributing to the national security strategy, the SGDSN, which reports to the Prime Minister, is thus a cybersecurity operator. It is he who proposes to the Prime Minister and implements government policy in the area of information systems security. To this end, it has the ANSSI, which is attached to it.

In collaboration with the competent administrations, the ANSSI examines and prepares government decisions relating to digital security and that of sensitive data. It also participates in the construction and maintenance of networks and secure terminals for government services. The agency thus supports the offices of the President of the Republic, the Prime Minister and members of the Government in securing their information systems. As part of its normative role, it is responsible for defining security standards, issuing security visas and qualifying service providers.

Reflections carried out within the framework of this strategic review, emerged the need to improve the current certification framework in order to contribute to the improvement of product security.

3.2.1 The normative role of the ANSSI

Defining security standards

Created to provide the State with an authoritative administration on cybersecurity issues, ANSSI was built around state-of-the-art scientific and technical expertise, further enriched by the experience acquired in processing wire of cyberattacks at the highest level of sophistication. Strengthened by its mission and skills, ANSSI has naturally established itself as a benchmark for defining the relevant security standards to ensure the protection of the most sensitive data and information systems, starting with the protection of secrecy of national defence.

For these same reasons, the ANSSI was responsible for negotiating security standards aimed at ensuring data protection and classified information systems in multinational frameworks (for example within the North Atlantic Organisation, within the European Union, etc.).

This standard-setting activity has gradually spread over time and at the same time as the affirmation of its role as a national authority, to cover in particular:

- the protection of digital exchanges between citizens and the administration on the one hand and between administrations on the other, by Ordinance through the General Security Reference System (RGS);
- the security of state information systems, by way of a Prime Minister's circular through the Information Systems Security Policy (PSSIE);
- the protection of sensitive state information (inter-ministerial instruction 901)
- the protection of the information systems of the OIVs participating in supporting their missions of vital importance, by legislative and regulatory means through Articles 1332-6-1 to 1332-6-7 of the defence regulations.

More recently, the ANSSI has been entrusted with the production of an Ordinance and Decrees in the Council of State relating to trust services within the framework of the law for a digital republic, with particular regard to electronic identity, registered electronic and digital safes.

Finally, the ANSSI participated, as a leader at the national level, in the negotiation of the following European regulations and in ensuring their interpretation or transposition at the national level:

- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, known as the 'eIDAS' regulation ";

- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures intended to ensure a high common level of security of networks and information systems in the Union, known as the "NIS" directive.

The now proven impact of regulations brought in or negotiated by the ANSSI confirms the choice of entrusting the national authority with the definition of legal standards specific to digital security. This is particularly true when it comes to developing confidence in digital uses. In this regard, the decision to designate the ANSSI as the authority for the certification of electronic identity means is certainly a step in the right direction.

In addition, while the digital transformation is in full swing, that the breaks in terms of technology and uses are linked in digital, and to the extent that digital security – essential condition of confidence in the digital transformation – remains today little regulated, there is no reason to consider that we are faced with a stack of standards in the field of digital security. In this context, it seems that government directives advocating that the implementation of any new standard is accompanied by the abolition of two already existing standards should, in this case, be subject to an exception for the field of digital security.

In addition to this exception, the ANSSI must, in the new standards it will be called upon to propose, as well as in the revision of existing standards, pay particular attention to guarantee the proportionality, consistency and legibility of the regulations on digital security, to simplify implementation by organisations subject to more than one.

Finally, it appears that compliance with the standards enacted by the ANSSI is sometimes insufficient for two reasons. On the one hand, following the example of the general security reference system, the implementation of existing sanctions regimes is sometimes only difficult to envisage because they are too little proportioned and do not allow escalation. On the other hand, following the example of the security policy for State information systems published by circular, the level of standards is sometimes insufficient in the hierarchy of standards. Particular attention should therefore be paid to improving the effectiveness of the standards defined by the ANSSI by guaranteeing relevant sanctions regimes and the most suitable levels of standards.

Security visas

The ANSSI has been issuing security visas for many years, on the basis of in-depth assessments launched on the initiative of the suppliers concerned, relating to an extended typology of security products: hardware or software, performing encryption functions, electronic signature, interconnection between secure networks, authentication, etc. These visas are essentially of distinct types:

- certification attests to the robustness of a security product with regard to the requirements (nature of the security functions, level of the attacker) set by a sponsor, who is not necessarily the State. It is thus presented as a toolbox allowing various contractors (State, private operators – banks for example -, independent authorities) to define their security criteria and to have the satisfaction of these criteria verified by a third party;

- the qualification by the State is worth recommendation of use in a given context; it involves product certification supplemented by verification of security and updating requirements claimed from suppliers over time. The qualification is valid both for the specific needs of the administrations and services of the State as for those of the OIV;

- approval is a regulatory decision which authorizes the use of a solution previously qualified for processing classified information.

The methods applied by private assessment centres certified by the ANSSI have largely demonstrated their relevance in terms of guarantee and responsiveness. The general framework for issuing security visas set up by the ANSSI also constitutes a very important lever for the development of the security of products manufactured or deployed in France.

However, the need for evaluation of increasingly varied products is increasing. They are no longer only products specifically designed to provide security for computer networks, but also industrial controllers, connected objects, etc. If the existing evaluation framework has been successfully extended to a significant proportion of these new needs, it is however totally unsuited to the foreseeable development of future certification and qualification requests.

Providers

In addition to product qualification, the ANSSI has more recently established a system for the qualification of service providers and IT security relating to their level of security (competence, the security of their own information system, data partitioning customer, as well as on quality of service commitments, defined in business standards.

This qualification concerns cybersecurity providers: Information systems security audit providers (PASSI), Security Incident Detection Providers (PDIS) and Security Incident Response Providers (PRIS).

It also applies to secure digital service providers, which provide guarantees in the execution of a digital service rather than specific cybersecurity expertise. This category includes trusted providers provided under the general security repository and the eIDAS regulation (providers of electronic signature, provision of electronic certificates, time stamping, etc.), and providers of cloud computing (cloud)[55]

Cybersecurity providers are qualified on the basis of an assessment of their business competence, on the one hand, and of the technical and organisational measures by which they ensure the protection of their customers' data, on the other. They provide expertise similar to that implemented by the ANSSI in its own missions, and therefore constitute an important vector for disseminating the know-how of the ANSSI. Their assistance also makes it possible to meet the needs of the private sector. The PASSI qualification process started in 2013 and, at the end of 2017, there were fifty service providers qualified or in the process of qualification. This rise in power reveals both the dynamism of this field of activity and the search by companies in the sector for accreditation by the ANSSI.

Fewer, secure digital service providers are assessed by the ANSSI according to a logic of compliance with a standard-setting, the security requirements applicable to the service they deliver.

3.2.2 Improve the certification framework to improve product security

The existing certification framework, although modulating the level of requirements according to security needs, remains nonetheless very focused on high-level certifications. It is ill-suited to the evaluation of products of current use (like connected objects), for which it presents a prohibitive cost and deadlines.

This is why this strategic review proposes the implementation, in addition to the existing certification framework, reserved for products and services at the top of the spectrum, of a basic cybersecurity certification. The latter could be inspired by existing systems in contexts other than cybersecurity, such as the CE marking required for the marketing of certain goods or services within the European area. This basic cybersecurity certification would essentially proceed from a compliance analysis, based on a predefined specification. This compliance check could be delegated to a private organisation, with the involvement of the public authorities limited to indirect actions (approval of private assessment centres). This approach appears suitable for certifications for which certain obligations of the current system, such as carrying out a “free” vulnerability analysis, outside specifications, and the issuance of certificates by the ANSSI, seem less justified.

[55] The general security reference system, taken in application of Decree 2010-112 of February 2, 2010 taken for the application of Articles 9, 10 and 12 of Ordinance 2005-1516 of December 8, 2005 relating to electronic exchanges between users and the administrative authorities, is the regulatory framework enabling confidence to be established in exchanges within the administration and with citizens. Its purpose is to strengthen users' confidence in the electronic services made available by the administrative authorities and thus imposes itself on them as a binding framework while being adaptable and adapted to the challenges and needs of all types of administrative authority.

The “elDAS” Regulation 910/2014 of July 23, 2014 aims to increase confidence in electronic transactions within the internal market. It establishes a common foundation for secure electronic interactions between citizens, businesses and public authorities.

By reducing the costs and times of certification, this reform is likely to favour the emergence of a product offer consistent with the need. The implementation of a basic certification mechanism could rely on certain conformity control providers with the help of the ANSSI. The national cybersecurity authority could contribute to the definition of basic certification protocols, accredit centres of expertise and evaluation, and animate the network, notably through training cycles.

After an initial implementation based on volunteering, the incorporation of this elementary certification into the regulations, by integrating for example elementary security rules in the European directives relating to the goods targeted by the CE marking would significantly increase its scope. and impact, transforming an optional differentiator into a prerequisite for market access.

Finally, it can be noted that the establishment of self-declaration mechanisms for compliance with security requirements is a recurrent demand from many digital solution providers, who put forward the minimum cost. A self-declarative framework provides only weak guarantees of security, and therefore does not constitute a priority for the State. However, it would be counterproductive to oppose the emergence of such schemes on the initiative of the private sector, in particular when this approach is supported by a representative group of providers of security solutions. A minimum support of such initiatives by the State, relating in particular to the definition of associated specifications, would encourage the dissemination of good development practices, including in sectors reluctant to turn to certification.

3.2.3 Responsibility by environment: involving all sectoral players to raise our level of cybersecurity

When the interests of the Nation justify it, in particular with regard to defence and national security or services essential to the maintenance of critical societal or economic activities, a cross-sectoral approach to cyber risk is essential. Responsibility is then entrusted to an inter-ministerial authority, the national security and defence authority for information systems. Such an approach guarantees a homogeneous and ambitious understanding of risk, independent in its objectives of sector specificities, making it possible to reduce cyber risk and prepare for the management of a possible major crisis. This approach is primarily intended to guarantee a minimum level of cybersecurity for the most critical entities, in order to protect the fundamental interests of France in the face of the cyber threat.

Although cross-sectoral, this type of approach requires, in its implementation, close coordination between the national authority and the key players in sectoral regulation, both ministerial supervision and any services with national competence, public establishments[56] and independent administrative authorities[57] in order to ensure a good articulation between the different policies applying to the sectors.

However, cross-sectoral approaches do not allow a detailed understanding of the risk management specific to each sector. In addition, the digital transformation, which leads in particular to the massive connection of objects to the Internet (medical devices, vehicles, buildings, cities, etc.), now requires the risk of cyberattacks to be taken into account at the sectoral level, particularly when these objects are likely to have a direct and material impact on personal security. Indeed, only the sectoral players have the business knowledge necessary to qualify the impacts of a possible computer attack on these objects and therefore to assess in a relevant way the cyber risk associated with their deployment.

These findings highlight the now imperative need for key players in sectoral regulation to understand the risk of cyberattacks in the same way as other risks and, if necessary, after a risk analysis carried out by business experts, to adopt appropriate measures, for example by issuing suitable cybersecurity requirements.

