Information & Security: An International Journal

Houssam Zenati, vol.37, 2017, 57-67 https://doi.org/10.11610/isij.3705

THE PERSISTENT NEED TO REFORM CYBER SECURITY SERVICES: A CASE STUDY ON FRANCE

Houssam ZENATI

Abstract: On February 21, 2014, following the terrorist attacks in France, the French prime minister declared that cyber security is a matter of major interest, and national interest of concern to all citizens, and it is important that the government is fully engaged. In the wake of the new challenges raised by terrorism in recent years and the cyber-attacks in Europe, the French Government presented in 2015 a national cybersecurity strategy emphasizing training and international cooperation. France's enhanced participation in the multilateral negotiations on cybersecurity within the UN and the OSCE is an indicator of the necessity of reforming and adapting cyber security services. However, the new French President has emphasized the need to reform further the cyber security services and the urge to master ever-evolving technologies in terms of data collection and cryptology. This article discusses the need to continue the reform of the French intelligence services, and to enhance the cooperation and the speed of innovation in the field cyber security – a general challenge for Western Europe.

Keywords: technology, research, collaborations, legislations, policy, communication

Introduction

Cyberspace is closely related to defense and national security. Likewise, the concerns on cybersecurity ever needs to be considered as technology changes at an ever increasing pace. Indeed, in thirty years, digital technologies have started to take down the boundaries between our personal and professional lives,[1] raised corporate competitiveness to unprecedented levels [1] and even promoted a transparency drive in France’s institution in the wake of the French Presidential elections of 2017 and latest France cabinet reshuffle in June 2017.

The impacts of new technologies by mere citizens have become more visible on France's institution these years. Therefore, the attacks on governments, companies or even violent acts of cybercriminals raise a fortiori greater concerns. Even if they are most of the time only visible to specialist, they can be subject to wide media coverage, especially when it comes to strategic positions for the country or when it comes to terrorism such as the cyberattack carried out on April 2015 at French TV channel TV5 Monde by cybercriminals claimed to be from ISIS.

Besides, more than compromising information related to France's sovereignty[2], cyberspace may become a place for appropriation of personal data, spying on the scientific, economic and commercial assets of companies which fall victim to competitors or foreign powers.[2] It therefore raises tremendous economic concerns for companies, which investments on cybersecurity have increased dramatically for the last years.[3]

Due to the changes in the field of national security and the necessity of reforming cyber security services, the French government decided to provide France in 2009 with the ANSSI [2] (which stands in English for French Network and Information Security Agency). In July 2010, the President decided to make the Agency responsible for the defense of information systems in addition to its security role.

ANSSI now plays in France a major role in strategic decisions and reforms on cyber security. It has identified several areas of work or possible reform, featuring[2]:

- Technology expertise
- Improving research and education
- Joint efforts on cyber security
- International partnerships
- Legislations and communication.

In this article, we discuss the need to reform cyber security services, the need to master technologies and the decision to enhance research and education in the last years. We then give an overview of reforms on cyber security services in terms of collaborations and in terms of legislations and communication.

1. Mastering technology, improving research and education

Reforming the cyber security services relies on adapting to changes, risks and threats that evolve rapidly in cyberspace. The security of information systems can be threatened by ever changing software, products and the development of new technologies or practices.[4] Keeping cyber security services up to date on latest technology development and analyzing the actions of companies, groups, or even states is the first step to ensure the security and defense of information systems and even the interests of a nation.[4]

Mastering Technology through Research

Security of information is based on mastering technology[5] that is both accessible to the security services and to organizations and individuals planning to spoil them. Mastering technology implies to be at the top of research in many fields, and in the case of cyber security, to develop research teams, collaborations, and facilities for research on information system security and cryptology.

Cyber security services responsible for information systems must be tremendously familiar with the latest technologies, and should even be able to foresee technology leaps by laying the foundation to research,[5] thus creating an advantage for the defender over the attacker. France has world-class research teams in the areas of cryptology and formal methods. In other areas, such as security architecture of information systems, it is rapidly catching up with the most advanced nations.

