Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Strategic review of cyber defence

February 2018

SGDSN

Strategic review of cyber defence

The strategic review of cyber defence, entrusted by the Prime Minister to the Secretary General for Defence and National Security, was drawn up during a round of dialogue involving nearly 200 people, including French nationals and foreigners, representing all stakeholders in the field.

The very extensive work undertaken, which was completed in less than six months, has led to the production of a fully-fledged White Paper on cyber defence. It is the first major strategic review exercise in this field. Divided into three parts, it provides an overview of the cyber threat, makes proposals for improving the nation's cyber defence and highlights opportunities for improving cybersecurity in French society.

Far from being complete, this piece of work marks the start of implementing a cyber defence strategy in France, based on tightening the protection of information systems, those of both the State and organisations of vital importance, as well as strengthening digital security for citizens, institutions and all stakeholders that play a part in the economic, industrial, social and cultural vitality of our country.

Executive summary

At a time when cyberattacks are likely to cause serious harm to the Nation's interests, France must adapt its stance on cyber defence by setting out to better enforce its digital sovereignty. With cyberattacks growing in number, intensity and sophistication, France must respond with a robust national system of cyber protection and defence. This requires the mobilisation of appropriate resources, as well as different skills and capabilities, within the State but also in society as a whole.

France's primary objective must be to strengthen the resilience of its vital systems, both those of the State and critical infrastructures, to be capable of withstanding a major cyber shock. Operators essential to the functioning of our economy and society, to the continuity of public services and to the preservation of our democratic life, must also be better protected. Finally, France's cyber defence depends on a rise in the overall level of cybersecurity in society. In keeping with the notion of digital sovereignty, cyber defence must be considered across our country in its entirety, including local authorities, businesses and citizens.

France must also reinforce its strategic thinking with regards to cyberspace and build specific diplomatic relations in this area. France's international positions must demonstrate the country's willingness to build the strategic stability of a peaceful and prosperous cyberspace, where fundamental freedoms are respected.

In this context, the review proposes placing seven main principles at the heart of France's ambition on cyber defence:

- place a priority on protecting our information systems;
- adopt an active stance of attack deterrence and coordinated response;
- fully exercise our digital sovereignty;
- provide an effective penal response to cybercrime;
- promote a shared culture of information security;
- help bring about a digital Europe that is safe and reliable;
- act internationally in favour of a collective and controlled governance of cyberspace.

Part I. The dangers of the cyber world

1.1. Rapidly changing threats

The cyber threat continues to grow very rapidly. A number of systemic factors contribute to this, including the increasing digitisation of society, a still insufficient awareness of cybersecurity issues, the wide accessibility and proliferation of malicious tools as well as the professionalisation of attacker groups. A major cyberattack could now have critical consequences for the Nation.

Among the purposes of cyberattacks, most are cases of economic, technological, strategic or political espionage. Acts of sabotage are however becoming more and more frequent, with attacks that are worryingly large in scope, carried out by professional, coordinated groups. Large-scale destabilising activities have also been recorded, through use of different means, such as exfiltration and the subsequent mass disclosure of sensitive data.

With regard to the types of attack experienced, it is clear that simple attacks are all too often successful, due to a continued lack of good IT practice. While most attacks recorded involve denial of service operations, website defacement or acts of cybercrime, the rise of very sophisticated and stealthy attacks, with high levels of anticipation and preparation, is particularly concerning, as are their changing effects.

1.2. International regulation still has a long way to go

The increased cyber threat falls within an international context where no binding multilateral agreement has yet been reached to establish a common framework and security architecture governing relations between States and between public and private stakeholders in cyberspace.

While negotiations of the different Groups of Governmental Experts (GGE), which have been held since 2004 under the aegis of the United Nations, have served to recognise the applicability of international law to cyberspace and consolidate voluntary norms of responsible behaviour for States in this area, the failure of the 2016-2017 GGE is a sign of a fundamental divergence in perception, among the various countries, of the international security architecture that should govern relations between States in the digital age. Still, the failure of this last round of negotiations must not end the efforts of France and the international community to promote standards of behaviour and confidence-building measures for ensuring the international stability and security of cyberspace.