Sensitize the key players in sectoral regulation to the risk of cyberattacks

The key players in sectoral regulation generally do not have cybersecurity expertise. As such, the understanding and taking into account the risk of cyberattacks by these actors are extremely underdeveloped, even non-existent. At a time of digital transformation, they must now understand this risk, using the risk analysis methods available and calling on external assistance, provided by qualified service providers, or even by the ANSSI itself, in order to analyse relevant cyber risks at the sectoral level and identify those that deserve action in order to be reduced.

Provide tools to key players in sector regulation

[56] For example, the National Agency for Food, Environmental and Occupational Health Security (ANSES), the National Agency for the Security of Medicines and Health Products (ANSM), the Directorate for the Security of 'civil aviation (DSAC).

[57] For example, the Supervisory Authority and Resolutions (ACPR), the Financial Markets Authority (AMF), the National Frequency Agency (ANFR), the Regulatory Authority for Electronic Communications and Posts (ARCEP), the Nuclear Security Authority (ASN), the Energy Regulatory Commission (CRE).

When the assessment of the exposure to the risk of cyberattacks has been carried out in a sector and concluded that there is a need to reduce certain risks via regulatory requirements, whether at national or European level, the key players in the regulation of the sector must be able to design the necessary cybersecurity measures, simply express their cybersecurity requirements within the sectoral regulations for which they are responsible, and monitor compliance with the requirements.

However, these actors do not have, and generally will not have to have, cybersecurity expertise. Consequently, they should be able to rely on tools enabling them to define their security criteria and to have the satisfaction of these criteria verified by competent third parties. The European cybersecurity certification framework proposed in September 2017 by the European Commission, as part of the "cyber package" designed for this purpose and currently being negotiated, should make it possible to meet this need.

Prioritize the commitment of ANSSI resources in its work with the key players in sectoral regulation

By drawing on its expertise in awareness-raising, and thanks to the tools and methods it has developed in the area of cyberattack risk management, the ANSSI is able to effectively support the key players in sectoral regulation in order to allow them to understand cyber risk in general, to analyse the corresponding risks at the sector level which concerns them and to identify those calling for corrective action (risk reduction and strengthening of the level of cybersecurity).

Nevertheless, as a national authority, the priority of the ANSSI must remain the protection of the fundamental interests of France through a cross-sectoral approach to risk. It is therefore important that the ANSSI prioritize its actions to support the key players in sectoral regulation.

Three criteria naturally contribute to determining the level of priority that the ANSSI must give to the support of actors in a sector at a given time: the next arrival or in progress of a phenomenon of rupture linked to the digital transformation of the sector (for example, autonomous vehicles), the level of cyber threat to the sector, and the level of risk to personal security.

3.2.4 Trusted providers: developing a range of cyber defence services

Cybersecurity providers currently cover, through the specific expertise they provide, three of the four stages of the life cycle of a secure information system: security verification (PASSI), long-term security management (PDIS) and reaction to attack (PRIS). However, no qualification scheme covers the skills necessary for the initial stage of designing a secure information system. It should also be noted that existing providers do not strictly cover all of the skills contributing to other stages: for example, there is no provider specializing in security certification (see glossary), or in maintaining security condition[58].

[58] It should however be stressed that these uncovered competences fall more particularly under the obligations of the entity responsible for the information system, and are therefore difficult to outsource.

Project management assistance providers

It therefore seems desirable to complete the catalogue of qualified cybersecurity providers with a new type of provider specialised in the initial phase of designing a secure information system. Indeed, certain specific expertise mobilised at this stage of the life cycle, in particular that relating to risk analysis and security architecture, is not widespread within administrations and companies, and in fact already largely under-processed by these entities to project management assistance providers. The implementation of a qualification scheme focused on these trades would provide significant guarantees in terms of competence and confidence in this use of outsourcing.

Basic level qualification

The various qualification standards for cybersecurity providers are currently designed to meet the high level of requirements specific to sensitive government systems and vital information systems for OIVs. This positioning is found in particular in the constraints imposed in terms of security of the information systems underlying these services, which must be capable of processing Restricted Diffusion information. This level of requirement has natural repercussions on the price of associated services, which is therefore not fully adapted to the needs of other entities, or less critical information systems, for which the nature of the threat does not justify not necessarily such a level of service.

There would therefore be an interest in exploring the possibilities of less demanding qualifications, for less ambitious levels of services corresponding better to the needs of non-critical information systems of companies, administrations and communities. The associated reference systems would naturally aim to cover the same skills as the existing qualifications, but by relaxing certain constraints, in particular the architecture and security of the information systems associated with the services.

Like the elementary certification system proposed above for products, the role that the State would be called upon to play in such an elementary qualification of service providers would still have to be clarified. Involving the public authorities, drawing on both their experience and their knowledge of the threat, in the definition of qualification benchmarks seems a priori relevant. On the other hand, the interest of an extended involvement in the functioning of the qualification scheme, once it has been established, is more debatable: these qualifications could potentially be delegated to specialised private actors, the State confining itself to verifying the ability of the latter to conduct qualifications.

3.2.5 Developing the qualification of secure digital service providers

The providers of secure digital services qualified to date are mainly concentrated in very specific business sectors, notably related to electronic signature. An extension of the assurances provided by these qualifications to more general digital activities seems relevant, in particular because of the significant contribution that it could have on the security of entities which very largely outsource their use of digital technology.

Cloud providers

The development of cloud computing is a very structuring evolution of information systems. In addition to its economic or functional advantages, the cloud is a very attractive solution for entities with only limited IT skills, who can find in cloud providers an information system base much better controlled than they would be likely to put themselves in place. On the other hand, this development of the cloud, resulting in massive outsourcing of information systems, and their concentration under the control of the main cloud providers, creates a reinforced need for confidence in these providers. This observation motivated the development by the ANSSI of the qualification scheme for cloud service providers called SecNumCloud.

The final version of the associated repository having been made public in September 2017, the first qualifications should be announced during 2018. This repository sets a set of technical, legal and contractual requirements which decline, in the context of the cloud, good security practices digital. However, the SecNumCloud qualification is not backed by any regulatory requirement, and its attractiveness could be improved in order to bring more cloud players to make the efforts necessary to bring them into compliance with the standard. In addition to the leverage of public procurement – relatively limited to date in the cloud – a significant factor of attractiveness could be found in bringing the requirements of the standard closer to the constraints resulting from the new European data protection regulation personal data (GDPR), coming into force in mid-2018, which will have a very structuring effect on this sector of activity.

Managed services providers

Outsourcing is an alternative and complementary model to cloud computing instead of outsourcing its information system to a cloud, the client outsources the sole management (administration, updates, supervision) of its information system, which also remains physically under its control. The quality of the managed services can constitute a powerful lever to improve the level of security of the customers of this service, who generally do not otherwise have the capacity to secure themselves. This is why the establishment of a qualification scheme for service providers in secure outsourcing appears necessary.

3.2.6 The establishment of a certification framework harmonised at European level

An important factor in the lack of attractiveness of security certification for certain use cases is the lack of international recognition of the certificates issued, in view of the investments made to obtain these certificates. Indeed, the certifications established in France under the so-called "Common Criteria" standard only benefit from partial recognition under international agreements, notably the SOG-IS agreement allowing mutual recognition between 14 European states, while those falling under First Level Security Certification (CSPN), which are less expensive, are only recognised in France.

An important factor in the lack of attractiveness of security certification for certain use cases is the lack of international recognition of the certificates issued, in view of the investments made to obtain these certificates. Indeed, the certifications established in France under the so-called "Common Criteria" standard only benefit from partial recognition under international agreements, in particular the SOG-IS agreement allowing mutual recognition between 14 European states, while those falling under First Level Security Certification (CSPN), which are less expensive, are only recognized in France.

The European Commission presented, on 13 September 2017, a package of cybersecurity measures, which notably proposes the establishment of a European regulatory framework for the certification of the security of digital products and services. This initiative offers a unique opportunity to harmonize security certification at European level, and therefore to ensure recognition extended to all Member States, a pledge of greater attractiveness. The work of the Commission in this area must, therefore, be encouraged and supported.

However, care should be taken to ensure that this new framework and its implementation perpetuate the experience acquired by the pioneering Member States in the area of certification, including France, and integrate the good practices established in this regard. In particular, in addition to elementary conformity certifications according to the guidelines presented in the previous Paragraph, the European framework must incorporate a certification component capable of meeting the highest levels of security requirements, essential to meet the needs of States and the most exposed industrial activities, and to this end integrate the essential principles which guarantee the effectiveness of the current system and its adaptation if necessary.

Furthermore, it will also be necessary to ensure that European harmonisation does not result in the national capacity to issue security qualifications, incorporating additional criteria, to meet the needs related to national security.

Like the qualification of security products, that of service providers covered by a national system without international recognition, with the sole exception of trusted providers qualified under the eIDAS regulation. However, an extension, total or partial, of the French model of qualification of service providers would have a double usefulness, by reinforcing the attractiveness of the system for service providers established on the whole of the European market, on the one hand, and by helping to significantly improve the security of the digital single market, on the other hand.

Such an extension seems particularly relevant in the field of secure digital service providers, insofar as the suppliers concerned generally have a market and an offer extended to the whole of the European market, even on a global scale for the main cloud providers. Furthermore, the security of these digital services constitutes an important part of the European Network Information Security Directive, and a apparel for validating this security would, therefore, find its place in the implementation of this directive from mid-2018. Finally, the requirements carried by these qualifications, and the associated verification procedures, seem fairly easily integrated into the harmonised framework for the certification of products and services recently proposed by the European Commission. In this particular case, the national qualification would easily become certification at European level.

At first glance, the relevance and the feasibility of a European extension of the qualifications of cyber defence providers seems more questionable: the corresponding professions more generally constitute local services, the market of which often remains local. Furthermore, the specificity of these qualifications, which necessarily imply an assessment of the providers' professional skills, and not only of technical or organisational requirements on their information system, makes their harmonisation at a multinational level much more complex. In particular, such assessments seem difficult to integrate into their current state within the framework of certification proposed by the European Commission, which would require significant adaptations to allow competence tests.

However, a European extension of these qualifications would be of indisputable interest, in particular because of the wide use of European institutions for such providers, through markets in which a significant portion of qualified providers in France are generally candidates. The recognition, at a minimum, of the qualifications of cybersecurity providers by the European institutions would thus present a double advantage of valuing the investments made by the qualified providers, on the one hand, and of improving the security of the European institutions, on the other go.

