CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Pascal Brangetto

National Cyber Security Organisation: France

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in Italy

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Upcoming in 2015

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of March 2015.

About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations and Austria as a Contributing Participant. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

FRANCE

By Pascal Brangetto
Researcher, NATO CCD COE

Table of Contents

1. Introduction: information society in France

1.1. Infrastructure availability and take-up

The increasing availability and affordability of the internet has modified the behavioural patterns of French citizens and consumers, but has also made the French economy highly dependent on information and communication technologies. While French society and the internet have not reached levels of integration as high as countries such as the United States or United Kingdom, the information technology sector is slowly solidifying its importance to the service-oriented French economy, representing over 4.5% of GDP in 2012.[12] In real terms, total revenue from the electronic communications sector in France exceeded €50 billion in 2012, the third largest across the EU.[3]

Internet penetration in France as of 2013 was well above the EU average, with 78% of households and 98% of enterprises holding fixed broadband subscriptions. Considering that 100% of France is covered by existing fixed broadband infrastructure with subscriptions increasing at an annual uptake rate of 38.17 per 100 people, the country has the potential to connect the entire population in the near future.[4] Of those fixed broadband subscribers, 98% have access to a minimum speed of 2 Mbps,[5] while a further 91%, 8%, and 5%, have access to minimum speeds of 10 Mbps, 30 Mbps, and 100 Mbps respectively.[6] Only those subscribers accessing 30 Mbps fall short of the EU average, while the remaining speed metrics exceed the majority of other EU fixed broadband subscriber indicators.

Similarly, France has strong mobile data coverage, with advanced 3G mobile broadband reaching 97% of households with 111 mobile broadband subscriptions per 100 people.[7] Although 66% of the French population are considered frequent internet users accessing the internet once or more a day, only 28% (2012) of mobile subscribers use their devices to access the internet.[8] However, this figure is still well above the EU average of 18% (2012).[9]

The impressive growth of France's digital economy and information and communication infrastructure is in large part the result of the government's Future Investments Programme (*Investissements d'Avenir*, FIP),[10] launched in 2010, comprising an initial €35 billion pool for government investment in technology and industrial projects, which was followed up with an additional €12 billion in 2013. Substantial FIP investments directed toward the digital economy have already made substantial progress towards empowering France's information society goals, allocating €69 million to cloud computing research, €83 million to 'smart grid' projects, and €70 million to develop high-speed (30 Mbps) broadband internet satellites.[11]

---

[1] 'France Selected Issues Paper', IMF Country Report, No. 13/252, Washington D.C.: IMF, 2013, 9 <http://www.imf.org/external/pubs/ft/scr/2013/cr13252.pdf>.

[2] This regards only the 'Internet sector' and does not comprise the indirect activities that rely on Internet such as retailing. For a thorough study, see 'L'impact d'Internet sur l'économie française' ('Comment Internet Transforme Notre Pays'), McKinsey & Company, 2011 <http://www.observatoire-du-numerique.fr/wp-content/uploads/2013/02/2011-mckinsey-company-impact-dinternet-sur-l%C3%A9conomie-fran%C3%A7aise.pdf>.

[3] Unless explicitly stated otherwise, the statistics in this section are taken from the EU Digital Agenda Scoreboard for France: EU Digital Agenda, 'Analyse one indicator and compare countries', 2013 <http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-countries#>, see 'Total Revenues of the Electronic Communications Sector'.

[4] ibid, 'Broadband Take-up and Coverage'.

[5] This speed is considered to be the minimum to be considered as high speed internet in France.

[6] EU Digital Agenda (n 3) 'Broadband Speeds and Prices'.

[7] ibid, 'Mobile Market'.

[8] ibid.

[9] ibid.

[10] 'Programme d'investissements d'avenir – situation et perspectives', Commissariat général à l'investissement (CGI), 2014 <http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2014/11/rapport_cgi.pdf>.

[11] ibid 45-46.

The additional pool has specifically allocated funds under the Public Networks Initiative to support the France Very High Speed (*France Très Haut Débit*) Plan,[12] which was launched in February 2013 for the purpose of ensuring that, by 2022, the entire country will have access to fixed and wireless broadband connectivity of no less than 30 Mbps with 80% of homes supported by fibre optic lines. Additionally, the France Very High Speed Plan is actively working towards comprehensive 4G mobile networks, utilising substantial infrastructure upgrades, as well as installing terrestrial repeaters and next generation satellites to support public internet subscriptions.

1.2. E-government and private sector e-services

1.2.1. E-government

France has historically relied on a significant public workforce in order to make public services function. Since 2010, policies have been implemented to render the state's activities more efficient and productive (General Review of Public Policy Reform);[13] one of the main tasks of this public policy reform was to prioritise digital administration, envisioned as a better experience for users of public services. To this end, the state portal (*servicepublic.fr*) has served as the central hub for French citizens to access e-government publications and services.