In addition, the advent of digital technology as a new tool and forum for debate gives the private sector, and in particular certain systemic stakeholders, a new role and new responsibilities in maintaining international peace and security. Dynamics and power relations in cyberspace are made even more complex by the ambiguous roles of Google, Apple, Facebook, Amazon and Microsoft (GAFAM), among others, who own the vast amount of data they collect, placing it, even when it is stored in centres located outside US territory, within the reach of federal agencies and the US judicial system. In a context where technological advances are challenging sovereign prerogatives, the extraterritoriality of data calls for the structuring of new theoretical foundations.

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

2.1. Consolidating the organisation of French cyber defence

Our country's cyber defence depends on an organisational and governance model which separates offensive missions and capabilities from defensive missions and capabilities. This model is distinctly different from that chosen by Anglo-Saxon countries, whose cyber defence capabilities are concentrated within the intelligence community. It has clear advantages. By distinguishing the missions and resources dedicated to cyber protection, which are entrusted to the National Cybersecurity Agency of France (ANSSI), from those whose aims involve intelligence and offensive action, it facilitates the acceptance of State intervention in the security of information systems, whether in public administration or the economic sphere.

However, our model still lacked confirmation of its core principles, a clear description of its governance, clarification of its operational organisation, as well as a better appreciation of objectives relating to intelligence missions and judicial proceedings. For this reason, the cyber review clarifies the organisation of French cyber defence by formalising it around four operational chains, strengthens its governance mechanisms and defines an operational process for cyber crisis management.

2.1.1. Four operational chains

The review classifies cyber defence missions into six categories: prevention, anticipation, protection, detection, attribution and reaction. In addition, it organises State action into four operational chains, with each one contributing to one or more of these missions:

- the "protection" chain. Under the responsibility of the Prime Minister, its purpose is to ensure national security in the event of a cyberattack. The SGDSN (General Secretariat for Defence and National Security) runs this chain, with responsibility for operations management falling to the Director General of ANSSI. Through delegation from ANSSI, the commander of cyber defence is responsible for operations carried out within the scope of the Ministry of the Armed Forces;
- the "military action" chain. Under the authority of the President of the Republic, head of the armed forces, it can use active cyber warfare and must allow national defence operations to be carried out;
- the "intelligence" chain. Under the authority of the Government, it covers all action undertaken for intelligence purposes, in particular with the aim of attributing cyberattacks, including implementing offensive capabilities;

- the "judicial investigation" chain. This covers the actions of the police, gendarmerie and justice services. Within investigative frameworks, the police and gendarmerie work under the control of the judicial authority.

2.1.2. Strengthening governance and cyber crisis management

The review strengthens governance mechanisms through two bodies: the Cyber Defence Management Committee and the Cyber Defence Steering Committee. The Management Committee will be responsible for monitoring the implementation of policy decisions on development and general organisation in this area, and its work will be prepared by the Steering Committee, under the direction of the Prime Minister's cabinet.

The review also found that, although the State is well organised to deal with a major crisis of cyber origin, there is still room for improvement where the management of smaller-scale crises is concerned. For this reason, the review advises the creation of a Cyber Crisis Coordination Centre (C4). As a permanent interministerial mechanism for threat analysis, preparedness and coordination, C4 will bring together all stakeholders concerned, beyond the technical sphere alone, in order to ensure the exchange of information on and analyses of cyberattacks and to facilitate the preparation of the State's response options, whether in relation to technical, diplomatic or judicial factors.

2.2. Strengthening the protection of our systems

2.2.1. Safeguarding State information systems

The State's network security must be one priority of France's cyber defence strategy. Beyond the most sensitive networks, which must have an uncompromising level of security, all of the State's networks must be given special attention.

For this reason, the review recommends that the State's most important and sensitive IT projects are submitted to ANSSI for opinion as soon as they are launched. The review also advises optimising use of the State's interministerial network and encouraging ministries to make systematic use of the security services it offers, which is not currently the case. These security functions make it possible to react effectively in the event of a cyberattack, for example by taking measures to block malicious traffic.

