Protecting critical infrastructures: Five years after an act of law

Yves Verhoeven,
Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Abstract:
As of 2008, the French government was aware of the growing risks of cyberattacks against the public and private operators and infrastructures that are critical for our society, economy and national defense and security. To limit these risks, state authorities offered assistance to firms, in particular those in critical fields. Given the scope of what was to be done however, the state set up, under a military program act in 2013, a regulatory framework for imposing a minimum level of cybersecurity on all information systems critical to national defense and security. Implementing this regulation has made France a pioneer in the cybersecurity of critical infrastructures. This innovative form of regulation has had several international developments. It has inspired the EU's Directive on the Security of Network and Information Systems with its measures for a high joint level of security for networks and information systems in the European Union.

Origins of a regulatory framework

Waking up to a global issue

The stakes in cybersecurity are well known. Following successive waves of virus attacks on the general public since the start of the century, reports have revealed that highly sophisticated, targeted attacks have been conducted under the auspices of foreign governments. A step beyond cyberespionage, cybersabotage takes as target economic or industrial infrastructures, such as: Operation Olympic Games against Iranian centrifuges in 2010; the cyberattack against the French television network TV5Monde in 2015; and the attacks in 2015 and 2016 against Ukraine's grid that cut off the electricity supply to hundreds of thousands of households in the country.[1]

These events shed *post hoc* a light on the solicitude that a few countries have, since the end of the 20th century, had about the risks of major destabilization caused by cyberattacks, whence their active efforts in this field. The first United Nations resolution on this topic was, on the initiative of Russia, adopted by the General Assembly on 4 January 1999; "*Developments in the field of information and telecommunications in the context of international security*". The cybersecurity of critical infrastructures soon became a priority. Further work on this topic at the UN led in 2004 to the adoption of Resolution 58/199 on the "*Creation of a global culture of cybersecurity and the protection of critical information*

[1] This article, including quotations from French sources, 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.

infrastructures".[2] In this new resolution, the General Assembly, "*as a result of increasing interconnectivity, critical information infrastructures are now exposed to a growing number and a wider variety of threats and vulnerabilities that raise new security concerns*", invited "*member states and all relevant international organizations to take these elements and the need for critical information infrastructure protection into account.*"

A few years later, on 30 April 2008, the Organization of Economic Cooperation and Development (OECD) adopted a recommendation on the protection of critical information infrastructures. The OECD's Council recognized "*that the functioning of our economies and societies increasingly relies on information systems and networks that are interconnected and interdependent, domestically and across borders; that a number of those systems and networks are of national critical importance; and that their protection is a priority area for national policy and international cooperation.*"[3]

France's actions

These recommendations were echoed in France as of 2008 in a white book on national defense and security.[4] For the first time, the risk of cyberattacks against the country was listed among strategic threats: in third place given the high probability of occurrence and the potential impact. This led France to set up the Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) in 2009. ANSSI soon started working with public and private operators of critical infrastructures; and this model of public-private cooperation is now admired outside the country. Not until 2011 and Article L33-10 of the Code of Electronic Communications would the information technology (IT) used for electronic communications become the first critical infrastructures in France to be subject to cybersecurity regulations. And not until 2013 was the concern for cybersecurity extended to all infrastructures critical for national defense and security.

In 2013, another white book on national defense and security was published with a section on "*the fight against cyberthreats*",[5] which states: "*As for activities of vital importance for the normal functioning of the nation, the state will define the security standards to be met with respect to IT threats, by means of an appropriate legislative and regulatory procedure, and will ensure that operators adopt all necessary measures to detect and handle any such incident affecting their sensitive systems. This procedure will specify the rights and obligations of public and private actors, particularly in relation to audits, the mapping of their information systems, notification of incidents and the capacity of the national agency responsible for the security of information systems (ANSSI), and, where applicable, of other state agencies, to intervene in the event of a serious crisis.*" More than 250 "operators of vital importance" (OIVs), public and private, were placed on a classified list. They are subject to the requirements of cybersecurity in addition to those that already apply to the physical security of their installations. This orientation of the 2013 white book on national defense was

---

[2] Respectively: UN Resolution 53/70 adopted by the General Assembly on 4 January 1999 "*Developments in the field of information and telecommunications in the context of international security*", available via https://undocs.org/en/A/RES/53/70; and UN Resolution n°58/199 "*Creation of a global culture of cybersecurity and the protection of critical information infrastructures*" adopted by the General Assembly on 30 January 2004, available via https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf.