According to Eurostat, the European Commission's statistics office, in 2013, 60% of the French population had used the internet to gain access to a public service (tax revenue, social benefits, administrative documents requests, etc.).[14] As an example, almost 30% of tax revenue tax reports were submitted through online services in France in 2013.[15]

1.2.2. E-commerce and digital economy

The internet has empowered consumers to become more decisive in the consuming process, at the same time enabling net-retail companies to increase their gains of productivity.[16] This phenomenon can be observed in France as these services are widely used today. Tremendous changes have taken place, reflecting the increasing footprint of digitisation on the economy. As pointed out in a report from January 2012, 80% of the economy relies on or is concerned with information networks or IT-services to support their activities, whether part of their core-activities or as a supporting infrastructure.[17]

In this light, the FIP, beyond innovation and infrastructure support, has set aside €1.4 billion for direct investment in to the 'digital economy,' and €300 million as part of a mutual fund to support the growth of SMEs in the IT sector.[18] [19] France's online economy is strong but not overly thriving. Although in 2013, 59% of

[12] France Trés Haut Débit, 'Comprendre le Plan France Très Haut Débit' <http://www.francethd.fr/comprendre-le-plan-france-tres-haut-debit/>.
[13] Marianne Bondaz et al, 'Bilan de la révision générale des politiques publiques et conditions de reussite d'Une nouvelle politique de reforme de l'Etat, 2012' <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/124000520/0000.pdf>.
[14] EU Digital Agenda, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard', 2013 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"egovernment","ref-area":"FR","time-period":"2013"}>.
[15] Le portail de l'Économie et des Finances, 'Impôt sur le revenu : les télédéclarations progressent de près de 6%'. <http://www.economie.gouv.fr/teledeclarations-progressent>. Of the 36.7 million tax revenue submissions, 13.5 million were done online.
[16] Alternatives économiques, 'La nouvelle société de consommation', n° 331, 2014 <http://www.alternatives-economiques.fr/la-nouvelle-societe-de-consommation_fr_art_1268_66464.html>.
[17] A report issued by the Inspection générale des finances-IGF (Auditing body of the ministry of Economy) in 2012 has given a thorough insight of the weight of digital economy in France. Report number 2011-M-060-02 issued in January 2012 regarding the support to the digitised economy and innovation. Inspection générale des finances (IGF), 'Le soutien a l'Économie numérique et a l'Innovation', n° 2011-M-060-02, 2012 <http://www.igf.finances.gouv.fr/webdav/site/igf/shared/Nos_Rapports/documents/2012/2011-M-060-02.pdf>.
[18] ibid.

the French population had ordered goods and services online, only 18% of online shoppers engaged in cross-border transactions, which, given the French economy and internet infrastructure, is low in comparison to other EU member states.[20] However, online retail services still represent a significant volume: €53 billion were actually spent in 2012, making France the sixth country for e-retail services.[21] Notably, the low rate of e-commerce turnover among domestic large enterprises (18%) and SMEs (10%)[22] in 2013 might suggest that the digital economy in France has not radically altered consumer practices. However, it is widely used – in 2013, 70% of the population reported having recently used the service.[23]

Even though its economy is now increasingly driven by the dynamics of the internet, France still has some work to do to improve access to high speed broadband and to promote the use of the internet among the population, whether accessing public or private services. France is deemed by the IGF to be an intermediate country regarding its global position in the world's digital economy.[24]

Public authorities have sought to address France's dependence on ICT. In the midst of the re-industrialisation of the country, the French Minister of Economy launched 34 projects to 'reconquer industrial France'[25] in September 2013. Among these projects is one aiming at developing cyber security in France with a proposed plan to come up with new and innovative industrial programmes.[26] This programme was placed under the lead of the director of the National Information Systems Security Authority.

2. Strategic national cyber security objectives

Since 2008, France has drafted three high-level policy documents, which serve as a comprehensive strategy in regard to cyberspace:

- White Paper on National Defence and Security of 2008;[27]
- France's Cyber Strategy 2011; [28] and
- White Paper on National Defence and Security of 2013.[29]

As a matter of national security, cyberspace and cyber security were first considered in the White Paper on Defence and National Security (*Livre blanc sur la défense et la sécurité nationale*) released in 2008. This official document is the first to acknowledge cyber threats as major threats, citing attempted attacks by non-state actors, hackers, hacktivists or criminal organisations.[30] The White Paper outlines a number of actions that should be undertaken in order to properly address and tackle these threats, including development of system

[19] ibid.
[20] EU Digital Agenda Scoreboard (n 3) 'eCommerce'.
[21] Institut national de la statistique et des études économiques, 'Le commerce électronique en 2012' <http://www.insee.fr/fr/themes/document.asp?reg_id=0&ref_id=ip1489>.
[22] EU Digital Agenda Scoreboard (n 3) 'eCommerce'.
[23] EU Digital Agenda (n 14) 'Internet services'.
[24] 'Le soutien a l'Économie numérique et a l'Innovation' (n 17). This benchmarking process has assessed every aspect of the digital economy ecosystem (environment, innovation, human resources, size of private companies). In most of these rankings, France remains in the intermediate section.
[25] Le Gouvernement, 'La nouvelle France industrielle. Présentation des feuilles de route des 34 plans de la nouvelle France industrielle' <http://www.economie.gouv.fr/files/files/PDF/nouvelle-france-industrielle-sept-2014.pdf>.
[26] Le portail de l'Économie et des Finances, 'A la une' <www.redressement-productif.gouv.fr>.
[27] Jean-Claude Mallet, 'Défense et Sécurité nationale: le Livre blanc', 2008 <http://www.ladocumentationfrancaise.fr/rapports-publics/084000341/>.
[28] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 'Défense et sécurité des systèmes d'information. Stratégie de la France', 2011 <http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf>. English text available at <http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf>.
[29] French Government, 'French White Paper on National Defence and Security', 2013 <http://www.rpfrance-otan.org/IMG/pdf/White_paper_on_defense_2013.pdf>.
[30] 'Défense et Sécurité nationale : le Livre blanc' (n 27).