2.2.2. Protecting critical infrastructures

The review presents a series of recommendations to strengthen the protection of operators of vital importance, which calls for a number of legislative and regulatory changes. In particular, it proposes increasing the security regulation requirements applicable to operators in the electronic communications and electricity supply sectors, where any cyberattack has the potential to gravely impact the resilience of the Nation as a whole. It also recommends paying special attention to digital services companies, which can be a source of weakness for any of their clients who are operators of vital importance.

As well as operators of vital importance, which are the cornerstones of the Nation's resilience, other stakeholders provide services that are essential to the day-to-day functioning of the economy and society. For this reason, the review recommends the ambitious transposition of the Networks and Information Systems (NIS) Directive, which is an opportunity for France to equip itself with the means to protect a wider range of activities. In the context of this transposition, the review recommends that, for operators of essential services, the State establishes a common set of proportionate rules on cybersecurity. The review stresses the importance of seeking the gradual harmonisation of these rules at European level, adapted to each Member State's levels of maturity in this area.

2.2.3. The role of electronic communications operators and web hosts

Faced with attackers who are now using indirect means to achieve their goals, the increased involvement of electronic communications operators and web hosts, whose servers and networks act as channels for attackers, is needed. While ANSSI already relies on these stakeholders, the purely contractual framework within which this cooperation exists is proving insufficient. The measures proposed in the review, which are supported by the 2018 Military Planning Bill, will provide better regulation for these activities.

The first part of the proposed plan allows electronic communications operators to implement detection systems in their networks to detect cyberattacks targeting their subscribers. These are technical devices which compare the activity of a network against attack markers. As with X-ray scanners used in the physical world, these devices automatically analyse traffic without looking at the content, being interested only in comparing it against the attack markers. To enable them to detect sophisticated attacks, ANSSI will provide operators with markers. In the event of a cyberattack associated with one of these markers, the detection systems deployed by an operator will produce a security alert, containing only the technical information related to the attack. The operator will then inform ANSSI of this alert.

The second part of the plan allows ANSSI, once it is aware of a serious threat, to set up a local detection device on a web host's server or on the equipment of an electronic communications operator under the control of an attacker. The detection system then deployed only produces data intended to characterise the attack. This technique lies at the core of ANSSI's operational activity. It enables the characteristics of an attack to be understood in real time and its victims to be identified, and ANSSI can therefore reactively adjust the detection, protection and remedy measures it takes. This collaborative plan, based on cooperation between ANSSI and the operators concerned, will be overseen by ARCEP (the French regulatory authority for electronic and postal communications).

2.2.4. Protecting local authorities

The State must support local authorities in strengthening their cybersecurity. The review recommends supporting the creation, by local authorities themselves, of regional cybersecurity resource hubs, in order to create appropriate forums for dialogue with ANSSI's regional teams and other ministries. These initiatives will mean that skills in information systems security are pooled and will serve to support local authorities in implementing their digital projects, in complete security and in a relationship of trust.

2.2.5. Protecting democratic life

The use of internet voting raises important security issues, and its implementation is fraught with known risks of cyberattack which may adversely affect, on a large scale, not only the fairness and sincerity of the ballot, but also the secrecy of the votes cast. In this context, the review stresses that the possible widespread adoption of internet voting must be subject to ambitious prerequisites, in particular the pre-deployment of a robust digital identity extended to all voters.

In addition, recent elections in a number of democratic countries have highlighted new propaganda techniques, which use all digital means available, without necessarily resorting to computer hacking. The review therefore recommends instituting an independent observatory responsible for analysing the propagation of *fake news* in order to establish, in cooperation with operators, an approach aimed at reducing it. Its implementation should form part of the Bill announced by the President of the Republic on 3 January 2018.

2.3. France's international action in the cyber domain

2.3.1. Strengthening dialogue and cooperation with our allies and partners

The review stresses the need for France to step up its international efforts and continue building its bilateral dialogues on cyber defence, with a view to consolidating the stability of cyberspace and the resilience of all States in dealing with cyber crises. France must forge strategic bilateral relations and develop channels for frank and open dialogue with key cyberspace stakeholders. These exchanges provide the opportunity to monitor and organise projects of common interest on a strategic level, to improve understanding of the organisation and strategy of these countries, to clarify France's position on major cyber issues and to share information on potential incidents.