3.3 The cybersecurity economy

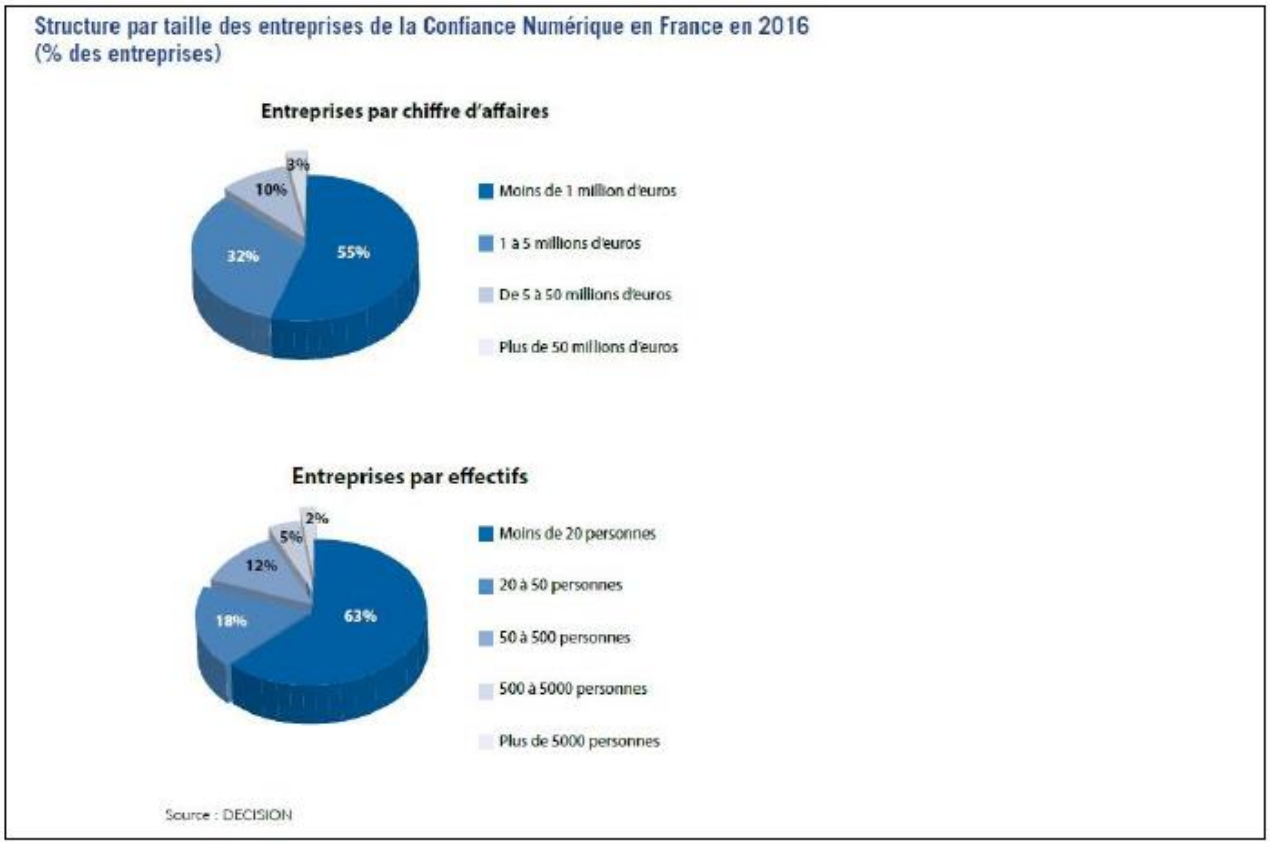
To establish its digital sovereignty, France should have a real industrial strategy. Such an approach would involve identifying the objectives to be achieved in terms of national industrial offer or confidence to meet the needs of the Nation in the field of cybersecurity and by defining the means to be implemented to achieve these objectives.

In this regard, the reflections conducted within the framework of this strategic review lead to consider strengthening in several directions the French industrial base and the foundation of a European cybersecurity industrial base. They also show the need for the State to have efficient and certified security products.

3.3.1 The national industrial base

Today, the development of an ambitious trusted industry in the field of cyber defence products and services is essential to relay and extend the action of the State, whether at national or European level. It is a question of developing an industrial capacity which is able to offer products and services at the same time of a very high level of security while being economically viable.

The French cybersecurity industry can be characterised by the presence of a few large groups with a large international footprint and many small or very small companies. There is, in fact, almost no medium-sized company, which is more in the field of cyber defence products.



The activity covered by large groups is built around three axes.

The first is linked to the government's high level of security needs for which the French State has decided to maintain a sovereign capacity, in particular in the field of cryptography and encryption. These high-security needs made it possible to bring out a civil offer. France thus has equipment which guarantees it control over the security of its networks, including in the face of attackers of very high technical level. However, the national civil service is struggling to impose itself abroad and would benefit from being renewed.

The second axis is linked to the field of smart cards, with historical players such as GEMPLUS, SCHLUMBERGER or OBERTHUR. These players now rely on the skills and knowledge acquired to develop world-class authentication and access management solutions.

Finally, French IT service companies have positioned themselves globally to oversee the security of their customers' networks and operate today worldwide. These manufacturers also integrate cybersecurity solutions into the information systems they design wherever they administer.

These fields are intended to come together as illustrated by the rapprochement between BULL and ATOS or more recently that of GEMALTO and THALES.

In addition to the activity covered by large groups, some experts are embarking on the creation of start-ups. The available funding and the lack of expertise in the field of cybersecurity allow them to develop, even in the absence of a successful industrial strategy and without being forced to conquer international markets. In fact, the high-level expertise services they can provide to French customers are most of the time sufficient to support these small businesses whose structure costs can be quite reduced. However, despite these proven technical skills, it remains a challenge for these SMEs to become international champions.

Faced with these findings, this strategic review has identified three areas for improvement:

- encourage major French industrialists in the sector to complete their range of cybersecurity products and services for the civilian sector, in order to enable them to become international cybersecurity champions;

- encourage the creation of medium-sized enterprises (ETI) by helping the most successful SMEs to grow quickly and make relevant acquisitions. Today, it is the only option available to enable them to reach a size that puts them in a position to compete with their foreign counterparts or to conquer the European market. The State will support and encourage these external growth strategies by mobilizing investment funds interested in the field of cyber defence;

- increase the number of start-ups by encouraging and supporting experts from the administration or large companies to embark on this challenge. In order to achieve this objective, it is essential for the State to support the establishment of accelerators, studio start-ups and more generally support structures for start-ups dedicated to cyber defence. Efforts should be concentrated on innovative companies whose strategy can enable them to achieve a global footprint.

3.3.2 Define an industrial cybersecurity policy and build a European cybersecurity industrial base

The construction of an industrial cybersecurity and cyber defence base faces two difficulties today.

The first is the absence of a real European cybersecurity market, which does not allow, contrary to what can be observed for American or Chinese companies, the growth of companies on the basis of the single internal market. This is due both to a heterogeneity of practices and standards between countries, to certain constraints existing at European level which can paradoxically complicate overall market access, but also to the fact that the European market remains easily today accessible to non-European companies.

The second difficulty is a certain difference in conception between Member States of the European Union on the nature of a "European enterprise". For some, it is simply a company with solid bases in Europe or a head office in Europe. For others, on the contrary, are companies which belong, in a stable and long-term manner, to European investors.

In addition, the question of trusted European companies very clearly poses the question of the sphere of sovereignty and the link between sovereignty and economic development.

These issues should not, however, curb France's desire to encourage the construction of European cybersecurity players. Several axes of effort could allow the constitution of such an industry.

The first effort is to identify the areas in which France believes that a European industry must be set up to maintain or even regain strategic autonomy. This effort must in particular be concretised by the establishment of European financial supports no longer solely to support research but according to a much broader approach integrating in a coherent manner all the dimensions of capacity programmes, support for innovation, support for export, etc.

The second axis is to promote the emergence of a real European market supporting the development of efficient European solutions. If this line of effort should not oppose an open market logic, it nevertheless constitutes a necessity to guarantee the strategic autonomy of Europe and its member states in the digital field.

The implementation of a European certification scheme would also allow security offers to progress at European level while leading manufacturers to demonstrate greater transparency on their solutions.

Finally, for certain areas, the establishment of European systems for the protection of companies deemed to be sensitive to foreign investors, or even the possibility of reserving certain sensitive public procurement contracts for European companies, are essential conditions for the success of this approach. These markets could be opened to foreign players, provided that both transparency and independence commitments are imposed.

3.3.3 Having efficient and certified products

Qualification is a proven mechanism well suited to validating state security requirements for conventional security products. France, however, suffers from an insufficient catalogue of qualified products, both in terms of diversity of suppliers and coverage of certain needs of administrations or OIV, especially in emerging areas such as that of detection probes. Furthermore, the current qualification mechanism, focused on security assessment, does not take into account functional expectations in the broad sense (richness of functionality, performance, ergonomics) of the client, and therefore suffers from a negative image (qualified products are often perceived as functionally inferior). The pioneering work on modernisation, already underway for the qualification of detection probes, could serve as a model, based on feedback, for the qualification of functional requirements.

Qualification of attack detection probes

The military programming law relating to the 2014-2019 period, introduced, for OIVs, an obligation to deploy probes qualified to detect attacks. As such, the ANSSI has initiated work to define the requirements underlying the qualification of such products. Breaking with previous approaches, these requirements relate not only to the intrinsic security of the product, but also to its functional efficiency and performance. Both types of requirements, security as well as functional, must be analysed by private assessment centres which have so far carried out only security assessments. The first probe qualifications should be pronounced during 2018. This site has a high degree of priority, both in terms of meeting the regulatory needs of OIVs and as a precursor to what could be a qualification integrating functional requirements.

Functional testing of qualified products

Beyond this pioneering work, it seems desirable to generalize, as much as possible, the integration of functional tests in the product qualification process. This generalisation could also be inspired, in addition to work aimed at qualifying detection probes, the approach implemented by NATO, which, for the acquisition of security products, has for many years combined security evaluation (SECEVAL) and operational evaluation (OPEVAL). It might also be relevant to explore different avenues for carrying out functional tests, the model chosen for the probes (functional and security assessment conducted by the same actor) not necessarily being applicable to all use cases. Functional validation could thus be carried out by other types of private actors, by technological research institutes (IRT), or even by user clubs. San result could also differ depending on the use case: certificate of compliance when a precise specification can be defined, or classification in relation to the state of the art of the market in other cases.

Diversification of suppliers of qualified products

The suppliers of currently qualified products are in their vast majority French, which contributes to a reducing image of the apparatus, harms the diversity of the catalogues, and does not allow the satisfaction of certain needs. However, this preponderance of national suppliers does not result from a choice, but rather from a combination of factors: low attractiveness of the system for foreign suppliers, low readability of its criteria, or difficulty for a foreign player to fulfil some of the commitments associated with the qualification (access of the evaluator to the source code for example).

Improved accessibility of the system to new suppliers, especially foreign ones, naturally subject to compliance with security and confidence requirements, would be likely to increase the rate of coverage of needs. In particular, greater use of this system by European suppliers appears desirable as part of the consolidation of European strategic autonomy.

The publication in 2017 of a detailed qualification process, and of all the objective criteria and associated commitments, contributed significantly to the improvement of the readability of aa apparatus long considered opaque. In addition, the extension through the LPM 2014-2019 of the field of application of qualification to OIV, and no longer only to administrations, has significantly increased the attractiveness of the system. The ability of a foreign supplier to fulfil certain commitments remains problematic, however, for various reasons (limits on the export from the country of origin of sensitive design information, the supplier's general policy on the protection of intellectual property, etc.). Insofar as these commitments are directly linked to security and confidence considerations inherent in the intended use, it would not be appropriate to reduce the level of requirement in this area. However, alternative approaches (access by the evaluator to the source code under the control of the supplier, rather than supplying the source code) or complementary approaches (reciprocal commitment of the State vis-à-vis the supplier) could be explored in order to facilitate keeping commitments, and promoting diversification of suppliers of qualified products.