[3] Drafted by its work group on the security of information and privacy, Recommendation C(2008)35 on the Protection of Critical Information Infrastructures adopted on 30 April 2008, available at https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0361.

[4] *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.

[5] Pages 101-103 of *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.

embedded in Article 22 of the program act for the armed forces of 18 December 2013, which led to articles (from L1332-6-1 to L1332-6-6) in the Defense Code.

ANSSI was thus assigned the tasks of setting security requirements for "*information systems of vital importance*" (SIIVs) and of seeing to the control of these systems. Their operators have to report incidents on information systems to ANSSI. Under this legal framework, ANSSI will certify service-providers for executing certain tasks required under the regulations (in particular audits and the detection of security incidents). Finally, an omission of compliance with these requirements may be penally sanctioned by a fine of €150,000. Although ANSSI is in the position of an across-the-board regulatory agency in cybersecurity, it cannot preclude the authority that specific ministries and regulatory agencies exercise over the operators of vital importance in their domain of competence. For this reason, ANSSI, these ministries and regulatory agencies are expected to coordinate their actions for an effective articulation of the public policies in their charge.

Despite its lag of nearly ten years as compared with countries that had paid more attention to the cybersecurity needs of their critical infrastructures, France has, thanks to this regulatory framework, become a forerunner in this field.

Enforcing the regulatory framework

Given the potential impact of this new regulatory framework and the need for it to be accepted by operators of vital importance, ANSSI chose to codraft with them the texts to be applied. In 2014 experiments were conducted with a few OIVs; and the following years were devoted to cooperating with work groups by sector for the purpose of drafting rules consistent with the sector's characteristics. Following more than 200 such meetings, decisions were worked out for each sector of vital importance. These decisions contain twenty rules on IT security organized around the following themes: governance, risk management, protection, detection, reaction and crisis management. These rules correspond to a set of good practices, each rule setting a deadline for compliance by the OIVs concerned.

The decrees that have come out of this decision-making process have been enforced in phases:

- on 1 July 2016 in food, the water supply and health products;
- on 1 October 2016 in transportation and energy (apart from nuclear power);
- on 1 January 2017 in finance, electronic communications, the Internet and the manufacturing and audiovisual industries;
- on 1 April 2017 in civilian nuclear energy;
- on 1 October 2017 in the weapons and space industries; and
- on 1 October 2019 in the state's nonmilitary activities.

A plan for cyberemergencies

Article 22 of the aforementioned armed forces program act contains provisions on crisis management: "*To respond to major crises that menace or affect the security of information systems, the Prime Minister may decide which measures the operators [of vital importance…] have to implement.*"

The government adopted Piranet, a plan for managing cyberemergencies and preparing for a situation in which an attack against OIVs would try to incapacitate the nation. Exercises under Piranet at the national level and CyberEurope at the European level are regularly planned to test the preparedness of stakeholders (in particular government services and OIVs). Regulators or operators in the sector also organize exercises. Besides participating in these exercises, ANSSI offers its expert assistance for planning and organizing exercises.

Obtaining compliance

ANSSI had already made headway in its assignments for raising awareness and providing assistance to organizations of vital importance (in particular the victims of cyberattacks) when the armed forces program act was adopted in 2013. As a consequence, some information systems that would be declared SIIVs had already been made secure before the decisions about their sectors were published.

Once published, each decree by sector required that, within three months, the list of SIIVs of each OIV in the sector would be declared to ANSSI. By the end of 2018, more than 1500 SIIVs had been declared, the vast majority of OIVs having done so voluntarily. Till now, no failure to comply has been sanctioned with a fine. Another sign that SIIVs are complying with regulatory requirements is that the order books are full of the service-providers certified to intervene to help make information systems secure.

A major measure — the requirement for detection systems to be certified by ANSSI — was still pending till quite recently due to a lack of service-providers. This barrier was lifted in April 2019 thanks to the certification of the Thales and Gatewatcher probes.