resiliency and capacity building for cyber conflicts, which constituted the first steps in a strategic shift, placing cyberspace into the context of national security. The Bockel Report,[31] drafted by the French Senate in 2011, evaluated the accomplishments that France has made in addressing cyber-related issues since the 2008 White Paper. Even though the report laments France's poor definitional and political approaches towards cyber defence policy, the work notes that the creation in 2009 of the National Network and Information Security Agency (ANSSI) under the Prime Minister and the Secretary General for Defence and National Security (SGDSN), as the central coordinating authority for cyber security in the French government, was an important step.[32]

One of the tasks given to the ANSSI under the supervision of the SGDSN was to draft a cyber security strategy. The strategy was issued in February 2011 and titled 'Information systems defence and security, France's strategy.' In it, four major objectives are identified:[33]

- Become a world power in cyber defence;
- Safeguard France's ability to make decisions through the protection of information related to its sovereignty;
- Strengthen the cyber security of critical national infrastructures; and
- Ensure security in cyberspace.

It is clear that France has emphasised the protection of national informational assets and critical infrastructures as its main focus points.

In 2012, President François Hollande urged a reinterpretation of France's cyber posture, emphasising the financial constraints and geopolitical challenges, which subsequently prompted a new White Paper on National Defence and Security in 2013.[34]

The 2013 White Paper underlines the effort that needs to be made to achieve a secure cyberspace and calls for resources to be dedicated to this domain. Importantly, it clearly states that the development of offensive cyber capabilities are a part of the French cyber defence strategy.[35]

As another guiding document, a Cyber Defence Pact (*pacte défense cyber*)[36] was presented on February 7th 2014 by the Minister of Defence.[37] It emphasises the latest objectives drafted following the White Paper of 2013 and the Military Planning Act (*loi de programmation militaire* 2014-2019, LPM) in December 2013.[38] The Pact revolves around 6 axes:

---

[31] Par M. Jean-Marie Bockel, 'Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense', n° 681 (Sénat session extraordinaire de 2011-2012), 18 juillet 2012 <http://www.senat.fr/rap/r11-681/r11-681.html> (Bockel report).

[32] Decree n° 2009-834 of 7 July 2009 creating the National Agency for the Security of the Information Systems. Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé 'Agence nationale de la sécurité des systèmes d'information'', 2009 <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212>.

[33] Patrice Tromparent, 'French cyberdefence policy', 79. In C. Czosseck et al (Eds.), 4th 'International Conference On Cyber Conflict. Proceedings 2012', Tallinn: CCD COE Publications, 2012.

[34] 'French White Paper on National Defence and Security' (n 29) 43.

[35] France will develop an approach based on a cyber-defence organisation closely integrated with the armed forces, made up of defensive and offensive capacities to prepare or support military operations. ibid, 72.

[36] Ministère de la Défense, 'Pacte Défense Cyber. 50 mesures pour changer d'échelle', 2014 <http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf>.

[37] Ministère de la Défense, 'Présentation du Pacte Défense', 2014 <http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber>.

[38] Law 2013-1168 of 18 December 2013 on the military planning for the years 2014 to 2019 and containing various provisions relating to defense and national security often referred to as the Military Planning Act (LPM), this law provides for substantial modifications in the Defence Code which is the collection of all the legal provisions pertaining to the matters of national defence in France. Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale', 2013

1. **Strengthening the security of information systems** by reinforcing the security level of the information systems as well as the defence and intervention assets of the Ministry and its major trusted partners;
2. **Augmenting cyber security research** by preparing the future through an intensification of the research efforts in the technical, academic and operational domains, while supporting France's industrial basis;
3. **Education and training**, thereby reinforcing the manpower dedicated to cyber defence and developing the associated career paths;
4. **Developing the cyber defence centre** in Brittany for the Ministry of Defence and the national cyber defence community;
5. **Furthering international cooperation** by keeping up a network of foreign partners, in Europe, within the Atlantic Alliance or in areas of strategic interest; and
6. **Furthering the emergence of a national cyber defence community**, relying on a group of partners and on the reserve's networks.[39]

In regard to international cooperation, France is a strong advocate of a stronger link between NATO and the EU in terms of cooperation. France envisions this potential cooperation as mutually beneficial: both organisations might profit from each other's skills and experiences since their areas of focus are different. France differentiates between cyber security (economic and CII) and cyber defence (military and intelligence) when it comes to prioritising cooperation with NATO and the EU. NATO is mentioned specifically in the Cyber Defence Pact, while the EU is not. However, economic and industrial cyber security standards are favoured to be discussed within the EU framework.