Increased support from public procurement on qualification

The use of qualified products generally results from a simple recommendation of use, rather than from an obligation. The obligation for OIVs to use qualified detection probes is a notable exception in this respect. Conversely, the rate of use of qualified products by administrations remains very low, public procurement representing, according to a study conducted by the ANSSI in 2015, barely 10% of purchases of qualified products.

Greater exemplarity of administrations in the use of qualified products would have many beneficial effects: improvement of the security level of administrations by the use of verified solutions, strengthening of the attractiveness of qualification, economic development of suppliers of qualified products, ultimately promoting their functional improvement, etc. If the introduction of a general obligation to use such products appears premature, in particular with regard to the insufficient coverage of certain needs, more targeted actions could be taken, either to facilitate the acquisition of these products by administrations (inter-ministerial framework markets, release licenses) or to make their use compulsory in certain contexts.

The international scope of the qualification

Qualification is a purely national device, even if comparable approaches are found in several countries, at least for state needs. Insofar as it is a tool intimately linked to the preservation of national security, it does not seem opportune at this stage to seek to give it regulatory support at European level. On the other hand, the bilateral or multilateral promotion of this model and its virtues with the other Member States of the European Union seems justified in terms of sharing good practices contributing to the defence of sovereign information systems and, therefore, to the preservation of European strategic autonomy. Wider dissemination of the model would also help develop its acceptability and encourage solution providers to engage in such an approach.

3.3.4 The cybersecurity rating and compliance issues

Large-scale computer attacks can have very significant consequences on the financial health of companies. The *Autorité des Marchés Financiers* has also highlighted cyber risk in its "2017 Risk Mapping".

To take just one example, the Notpetya malware created a lot of damage to Saint-Gobain's information system and loss of production that the company estimated at 250 million euros in sales and 80 million euros on its operating profit for 2017. The consequences of this attack may, therefore, impact the shareholders of the company, who might want to know the risk incurred in the event of a new attack of the same type.

To answer this legitimate question, many companies offer cyber rating services. The largest, now American, are called BITSIGHT, SECURITY SCORECARD or even QUADMETRICS (bought by the financial risk rating company FICO) and offer to rate the cybersecurity of companies, their subcontractors but also that of 'a country or industry sector. These ratings, which are carried out today from outside of information systems, thus making it possible to rate many players without their knowledge. This first assessment of cyber risk is obviously not satisfactory, but it constitutes a first step which will encourage the financial markets, insurers but also customers to institutionalize these ratings. The major players in the field will, therefore, become factual references which will be difficult to dislodge. Companies, and perhaps even states, will then have to finance their own rating with these companies. The rating will be established with an external evaluation at first, but quickly the rated actors will be called upon to provide information on their information system, to have internal audits carried out and perhaps even to report their incidents to these new rating agencies.

In this context, it is essential that the European Union develops an offer in this area, so that French and European companies are not de facto subject to uncontrolled rules. An incentive approach could thus be put in place to encourage the emergence of European players in cyber rating. France is not helpless in this respect and has a recognised cybersecurity service offer likely to bring out competitive companies in this new field. The labelling of this French offer by the State or by groups of private companies could promote the structuring of this area and allow an improvement in the quality of ratings.

This approach could be supported by a modification of financial accounting standards to take into account cyber risk for larger companies. As the Bank for International Settlements' 87th annual report points out: “Technologies based on large volumes of personal data (...) present new challenges in the protection of privacy and data security. Growing concerns about cybersecurity highlight the potential risks of technology-based financial services. In order to maintain the integrity of the IT systems, it may be necessary to apply criteria of vigilance with regard to potentially multiple internal and external service providers”[59].

This approach could also be encouraged by funding cyber rating by European players, in addition to projects already funded, for example in the context of RO projects or public contracts that concern sensitive areas.

3.3.5 The establishment of a virtuous circle for securing systems through a relevant insurance mechanism

The insurance market has always been structured independently. Yet cyber insurance is struggling to establish itself today and the European market is far from mature. Various structural factors explain the difficulty of modelling an offer and meeting the market. Within a company, cyber risk must be seen as a risk among the others and considered from an economic angle, conducive to its insurability. On the other hand, for insurers, the absence of baseline data on cyber risk, as well as its potentially systemic nature, constitute difficulties today that have not been overcome.

The lack of a common vocabulary (recognised technical standards on security incidents reporting and classification) prejudices a true international comparison of national systems and data collected in each country under threat. In general, methodological problems prevent the determination of probabilities of the occurrence of digital risk incidents, thus reducing the capacity of politicians to effectively allocate public funds, insurers to assess their coverage or risk managers to reduce or transfer the identified risks.

[59] 87th annual report of the Bank for International Settlements, p. 104 (https://www.bis.org/publ/arpdf/ar2017_fr.pdf).

Collecting quantitative information on cyber risk is a second major difficulty. The information relating to the incidents is little or not shared[60] at no place of centralisation of such information and no reflection has yet been carried out as for its structuring. Furthermore, this absence of statistics prevents modelling the offer (although in France, the government platform cybermalveillance.gouv.fr is starting to do so and that internationally other initiatives have been launched). The establishment of a European database listing the majority of cyber incidents would, therefore, be a step forward. Data could be aggregated to analyse threat trends, identify security needs for products and services on the market, and provide cost information. The current establishment of mandatory mechanisms for the notification of incidents within the European Union (notably through the GDPR, the NIS directive and the telecoms package) could usefully contribute to the establishment of an inventory of digital risk.

A final difficulty relates to the question of the valuation of intangible goods which constitute 85% of the value of companies today. An information asset, as understood in a digital economy, is an intangible which is neither qualified in legal terms nor quantified in accounting terms. It is therefore not an insurable asset. The insurability of the intangible asset represents an essential stake for the valuation of the company in a digital economy.

Another key issue is the implementation of a cyber risk management policy, integrated into business risk management. Listed companies have had an obligation since 2011 to adopt risk management practices, based on mapping tools, a governance committee and audits. These good practices must be developed in all companies, while taking into account their level of maturity and their size, because they make it possible to raise awareness among the governing bodies and constitute a prerequisite for the reasoned subscription of a cyber insurance offer.

3.4 Human challenges

The level of cybersecurity in our society is directly linked to the behaviour of all French people – individuals, businesses and administrations – and therefore to their degree of understanding and mastery of cybersecurity issues. State services, businesses and individuals are indeed increasingly connected by technologies offering new ways of working, interacting and transacting. Under the pressure of mobility, massive use of data and the Internet of Things, digital is spreading faster and deeper. If the spread of the digital security culture does not follow, then the conditions for peaceful and confident use of the Internet as connected objects cannot be met. It is an educational approach, positive and rooted in the reality of the different audiences of the digital security culture that this strategic review proposes, in order to reinforce its impact and to awaken the interest of each to the maximum digital. Businesses, administrations and citizens must be given keys so that they become actors of digital security, in their personal and professional lives.

[60] According to OECD estimates, between 60 and 89% of incidents go unreported.

This is why cybersecurity must be integrated, from elementary school to high school, into the students' training path. Playful approaches must, in parallel, be offered throughout life, adapted to the different degrees of familiarity that French people have with information and communication systems and their use of everyday connected objects. A greater dissemination of the digital security culture in businesses and in public administrations also appears desirable, while responses must be provided to the recruitment needs of cybersecurity specialists among them. Our country cannot be content to train cybersecurity and cyber defence specialists, it must also give itself the means to keep them and attract foreign talent.

3.4.1 Educate cybersecurity issues from an early age

Cybersecurity education from an early age should be a priority. Children and adolescents have a daily practice, and early compared to the generations that preceded them, of connected objects, the Internet and social networks. According to an IPSOS “Junior Connect” study dating from 2015, the average age of the first mobile phone is 9 years and that of the first smartphone is 12 years. Young people from 13 to 19 years old connect on average at 13h30 per week and 78% of them are registered on social networks[61]. However, many of these young people do not control the dangers linked to the communication of personal information, to the connection with strangers or to the publication of private photos[62].

It is up to the school of the Republic to educate students in cybersecurity. This must go through a first digital awareness in the kindergarten years and digital education including mastering the cybersecurity requirements in elementary school, middle school and in all high school courses. Digital education from an early age is structuring for future behaviour. The early opening to the great concepts of computer science techniques will give students the keys to understanding the world around them and will later allow them to become players in this world and not just digital consumers. It is about teaching students to use digital in all areas of life, to enable them to acquire a digital culture, from initiation to code to understanding the logic of computers sciences, passing by the acquisition of data processing skills and the ability to adopt behaviours that respect security rules.

[61] In view of the trends observed in recent years, it can be estimated that these figures are, if not increasing, at least stable since 2015.

[62] According to the same IPSOS "Junior Connect" study, 57% of 11-12 year olds have a FACEBOOK profile despite the prohibition to connect before the age of 13, 43% have already added strangers to their list of friends and 12% sent photos or videos to strangers.

In elementary school, it is important to show the links which unite the concepts of data processing and those which are taught in the other disciplines, then those which unite them with the familiar objects of the daily newspaper[63].

In college, the teaching of mathematics and technology, which integrates the learning of algorithms and computer programming, must constitute the main vector for transmitting the rules of cybersecurity.

Obviously, learning the rules of cybersecurity must not stop at the doors of high schools, at the risk of seeing future young adults quickly overwhelmed by issues that are sure to renew themselves extremely quickly. This is why it seems essential that training to raise awareness of the challenges of cybersecurity must be integrated into the paths of general, technological and professional high school students, from the second to the final year class.

The initial and in-service training courses for teachers, particularly in mathematics and technology, will have to integrate this new requirement of transmitting the rules of cybersecurity to students. MOOCs[64] dedicated to teachers in initial training and in-service training could be designed by the Ministry of National Education with the support of the ANSSI. New educational resources dedicated to raising students' awareness of IT security rules will have to be regularly made available to teachers[65].

The effectiveness of raising awareness among young people about the challenges of cybersecurity can be enhanced by fun actions. Certain programmes have already demonstrated their effectiveness in the field of the dissemination of digital culture. The Internet Permit offered to children, a national prevention programme developed by the National Gendarmerie, the National Police, the Police Headquarters and the association AXA *Prévention*, thus makes it possible to raise awareness among CM2 children and their parents about vigilant Internet use, safe and responsible[66]. The Internet School system, developed by the association Ville Internet and which promotes the use of the Internet for French-speaking nursery and elementary school students by labelling participating schools, promoting their actions and encouraging exchanges of experience, also constitutes an interesting initiative. By taking inspiration from this system, we could, for example, imagine approaches to enhance, even label, the educational establishments most committed to cybersecurity.

[63] Learning the rules for using the Internet must in particular be a priority. Students must know the principles of civic and legal responsibility of the Internet user, the rules of downloading, learn to be informed on the Internet but also to master social networks and protect their privacy on the web.

[64] MOOC (Massive Open On Line Course): online training open to all.

[65] The portal of the Ministry of National Education Eduscol already offers first educational resources to raise computer awareness among primary and secondary students. The department of digital education for this ministry also manages a national resource pooling bank called Edu'base.

[66] https://www.permisinternet.fr/.

This strategic review recommends the rapid establishment of a working group, under the guidance of the Ministry of National Education, responsible for defining the actions to be carried out, and if necessary, the modifications to be made to the programmes so that all students leave the education system with a high level of mastery of cybersecurity issues.

