



Information systems defence and security

France's strategy



Foreword



In the *French White Paper on Defence and National Security* presented by the President in June 2008, information systems security emerged, alongside deterrence, as an area in which the sovereignty of France should be fully expressed. More collective work remains to be done in order to fully achieve this.

Yet cyberspace may seem only remotely related to defence and national security. In twenty years, digital technologies have eroded the boundaries between our personal and professional lives, raised corporate competitiveness to unprecedented levels, made public services more accessible to users and promoted a transparency drive in our country's institutions.

Cyberspace, the new Tower of Babel, is a place where the cultures of the world can be shared, ideas and information circulated in real-time, and topics discussed among individuals. Exclusion from the digital world condemns individuals to isolation, companies to decline and nations to dependency.

In the material world, the violent acts of criminals and the destruction caused by wars and terrorism are highly visible and usually subject to wide media coverage. In cyberspace, the consequences of computer attacks on government, companies or individuals' information systems are most of the time visible only to specialists and remain unknown to the general public.

Cyberspace, like a virtual battleground, has become a place for confrontation: appropriation of personal data, espionage of the scientific, economic and commercial assets of companies which fall victim to competitors or foreign powers, disruption of services necessary for the proper functioning of the economy and daily life, compromise of information related to our sovereignty and even, in certain circumstances, loss of human lives are nowadays the potential or actual consequences of the overlap between the digital world and human activity.

Given the sudden emergence of cyberspace in the field of national security and the extent of the challenges ahead, the French government decided to provide France with a structured defence and security capability. In 2009, therefore, it set up the French Network and Information Security Agency (*Agence nationale de la sécurité des systèmes d'information* or ANSSI), to meet the needs of public institutions, companies and individuals. In July 2010, the President decided to make the Agency responsible for the defence of information systems in addition to its security role.

The purpose of this document is to outline the strategy undertaken by France since the publication of the *French White Paper on Defence and National Security* in order to safeguard the security of our citizens, our companies and our nation in cyberspace.

A handwritten signature in black ink, consisting of a long, sweeping horizontal stroke followed by a stylized, cursive 'F' and 'D'.

Francis Delon

Secretary General for Defence and
National Security

Words followed by an asterisk are defined in the glossary.

Photo credits :

cover	Jean Mottershead (CC BY-NC-ND 2.0), or free of copyright
page 11	Ruby MV (CC BY-NC-SA 2.0)
page 12	Simon BISSON (CC BY-NC-ND 2.0)
page 13	MrFenwick (CC BY-NC-ND 2.0)
page 14	Runran (CC BY-SA 2.0)

Contents

Foreword

Summary

Four strategic objectives

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

Seven areas of action

- Anticipate and analyse
- Detect, alert and respond
- Enhance and perpetuate our scientific, technical, industrial and human capabilities
- Protect the information systems of the State and the operators of critical infrastructures
- Adapt French legislation
- Develop our international collaborations
- Communicate to inform and convince

Glossary

Summary

Among the major threats that France will have to face over the next fifteen years, the 2008 French White Paper on Defence and National Security cited large-scale cyberattacks on national infrastructures.

This observation led to the French Government's decision to significantly strengthen national cyberdefence capabilities. The creation of the French Network and Information Security Agency (ANSSI) in 2009 was the first step of this process.

This description of the national strategy on information systems defence and security presented in this document reflects the ambitions set out in the White Paper. This strategy is based on four objectives.

1. Become a world power in cyberdefence

While maintaining its strategic independence, France must work to ensure that it belongs to the inner circle of leading nations in the area of cyberdefence. We will thus benefit from the knock-on effect of cooperation both at an operational level and in the implementation of a unified strategy to face common threats.

2. Safeguard France's ability to make decisions through the protection of information related to its sovereignty

Governmental authorities and crisis management actors must have the resources to communicate in any situation and in total confidentiality. The networks that meet this need must be expanded, particularly at the local level.

Ensuring the confidentiality of the information circulating over these networks requires mastered security products. We must keep the necessary expertise to design them and optimise their development and production methods.

3. Strengthen the cybersecurity of critical national infrastructures

To function correctly, our society is increasingly dependent on information systems and networks, particularly the Internet. A successful attack on a French critical information system or the Internet could have serious human or economic consequences. In close collaboration with the relevant equipment manufacturers and operators, the State must work to guarantee and improve the security of these critical systems.

4. Ensure security in cyberspace

The threats to information systems simultaneously affect public services, private companies and citizens.

Public services must operate in an exemplary fashion and improve the protection of their information systems and the data entrusted to them.