Certifying service-providers

Given the ambit of security works in all SIIVs, the original law foresaw that ANSSI may delegate tasks to private firms. ANSSI's "security visas" program thus provides for two categories: *a)* the firms that audit the security of information systems (in particular the audits required prior to classification as a SIIV) may offer advisory services in SIIV security and perform controls with ANSSI's permission; and *b)* the firms that operate the certified systems for detecting incidents as required under regulations. These service-providers play a key role in implementing France's regulations on the cybersecurity of organizations of vital importance. The creation of these two categories has helped shape the market. By September 2019, there were thirteen certified firms in the first category and four in the second.

An ambitious approach to the cybersecurity of critical installations

The EU directive about "operators of essential services"

Drawing on France's approach, the European Union started, in 2013, work to draft a directive on cybersecurity. Negotiations were concluded by the adoption on 6 July 2016 of the so-called NIS directive on the security of network and information systems.[6] This directive calls for a cybersecurity strategy, for setting up a national authority with competence in this domain and developing the technical capacity for networking. It also requires a setup very close to what France has instituted for organizations of vital importance. During negotiations at the EU level, French authorities were able to preserve and promote their country's approach. The operators who fall under this directive are said to be "*operators of essential services*" (OESs) — essential to the economy or society given the disruption that would result were an "essential" information system to not operate. However the directive's legal grounds are the "*functioning of the internal market*", since national defense and security remain a prerogative of member states.

Nearly all member states have transposed the directive into national law so as to cover cybersecurity without distinction both in the economy and society and in national defense and security. France has chosen to duplicate the arrangements existing in its Defense Code, thus having distinct legal grounds for covering activities complementary to those covered under the armed forces program act. Moreover, it has set high ambitions for transposing the NIS directive. This transposition is not restricted to the essential services listed in the directive's annex; new sectors have been added to this list.

French authorities are currently in the process of classifying operators as OES.

France's approach to international law on critical installations

Based on its experience, France has undertaken two actions in favor of international security and for keeping attacks on information and communications technology (ICT) from destabilizing cyberspace:

- The first action, in 2015, was to advocate a principle of "cyber due diligence". This principle, one of the "*Norms, rules and principles for responsible behavior*" in the report by the competent UN task force provides that: "*States should respond to appropriate requests for assistance by another state whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another state emanating from their territory, taking into account due regard for sovereignty.*"[7] This is consistent with the principle of state sovereignty in cyberspace but with a heavy emphasis on cooperation. It delegitimates interventions that a state that has fallen victim to an attack might make in states that were involuntarily implicated in the

[6] The NIS Directive: Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union available at http://data.europa.eu/eli/dir/2016/1148/oj.

[7] Document A70/174 of 25 July 2015 from the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security available via https://digitallibrary.un.org/record/799853/files/A_70_174-EN.pdf. Also the eight point in the G7 declaration on responsible states behavior in cyberspace in 2017 at https://securityaffairs.co/wordpress/57932/cyber-warfare-2/g7-declaration-responsible-states-behavior-cyberspace.html.

attack — under condition that the latter respond effectively to the victim's requests for cooperation.

- The second action[8] was to adopt a scale for ranking the seriousness of cyberincidents as a function of their real-world effects. The objective is to provide political officials the means for adjusting their response to the gravity of an attack and the subsequent crisis.

This approach, which relies on Anglo-American research, is now the keystone of France's policy of cyberresponsiveness. It is advocated within the Organization for Security and Cooperation in Europe (OSCE) and has been discussed at the United Nations.

Conclusion

The French regulatory framework with its broad vision of the cybersecurity of critical infrastructures has made France a pioneer in this field. Despite this ambitious approach however, regulations still do not cover a few critical systems, *e.g.*, medical devices, driverless vehicles or voting machines. For these systems to take cybersecurity into account, strong cooperation is necessary with authorities in these sectors. The objective will be for them to take account of cybersecurity requirements in line with the approach described by the *Revue stratégique de cyberdefense* in 2018.

[8] Cf. SGDSN (2018) *Revue stratégique de cyberdéfense* of 12 February, 167p., available via http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.