3.4.2 Raising awareness among the general public through educational actions

If awareness of the school public about cybersecurity issues is essential, awareness of the general public must at the same time be conducted.

The already existing initiatives in the dissemination of digital culture constitute the first bases on which to build. We are thinking in particular of the civic service programme "the D-CoDeRs", launched in 2016, which involves volunteers committed to digital inclusion, by targeting three populations as a priority the poorly connected populations (who are offered workshops in places of local digital mediation), school and extracurricular audiences and seniors (through actions implemented in retirement homes or senior citizens' clubs). We also think of the EDUCNUM collective, initiated by the CNIL in May 2013 and made up of sixty structures[67], to carry and support actions aimed at promoting a true “citizen digital culture”, in particular through initiation and promotion of actions awareness and training for all audiences, especially the youngest, on responsible and informed use of digital technologies. The cybermalveillance.gouv.fr platform plays a role in raising awareness, prevention and support in terms of digital security for the French population.

But it seems essential to go further by amplifying the actions in progress, by communicating more effectively and more strategically, and by developing awareness actions specifically dedicated to the challenges of cybersecurity.

This strategic review, therefore, recommends that a fun application, available on smartphones, be created allowing French people to test their level of knowledge in the field of digital security and offering them, whatever their initial level of proficiency, many challenges. The realisation of this application could be supported by the ANSSI (which already offers, with the MOOC SecNumacadémie, an online programme to raise awareness of digital security which is aimed at all[68]). To design this educational application on digital security, the agency could notably draw inspiration from the online platform for the assessment and certification of digital skills PIX, currently developed by the Ministries of National Education and Higher Education[69].

[67] Companies, organisations, associations from the world of education, research, the digital economy, civil society, corporate foundations and other institutions.

[68] https://www.ssi.gouv.fr/particulier/formations/secnumacademie/.

[69] https://pix.beta.gouv.fr.

The PIX platform is an online digital skills repository for lifelong digital certification. Its objective is to support the rise in the general level of digital knowledge and skills.

An original and innovative avenue of research would also be to study the contribution of nudges to the development of citizens' autonomy in cybersecurity. These incentive-based approaches, based on the behavioural sciences, received resounding recognition with the award of the 2017 Nobel Prize in economics to Richard THALER, one of the fathers of the nudge economy. Nudges are used to support public policies in the United States and the United Kingdom. In France, a nudge project manager has been recruited at SGMAP and could be asked by the ANSSI to think about setting up nudges to encourage more responsible behaviour by users in the face of cyber threats.

3.4.3 Spreading the culture of digital security within businesses and public administrations

The dissemination of the digital security culture must also be reinforced within businesses and public administrations.

The ANSSI publishes guides for this purpose such as the "Guide to good IT practices", which presents twelve recommendations from the analysis of successful attacks aimed at very small businesses and SMEs[70], or the guide on “Cybersecurity of industrial systems”, which offers, by illustrating it through real situations, to the actors concerned a simple and suitable methodology for securing their industrial systems. The agency also publishes a set of requirements applicable to cloud computing service providers (SecNumCloud), developed in consultation with market players. At the same time, there are many initiatives to promote cybersecurity within companies, from the organisation in October 2017 by ENISA (European agency responsible for network and information security)[71] of the "European Cybersecurity Month" actions led by CIGREF[72] and the European Circle of Security and Information Systems, via the International Cybersecurity Forum (FIC)[73] or the European cyberWeek[74]. These initiatives, which are really effective, must be further amplified, their strengthened coordination and their dissemination widened to the greatest number of economic actors. Finally, the ministry responsible for the industry will contribute to this effort, in particular by integrating a cybersecurity dimension into its programme to support the digital transformation of businesses.

[70] http://www.ssi.gouv.fr/publication/lanssi-et-la-cgpme-publient-le-guide-des-bonnes-pratiques-de-informatique/.

[71] https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2017.

[72] Association whose mission is to develop the capacity of large companies to integrate and master digital technology.

[73] https://www.forum.fic.com. The FIC is one of the benchmark events in terms of cybersecurity and digital trust, bringing together all the players in France and in Europe.

[74] https://european-cyber-week.eu/fr/accueil/.

Within public, central, territorial and decentralised administrations, the culture of digital security must be disseminated to all agents, whatever their level of responsibility or their sector of specialisation. Mastering the culture of digital security must be given priority in initial training and continuing education programmes. The development of initial and continuous training modules in national and territorial public service schools and the development of cyber training at the Institute for Advanced National Defence Studies (IHEDN) and at the National Institute for Advanced Studies of Security and Justice (INHES]) thus appear essential. Management must take up digital security issues, which cannot be the sole responsibility of the personnel and departments responsible for IT security. The integration of this in the definition of the missions of the executives of the public service should be considered.

3.4.4 Develop the professional training offer on cybersecurity challenges

France's level of ambition in the areas of cyber defence and cybersecurity is today constrained by the capabilities of its human resources, particularly with regard to engineers specialised in IT and telecommunications (computer networks, security, IT, crypto-analysis, etc.). Building a solid national digital culture requires training the experts of tomorrow.

Associative and union approaches exist to promote the digital professions and bring down the self-censorship reflexes of certain audiences with regard to these professions. *Syntec Numérique* (professional union of digital service companies, software publishers and technology consulting companies) has thus embarked on numerous actions to enhance the attractiveness of training in digital, such as the JEM'NUM program ("digital businesses and professions journey") or the Pascaline Association to encourage young people to go to engineering schools (see box below). Associations such as *Femmes du Numérique* or *Informatique au Féminine* raise awareness among young people in order to combat prejudice against women working in IT.

Syntec Numérique's initiatives to promote the attractiveness of digital training

The Days of digital businesses and trades (JEM'NUM) organised by Syntec Numérique are days of exchanges between students, universities and digital companies. These forums are an opportunity for students to learn about the training offered by universities in the digital field and to meet companies in the digital sector. They also allow universities to present digital training programmes to their companies, their responses to the skills needs of the sector and to build partnerships. Finally, they are a showcase for companies in the digital sector to present the attractiveness of the sector and the opportunities it opens.

Created in 2006, the Pascaline Association (http://www.assopascaline.fr) is a space for exchanges and reflections between companies and higher digital education establishments, the objective of which is the development of attractiveness of training and digital professions to young generations. The association brings together eighty-five higher education establishments and 2,700 companies in the sector grouped around Syntec Numérique and the syndicate of entrepreneurs in the digital industry CINOV-IT.

Launched by the ANSSI in 2013, following the publication of the White Paper on defence and national security, the CyberEdu project promotes the integration of digital security in higher computer training not specialised in the security of information systems by providing educational content to teachers. In order to extend the actions taken by the ANSSI to initiate this approach, an association bringing together IT teachers, specialists and non-specialists in security, was created to carry it throughout France, in particular through seminars. It also labels French higher education in IT which does not fall within the domain of digital security. Although the CyberEdu approach was initially intended for digital training, the association plans in the future to address other types of training, to raise awareness of all actors or users of the information systems chain.

The second notable initiative carried by the ANSSI, SecNumEdu is a label of initial training in cybersecurity of higher education. The objective of this labelling is to provide assurance to students and employers that training in the field of digital security meets a charter as well as the criteria defined by the ANSSI in collaboration with stakeholders and professionals in the field (higher education establishments, manufacturers, etc.). The label also plays in favour of strengthening and developing lessons relating to digital security. It is based on a labelling reference system, the development of which was piloted by the ANSSI with the contribution of manufacturers, schools, the Cyber Pole of Excellence and the Ministry of National Education, Higher Education, Research and Innovation. It is awarded for a renewable period of three years and allows the training which benefits from it, to appear in the SecNumEdu catalogue of the ANSSI. Forty training courses have been SecNumEdu certified.

The ANSSI has, finally, conducted an approach to identify cybersecurity professions and a title of expert in information systems security (level 1 bac+5 certification) has been registered in the National Directory of Professional Certifications (RNCP).

3.4.5 Perfecting skills management in the state's cyber defence services: retaining and attracting our talents

In addition, the ANSSI carries out several actions for cybersecurity training and awareness within the framework of its Information Systems Security Training Centre (CFSSI)[75]. The Training Centre offers short courses on topics such as cryptography, risk analysis or security auditing, and welcomes nearly 2,000 people, mainly from the administration, each year. It also provides long training over thirteen months, leading to the issuance of a title "information systems security expert" equivalent to a bac+5.

To complete this internal training system, the ANSSI could also label continuing training in cybersecurity for public sector agents and thus allow a multiplication of its training capacity. This strategy should make it possible to establish a minimum training in cyber defence for all executives and in particular those whose services or departments must defend the interests of cyber defence companies.

The large employers of cyber defence that are the ANSSI and the Ministry of the Armed Forces today have no particular difficulty in recruiting the talents they need. However, they are faced with a high turnover of their teams which requires devoting a significant effort to the recruitment and integration of these new experts. This mobility has many advantages, however, because it allows these experts to spread the knowledge and good word of the ANSSI or the Ministry of the Armed Forces within the companies that host them. However, care must be taken to ensure that these skills are not caught up by the large American or Chinese digital players to the detriment of French or European companies.

Conversely, other employers not specialised in cyber, whether public or private, are struggling to recruit personnel competent in cyber defence and especially to keep them. In fact, in structures not specialised in cyber, the specialist can quickly find himself isolated and blocked in his progression both by what he will have little outlets internally but especially because his hierarchy will want to keep him in this position. This lack of perspective is one of the main causes of the difficulty in recruiting and retaining quality specialists.

[75] https://www.ssi.gouv.fr/particulier/formations/.

There are three ways to resolve this difficulty.

The first would be to bring together cyber skills within the same structure which works for the benefit of several entities. Thus, the regions could set up, in conjunction with the ANSSI, centres of cyber competence capable of supporting, for example, all of the local authorities. The specialists would then be grouped together and could lead a coherent approach across an entire region, whether for the provision of technical advice, the drafting of specifications or the establishment of a market framework for the acquisition of cybersecurity solutions.

The second solution would be to manage interdepartmental career paths. This type, of course, is already in place for large bodies of the state but the contract workers who constitute the majority of the personnel recruited in cyber are not concerned and have the greatest difficulties in changing administration without having to resign. The ANSSI could thus be responsible for steering these career paths and allowing real inter-ministerial progress for these agents.

Lastly, the third solution would consist in promoting within the professional paths of the various administrations, the passage by a post in the field of cyber defence. One can thus imagine, for example, that the IT director or digital director positions are only accessible to personnel who can demonstrate previous cyber experience.

Conclusion

For the first time in such depth, the Cyber Defence Strategic Review provided a comprehensive overview of the cyber threat. It turns out that this threat continues to grow extremely rapidly. A certain number of systemic factors contribute to this, including the increasing digitisation of society, a still insufficient awareness of cybersecurity challenges, the wide accessibility and proliferation of malicious tools as well as the professionalisation of groups of attackers. The consequences of a large-scale cyberattack could now be critical for the Nation.

Faced with multiple risks that can have the most serious consequences and devastating and / or systemic effects, the State must consolidate its organisation, around four operational chains dedicated to protection, military actions, intelligence and judicial investigation. The necessary coordination of these chains and the definition of a long-term strategy also implies the creation or revitalisation of steering, direction, crisis management and technical coordination bodies.