2.3.2. Establishing a doctrine for action

The review advises the establishment of a doctrine for action. The options for responding to a cyberattack must be prepared in advance so that the authorities can respond to a crisis as it unfolds. In order to build such a doctrine, the review proposes a scheme for classifying cyberattacks. Incorporating national and international legal standards, it will be both a decision-making tool for authorities, which for France is a key feature of a doctrine for action, and a support for international cooperation. Obviously, this doctrine will also be based on France's interpretation of the application of existing international law to cyberspace, which is accounted for in the review.

2.3.3. Rules and standards applicable to States

France must continue to work towards the universalisation of certain standards applicable in cyberspace with a view to strengthening its security. This approach centres on three principles:

- the principle of prevention: the uncertainty intrinsically linked to the attribution of an attack should encourage States to focus their efforts on preventive measures;
- the principle of cooperation: improving cooperation within the international community in cyberspace is an effective way to increase stability, through greater mutual knowledge and even trust between stakeholders, as well as establishing mechanisms for joint crisis management, communication and de-escalation. France must in particular work towards reaching an agreement at international level on the obligations of a State whose infrastructures could be used for malicious purposes;
- the principle of stability: France must continue to promote the principle that certain rights exist allowing States targeted by cyberattacks to take appropriate measures in order to maintain international peace and security.

2.3.4. Rules and standards governing the responsibility of private stakeholders

The review identifies three priority areas for the improved regulation of private sector activities:

- greater control of offensive action by the private sector in cyberspace: France proposes, firstly, to promote the prevention of the use of offensive cyber capabilities by non-state actors and, secondly, to support a ban for non-state actors on carrying out offensive activities in cyberspace on their own behalf or that of other non-state actors;
- export control for attack tools: limiting the proliferation of offensive technologies is a key issue for the stability of cyberspace. Today, it is important to consolidate this development by working towards deepening the export control regime in the cyber domain;
- corporate responsibility in designing and maintaining digital products: France must mobilise the private sector in order to disseminate good practice and codes of conduct and contribute to the integration of these issues in contractual clauses; for the most sensitive products, regulatory initiatives could be considered, in particular at European level.

The review recommends the launch of a French initiative within the framework of the G20 to regulate private sector activities having an impact on the international security of cyberspace, based on these three priority areas. It also advises the creation of a new national or European *think tank* dedicated to cyber defence issues, which could be an effective means of exporting French ideas.

Part 3. The State, guarantor of cybersecurity in society

3.1. Digital sovereignty, an essential part of national sovereignty

Digital sovereignty can be described as the ability of France to retain in the digital space the autonomous ability of appreciation, decision and action, as well as to preserve the most traditional elements of its sovereignty in the face of the new threats that exploit the increasing digitisation of society. The review reaffirms the need for our country to fully exercise its digital sovereignty.

3.1.1. Digital sovereignty and mastering key technologies

The review stresses that mastering certain technologies is essential for the exercise of our digital sovereignty. The review therefore proposes the formulation of a digital industrial policy based on the mastery of technologies that are key to our digital sovereignty, relying largely on the qualification by the State of trustworthy solutions. In this respect, the review recommends setting up an interministerial team to analyse key technologies and foster the development of trustworthy solutions in liaison with industry.

Among the key technologies that need to be mastered in order to exercise our digital sovereignty, the review has chosen to highlight three: encryption of communications, detection of cyberattacks and professional mobile radios; for the latter, 5G could be an adequate transmission medium. In particular the review recommends maintaining a national industry at the forefront of IP encryption, as well as supporting the emergence of at least one leading national industry player in the field of *threat intelligence*.

In addition, the review stresses the importance of sovereignty issues surrounding artificial intelligence. In particular, it recognises that the mastering of artificial intelligence systems as applied to cyber defence as a major challenge for France.