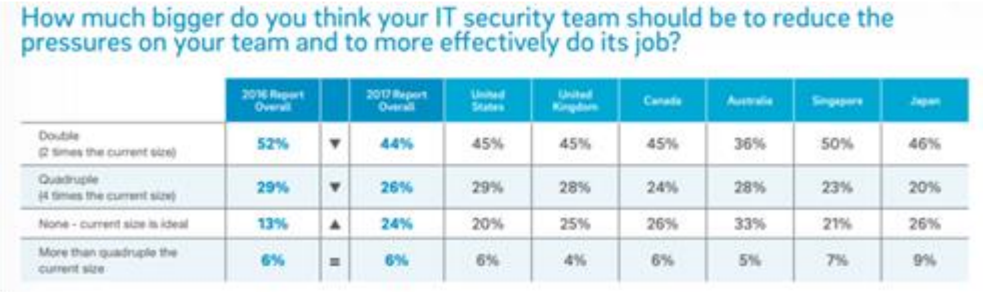
ANSSI (French Network and Information Security Agency) promotes research and supervise teams of scientists who work for them in order to detect and alert on possible security problems, build algorithms or processes to test or break securities. For example, two researchers from ANSSI have been working on injection of voice commands on computers[6] and warned against dangers of pirating voice-based authentication systems, such as Siri from Apple or recent Google now. ANSSI also supervises PhD thesis and multiple scientific articles every month.[7] ANSSI, as the agency for information systems security, concentrates on research and innovation.

Likewise, France is insisting on research in universities in order to promote the mastering of technology. France is creating a cluster of universities and schools in order to promote research and innovation. The University of Paris Saclay gathers top French engineering schools, universities and research centers in order to promote a nationwide collaboration on technology in particular. French top universities create research collaborations on cryptology and on security architecture in order to keep up with the pace of technology’s evolution. CADS is a research group at Paris Saclay which goal is to make scientific advances on data securing.[8]

Mastering Technology through Education

Research and education are generally related, and in the case of cybersecurity, France is deploying considerable means to create trainings, courses and options for students to specialize on it, whether on cryptology for formal mathematics students or on security architecture for computer science students for example.[9] The range of domains in large, and it is said that 50 % of jobs in cybersecurity in France are not filled because of a lack of applicants.[9] Joblessness does not exist in cybersecurity for qualified students in France.[9]

Recent 2017 security pressures report from Trustwave [10] shows top worrying outcomes for enterprises and studies the demand for students and qualified applicants in cyber security jobs, in other countries than France.



How much bigger do you think your IT security team should be to reduce the pressures on your team and to more effectively do its job?

	2016 Report Overall		2017 Report Overall	United States	United Kingdom	Canada	Australia	Singapore	Japan
Double (2 times the current size)	52%	▼	44%	45%	45%	45%	36%	50%	46%
Quadruple (4 times the current size)	29%	▼	26%	29%	28%	24%	28%	23%	20%
None - current size is ideal	13%	▲	24%	20%	25%	26%	33%	21%	26%
More than quadruple the current size	6%	=	6%	6%	4%	6%	5%	7%	9%

Figure 1: Cyber Security demand on countries similar to France (Trustwave 2017 [10]).

Figures are quite the same for NATO allies, showing a need to double or even to quadruple the size of the IT security team. We can assume that France has same global trends for investing in education and for the need to master technology.

Challenges and hackathons are organized in France in order to promote cybersecurity and to inform students on the possibility of creating jobs in that field. Conferences are organized on those topics, with courses and challenges, such as Hack in Paris 2017, a cyber security conference from June 19th to June 23rd, where top international experts come to present courses and remarkable contents for students and interested people.

However, it remains a field that still needs to be promoted, in universities or in top schools, as some great events of technology sometimes do not insist on the need to secure the systems but only present new technologies and the potential they have. Orienting young people towards such jobs will be encouraged in order to expand the expertise available in the country.[2] As a general rule, scientific and technical training on information technology must incorporate courses on information systems security.[2]

Providing cyber Security Services with Technological Structures

New authentication systems have been introduced in ministerial networks,[11] and is adopting the latest smart card technology[11], in which France has an impact on international technology innovations. Governments authorities are being provided with secure interdepartmental intranet,[11] secure messaging,[11] videoconferencing systems [11] which are also being deployed in local administrations.

France has invested in multiple CERT these last years (*Computer Emergency Response Team*) and CSIRT (*Computer Security Incident Response Team*) which missions are:[12]

- Centralization of requests for assistance following security incidents
- Processing of alerts and responses to computer attacks
- Exchange of information with other CERTs
- Establishment and maintenance of a vulnerability database
- Possible coordination with other technical structures.

Those centers are equipped with great technologies and are located throughout France. Those centers are headed by either public or private actors.