The protection of sensitive state networks and critical infrastructure must remain a priority. Cooperation between the State and private actors, at the forefront of which are electronic communications operators, is therefore essential and must be strengthened. It is also necessary to develop the capabilities of the security forces and the judicial system so that they are able to respond to the explosion in the number of cybercrime crimes, by providing the investigative and judicial services with specialised skills. Finally, the State must provide support to local authorities in strengthening their cybersecurity, in particular by encouraging the development of shared skill centres.

France must consolidate its doctrine in cyberspace and maintain specific diplomatic relations in this area. Depending on the partners, these dialogues can be either cooperative (for example to allow mutual assistance in the event of an attack of regional or global scope) or assertive in order to contain the level of the threat.

It is also essential to make all stakeholders (general public, companies of all sizes, administrations) aware of this threat. This awareness must translate into taking into account cyber defence in education, from the youngest age to higher education. It could also translate economically with the modification of accounting standards in order to take this risk into account, or the development of insurance covering cyber risk.

The economic stakes linked to all of these measures still need to be strengthened and better mapped. In any case, it is necessary that France encourages and supports industrial development in the field of cyber defence, by maintaining a national industrial offer, facilitating the incubation of start-ups and contributing to the European emergence of world leaders. If the stakes are mainly on this European scale, such as, for example, the emergence of a cloud of confidence, those related to (digital) sovereignty should not be forgotten.

Finally, it is essential to develop the capabilities of the security forces and the judicial system so that they are able to respond to the explosion in the number of crimes linked to this growing cyber threat by providing the investigative and judicial services with specialised skills. Initiatives like ACTMA should be encouraged.

4 Priority recommendations

Recommendations		Implementation schedule	Development in the strategic review
Consolidation of the French cyber defence organisation	• Set up 4 operational chains: “protection” chain, “military action” chain, “intelligence” chain, “judicial investigation” chain. • Establish a cyber steering committee responsible for monitoring the implementation of decisions taken in matters of development and general organisation of the field by the Defence and National Security Council (CDSN). • Establish a cyber defence steering committee that strives to improve knowledge of the cyber threat, to develop an industrial, regulatory and normative digital sovereignty policy and to set up an official doctrine of global response to a cyber crisis. • Set up a cyber crisis coordination centre (C4) responsible for managing non-major crises.	Immediate and short term	2.2. Consolidate the organisation of cyber defence
Strengthening the security of state information systems	• Submission for opinion to ANSSI of the most important and most sensitive IT projects in the State from their launch phase. • Progressive connection of all the ministries to the Internet access platform of the Interdepartmental State Network (RIE) and full use of the services it offers. • Impose full coverage by a system for supervising the security of IT services used by the State, including in cases where these services are outsourced, and allow the ANSSI	Immediate and short term, transmitted legal, economic impact study being finalised	2.3.1. The protection of state information systems

Recommendations		Implementation schedule	Development in the strategic review
	to impose for this purpose the establishment of its detection systems or equivalent detection systems.		
Strengthening the protection of operators of vital importance (OIV)	• Reinforcement of the level of requirement of the security rules which apply to the OIV of the sectors of the electronic communications and the supply of electric energy.	Short term with a financial and legal impact study	2.3.2. The protection of OIV
Strengthening the protection of essential activities	• A common foundation of elementary proportional security rules to protect actors providing essential services. • Search for harmonisation within the European Union of cybersecurity rules applying to operators of essential services.	Short and medium terms	2.3.3. Protection of essential activities

Recommendations		Implementation schedule	Development in the strategic review
Increased involvement of electronic communications operators and hosts	• Allow the ANSSI to rely on detection systems implemented by electronic communications operators to detect computer attacks Allow the ANSSI, when it becomes aware of a particularly serious threat, to put in place on the network of an electronic communications operator or the information system of a host, a local and temporary detection device	Short term with a financial and legal impact study	2.3. Improving the protection of sensitive activities
Improvement of cyber protection for local authorities	• Support for the creation, by the local authorities themselves, of a network of cybersecurity correspondents. • Improvement of the integration of needs and constraints specific to local authorities in the ANSSI standards and in its catalogues of qualified products and services.	Middle term	2.3.4. The protection of local authorities
Strengthening the fight against cybercrime	• Conducting a reflection on the relevance of investigating cybercrime acts more systematically, including in the absence of a complaint, when the information gathered suggests the probable existence of criminal offences. • Obstacles to the most popular criminal platforms in order to reduce the feeling of impunity, which animates a certain number of cybercriminals. • Development of an active collaboration network between magistrates and investigators in Europe and internationally.	Middle term	2.4. Strengthening the fight against cybercrime

Recommendations		Implementation schedule	Development in the strategic review
Promotion of responsible behaviour standards in cyberspace	• Strengthening export control mechanisms in the cyber domain for the most dangerous elements • Creation, at French or European level, of a think tank of international scope dedicated to geostrategic and legal questions of cyber defence within which the ideas of France could find a relay.	Middle term	2.5. France's international action in the cyber field 3.1.5. Regulate the production and export of arms and offensive cyber activities
Supervision of the activity of private actors in cyberspace	• Launch of a French initiative as part of the G20 to regulate private sector activities having an impact on the international security of cyberspace. • Promote the prohibition of Hack back by private sector actors in cyberspace. • Establish at the international level a principle of security responsibility for systemic private actors in the design and maintenance of their digital products and services.	Short term	2.5. France's international action in the cyber field
Definition of a doctrine of action in the face of a cyberattack	• Adoption of a classification scheme for computer attacks. • Definition of options for responding to cyber incidents.	Immediate	2.5.3. Define a doctrine of action

Recommendations		Implementation schedule	Development in the strategic review
Structuring of an industrial digital policy based on mastery of key technologies	• Establishment of an interdepartmental team responsible for analysing key technologies and bringing out trusted solutions in connection with manufacturers (technological watch and proposal of choices dedicated to the emergence of key technologies • Maintaining a state-of-the-art national industry in the field of communications encryption. • Development of a new generation of professional mobile radios for the benefit of the security forces and rescue units. • Support for research and development in the field of artificial intelligence applied to cyber defence.	Short term	3.1. Digital sovereignty, an essential component of national sovereignty
Secure communications	• Identify a critical compost controlled by France and integrated into terminal equipment to be able to make secure mobile telephony. • Develop encryption and software partitioning techniques. • Study new services related to professional radio, based on civil technologies (5G) to bring resilience.	Short and medium terms	3.1.2 three technologies essential to our digital sovereignty

Recommendations		Implementation schedule	Development in the strategic review
Cloud	• Establish a comprehensive state policy for using the cloud. • Encourage the development of encryption solutions for the cloud. • Support strategic autonomy in this area. • Establish a global trust framework in order to orient the market towards SecNumCloud qualified products.	Short and medium terms	3.1.4 For cloud computing, invent a recovery strategy
Improvement of the current certification framework in order to help improve product security	• Implementation of an elementary cybersecurity certification, on the model of the CE marking required for the marketing of certain goods or services within the European area.	Middle term	3.2.2. Improve the certification framework to improve product security
Consolidation of our trusted national industrial base in the field of cyber defence	• Carry out and maintain an industrial map • Support for the emergence of at least one benchmark national industrial player in the area of Threat Intelligence and the development of markers capable of competing with large American, Russian and Israeli companies in the field. • Encourage major French industrialists to complete their product and service offerings for the civilian sector, so that they become international cybersecurity champions capable of competing with the American, Russian, Chinese or Israeli cybersecurity giants. • Support the most successful external growth strategies of SMEs dedicated to cyber defence by mobilizing investment	Short and medium terms	3.3. The economics of cybersecurity

Recommendations		Implementation schedule	Development in the strategic review
	funds interested in the area of cyber defence to promote the creation of French mid-size companies in this sector. • Support for the establishment of accelerators, studio start-ups and more generally support structures for start-ups dedicated to cyber defence, by focusing efforts on innovative companies whose strategy can enable them to reach a global footprint.		
Support for the private sector to take into account cyber issues	• Support for the emergence of national or European players in cyber ratings. • Study support for the development of a relevant cyber insurance mechanism by helping to better assess risks. • Support for the implementation of a CYBER risk valuation within accounting standards and for inclusion in accounting and financial documents.	Middle term	3.3. The economics of cybersecurity

Recommendations		Implementation schedule	Development in the strategic review
Integration of cybersecurity rules in the learning transmitted by the School from elementary school to the final year class	• Digital education including mastery of cybersecurity requirements in elementary school, middle school and all high school courses. • MOOCs on the transmission of cybersecurity rules dedicated to teachers in initial training and in-service training designed by the Ministry of National Education with the strong support of ANSSI.	Middle term	3.4. Human issues
Spreading the culture of digital security throughout society	• Creation by ANSSI of a fun application, available on smartphones, allowing French people to test their level of knowledge in the field of digital security culture and offering them many challenges. • Study of the contribution of nudges to the development of citizens' autonomy in cybersecurity. • Integration of a cybersecurity dimension into the support programme for the digital transformation of businesses of the Ministry of Economy and Finance and the State Secretariat for Digital Affairs. • Improvement of skills management in the state's cyber	Middle term	3.4. Human issues

Recommendations		Implementation schedule	Development in the strategic review
	defence services.		

5 Annexe 5 – Glossary

Product approval: validation by ANSSI of the ability of a product to protect classified information.

APT: Advanced Persistent Threat: a group of computer attackers with high skills and significant resources, capable of carrying out sophisticated computer attacks, often characterised by a set of specific tools or techniques.

Botnet: a network of machines compromised by an attacker, structured to allow him to transmit orders to them and to activate them as he pleases.

Product certification: validation of the security of a product through an assessment carried out by a third-party actor qualified by the ANSSI.

Trojan Horse: seemingly legitimate, but has a malicious hidden function.

Malicious code (malware): any programme developed for the purpose of damaging an information system.

Common Vulnerabilities and Exposures (CVE also known as One-day): vulnerability in a computer product known to the IT security community and which has generally been the subject of a security patch. The CVEs are listed by year and a unique identifier number. Thus the CVE 2017-0143 is the fault called ETHERNAL BLUE and used by the WANNACRY ransomware.

Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT): centre for alert and reaction to computer attacks, intended for companies or administrations, but the information of which is generally accessible to all.

Dark web: set of websites which operate on networks only accessible via software, configurations or specific authorisations, generally allowing a form of anonymity.

Disfigurement (or defacing): computer attack consisting in modifying the presentation of a website.

Denial of Service (DoS): computer attack designed to make a service unavailable by overwhelming its IT resources with unnecessary traffic. When the attack is carried out using several sources of malicious traffic, this is known as distributed denial of service (DDoS).

Exploit: malicious code associated with a vulnerability affecting computer equipment, allowing an attacker to take control by exploiting this vulnerability.

Flooding: action consisting of “flooding” information by drowning it under a rain of useless information to make it inaccessible.

Hackback: computer counterattack used in response to a computer attack with the aim of stopping the attack, recovering stolen data or imposing a penalty on the attacker.

Fishing (phishing): technique consisting in bringing, often by means of a fraudulent e-mail, an individual to communicate confidential information (passwords, banking data, etc.) on Internet, to open a trapped file or to click on a malicious link.