3.1.2. Cloud computing strategy

If outsourcing to a cloud potentially provides proven gains, in terms of cost as well as reliability and flexibility, even information security, the review stresses that use of the cloud nevertheless carries new risks. With the cloud market strongly dominated by a small number of foreign stakeholders, these risks take on a dimension of national sovereignty.

In view of this observation, the review submits the following recommendations:

- establish a global policy for use of the *cloud* by the State, by combining use of the State's internal *clouds* and the use of *cloud* providers certified by ANSSI;
- promote the development of *cloud* encryption solutions. In particular, homomorphic encryption techniques, which allow the processing of encrypted data within the *cloud*, should remain a forthcoming priority area;
- support European strategic autonomy on the subject, both by investing in breakthrough technologies likely to produce the champions of the future, and by

ensuring, through the use of tax measures, that fairness is restored between European players and their international competitors;

- establish a global framework of trust so that businesses, communities and individuals can assess the risks associated with use and guide the market by developing the *SecNumCloud* certification for *cloud* providers, including at European level.

3.2. Regulating cybersecurity

As the guarantor of cybersecurity in society, the State intervenes in this area as a prescriber, reformer and provider of security solutions. Alongside Parliament, which enacts the law, the government plays a normative role in the field of cybersecurity.

3.2.1. Involving all sectoral players in order to raise the level of our cybersecurity

Where the Nation's interests justify it, particularly where defence and national security are concerned, a cross-sectoral approach to cyber risk is required. Responsibility for this is entrusted to an interministerial authority, ANSSI. Such an approach guarantees a cohesive and ambitious assessment of the risk, which is independent from sector specificities in its objectives. This approach is above all intended to guarantee a minimum level of cybersecurity for the most critical entities, in order to protect France's fundamental interests in face of the cyber threat.

Nevertheless, cross-sectoral approaches do not lead to a detailed understanding of managing risks specific to each sector. Moreover, digital transformation, which results in huge numbers of objects being connected to the Internet, now requires the risk of cyberattack to be recognised at sector level, especially when these objects are likely to have a direct and material impact on personal security. Indeed, only sectoral players have the necessary business knowledge to qualify the impact of any cyberattack on these objects and therefore to appropriately assess the cyber risk associated with their deployment.

The review therefore stresses the pressing need for key players in sectoral regulation to understand the risk of cyberattack in the same way as other risks and, where necessary after a risk analysis has been carried out by business experts, to adopt appropriate measures, for example by issuing suitable cybersecurity requirements.

3.2.2. Improving the certification framework in order to improve product security

The current certification framework primarily focuses on the certification of high-level security products. It is ill-suited to the evaluation of products that are in common use, such as connected objects, for which the cost and timeframe involved are prohibitive. For this reason, the review advises the introduction of a basic cybersecurity certification, in complement to the existing certification framework. The latter could draw on existing systems already in place in contexts other than cybersecurity, such as the CE mark required for the marketing of certain goods and services within the European area. This basic cybersecurity certification would essentially involve a compliance analysis, based on predefined specifications and under the control of a private body, with the involvement of public authorities limited to indirect actions, such as the approval of assessment centres.

The review also stresses that the cyber package presented by the European Commission in September 2017 provides a unique opportunity to harmonise security certification at European level. The Commission's work in this area must therefore be encouraged and supported. The review nevertheless advises that this new framework and its implementation should build on the experience gained by Member States at the forefront of certification, including France, and incorporate established good practice in this respect. In particular, in addition to basic conformity certification following the guidelines given in the previous paragraph, the European framework should incorporate a certification component able to meet the highest levels of security requirements.

3.3. The economics of cybersecurity

3.3.1. Consolidating the national industrial base

The review advises consolidating the trusted national industrial base in the field of cyber defence products and services. This is essential for communicating and extending the State's action. The aim is to develop an industrial capability that is able to offer products and services with a very high level of security while at the same time being economically viable.

In order to achieve this ambition, the review sets out three areas for progress:

- Encourage French industry leaders in the sector to complete their cybersecurity products and services offer for the civilian sector, so they will become international champions of cybersecurity;
- Promote the creation of medium-sized companies by helping the best-performing SMEs to grow and make appropriate acquisitions. The State will support and encourage these external growth strategies by mobilising investment funds interested in the area of cyber defence;
- Encourage and support government and corporate experts to create start-ups in the area of cyber defence. With this aim in mind, it is essential that the State supports the establishment of accelerators, start-up studios and, more generally, support structures for start-ups dedicated to cyber defence.