3. National organisational structure for cyber security and cyber defence

3.1. Cyber security policy coordination

Since the modification of the Defence Code in 2013,[40] the Prime Minister conducts the French cyber security policy and sets out the rules regarding the enforcement of the security of the information systems.[41]

The decree creating the ANSSI also extends the overall management of cyber security policy in France to the **Information Systems Security Strategic Committee** (*comité stratégique de la sécurité des systèmes d'information*). Under the supervision of the **Secretary General for Defence and National Security** (*secrétariat général de la défense et de la sécurité nationale;* SGDSN), this committee coordinates and implements measures pertaining to the security of information systems.

In addition to the SGDSN, the Committee includes:

- the Joint Chief of Staff (*Etat-major des armées*);
- the General Secretary of the Ministry of Home Affairs (*Ministère de l'intérieur, de l'outre-mer et des collectivités territoriales*);
- the General Secretary of the Ministry of Foreign Affairs (*Ministère des affaires étrangères et européennes*);
- the Director of the Defence Procurement Agency (*Direction générale de l'armement*);

<http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id> (Military Planning Act).

[39] 'Pacte Défense Cyber. 50 mesures pour changer d'échelle' (n 36).

[40] Military Planning Act (n 38).

[41] Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article L.1332- 6-1', <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=2A19E78A79324EAE15BA68EC963C8968.tpdjo09v_2?idSectionTA=LEGISCTA000028342651&cidTexte=LEGITEXT000006071307&dateTexte=20140401>.

- the director of the External Intelligence Directorate (*Direction générale de la sécurité extérieure*);
- the Director of the Defence information and communication systems (*Direction générale des systèmes d'information et de communication*);
- the interdepartmental Director of the State's information and communication systems (*Direction interministérielle des systèmes d'information et de communication de l'Etat*);
- the interdepartmental Director for the modernisation of public policies (*Direction interministérielle pour la modernisation de l'action publique*);
- the Director of the Internal Intelligence Directorate (*Direction générale du renseignement intérieur*);
- the co-chair of the National Council on Economy, Industry, Energy and Technology (*Conseil général de l'économie, de l'industrie, de l'énergie et des technologies*);
- the Director of the ANSSI.

The list of the main actors in charge of cyber security shows the global footprint of cyber security among French authorities.

The SGDSN is in charge of assisting the Prime Minister with respect to all domestic and external security policy.[42] Among his missions, the SGDSN *'proposes to the Prime Minister and implements the Government's policy regarding the security of information systems. To that end, it has at its disposal an agency with national authority named Network and Information Security Agency'.*[43]

3.2. Policy implementation and incident response coordination

Under the subordination of the Prime Minister and the SGDSN, the **National Network and Information Systems Security Agency** (Agence nationale de sécurité des systèmes d'information; ANSSI) is an interministerial organisation in charge of coordinating the national effort regarding the security of information systems.[44]

ANSSI is the main entity in charge of cyber security in France. As the national authority in respect of information system security, ANSSI has tasks towards different entities. ANSSI sets the government electronic security standards to be implemented in communications systems, conducts audits of sensitive governmental information security infrastructure, detects and coordinates proper reactions to cyber incidents, develops international cooperation, and trains the personnel of the administration.

In relation to security providers, ANSSI has a mission to conduct and perform electronic signature certification and the certification of security solutions provided on the French market. ANSSI also authorises cryptography services.

In the area of electronic communications, ANSSI provides advice to the Ministry of Communications concerning the integrity of public networks and advises Ministers who have oversight of French critical infrastructure sectors.

Additionally, the ANSSI hosts the **Operational Centre for the Security of Information Systems** (*Centre* opérationnel de la sécurité des systèmes d'information; COSSI), whose mission is to detect and mitigate attacks directed at the state's information systems designated as critical infrastructure. The COSSI hosts the French **CERT** (Computer Emergency Response Team),[45] which provides in-depth analyses of identified vulnerabilities

[42] The legal provisions regarding the SGDSN can be found here: Secrétariat general de la defense et de la sécurité nationale, 'Textes concernant le SGDSN' <http://www.sgdsn.gouv.fr/site_rubrique58.html>.
[43] Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article R-1132-3 § 7',
<http://www.legifrance.gouv.fr/affichCode.do;jsessionid=2A19E78A79324EAE15BA68EC963C8968.tpdjo09v_2?idSectionTA=LEGISCTA000028342651&cidTexte=LEGITEXT000006071307&dateTexte=20140401>.
[44] 'Décret n° 2009-834 du 7 juillet 2009' (n 32).
[45] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 'CERT-FR. Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques' <http://www.cert.ssi.gouv.fr/>.

and malicious code, as well as alerts for incidents reaching a potential threshold of an attack. It also regularly takes part in investigations as an auxiliary of the justice system and it can assist law enforcement authorities during investigations. In 2012, it issued 766 advices, 10 alerts and 52 news bulletins.[46]

As part of its mission to protect, the ANSSI has been granted the right to have access to certain personal data handled by internet service providers (ISPs) in order to warn certain operators regarding the vulnerabilities present or detected in their systems. [47]

In 2009 when it was created, the ANSSI numbered 120 personnel; under the goals of the Cyber Defence Pact[48] the objective is to reach 500 by the end of 2015.[49] The ANSSI's budget has also increased from €45 million in 2009 to €75 million in 2012, with €55 million for investment and €20 million for personnel costs, but it still falls short of its envisaged budget of €90 million.[50] The Senate report on the 2014 Budget Act shows that these figures are yet to improve as the investment budget (personnel cost aside) is set around €60 million per year until 2015.[51]

