The French model of cybersecurity: Priority for defense

Guillaume Poupard,
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Abstract:
Whereas cybersecurity is now a strategic priority for several countries, France's point of view is independent and balanced mainly because of its cybersecurity model, which makes a clear separation between two sorts of activities: on the one hand, cyberoffensives and, on the other, security in digital technology. The latter is mostly entrusted to ANSSI, the national security agency of information systems. This original, interministerial model of protection has enabled the country to draft ambitious laws and public policies about global cybersecurity in behalf of public administrations, firms and citizens. By coping with an ever increasing number of ever more variable digital threats and with the offensive, sometimes hegemonic strategies of the world's cyberpowers, this model has, for ten years now, proved pertinent. We must take advantage of the opportunities it provides by forming a French ecosystem of cybersecurity that will associate all architects of the digital society.

2019: ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) entered its tenth year of existence. The past ten years have solidly established this French agency in national, European and international cybersecurity. During this decade, cyberthreats have continuously grown and adapted. These ten years have also confirmed the French model's pertinence and the boldness of the decision not to bunkerize cybersecurity in a single sector but to strictly separate activities as either defensive (assigned to ANSSI) or offensive.[1]

In these more than ten years, cybersecurity has become a major strategic priority for nation-states. At the planetary level, we observe the consolidation of a "first circle" of cyberpowers including, without surprise, the United States, United Kingdom, China, Russia and Israel. The dimension of digital technology is now fully integrated in foreign powers' strategies of influence, interference or dissuasion. In cyberspace, tensions are mounting, constantly increasing instability; they stem from strategies that, definitely offensive, sometimes even aim at hegemony.

In this context, France remains a cyberpower. Its bold strategy has enabled it to rapidly develop its own capacities. It is one of the very few nations capable of speaking out with a balanced, independent, clear voice in European and international centers of power. Its special position can largely be set down to its organization, which has enabled the country to follow up on changes in cyberthreats while deploying a genuine cybersecurity policy, the condition for a reassuring "digital transformation".

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in February 2020.

A constantly evolving menace

The everyday experience of defenders — anyone in risk management — is that they are seen as spoilsports. They are sometimes asked to stop playing Cassandra (a person, it is forgotten, whose predictions were never wrong). They are sometimes criticized for painting the situation black or indulging in alarms in order to raise the awareness of security issues or even to justify their reason for being. Besides, defenders are forced to use the conditional when speaking… lest they be compelled to talk about the past!

There is no need to exaggerate. As ANSSI's activities have constantly shown, cybermenaces are anything but virtual; and the taunts made to cybersecurity are enormous. There is a reason for this: digital threats now have a new dimension, as the hacking of information systems becomes more sophisticated, better designed and more destructive. It affects all of society, from citizens to big firms and even our democratic institutions. Given the proliferation of the uses of digital technology and the increase in outsourcing, the attack surface has constantly expanded. However this is far from having mechanically increased the requisite level of security.

A recrudescence of attacks "by rebound"

In a globalized, synchronized, externalized environment where movements are both physical and digital, the growth of interdependence exposes each actor to the lapses and failures of any member of the ecosystem. For this reason, the supply chain — including the relations arising out of subcontracting and outsourcing — is both a powerful driving force of economic performance for firms and public administrations, and, too, a genuine cybersecurity issue.

Hackers have clearly understood this. They now exploit this vulnerability for their own ends, by taking aim at a firm's suppliers in order to reach their major target in the firm itself. This trend, pervasive in recent months, mainly concerns digital service-providers but also many other suppliers. This sort of attack complicates the mission of those in charge of defense, who have to overcome the technical and regulatory hurdles related to the type of victims and the (often) international scope of their activities.

The (nearly) new risk of sabotage

Besides cyberespionage against which ANSSI has mustered a significant share of its resources, there has, in recent months, been a recrudescence of threats of cybersabotage. Sabotage is not new, but cybersabotage is new owing to its potential impact. The human and economic effects of large-scale or smartly targeted attacks could prove catastrophic. Imagine shutting down public transit in a capital city, thus paralyzing the country's economy within a few hours. If, tomorrow morning, automated teller machines no longer distributed cash, the odds are high that this would cause major disturbances.