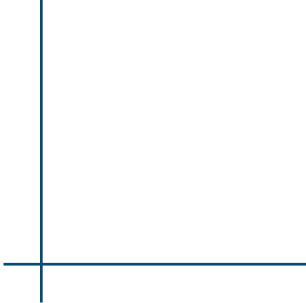
Simultaneously, campaigns to raise information and awareness among companies and citizens must be undertaken.

In terms of the fight against cybercrime, France will promote the strengthening of the current legislation and international judicial cooperation.

In order to meet these objectives, seven areas of action have been identified:

1. Effectively anticipate and analyse the environment in order to make appropriate decisions.
2. Detect and block attacks, alert and support potential victims.
3. Enhance and perpetuate our scientific, technical, industrial and human capabilities in order to maintain our independence.
4. Protect the information systems of the State and the operators of critical infrastructures to ensure better national resilience.
5. Adapt French legislation to incorporate technological developments and new practices.
6. Develop international collaboration initiatives in the areas of information systems security, cyberdefence and fight against cybercrime in order to better protect national information systems.
7. Communicate, inform and convince to increase the understanding by the French population of the extent of the challenges related to information systems security.

This document summarises the public part of the guidelines and actions approved by the strategic committee on information systems security instituted under Decree No. 2009-834 of 7 July 2009 creating the French Network and Information Security Agency* (ANSSI)



« France must retain its areas of sovereignty, concentrated on the capability necessary for the maintenance of the strategic and political autonomy of the nation: nuclear deterrence; ballistic missiles; SSBNs and SSNs; and cyber-security are amongst the priorities. »

« French White Paper on Defence and National Security », p.306

Four strategic objectives

I. Become a world power in cyberdefence

The development of an information society, supported by electronic communication networks, is a tremendous driver of French growth as it creates value and employment. It significantly contributes to the competitiveness of our economy and therefore to France's international standing.



Yet electronic communication networks are subject to illicit activities carried out either directly or indirectly by foreign States. Some conduct wide-scale espionage operations through these networks in order to access information relating to our sovereignty such as classified national defence material, or to the scientific, technological, commercial or financial assets of companies operating in our nation's strategic sectors.

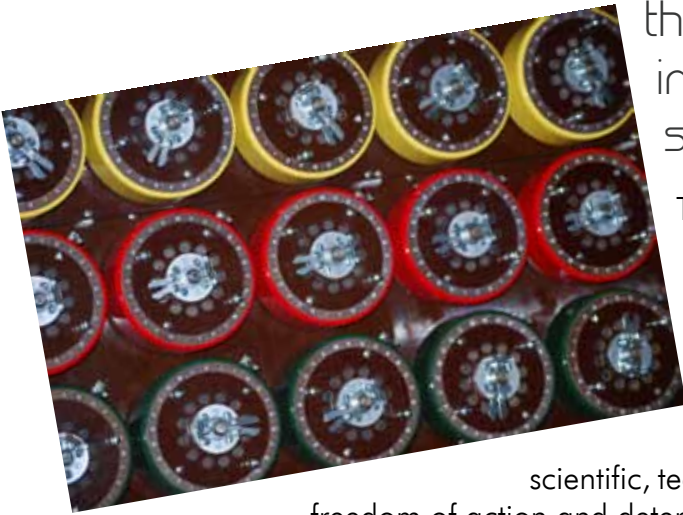
Terrorist groups also use these same communication networks to spread their ideas, disseminate operational information to their organisations and conduct propaganda activities.

In the near future, foreign States or terrorist groups could attack the critical infrastructures of States that they consider as ideologically hostile.

It is therefore essential for France to acquire a cyberdefence capability.

Yet, unlike in the material world, confrontations in cyberspace know no boundaries. Thus credible cyberdefence cannot be limited to national level. It must rely upon a network of allies with whom real-time information can be exchanged on vulnerabilities, protection mechanisms, attacks and countermeasures that can be implemented against cyberattacks led directly or indirectly by States or terrorist groups. France will strengthen its operational partnerships with its closest allies and will build on its expertise to actively contribute to formulating cyberdefence policies within international organisations, in particular the European Union.

2. Safeguard France's ability to make decisions through the protection of information related to its sovereignty



The need to instantly access and share information in multiple formats is increasingly becoming a trend in today's society. Nevertheless, part of the world's stability still lies in the ability to conceal the «information related to our sovereignty», i.e. the fragments of diplomatic, military, scientific, technical and economic information that allow freedom of action and determine the prosperity of nations.

Just as in the past, intelligence services around the world, among others, attempt to obtain information related to our sovereignty. Communications networks, particularly the Internet, the information they contain and the data available on the terminals connected to them have become both sources of information and a means of collecting it.