Security certification: formal decision, taken by the head of an organisation, which certifies that he assumes the risks weighing on the security of an information system.

Implant: malicious code used by an attacker to maintain and evolve in an infected information system and produce the desired effects (data exfiltration, sabotage, etc.).

Attack infrastructure: a set of servers controlled by an attacker and used to conduct a computer

attack.

Labelling: label given by the ANSSI to a product or service corresponding to a specification that it has defined.

Lateralisation: phase of a computer attack consisting of an attacker extending his control over the targeted information system by propagating within the infected network.

Firewall: software or hardware equipment used to filter or block data flows to protect an information system.

Backdoor: hidden functionality of IT equipment, provided by its publisher or implemented by a malicious actor, allowing access without the knowledge of its legitimate user.

Honey pot (honeypot): cyber defence technique consisting of luring an attacker by luring him towards a false target in order to observe his operating mode.

Qualification of service provider: validation by the ANSSI of the capacity of a service provider to perform services.

Product qualification: security certification for which the administration has defined the scope of the assessment.

Ransomware: a malicious programme which encrypts the data present on an information system and requests a ransom in exchange for their decryption.

Remediation: following a computer attack, all actions intended to eradicate the attacker from the victim information system and to tighten his security.

Script kiddies: a pejorative term designating neophytes who use without real skills computer attack tools designed by others.

Sink-holing: cyber defence technique consisting of redirecting malicious traffic to a controlled server in order to observe the operating mode of an attacker.

Command and control system: part of an attack infrastructure used to supervise and control all the malicious code deployed as part of an attack.

Worm: standalone malicious code that replicates itself in order to spread to other machines.

Vulnerability: design error or weakness in computer equipment likely to allow an attacker to carry out a malicious action against it.

Zero-day: vulnerability in an IT product that has not been published and of which the IT security community has no knowledge.

6 Annexe 6 – the four phases of the information system life cycle

6.1 Design a secure information system

The design of an information system is a crucial step in securing it, which applies as well to ad hoc software development as to the implementation and integration of a complete information system. It should allow the definition of a global security strategy, and the major choices that underpin it, both on a technical level (general architecture of the system and positioning of security functions, choice of development or configuration) and organisational (definition of roles and responsibilities, procedures to be developed and applicable security policy).

As a general rule, these choices must result jointly from the variation of generic good practices, applicable to any system, and from a risk analysis specific to the system considered. The applicable good practices, which form a global security foundation, can come from an applicable regulatory framework (for example the security measures fixed by sectoral Decrees applicable to VLVs) or failing this, a set of basic good practices, adaptable to any information system, generally called computer hygiene practices. The risk analysis aims to complete this base, by methodically defining the essential assets of the system to be protected and the applicable threat scenarios, to deduce additional measures.

The preventive measures ultimately adopted, if they are specific to the system studied, do not in general decline from some of the main proven principles of protection or mitigation of impacts, which it is useful to recall here:

- defence-in-depth, which consists of setting up redundant security barriers distributed throughout the information system, so as to counter the possible failure of a given barrier;
- the principle of least privilege, which aims to confer on each component (software, server, etc.) or actor of the information system only the rights which it strictly needs to fulfil its role, so as to limit the scope of its failure or possible malice;
- the separation of roles, which completes the previous point by effectively limiting the privileges that it is necessary to grant to a given actor; the security of the administrative role, and its strict isolation, are of particular importance with regard to commonly encountered attack techniques;
- logical partitioning, which consists of dividing the information system, on different planes (network, hardware, software), into logical compartments that are as tight as possible between them, so again limiting the scope of an attack;

- the correct use of cryptography, and in particular the systematic encryption of sensitive data during their transmission or storage, and the robust authentication of all accesses to the system;

- securing the system interfaces, so as to validate the security of all incoming data (validation of format and provenance, search for known malicious codes, etc.).

These choices, which are imperatively documented, must also ultimately guarantee the ability to maintain and supervise the system over time, in particular by including mechanisms for updating the various components of the system, by developing a logging policy. adapted to the investigation of potential incidents, and by the adequate positioning of attack detection means adapted to the system.

6.2 Check security

At the end of the design of an information system (whether it is its initial design or that of a significant evolution), it is imperative to carry out a formal verification of its security, respecting a fundamental principle of separation of roles and responsibilities between the actors who design or develop the system, and those who verify it in fine. This verification, which completes the functional acceptance of the system in terms of security, must pursue a triple objective of validation of the conformity of the system with its specification and security requirements, of independent vulnerability test, which aims to simulate the interaction of 'an attacker with the system to identify residual vulnerabilities, and a formal commitment of responsibility as to the adequacy of the system with its security needs.

In the case of an individual security product (software for example), security certification, or additional devices such as security qualification or approval, is generally the preferred vehicle for verifying security. It is based on an assessment by a third party, whose competence and independence are recognised, for validation of conformity and the vulnerability test, and on a certification decision pronounced by the ANSSI, which engages its responsibility and attests to adequate resistance of the product.

Conversely, in the case of a complete information system, security verification is generally based on a system approval procedure. This is based on a system security audit, conducted by a third party, in order to gauge the system's compliance with good practices and its resistance to an attacker, and on a homologation decision, which formally authorizes the implementation system service based on the results of the audit and an update of the initial risk analysis. This decision can only be taken by the system's employment authority, which alone can judge the right balance between the security and functional needs applicable to it.

6.3 Manage security over time

The level of security initially established when the information system was put into service must be actively managed in order to be maintained over time. This, supported by a clearly established organisation, pursues a double objective. The first is to maintain preventive measures in security conditions, in particular through the regular updating of the software components of the system, the management of hardware obsolescence and the regular updating of user rights. The second is the supervision of the effective security of the system, in particular by the regular collection and analysis of its operating logs, in order to detect possible abnormal events, and by the implementation of specialised detection means computer attacks (network detection probes, antivirus or detection agents deployed on computer workstations, etc.).

Attack detection mechanisms are generally based on a base of markers, or signatures, characteristics of known attacks, which must be regularly updated. The verification of the authenticity of the updates of this database, like those of the software components of the system, constitutes an important point of attention.

When the information system to be protected has a significant extent, the effective conduct of the various security management operations requires the establishment of an operational security centre, or Security Operations Centre (SOC). A real cockpit for system security, it has specialised tools and personnel, and is continuously supplied by the various system supervision means, so as to present an up-to-date table at all times. security status, known weaknesses and planned operations, and abnormal events, malfunctions or attacks in progress. Integrated at the heart of the system's life cycle, it is a primary vector for continuous improvement of its security, and the decision-making body that makes it possible to trigger reactive processing of an attack.

6.4 Respond to attacks

The identification of a proven attack must trigger the activation of reaction and incident handling procedures. In the implementation of these, the natural temptation to block or oust the attacker as quickly as possible must be tempered by the need to observe him in order to better understand his mode of action. Thus, with rare exceptions where urgency prevails, the initiation of active remediation operations must be preceded by a passive analysis phase, aimed at better understanding the method and the tools implemented by the attacker, the weaknesses it exploits or seeks to exploit, the scope that it has effectively managed to compromise within the information system, and as far as possible the purposes of its action.

Discretion is an essential component of this observation phase, with the attacker never having to discover that he has been identified. The analysis generally mobilizes a wide range of technical skills, such as the analysis of malicious code, the forensic analysis of newspapers or IT media, or even the configuration audit, and must be subject to adapted piloting which guarantees its completeness, consistency and discretion.

The finalisation of this analysis phase allows the development of a remediation plan, which primarily targets the effective eviction of the attacker and the restoration of the system to a nominal state, but also the adoption of additional preventive measures (so-called “hardening” measures), immediately before or after the restoration, so that the attacker does not subsequently regain a foothold in the system. In the case where the compromised system is large and has been the subject of a large-scale compromise, remediation is generally done in successive phases, with the creation initially of a healthy heart of trust, to a reduced perimeter, then the gradual and planned extension of this healthy perimeter to the rest of the system.

It should be noted that beyond the actual successful attacks, the identification of failed attack attempts can, in certain cases, also constitute a significant incident, justifying the implementation of reactive measures. Indeed, these attempts are potentially foreshadowing of other hostile operations to come, of which they would constitute, for example, the exploratory phase aiming to better define the defences of the system. In this case, the implementation of a response plan may be necessary, with at least an observation phase and, if necessary, the implementation of permanent or temporary security measures.

In all cases, the completion of the reaction to an attack work must give rise to capitalisation work and feedback, leading, if necessary, to the development of a plan to improve the security of the system. information, which will result in the initiation of a new design and verification cycle.

7 Annexe 7 – options for responding to computer attacks

7.1 Preventing and managing crises through international cooperation

In the event of a cyber or national or international cyber incident or crisis, regardless of the qualification chosen for this incident or crisis, France may activate certain political-diplomatic mechanisms in order to participate in the management of this crisis, to its resolution and to the control of any potential escalation.

7.1.1 Objective 1: prevent crises and discourage aggression

Even before options for responding to a cyber crisis are presented, it should be recalled that the first objective pursued by France is the prevention of such crises. In addition to strengthening the overall resilience of cyberspace, cooperation between states and international regulation of the digital space, this also requires a strategy to discourage all attacks. Through its positions, France thus signals the behaviours it considers acceptable and what is not and reserves the possibility of notifying the aggressor of the latter as well as the means at its disposal aimed at sanctioning aggressive behaviour.

France will also respond to the commitments it has made to its allies and partners in the European Union and in NATO who would be faced with attacks of this type, while respecting their sovereignty and taking account of their responsibility main in network protection. Solidarity with our partners can only be effective in support of a cyber defence effort led by all at the national level.

Sometimes, the appropriate response to a computer attack can be given to more than one. In all cases, it will be based on a completely sovereign decision, of France, as of its allies.

7.1.2 Objective 2: Contribute internationally to the treatment of an attack

Uncover the attack

The revelation of elements concerning the attack constitutes the first form of response insofar as these can limit the attacker's ability to act or even be destabilizing for the latter. In addition, this approach potentially opens the way for a public response from France.

Contribute to the technical resolution of the incident

International cooperation is a key element in dealing with attacks transiting through a third state. This is why France has promoted in the framework of the United Nations the standard according to which “States should respond to appropriate requests aimed at mitigating the consequences of malicious computer activities directed against an essential infrastructure of another State and carried out since their territory”[76]. This standard, which has the advantage of being neutral with regard to attribution, could ultimately encourage the establishment of a "chain of responsibility" allowing the victim State to benefit from the assistance of the States through which transits the attack.

[76] Report of the UN group of government experts on cybersecurity of June 2015.

In the practical implementation of the standard on State responsibility, the diplomatic network could be used.

Communicate effectively on an attack in progress

France must be able to respond to requests for information from its partners. The communication on an attack suffered, in fact, makes it possible to establish a bond of trust with our partners and possibly to obtain their subsequent support in the event that a response is envisaged.

Such a communication could also be brought by French representatives within the PSC or the North Atlantic Council (possibly under Article 4 of the North Atlantic Treaty, relating to political consultations at the request of an Ally).

7.1.3 Objective 3: Participate in the resolution of the crisis

The risks of erroneous perception due to the complexity of the attribution, as well as the difficulty in appreciating the extent of an attack and in defining a proportional response, are all factors that could complicate a strategy of controlling escalation in a crisis. The use of multilateral and bilateral preventive diplomacy instruments should, therefore, be favoured.