2. Developing the Co-operations on Cyber Security

The dependence of companies, infrastructures and services on the Internet is increasing, it is therefore crucial to be able to detect and attacks as soon as possible and offer assistance to victims. French White Paper on Defense and National Security [4] organizes the development of detection facilities which can countermeasure the attacks and assist the defenders. However, monitoring mechanisms in not enough to manage the work, information provided by partners are needed, on order to have a current statement of the network situation whether it is at a nationwide scale, or at more global scale.[13]

Besides, in order to deal with crises or threats to the security, the sharing of strategic information and knowhow is precious for security of information systems. Reforming the cyber security services therefore relies on developing more collaborations at a different scale. Those collaborations can be at a public-private scale or at a worldwide scale.

Developing Public-Private Co-operations

Public-private partnerships are being set up in France [4] and in Europe,[14] as regards to the security of the information systems of operators of critical infrastructures raise major concerns. Operators can take advantage from information gathered on their own information system security, and the threat analysis from operators can benefit the state to protect what is necessary for the nation.

Possibilities of creating a cyber defense research center in collaboration with industrial partners are being examined.[11] This center would carry out scientific research activities (cryptology studies, analysis of attacking groups and their methods, expertise on malware and software flaws, development of secure open source software, drafting of cyber defense concepts, etc.).

Issues on cyber security relating to both public structures and private companies must be addressed through broad common research projects leading to synthesis and collaborations on effective knowhow to deal with security on information systems.[15] France has created in 2015 the label « France Cybersecurity » that is governed by a structure composed of representatives of users, private industrials and competent State services, in order to promote French knowhow on cybersecurity and developing collaborations.[16]

Developing International Intelligence Services Collaborations

The need for international oversight of multilateral intelligence collaboration and the issues at hand have been cited many times in a range of intelligence publications. Multilateral intelligence collaboration can bring a new light to global problems because it is difficult to effectively cover all the areas of interest that each country intelligence collection requirements demand.[17] By collaborating on areas of cyber security amongst partner nations, France can develop better solutions to security concerns.

Cyber security depends considerably on data exchange between intelligent services of allied countries. France has sought those last years to establish wide network of foreign partners, which mainly remain the partners from EU and NATO.[4] Concerning classified information, the French strategy has been redefined. It takes full account of France joining NATO integrated command.[4] It enables the collaboration on essential data which creates deep operational exchanges.

However, those collaborations still need to be developed because of influences that limit the nature and extent of intelligence co-operation explained by experts:[18]

- Differences on perceptions of a threat and on foreign policies
- Asymmetrical power relations between states
- Differences in legislations
- Abuse or misuse of intelligence that has been shared.

These general factors help to highlight the need for governance and oversight in French intelligence collaboration.

Developing International Co-operations on Scientific Research that Benefits the Intelligence Services

Likewise, the collaboration of cyber security services relies on collaboration on research. Here we give some examples of France's collaboration on technology research, notably on cyber security.

In Europe, Horizon 2020 is an unprecedented initiative and is biggest EU Research and Innovation program ever with nearly €80 billion of funding available over 7 years (2014 to 2020). This research program promises more breakthroughs, discoveries and world-firsts by creating cooperation between labs and markets. It also includes massive research on security and cyberspaces, for which it explains:[19] "Research and innovation activities should aim at understanding, detecting, preventing, deterring, preparing and protecting against security threats." The cyber security services can therefore benefit from a large technology and research program.

The EU Framework Program for Research and Innovation will be complemented by further measures to complete and further develop the European Research Area.[20] These measures will aim at breaking down barriers to create a genuine single market for knowledge, research and innovation, and it will be a unified area open to the world, in which scientific knowledge, technology and researchers circulate freely.

France is also developing research partnerships with leading countries on cybersecurity. Following to the true success and interest issued from workshops held in Tokyo last years, the collaboration between French and Japanese researchers on cybersecurity has been strengthened:[21] this year the third great meeting on French-Japanese collaboration on cybersecurity was held in Tokyo on April. Partnerships with the US also exists, notably between French CNRS, INRIA and GeorgiaTech University,[22] and currently aim at developing transatlantic innovation and strategies on cybersecurity.

France also has academic partnerships with NATO allies and countries from all over the world. Those partnerships lead to further education and eventually possible research collaboration between universities and research centers, on the topic of cryptology, cyber security, technology and policy programs… Those collaborations also have impacts on mastering the knowhow and technology which is necessary for reforming the cyber security services.

3. Reforming the Legislation and Communication

Reforming the cyber security services also implies to reform its legislations, its communication and sometimes to change general legislations. Those reforms often are correlated with great events such as changing governments, terrorist attacks or cyber-attacks and depend greatly on political views.