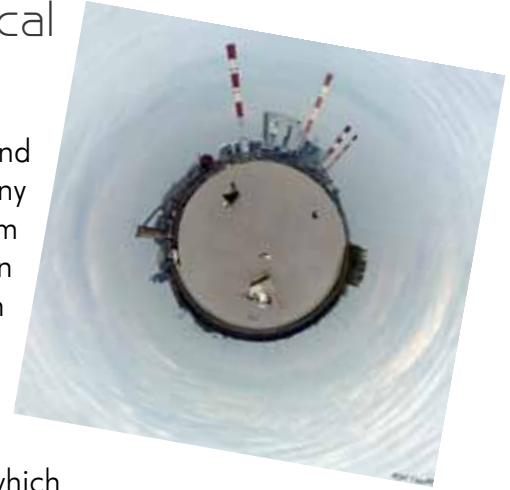
The most effective way to protect information related to our sovereignty is the use of cryptography* techniques which prevent, or at least delay, the understanding of information should it be disclosed or intercepted. Developments in cryptanalysis*, which mirror those in computer processing power, require the conception and use of methods and techniques that are more difficult to analyse and regularly renewed.

Preserving our strategic independence depends on our ability to master cryptographic techniques and key technologies needed to design our security products*; therefore we need to ensure that the field of information systems security remains attractive for young graduates in order to prevent the gradual erosion of our expertise.

In addition to the need to communicate in a safe and confidential way, both decision-makers and organisations involved in crisis management must have at their disposal means of communication which can be used in all circumstances. These secured resources for electronic data exchange, telephony and videoconferencing have already been designed and developed. We will keep on deploying them over the coming years, in particularly for operators of critical infrastructures*.

3. Strengthen the cybersecurity of critical national infrastructures

Through the convergence of multiple technologies, the real and virtual worlds are increasingly becoming overlapped. Many real world objects - from supermarket labels to refineries, from photocopiers to combat drones - have built-in information systems and are connected to others. Remotely, through networks, it becomes possible to collect the information transmitted by these objects, to keep them operating and to control them.



In its Defence Code, France defined critical sectors in which operators meet needs essential to the life of the population, the exercise of State authority, the running of the economy, the maintaining of defence capabilities and the nation's security, as these activities are difficult to substitute or replace.

Most operators of critical infrastructures make widespread use of communication networks, especially the Internet, both for the management of their activities and their work. However, in the long-standing relationship between the industrial world and the IT world, revolutionised by the interconnection of systems, the industrial world lacks training and awareness of information systems security, while the IT world often has a poor understanding of the constraints and functioning of industrial systems.

The dependence of all stakeholders on the Internet is increased due to the major trends of our economic and social organisation: outsourcing and cloud computing, pooling of support services, real-time and just-in-time management, roaming, task transfer to customers and citizens, creation or re-engineering of numerous processes.

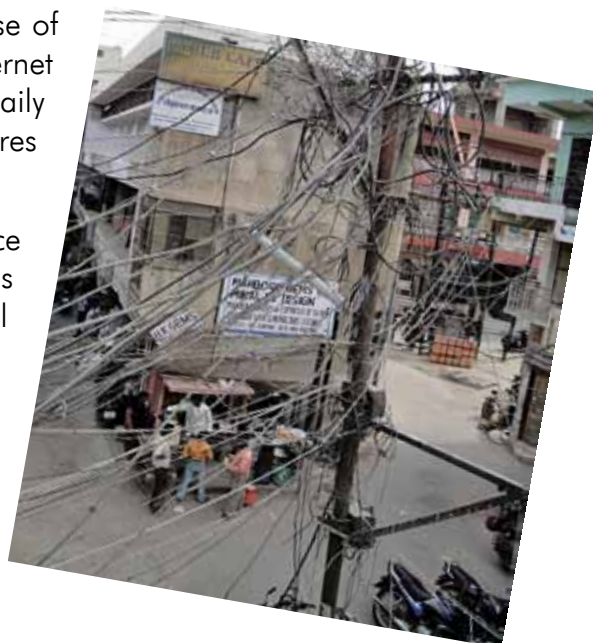
Should communications networks or the Internet be interrupted, the resources available to replace them may prove to be highly insufficient, especially because of the lack of qualified personnel capable of reinstating processes prior to the advent of the digital era. In the case of processes resulting directly from new practices linked to information technology, the resources to replace them do not yet exist.