At the bilateral level, France will endeavour to develop exchange and de-escalation mechanisms with the other cyber powers. In complement to existing systems, such as State links or diplomatic relations, these could be structured around two axes.

- the establishment of a communication channel between high-level cyber defence officials, which can be activated in particular in the event of a major cyber incident for dialogue purposes;

- the establishment of a notification process allowing in particular the sending of formal requests such as in matters of mutual assistance (e.g. request for official cooperation from the authorities on a malicious activity in transit through one of the two countries and targeting other).

Such mechanisms would:

- to reduce the risk of erroneous attribution of attacks of which France would be a victim, by leaving the possibility to the suspected country of bringing the elements possibly allowing him to exonerate himself or the measures which he would have taken in matters of cyber, diligence;

- to promote dialogue as the first tool in the resolution of disputes between the two countries likely to harm their mutual fundamental interests.

A signal of the French authorities' desire to work to preserve international peace and security in cyberspace, this type of mechanism constitutes a “confidence-building measure” in accordance with the recommendations of the reports of the group of governmental experts from the UN on cybersecurity approved by the two States in 2013 and 2015.

Such networks would complement those set up at regional level by certain organisations such as the OSCE (which has managed since 2013 a network of technical and diplomatic contact points aimed at facilitating communication between States in the event of a cyber crisis and consultation mechanism for crisis for States parties to a cyber crisis, with possible mediation by the OSCE or by a third participating State).

At the UN level, a referral to the Security Council under Article VI of the Charter of the United Nations (Peaceful resolution of disputes) could be envisaged, in particular in the absence of "armed aggression", if France believes that the situation is serious enough to qualify as a threat to international peace and security.

Mobilisation of the Security Council on the initiative of France could take the form of an emergency meeting or a formal expression of the Council (press statement, presidential statement, resolution).

Another possibility could be to seize, if conditions allow, regional cooperation and assistance mechanisms in the cyber field, whether within the OSCE or NATO and the European Union. Indeed, these last two organisations allow France to each benefit from an assistance mechanism by invoking Articles 4 and 5 of the North Atlantic Treaty and by Article 42.7 of the Treaty on European Union Police and Judicial Cooperation, both European and international, could also be sought.

7.2 Using retaliatory measures

If prevention, cooperation and negotiation do not produce the expected effects, France could choose to resort to retaliatory measures.

7.2.1 <u>At the national level</u>

Unlike countermeasures or reprisals, retaliatory measures are binding but lawful and legal acts within the meaning of international law by nature. They do not, therefore, imply the obligation to legally justify their adoption.

Thus, for any cyber incident concerning it, whatever its level of seriousness, and for which it would suspect the involvement, direct or indirect, of a State, France could activate a range of reversible retaliatory measures against this State, for example in diplomatic or economic fields.

Coordinated action can also be taken to initiate legal proceedings against the individual responsible for an aggression attributed to a State.

7.2.2 At European Union level

The EU and its Member States have recently agreed on a framework for a joint diplomatic response to cyber crises. These measures are part of international cooperation, prevention and communication mechanisms, but also provide for more restrictive types of response such as sanctions.

To these actions could be added others, falling within Community competences in response to cyber-espionage practices with an economic aim, for example, the European Commission could request the opening of a dispute before the Dispute Settlement Body of the WTO, on the basis of a violation of the ADPLC agreements.

7.3 Adopting countermeasures

In order to respond to a situation which in its opinion involves the violation of an international obligation by another State, France could adopt, in addition to retaliatory measures, measures which are not in conformity with its international obligations; we are talking about countermeasures. The adoption of such measures is lawful if the following conditions are met:

- France's action is taken in response to an initial internationally wrongful act (including the use of force), and has the sole aim of bringing it to an end;
- France's action is necessary and proportional to this objective, and must remain peaceful (below the threshold of the use of force).

These countermeasures may or may not be cyber. Indeed, the means to respond to an attack not being conditioned by the type of weapons used, in the event of a computer attack, France, like any State, may choose to respond with other means of action, such as through the adoption of sanctions.

7.4 Other response options

In accordance with fundamental principles of international law, the lawfulness of the use of armed force by a State on the territory of another State is limited to three assumptions

- if the State on whose territory the armed intervention takes place consents;
- if a resolution of the Security Council of the United Nations, placed under chapter VII of the Charter, authorizes such intervention;

- if the State intervenes on the basis of self-defence (individual or collective) to deal with armed aggression within the meaning of Article 51 of the Charter and pending action by the Security Council.

A major computer attack targeting France, in view of the serious damage it would cause, could constitute an "armed aggression" within the meaning of Article 51 of the Charter of the United Nations and thus justify the invocation of self-defence. The possible use of force by France in return could then include actions in the offensive IT fight, without being limited to these means alone.

8 Annexe 8 – French operational support for initiatives responding to the growing need for cooperation in the face of attacks on a European scale

The French approach will be based on 4 axes:

8.1 Axis 1: Maintain a clear position with regard to the distribution of powers and the preservation of national sovereignty in terms of operational response

Assume that operational cooperation, including sectoral, can only work on an exclusively voluntary basis to allow the development of confidence, by excluding in particular any constraint in terms of information sharing between States and with the institutions of the European Union (ex: notifications of incidents) or of response to an incident;

8.2 Axis 2: Promote the strengthening of national cyber capabilities on the human and technical levels, in particular via increased EU support to States

[Action 1] **Propose the adoption by the Council of the EU of a "Cyber Defence Pledge"** sovereignly committing all the states to reinforce their national capabilities, associated with a mechanism of "sponsorship" between states in order to support the efforts of States which express the need for it. Such a commitment was already made by the member states of the Atlantic Alliance at the 2016 Summit;

[Action 2] Continue to invite the EU to **step up its action in support of the training** of cyber experts, in particular through the EDA and CESD project to establish a platform dedicated to education and training;

[Action 3] Invite the EU to **reinforce its direct financial support for States** engaged in strengthening their human and material resources in terms of operational response (on the model of the Connecting Europe Facility);

[Action 4] Support the **significant strengthening of the ENISA budget** in support of its activities to support the capacity development of States, and of its role of facilitator of operational cooperation between Member States.

8.3 Axis 3: Encouraging the development of operational cooperation within the EU

[Action 5] Support the development by the Council of the European Union, on a proposal from the European Commission, of a **European cyber crisis management framework** clarifying roles and responsibilities, mechanisms and tools;

[Action 6] Contribute to the development of tools and procedures (in particular the "standard operating procedures" (SOPs) carried by the ENISA) called to support cooperation in the event of incidents and crises;

[Action 7] Continue to **participate in European cybersecurity exercises**, contribute to their development and ensure the inclusion of a cybersecurity dimension in other European Union crisis management exercises;

[Action 8] Promote **cooperation but also now coordination between national cybersecurity authorities** at European level in the event of incidents or crises (find an agreement between member states on the distribution of roles);

[Action 9] Continue to support the **"network of CSIRTs"** (information sharing, participation in the development of its tools and procedures, etc.) created by the NIS directive as a privileged body for multilateral operational cooperation between member states within the 'EU, with increased support from ENISA in its operation.

8.4 Axis 4: Promote an appropriate model of assistance to States in the event of an incident, in particular by supporting the development of a trusted European private sector providing cybersecurity services that can be mobilised in the event of a crisis

[Action 10] Promote the establishment of a **European framework for the certification of cybersecurity products and services** (detection, incident response, audit, etc.) and make available to all member states a European catalogue of suppliers certified to call upon in the event of routine and serious incidents;

[Action 11] **Examine the advisability of concluding a European framework contract for certified suppliers and service providers**, financed by the European Union and which can be used at the request of States in the event of a serious incident or cyber crisis after agreement by the Council of the European Union;

[Action 12] Propose within the Council of the European Union, the formalisation of a **process of mutual assistance** between States in the event of a serious incident;

[Action 13] In support of States which would formalize a request for assistance, **examine the advisability of establishing a European Rapid Reaction Team** composed of representatives of voluntary Member States, with a limited mandate strategic assistance in the most serious cases, the activation of which, like in NATO, relies on a decision-making mechanism at political level – in this context, the question of applicability and recourse to solidarity clause in the event of cyberattacks must be studied more precisely.

9 Annexe 9 – Operational description of the cyber measures included in the military programming bill

Cyber defence operations conducted by the ANSSI in 2017 revealed the appearance of new modes of computer attacks. Attackers now use indirect means to reach their targets, such as taking control of Internet access equipment, compromising service providers in order to reach their customers, or renting servers from French hosts to drive attacks.

Faced with these new threats, an increased involvement of electronic communications operators and hosts, whose servers and networks serve as relays for attackers, is necessary.

Involvement of electronic communications operators in the detection of computer attacks

Step 1: ANSSI transmits to the operator a technical marker relating to a given attacker (ex: IP address of a server belonging to the attacker, trapped website)

Step 2: The operator includes the marker transmitted by the ANSSI in its detection system

Step 3: The attacker seeks to compromise a victim via malicious communication (communication from the malicious IP address, email containing a link to the booby-trapped site)

Step 4: A security alert is generated by the detection system

Step 5: The operator transmits the alert to the ANSSI, as well as the technical elements necessary to characterize the attack if the victim is an OIV or a public authority

The first part of the proposed system consists of authorising electronic communications operators to implement detection systems in their networks in order to detect computer attacks targeting their subscribers. These are technical devices that compare the activity of a network to attack markers. Like the X-ray scanners used in the physical world, these devices automatically analyse traffic without paying attention to the content, limiting themselves to comparing it to attack markers. Everything is done in real-time and traffic is not retained.

To enable them to detect sophisticated attacks, the ANSSI will provide operators with attack markers. These are technical elements specific to certain attackers, such as the IP address of a malicious server or the name of a booby-trapped website. The elaboration of such elements constitutes an activity specific to the ANSSI, of very high technicality, involving a significant part of the human and technical resources of its operational centre.

In the event of a computer attack associated with one of these markers, the detection systems deployed by the operators will produce a security alert, containing only the technical information linked to the attack. The operator will then inform the ANSSI of this alert and, if the attack detected concerns a body of vital importance or a public authority, the ANSSI might request additional technical information to characterize the attack and establish protective measures and appropriate remediation in close connection with the victim.

Local and temporary supervision by the ANSSI in the event of a serious threat

Step I: An attacker uses a server of a French host to carry out an attack

Step 2: The ANSSI detects or is informed of the use by an attacker of this server

Step 3: ANSSI deploys a temporary detection device as close as possible to the server

Step 4: ANSSI operates the system and collects the information strictly necessary for characterizing the threat and identifying the victims

The second part of the system consists in authorizing the ANSSI, when it is aware of a serious threat, to set up a local detection device on a server of a host or equipment of a controlled electronic communications operator by an attacker. The detection system then deployed produces only data aimed at characterizing the attack, such as the characteristics of the malicious programmes used by the attacker, the IP addresses of its attack infrastructure as well as those of its victims.

This technique is at the heart of the operational activity of the ANSSI. It makes it possible to understand in real-time the characteristics of an attack as well as to identify the victims, and therefore to reactively adjust the detection, protection and remediation measures that it implements.