Reforming the Cyber Security Services Structure and Legislation

NSA scandal broke in early June 2013 when the Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans, and NSA was also accused of spying on European governments such as Germany or France. There is no denying that intelligent services in the world face more challenges to keep up with technological challenges that cybercriminals raise and to ensure full compliance with the law.

The legal tussle between Apple and the U.S. Federal Bureau of Investigation (FBI) over access to the iPhone used by a shooter in 2015 San Bernardino attacks has been largely covered by media in 2016 but the debate between technology firms and law enforcement authorities over data privacy and access remains. After the cyberattack WannaCry on May 2017, governments have strengthened their legislations, and now keep realizing the importance of cybersecurity. China has adopted new measures which aim at imposing more control on personal data transfers from China to other countries. Such decisions have huge impacts on companies, which also have to adapt to the changing economic and legislative context.

Reforming the cyber security services structure and legislation is a necessity. New practices introduced through the development of cyberspace can threaten the functioning of critical nation infrastructures and the stability of companies. If not enough attention is paid, it can also deteriorate individual freedoms. The legislative and law framework must adapt to new practices and developments in technology.[4] Laws are reviewed as new technologies and new practices emerge, knowing that the reforms are launched in order to strengthen the security of individuals and companies.

In France, during the presidential elections campaign, Emmanuel Macron announced that he would oblige the “highly encrypted instant messaging” to give the encryption keys to the authorities fighting terrorism. Such an obligation would change dramatically the legislation for companies.

The “cyber security” directive SRI (Network and Information Security) and the RGPD (General Data Protection Regulation) now have a certain impact on companies of all sizes within the EU.[23] Laws voted seek to standardize the rules on information security and data protection between member states of EU, with the aim of increasing protection and reducing the number of data leaks from which they are victims. Data collected should be used by research centers to ensure greater security. Likewise, France has voted in 2013 a bill called *Loi de programmation militaire* [24] and has been implemented since 2015. This law forces companies to set up specific infrastructures, undergo checks and report serious incidents to the National Agency for Information Systems Security (ANSSI).

Reforming the Communication and Information

Legislative reforms need technical expertise and also research studies, because often the reforms proposed would weaken the security for users (and a fortiori for the companies) if adopted. End to end encryption[25] for instant messaging that E. Macron wanted to restrict may cause a weaker security for all users.[25,26] Reforming the legislation or interacting with companies on encryption and technology therefore needs experts, and should thus include discussion with research capabilities.

Reforming the communication on cyber security relies on the fact that security of information needs personal vigilance from the users, as well as from people in companies, but also depends on choices and technical measures taken in order to insure the security.

However, ANSSI (French Network and Information Security Agency) states that communication and information on cyber security concerns remain insufficient.[2]

ANSSI has created the website CYBERMALVEILLANCE.GOUV.FR which aims at raising awareness on both companies and personal users on security concerns.[27] It is a structure devoted to alert on the issues surrounding the protection of digital privacy. With the collection of numerous statistics, an observatory will be created in order to anticipate the numerical risk. Following major attacks such as the ransomware WannaCry of May 2017 it has released articles on ransomwares, short videos explaining how to avoid being attacked, but it also releases articles on others topics, in order to anticipate and prevent similar problems.

In France, ANSSI will provide support to decision-makers to help them make decisions about the security of information systems essential to the performance of their organizations and the protection of their technical, scientific, commercial and financial assets. It will also conduct communication campaigns targeting the general public.[2]

Conclusion

In this paper we aimed to give an overview of the ever necessity to reform cyber security services, given the increasing pace of technology changes and security challenges. Among the major threats that France will have to face over the next fifteen years, the 2008 French White Paper on Defense and National Security cited large-scale cyberattacks on national infrastructures. This statement is still accurate and still justifies the reforms in the law, in cyber security structures and in the technology centers.

The need to reform the cyber security in France can be understood through the ever changing technological challenges, which raise research and education concerns, but also the need to develop new collaborations in order to manage to deal with cyber security concerns. Therefore, reforming the cyber security services is not only about reforming the intelligence services, it has to do with transforming a large area of industry, of public services and even sets of mind in companies in France. The cybersecurity awareness starts to grow, and it may ever grow with new challenges and new technical issues that engineers, specialists, and researchers have to deal with.