3.3. Military cyber defence

3.3.1. Ministry of Defence

The French **Ministry of Defence** (FR-MoD) is in charge of the defence of its networks and information systems. One of the major objectives of the French strategy is to be able to guarantee, at any time, 'information sovereignty' (i.e. to preserve the capacity to make decisions based on reliable information) and to safeguard the integrity of the French national defence systems. The potential impact of cyber incidents on military capabilities was experienced first-hand in 2009 when the Conficker worm infected French naval systems, and as a result, Rafale jet fighters were grounded until the vulnerabilities could be resolved.[52]

For these reasons, the French Ministry of Defence has devoted substantial energy to incorporating cyber defence planning into the functions of the **French Joint Chief of Staff** as it is outlined in the classified French *Cyber Defence Joint Doctrine* (*DIAdoctrine interarmées,* 3.40_Cyber-3). Particularly, the *Cyber Defence Cell*, whose head (Officer General Cyber, OG cyber) also serves as the head of the French cyber operational command. Notably, the FR-MoD extends operational control to cyber capabilities through the J6 Staff at the theatre level, as well as tactical units directly subordinate to the cyber defence department of the Joint Chief of Staffs.

The French cyber operational command has the following tasks:

- coordinate cyber defence efforts within the ministry of defence; and

[46] Par MM. Jacques Berthou et M. Jean-Marie Bockel, 'Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de loi de finances pour 2014', n° 158 (Sénat session extraordinaire de 2013-2014), 21 novembre 2013 <http://www.senat.fr/rap/a13-158-12/a13-158-121.pdf>.
[47] This provision was added with the 2013 Military Planning Act. Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article L.2321-3', <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=2A19E78A79324EAE15BA68EC963C8968.tpdjo09v_2?idSectionTA=LEGISCTA000028342651&cidTexte=LEGITEXT000006071307&dateTexte=20140401>.
[48] 'Code de la defense. En savoir plus sur cet article R-1132-3 § 7 ' (n 43).
[49] Xavier Biseul, 'Cyberdéfense : l'Anssi recrutera 150 experts d'ici fin 2015', 01Business, 2013 <http://pro.01net.com/editorial/604366/cyberdefense-l-anssi-recrutera-150-experts-d-ici-fin-2015/>.
[50] Bockel Report (n 31) 83.
[51] 'Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de loi de finances pour 2014 (n 46).
[52] Kim Willsher, 'French fighter planes grounded by computer virus', The Telegraph, 2009 <http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html>.

– plan and command cyber operations within the *Planning and Operations Centre*[53] located at the French Joint Staff. These operations consist mainly but not only of defensive cyber operations.[54]

OG cyber has also a functional responsibility to all the bodies of the Ministry regarding military cyber defence.

The **Defence Procurement Agency** (*Direction Générale à l'Armement*; DGA) also has a key role to play in French cyber defence strategy. The Information Assurance Division of the DGA (DGA/MI) is a prominent element, as it is in charge of conceiving secure weapon systems. It is composed of 250 experts and is becoming an increasingly important actor in the architecture of French cyber defence. Located in Brittany, the DGA/MI will be part of the cyber security cluster project involving industry, academia and government planned by axis 4 of the Cyber Defence Pact.[55]

3.3.2. French cyber defence organisation

In order to complete his duties, the head of French cyber defence relies on a vast joint chain of command that can address both the defensive and operational activities referred to above.

For the defensive task, an operational chain has been created in order to mitigate any threat to military systems. The **Planning and Operations Centre** has the lead in the conduct of cyber operations and their integration within the operational planning process. In order to better ensure the protection and resilience of military systems, the FR-MoD relies on an expertise centre, the Analysis Centre for Cyber Defensive Operations (*Centre d'analyse de lutte informatique défensive*, CALID), to provide round-the-clock detection, analysis, and response to cyber-attacks. On the operational level, the FR-MoD distinguishes offensive operations from defensive operations and includes this approach when planning operations.

As part of its global approach, the FR-MoD relies on a significant chain of command in order to guarantee the readiness and awareness of the armed forces in case of an attack. The Information System and Communication[56] chain is involved in implementing general security procedures.

Since the end of 2013, the COSSI and CALID have been co-located in Paris in order to enhance better information sharing and better coordination between the two bodies. This initiative will enable a better dialogue between the two organisations and facilitate their mutual support.

As appears from the Cyber Defence Pact and the Military Planning Act 2014-2019, the efforts on cyber have been tremendous, but aimed at mainly filling the gap between France and some of its allies in the cyber realm such as Germany and the UK.[57] These efforts are intended to develop cyber capabilities in order to address new challenges for the coming years and to support effectively military operations.

Concerning personnel, there are approximately 2000 people working on the security of information systems within the Ministry of Defence. [58] The Defence Procurement Agency will also see the creation of 200 new openings in its specialised cyber branch by 2019, mostly as top-level and highly qualified engineers.

3.3.3. International cooperation

France's involvement in NATO's cyber defence includes the participation in cyber defence exercises such as Cyber Coalition and the implementation of the Memorandum of Understanding signed in 2011 between the NATO Cyber Defence Management Board (CDMB) and the ANSSI.