3.3.2. Creating a European cybersecurity industrial base

The review reaffirms France's willingness to promote the creation of European cybersecurity players. It sets out several areas for action which could lead to the creation of such an industry:

- identify areas where France believes a European industry should be established in order for strategic autonomy to be gained or maintained. For this to become a reality, European financial support must be put in place, no longer solely to support research but to cater for a broader approach: capability-building programmes, support for innovation, support for export, etc.;

- encourage the emergence of a European market fostering the development of effective European solutions;
- in some areas, explore the introduction of European protection systems for companies considered sensitive to foreign investors, or even the possibility of reserving certain sensitive public contracts for European companies.

3.3.3. Cyber rating and compliance issues

In a context where cyberattacks can have serious consequences for the financial health of a company, the review considers that cyber rating constitutes an initial assessment of the cyber risk which, although approximate, is a first step which may encourage financial markets, insurers but also customers to institutionalise those ratings.

The review advises that the European Union develops a cyber rating offer, so that French and European businesses are not de facto subject to uncontrolled rules. An incentive approach could thus be put in place to encourage the emergence of European cyber rating players. The certification of the French offer by the State or groups of private businesses could help provide structure in this area. This approach could be supported by changes in financial accounting standards to take account of the cyber risk for larger companies.

3.3.4. Establishing a virtuous circle of security through an insurance mechanism

The review has highlighted the fact that cyber insurance is struggling to gain traction and that the European market is far from mature. While businesses consider cyber risk a risk in itself, which is conducive to its insurability, for insurers on the other hand, the lack of reference data on cyber risk, as well as its possible systemic nature, are challenges that have yet to be overcome.

In this context, the review advises creating a European database to list cyber incidents. The data could be aggregated to analyse trends in threats, identify security needs for products and services on the market and provide information on costs. The ongoing introduction of incident reporting mechanisms within the European Union will be able to make a valuable contribution to establishing a picture of the cyber risk.

3.4. Human issues

3.4.1. Promoting a culture of digital security in society

Finally, the review has emphasised how crucial it is that all participants in society are made aware of the cyber risk.

It therefore advises a pedagogical approach, which is positive and rooted in the reality of the various audiences concerned by the culture of digital security, in order to increase its impact and fully engage everyone’s interest in digital issues. In particular, the review proposes:

- raising awareness of the digital risk through digital education, including the control of basic good practice in cybersecurity in primary and secondary schools, where a knowledge of cybersecurity rules should count towards achieving the lower secondary school certificate, which should also form part of all upper secondary course curricula. Initial and continuing training for teachers should include this new requirement to teach students good practice in digital security. As such, a MOOC for teachers undergoing initial and continuing training could be developed by the Ministry of National Education with strong support from ANSSI;

- educational initiatives, based on the varying levels of familiarity French people have with new technologies. In particular, the review proposes the creation of a fun application available for *smartphones* where people can test their knowledge of digital security, as well as a study to examine how *nudges* can contribute in disseminating good practice in digital security;
- the integration of a cybersecurity dimension in the State programme to support the digital transformation of businesses.

3.4.2. Skills management

Finally, the report stresses that France's level of ambition in terms of cyber defence is limited by its human resource capabilities. In particular, employers, whether in the public or private sector, who are not specialised in digital security, struggle to recruit and above all retain skilled staff in this area.

In this context, the review advises:

- increasing the integration of digital security within higher education courses that do not specialise in digital security, as a continuation of the *CyberEdu* initiative, which could be extended beyond training programmes in the digital field alone;
- carrying forward ANSSI's work on accrediting digital training, by extending the initiative to continuing education programmes;
- pooling cyber skills under joint structures working for the benefit of several bodies. The Regions could thus set up cyber skills hubs capable of supporting, for example, all local authorities;
- ensuring, within the State, that experience gained by officials in the field of cybersecurity is optimised throughout their career.