Last but not least, we may expect major changes and reforms in France cyber security services following to the new government formed by fresh political party led by E. Macron and following to majority seats won by E. Macron's political party in legislatives elections few weeks ago. Technologies and information systems have now become part of France's priorities for the next years, including the priority to safeguard the security of citizens, companies and French nation in cyberspace.

Acknowledgement

We would like to show our gratitude to Prof. Minko Balkanski for sharing his pearls of wisdom on cryptology and cybersecurity awareness during the course of few discussions, it has inspired this research.

Endnotes:

[1] *French White Paper on Defense and National Security*, 2008

[2] ANSSI, "2016 Annual Report," 2017

[3] Steve Morgan, "Cybersecurity Market Report," Cybersecurity Ventures, 2017.

[4] *French White Paper on Defense and National Security*, 2013.

[5] Douglas Maughan, "The need for a national cybersecurity research and development agenda," *Communications of the ACM* 53, no. 2 (February 2010): 29–31.

[6] José Lopes Esteves and Chaouki Kasmi, " Injection de commandes vocales sur ordiphone, " 2015.

[7] "Les laboratoires de l'ANSSI contribuent à la recherche ouverte en matière de sécurité des systèmes d'information par la publication de leurs résultats dans les revues et conférences du domaine," 2016, https://www.ssi.gouv.fr/agence/rayonnement-scientifique/publications-scientifiques/.

[8] Universite Paris-Saclay, https://www.universite-paris-saclay.fr/frecherche.

[9] " La France booste la cybersécurité, " *Le Parisien*, 2016.

[10] "Security Pressure Report, " *Trustwave*, 2017.

[11] ANSSI, "Information systems, defense and security - France's strategy," 2011.

[12] ANSSI Cybersecurity in France, ISS in France, French CERTS, 2016, https://www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/les-cert-francais/.

[13] Janine McGruddy, "Multilateral Intelligence Collaboration and International Oversight," *Journal of Strategic Security* 6, no. 3 (2013): 214-220.

[14] European Union, "Archived by Publications Office of the European Union," September 24, 2016, https://ec.europa.eu/digital-single-market/en/cybersecurity-industry.

[15] Judith H. Germano, *Cybersecurity Partnerships: A New Era of Public-Private Collaboration* (NYU School of Law, 2014).

[16] Label France CyberSecurity, *Catalogue 2017 des offres labélisées*, 2017.

[17] Musa Tuzuner, *Intelligence cooperation practices in the 21st century: towards a culture of sharing* (Washington, D.C.: IOS Press, 2010), 150.

[18] Stéphane Lefebvre, "The Difficulties and Dilemmas of International Intelligence Cooperation," *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (2003): 527-542.

[19] Ministère de L'enseignement Superieur, "Description du programme Horizon 2020," 2013, http://www.horizon2020.gouv.fr/cid73300/comprendre-horizon-2020.html

[20] European Commission, "Research and innovation," 2016, http://ec.europa.eu/research/era/index_en.htm.

[21] "Joint collaboration between France and Japan on Cybersecurity Research," *Cybersecurity France-Japan*, 2015, https://project.inria.fr/FranceJapanICST/fr/.

[22] France Embassy at Atlanta website, "France-Atlanta 2016 brings French-American focus on cybersecurity," 2016.

[23] Thierry Karsenti, "Cybersécurité : comment se préparer à la nouvelle législation de l'union européenne?" *Economie Matin*, 23 décembre 2015.

[24] ANSSI, "Cybersécurité et loi de Programmation Militaire: Préparation des Règles de Sécurité," 2015, https://www.ssi.gouv.fr/actualite/cybersecurite-et-loi-de-programmation-militaire-preparation-des-regles-de-securite/.

[25] Iresh A. Dhotre, *Cryptography & Security Network* (Technical Publications Pune, 2008).

[26] Matt Bishop, *Computer Security Art and Science* (Pearson Education Inc., 2003).

[27] "Assistance et Prévention du Risque Numérique au Service des Publics," Cyber Malveillance, 2015, https://www.cybermalveillance.gouv.fr/.

About the Author

Houssam Zenati is currently pursuing a Master degree in Engineering Sciences at *CentraleSupelec* (*Ecole Centrale Paris*), in the field of applied mathematics and computer science. His research interests are in the field of data science, artificial intelligence, cybersecurity, cryptology, but also cybersecurity awareness, education and research in France. He is involved in volunteering associations that help international and local students studying mathematics at *CentraleSupelec*, but also in teaching structures fostering new standards of success through a deep commitment to society's needs for students from diverse backgrounds and under-represented minorities.