[53] Centre de planification et de conduit des opérations (CPCO) in French.
[54] 'Lutte informatique défensive' in French.
[55] 'Pacte Défense Cyber. 50 mesures pour changer d'échelle' (n 36).
[56] SIC (système d'information et de communication).
[57] Bockel Report (n 31) 82.
[58] Par Boris Manenti, 'Cyberdéfense : l'armée française va passer en mode "attaque"', O - Le cahier de tendances de l'Obs, 2014 <http://obsession.nouvelobs.com/hacker-ouvert/20140121.OBS3230/cyberdefense-l-armee-francaise-va-passer-en-mode-attaque.html>.

3.4. Cyber aspects of crisis management

3.4.1. Cyber crisis prevention

The modified Prime Minister's Order of 2 June 2006 'Establishing the List of Sectors of Critical Infrastructure and Designating Coordinating Ministers of these Sectors' lists 12 vital sectors relating to state issues, the protection of citizens, and the economic and social life of the nation. These are state civil activities, law enforcement, military activities of the State, food, electronic communication including broadcasting, energy, space and research, finance, water management, industry, health, and transportation.[59] As of 2014, 218 'Operators of Critical Importance' (*Opérateur d'importance vitale*, OIV) had been designated; however, the list detailing these operators is classified.

Operators of critical importance are 'public or private operator(s) referred to under L.1332-1 and L.1332-2 of the French Defence Code, who '[exercise] activities cited in Article R. 1332-2 and included in a critical sector,' and 'manages or uses for this activity one or more organisations or works, one or more facilities, whose damage, unavailability or destruction due to malicious action, sabotage or terrorism would directly or indirectly seriously compromise the military or economic capabilities, the security or the survival ability of the nation or seriously threaten the lives of its population.'

Operators of information systems when designated as operators of critical infrastructure are required by the updated provisions of French Defence Code outlined by Article 22 of the Military Planning Act to meet the obligations listed therein.[60] They are legally obligated to comply with 'sets of safety rules necessary for the protection of those information systems' outlined by the Prime Minister; to implement intrusion detection systems operated by service providers acting under the authority of ANSSI or the Prime Minister; to submit their information systems to either ANSSI or a service appointed by the Prime Minister to verify the level of security; and to comply with the Prime Minister's safety rules.

All of these operators report back to their responsible minister in case of a crisis. The ANSSI provides guidance and support to the relevant coordinating ministers in case of crisis.[61]

Plan Vigipirate

The major government plan implemented in France to thwart threats is known as the '*Plan Vigipirate*'. The plan was created in the late seventies as a prevention plan against terrorism. A part of this plan has been adapted to address cyber threats.

The Vigipirate[62] plan is an interministerial plan intended to identify threats and risks. It is a general plan that can be broken down into several domains, including the cyber threats. The ANSSI is in charge of drafting the prevention plan outlined in the Vigipirate plan and may also update it depending on needs.[63] The responsibility for this plan is given to the SGDSN and mostly focuses on terrorist threats. This, of course, may involve the

[59] Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Arrêté du 2 juin 2006 modifié fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs', Journal officiel de la République française, 2006 <http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20060604&numTexte=1&pageDebut=08502&pageFin=08502>.

[60] Military Planning Act (n 38).

[61] The ANSSI assists the coordinating ministers in charge of critical infrastructure for the protection of their information systems. 'Décret n° 2009-834 du 7 juillet 2009' (n 32) art. 5.

[62] This plan has been made public in its general approach: Vigipirate, 'Partie publique du Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes', n° 650/SGDSN/PSN/PSE, Paris: Secrétariat général de la défense et de la sécurité nationale, 2014 <http://www.sgdsn.gouv.fr/IMG/pdf/Partie_publique_du_plan_Vigipirate_2014.pdf>.

[63] Cybersecurity chapter of the Vigipirate plan. Vigipirate, 'Objectifs de cybersécurité', Paris: Secrétariat général de la défense et de la sécurité nationale, 2014 <http://www.ssi.gouv.fr/IMG/pdf/20140310_Objectifs_de_cybersecurite_document_public.pdf>.

action of law enforcement entities from the police or the gendarmerie specialised in the repression of computer crimes and attacks.

3.4.2.Cyber crisis management

Article 22 of the Military Planning Act mandates that in response 'to major crises threatening or affecting the security of information systems of critical infrastructure, the Prime Minister may decide on measures that operators […] must implement.' All requisite legal, organisational, and technical obligations are implemented at the expense of the operator of information systems designated as an operator of critical infrastructure. Thus, article L. 2321-2. of the Defence Code states that:

> *'to respond to a computer network attack that targets information systems that could threaten the military, economic potential or the Nation's security and capacity to survive, services of the State, within the limitations given by the Prime minister, can perform any technical operation deemed necessary to attribute the attack and to mitigate its effects by accessing the information systems from which it originates.'*

These provisions are designed to overcome the shortcomings of the current regulation, which did not allow national organisations to intervene more thoroughly during a cyber incident, and more importantly to provide the actors in cyber defence in France with a clear legal framework.

The second paragraph of this article allows state organisations specifically designated by the Prime Minister to possess technical equipment, computer programs or any data deemed necessary otherwise punished by the Criminal Code in order to analyse their conception and patterns.