An even greater cause of concern is that ever more attacks are apparently targeting our sensitive or critical infrastructures, for the purpose of mapping these installations and their activities and of prepositioning. Whether conducted by states or criminal organizations, today's hackers are busily preparing for tomorrow's conflicts or criminal activities. Despite the lack of clarity about their underlying motivations, these actions might well be reconnaissance operations for future acts of sabotage. This menace is all the greater as the geopolitical context becomes more unstable.

A proliferation of digital weapons and of points of vulnerability

The proliferation of electronic weapons and the disclosure of points of vulnerability in the hard- or software of information systems is enabling hackers to improve their techniques, whence the turning point in 2017 with attacks unprecedented as to their scale and harm.

By paralyzing many a firm, big and small, as well as other organizations, including hospitals, *WannaCry* and *NotPetya* proved that major attacks can be made against national interests without necessarily affecting critical infrastructures. To handle such attacks, defenders have to enlarge their scope of supervision so as to encompass a wider variety of victims and hackers. Furthermore, the anonymity of malware and its uses complicates the sensitive task of identifying the sources of an attack. The media has sometimes reported critical flaws in hard- or software before patches were released, thus offering hackers new possibilities for more massive, less visible acts of aggression.

Ever more lucrative attacks

Attacks ever more frequently have a moneymaking goal. Hackers exploit security loopholes to compromise equipment and devices. They might covertly install "mining" programs so that the cumulated computational power of the infected systems be surreptitiously used to reap cryptocurrency benefits.

Given the growing concern of organizations about digital security and the reinforcement of their defensive capacities, many hackers will be looking for less exposed but more vulnerable targets. For instance, phishing campaigns have been targeted local authorities or health establishments since 2018. Among their many objectives, the most frequent are: the theft of personal data, the payment of a ransom for decrypting stolen data, cryptocurrency mining, and the formation of fleets of *botnets*.

The right intuition for France's strategy

This increase in risks related to digital technology continuously tests the resilience and solidity of our model of protection, which is organized around a strict separation between cyberoffensive and cybersecurity activities, the latter mostly assigned to ANSSI.

At the origins of this strategy

France's cybersecurity strategy has come out of a succession of ambitious political decisions that arose out of the awareness that the digital transformation of the economy, society, and public interventions imply confidence, lest the transformation not be made.

In 2008, a few months after a major cyberattack (the first of its kind) had paralyzed essential activities in Estonia for several weeks,[2] a white paper on national defense and security was released in France.[3] As a result, the National Cybersecurity Agency of France (ANSSI) was set up in 2009 with a strictly defensive orientation. The creation of this interministerial agency prefigured an original approach for organizing cybersecurity nationally and following up on various aspects of

[2] This distributed denial-of-service attack (DDoS) blocked Internet sites of the government, media, political parties and banks. It stimulated a global consciousness of the risks related to digital technology. The Estonian government accused Russia of being at the origin of the DDoS.

[3] *Le Livre blanc de la Défense et de la Sécurité nationale de 2008* (Paris: La Documentation Française), 124p., available via http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf.

cyberdefense. In 2013, a new white paper on national defense and security broadened ANSSI's scope to "operators of vital importance", *i.e.*, highly sensitive, strategic private organizations.[4] The Prime Minister's Office released a national strategy for digital security in 2015 that confirmed the ambition of establishing a global cybersecurity policy that would reach out to the rest of society, in particular citizens.[5]

Strategic projects carried out in 2018 made a qualitative leap forward in the governance and steering of activities for responding to cyberattacks (mainly the more sensitive ones). The roles of the (now many) institutional actors in digital security have been clarified.

Countermodels

As among other cyberpowers, France's cybersecurity efforts fit into a trend for developing the country's capacity and strategy. This trend has spawned organizations, some of them very distinct, that reflect each nation-state's strategies and doctrines. Mainly guided by practical considerations and a concern for technical efficiency, some countries tend to group defensive and offensive cybercapacities within their defense department or intelligence services. Such is the case in the United States. The American model has the advantage of pooling technical know-how nationwide at the NSA. However it raises questions about the private sector's acceptance of government interventions in cybersecurity.

Furthermore, concentrating capacities for coping with cyberattacks within military or intelligence services soon leads, naturally, to an inclination for giving priority to cybersecurity's offensive aspects. Let us take as example the management of flaws in information systems. Defenders try to detect them and patch them, while "attackers" try to detect and exploit them. The value of these points of vulnerability is rising, and the world market is experiencing strong inflation. When attackers and defenders are one and the same, we imagine how hard it will be to relinquish such a strategic asset.