Piranet Plan

As part of the Vigipirate plan described in the previous section, the Piranet intervention plans are intended to address a threat coming from a specific domain, such as technological or environmental. In the case of a targeted cyber attack on information systems, the Piranet plan is to be implemented to respond to the threat. This plan is tested during specific exercises.[64] This plan is classified.

3.5. Involvement of the nation

Since France's transition from a conscript to a professional army in the beginning of 1996, the reserve component has played a prominent role in the operational capacity of the French Armed Forces.

In 2012, an initiative to create the Cyber Citizen Reserve (*Réserve citoyenne cyberdéfense, RCC*) was launched. The Citizen Reserve would be subordinated directly to the General Staff of the Armed Forces' Cyber Defence department.[65] The Citizen Reserve, according to article L.4241-1 of the Defence Code,[66] is aimed primarily at maintaining the nation's defence awareness. Thus the Citizen Reserve is composed of volunteers approved by the military authorities by virtue of their competence, experience and interest in national defence.

The aim of the Cyber Citizen Reserve is to engage and rely upon opinion-formers in order to explain, raise awareness, and organise events that will contribute to making cyber defence a national concern and priority, while emphasising the sovereign aspects of cyber defence. For the time being, the Citizen Reserve is composed

[64] Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 'Cyber-attaques : l'exercice PIRANET 2012 met l'État à l'épreuve d'une crise informatique majeure' <http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/cyber-attaques-l-exercice-piranet-2012-met-l-etat-a-l-epreuve-d-une-crise.html>.

[65] Military Planning Act (n 38) The Citizen Reserve at 2.11.2.

[66] Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article L.4241-1', <http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006540382&idSectionTA=LEGISCTA000006166989&cidTexte=LEGITEXT000006071307&dateTexte=20140402>.

of about 50 people (journalists, members of industry and academics) who promote cyber defence at different occasions.[67] The Citizen Reserve is not meant to be activated during times of crisis.

France is currently working on implementing the next step of the Cyber Reserve model, which would see the rise of a cyber operational reserve. This operational reserve would be activated along the same lines as the operational reserve in other domains: that is also to say that an individual volunteer to enter the operational reserve would be subject to the same constraints as any military personnel during a cyber crisis.

[67] See: Ministère de la Défense, 'Le réseau de la réserve citoyenne cyberdéfense', 2014 <http://www.defense.gouv.fr/reserves/monde-de-la-reserve/cyberdefense/le-reseau-de-la-reserve-citoyenne-cyberdefense>.

References

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 'CERT-FR. Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques' <http://www.cert.ssi.gouv.fr/>.

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 'Cyber-attaques : l'exercice PIRANET 2012 met l'État à l'épreuve d'une crise informatique majeure' <http://www.ssi.gouv.fr/fr/anssi/publications/communiques-de-presse/cyber-attaques-l-exercice-piranet-2012-met-l-etat-a-l-epreuve-d-une-crise.html>.

Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), 'Défense et sécurité des systèmes d'information. Stratégie de la France', 2011 <http://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf>.

Alternatives Economiques, 'La nouvelle société de consommation', n° 331, 2014 <http://www.alternatives-economiques.fr/la-nouvelle-societe-de-consommation_fr_art_1268_66464.html>.

Berthou, Par MM. Jacques, et M. Jean-Marie Bockel, 'Avis présenté au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de loi de finances pour 2014', n° 158 (Sénat session extraordinaire de 2013-2014), 21 novembre 2013 <http://www.senat.fr/rap/a13-158-12/a13-158-121.pdf>.

Biseul, Xavier, 'Cyberdéfense : l'Anssi recrutera 150 experts d'ici fin 2015', 01Business, 2013 <http://pro.01net.com/editorial/604366/cyberdefense-l-anssi-recrutera-150-experts-d-ici-fin-2015/>.

Bockel, Par M. Jean-Marie, 'Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense', n° 681 (Sénat session extraordinaire de 2011-2012), 18 juillet 2012 <http://www.senat.fr/rap/r11-681/r11-681.html>.

Bondaz, Marianne et al, 'Bilan de la révision générale des politiques publiques et conditions de reussite d'Une nouvelle politique de reforme de l'Etat, 2012' <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/124000520/0000.pdf>.

EU Digital Agenda, 'Digital Agenda Scoreboard', 2013 <http://digital-agenda-data.eu/charts/analyse-one-indicator-and-compare-countries#>.

'France Selected Issues Paper', IMF Country Report, No. 13/252, Washington D.C.: IMF, 2013 <http://www.imf.org/external/pubs/ft/scr/2013/cr13252.pdf>.

France Trés Haut Débit, 'Comprendre le Plan France Très Haut Débit' <http://www.francethd.fr/comprendre-le-plan-france-tres-haut-debit/>.

French Government, 'French White Paper On National Defence And Security', 2013 <http://www.rpfrance-otan.org/IMG/pdf/White_paper_on_defense_2013.pdf>.

Inspection générale des finances (IGF), 'Le soutien a l'Économie numérique et a l'Innovation', n° 2011-M-060-02, 2012 <http://www.igf.finances.gouv.fr/webdav/site/igf/shared/Nos_Rapports/documents/2012/2011-M-060-02.pdf>.