For want of a global system of cybersecurity, some countries almost have to attack in order to defend themselves and neutralize threats at the source, a sort of spearhead campaign; but such offensive strategies would be detrimental to the stability of cyberspace.

Advantages of the French model

A little more than ten years after the initial intuition, the French model has proven its pertinence. And it is still spawning emulation: countries as different as Japan, Singapore, Belgium and Israel have drawn on it, sometimes outright, in order to build or rebuild their own forms of governance for cybersecurity.

From ANSSI's viewpoint, this model has a few undeniable advantages. Unlike intelligence services, ANSSI's strictly defensive mission enables it to strike an unambiguous posture when dealing with third parties, whether the firms or administrations that have fallen victim to attacks, parliament, researchers, the media or even industries. Thanks to this model, ambitious, often pioneering, legislation has been passed, such as the regulations (which several other countries admire) about the security of the nation's vital activities. Thanks to this protective, reassuring model, recent legislation has significantly bolstered ANSSI's capacities for detection.

[4] *French white paper: Defense and national security 2013* (Paris: Ministère de la Défense), 137p., available via https://www.defense.gouv.fr/content/download/215253/2394121/White%20paper%20on%20defense%20%202013.pdf.

[5] *La Stratégie nationale pour la sécurité du numérique* (Paris: Prime Minister's Office), 44p. available via https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_fr.pdf.

Other countries have tried to set up a legally binding framework for private actors. As in the United States or Russia, these initiatives have often met with failure, since firms are reluctant to actively collaborate with intelligence services.

Another characteristic specific to the French model: ANSSI is an interministerial agency under the Prime Minister's Office. This position enables it to oversee coordination between ministries and the coherence of public actions in this field. It also gives ANSSI the right to review and control information systems in public administrations — and this has definitely improved state security.

An essential point in our strategy, the one that gives it force, is that the French model has made possible the deployment of a global cybersecurity policy. This policy is intended not just to defend the country's most critical infrastructures (public and private) but also to address security issues with as many actors as possible — all those involved in the digital transformation.

The clear-cut separation of missions, far from setting offensive and defensive activities at odds, allows, on the contrary, for a balanced distribution of means and an effective cooperation for the sake of defense and national security.

Taking advantage of these advantages

Digital risks stemming from the acceleration of technology and its uses mean that all parties must be involved in the digital transformation and better reckon with security issues. Security must not be compartmentalized separately; it must associate all the architects of the digital society. Beyond menaces to society, the economy, sovereignty and the stability of cyberspace, the very development of this technology is at stake.

State authorities can help create the conditions for reinforcing cybersecurity, in particular by shaping a French ecosystem and creating synergy between public authorities, businesses, research and education. As the vitality of some national players has shown, a French cybersecurity market is being built. It is now necessary to sustain this construction.

Other countries have made efforts to sustain the growth of their cybersecurity industry and thus ensure their digital sovereignty. Israel is an inspiring example of this. The Hebrew state soon asserted its ambition to organize its strategy around this synergy. In 2016, CyberSpark was created, a park that brings together Israeli and foreign firms, research centers (private and public) and special units of the army on a single location. In France, the prime minister has asked Michel Van Den Berghe to work out plans for a cybercampus — with the objective of bringing together worlds that do not communicate enough with each other. Likewise, ANSSI has recently adopted a novel approach of openness toward its ecosystem. Our model allows for this.

This implies changing in our view of cybersecurity. This security can no longer be seen simply as a budget item to be assigned a cost or as a patch to be applied once the process of innovation is complete. Ask the experts at ANSSI: this is an exciting field of innovation, a thoroughly multidisciplinary field that, rich with scientific developments, associates a wide variety of actors, private and public, national and international. Cybersecurity is a major intellectual challenge for innovators of all sorts.

Although these issues are a natural concern to engineers, public policy-makers and experts in international relations have not been left out. How to see to the stability of cyberspace? Should we let private parties take justice into their own hands — retaliate against attacks as firms become battlefields? The stability of cyberspace is a topic that unsettles habits in policy-making, both diplomatic and military. It raises several questions, and the perspectives are exciting and decisive.