Institut national de la statistique et des études économiques, 'Le commerce électronique en 2012' <http://www.insee.fr/fr/themes/document.asp?reg_id=0&ref_id=ip1489>.

Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Arrêté du 2 juin 2006 modifié fixant la liste des secteurs d'activités d'importance vitale et désignant les ministres coordonnateurs desdits secteurs', Journal officiel de la République française, 2006 <http://www.legifrance.gouv.fr/jopdf/common/jo_pdf.jsp?numJO=0&dateJO=20060604&numTexte=1&pageDebut=08502&pageFin=08502>.

Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article R-1132-3 § 7', <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=2A19E78A79324EAE15BA68EC963C8968.tpdjo09v_2?idSectionTA=LEGISCTA000028342651&cidTexte=LEGITEXT000006071307&dateTexte=20140401>.

Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article L.1332- 6-1', <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=2A19E78A79324EAE15BA68EC963C8968.tpdjo09v_2?idSectionTA=LEGISCTA000028342651&cidTexte=LEGITEXT000006071307&dateTexte=20140401>.

Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article L.2321-3', <http://www.legifrance.gouv.fr/affichCode.do;jsessionid=2A19E78A79324EAE15BA68EC963C8968.tpdjo09v_2?idSectionTA=LEGISCTA000028342651&cidTexte=LEGITEXT000006071307&dateTexte=20140401>.

Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Code de la defense. En savoir plus sur cet article L.4241-1', <http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006540382&idSectionTA=LEGISCTA000006166989&cidTexte=LEGITEXT000006071307&dateTexte=20140402>.

Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'Décret n° 2009-834 du 7 juillet 2009 portant création d'un service à compétence nationale dénommé 'Agence nationale de la sécurité des systèmes d'information'', 2009 <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212>.

Legifrance.gouv.fr, Le Service public de la diffusion du droit, 'LOI n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale', 2013 <http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id>.

Le Gouvernement, 'La nouvelle France industrielle. Présentation des feuilles de route des 34 plans de la nouvelle France industrielle' <http://www.economie.gouv.fr/files/files/PDF/nouvelle-france-industrielle-sept-2014.pdf>.

Le portail de l'Économie et des Finances, 'A la une' <www.redressement-productif.gouv.fr›.

Le portail de l'Économie et des Finances, 'Impôt sur le revenu : les télédéclarations progressent de près de 6%'. <http://www.economie.gouv.fr/teledeclarations-progressent>.

'L'impact d'Internet sur l'économie française' ('Comment Internet Transforme Notre Pays'), McKinsey & Company, 2011 <http://www.observatoire-du-numerique.fr/wp-content/uploads/2013/02/2011-mckinsey-company-impact-dinternet-sur-l%C3%A9conomie-fran%C3%A7aise.pdf>.

Mallet, Jean-Claude, 'Défense et Sécurité nationale : le Livre blanc', 2008 <http://www.ladocumentationfrancaise.fr/rapports-publics/084000341/>.

Manenti, Par Boris, 'Cyberdéfense : l'armée française va passer en mode "attaque"', O - Le cahier de tendances de l'Obs, 2014 <http://obsession.nouvelobs.com/hacker-ouvert/20140121.OBS3230/cyberdefense-l-armee-francaise-va-passer-en-mode-attaque.html>.

Ministère de la Défense, 'Le réseau de la réserve citoyenne cyberdéfense', 2014 <http://www.defense.gouv.fr/reserves/monde-de-la-reserve/cyberdefense/le-reseau-de-la-reserve-citoyenne-cyberdefense>.

Ministère de la Défense, 'Pacte Défense Cyber. 50 mesures pour changer d'échelle', 2014 <http://www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%20Cyber-1.pdf>.

Ministère de la Défense, 'Présentation du Pacte Défense', 2014 <http://www.defense.gouv.fr/actualites/articles/presentation-du-pacte-defense-cyber>.

'Programme d'investissements d'avenir – situation et perspectives', Commissariat général à l'investissement (CGI), 2014 <http://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2014/11/rapport_cgi.pdf>.

Secrétariat general de la defense et de la sécurité nationale, 'Textes concernant le SGDSN' <http://www.sgdsn.gouv.fr/site_rubrique58.html>.

Tromparent, Patrice, 'French cyberdefence policy'. In C. Czosseck et al (Eds.), 4th 'International Conference On Cyber Conflict. Proceedings 2012', Tallinn: CCD COE Publications, 2012.

Vigipirate, 'Objectifs de cybersécurité', Paris: Secrétariat général de la défense et de la sécurité nationale, 2014 <http://www.ssi.gouv.fr/IMG/pdf/20140310_Objectifs_de_cybersecurite_document_public.pdf>.

Vigipirate, 'Partie publique du Plan gouvernemental de vigilance, de prévention et de protection face aux menaces d'actions terroristes', n° 650/SGDSN/PSN/PSE, Paris: Secrétariat général de la défense et de la sécurité nationale, 2014 <http://www.sgdsn.gouv.fr/IMG/pdf/Partie_publique_du_plan_Vigipirate_2014.pdf>.

Willsher, Kim, 'French fighter planes grounded by computer virus', The Telegraph, 2009 <http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html>.