As world news regularly demonstrates, the possible consequences of malicious actions against the automated control systems of industrial processes used by operators of critical infrastructures have not yet been properly assessed. As a result, protecting electronic communication networks - and in particular the Internet - together with securing the core systems of critical infrastructures' operators have become national priorities.

4. Ensure security in cyberspace

For an increasing number of our citizens, the use of electronic communication networks like the Internet is permeating the most common activities of daily life such as shopping, administrative procedures and interpersonal communications.

Simultaneously, the techniques used in cyberspace by malicious individuals or groups of individuals are more and more efficient and aim to steal identities, obtain the information needed to access bank accounts or collect and resell personal data. Cases of malicious remote takeovers of computers, in order to incorporate them into networks of compromised machines («botnets*») to carry out illegal activities such as cyberattacks or sending malicious e-mails, have also been dramatically increasing.



Given these developments, public authorities must set an example by protecting public cyberspace. Users must be able to trust the electronic services offered by the administration, particularly in regard to protection of their personal data. The General Security Framework* (RGS) published in early 2010 provides a regulatory context for strengthening this security. Compliance and implementation by public authorities are priorities.

Securing cyberspace systematically involves providing companies and individuals with the relevant information on the risks and the ways to limit them. The long-term objective is to raise citizens' awareness of cybersecurity issues during the education process. This initiative will require the implementation of an active governmental communication policy.

Last but not least, laws must govern the Internet. France must support the strengthening or enactment of legal rules in cyberspace when existing legislation proves to be insufficient, and promote international judicial cooperation on repression of offences committed on or through electronic communication networks.

**In order to achieve our four strategic objectives,
7 areas of action have been identified.**

Seven areas of action

1. Anticipate and analyse

Risks and threats evolve rapidly in cyberspace. The release of a new product or a new version of software, the disclosure of an uncorrected flaw in a widely used software product, the development of new technologies or practices, or even a political statement can threaten the security of information systems within a very short period of time.

- In light of this, the first step to ensure our information systems' security and defence is to monitor the latest technology developments and analyse, fully understand and even anticipate the actions of public or private actors.

2. Detect, alert and respond

Given the increasing dependence of companies, infrastructures and services on the Internet, and because of the systemic risks related to some weaknesses, it is essential to be able to detect flaws and attacks as soon as possible, alert potential and known victims and offer them rapid assistance with the analysis and development of countermeasures.

- As planned in the *French White Paper on Defence and National Security*, France is developing a detection capability for attacks on information systems. Deployed in particular within ministry networks, these systems enable the relevant personnel to be alerted, help assess the nature of attacks and create appropriate countermeasures.
- In order to manage all the information either gathered by these detection tools, by monitoring mechanisms or provided by our partners, so as to obtain a real-time picture of the national network situation, and if necessary manage a crisis situation, the ANSSI has been equipped with an «operations room» adapted to the challenges.
- In order to respond to major crises affecting or threatening the security of the information systems of the administration or the operators of critical infrastructures, the State must be able to take the necessary measures rapidly. To this end, the ANSSI is the national Authority in charge of information systems defence.

3. Enhance and perpetuate our scientific, technical, industrial and human capabilities

The security of information systems is based on mastery of technology and know-how that is also accessible to organisations and individuals intending on damaging them. State actors responsible for information systems security must not only be familiar with state-of-the-art technology, they must also be able to foresee or even spur on technological developments by maintaining their research capabilities, as this is the only way of limiting the tactical advantage of the attacker over the defender.

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.

- In order to drive this research forward, the possibility of creating a cyberdefence research centre in collaboration with industrial partners is currently being examined. This centre 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 cyberdefence concepts,...), as well as expertise and training activities.

The development of the information society offers companies a worldwide market, currently dominated by actors located outside of Europe. As far as information systems security is concerned, this situation is neither desirable nor tenable. Yet France does have a state-of-the-art industrial base unique in Europe, with the potential to master a large part of the technologies needed for the design of security products, including components. This base is made up of a large number of innovative SMEs. However, these companies have not yet reached the required critical size and are not in sufficient demand.

- Industrial strengthening will be promoted using the various resources of the State, in particular through strategic investment funds.

In order to ensure better efficiency, the designers of IT products and information systems must take security issues into account from the very beginning of the development process. The presence of information systems security experts in our industrial base must therefore be increased. Orienting young people towards such jobs will be encouraged in order to expand the pool of expertise available in the country.

As a general rule, scientific and technical training on information technology must incorporate courses on information systems security.

4. Protect the information systems of the State and the operators of critical infrastructures

As stated in the *French White Paper on National Defence and Security*, France must «master and develop very high-security products to protect State secrets, as well as a range of guaranteed ‘trusted products and services’ for use by government agencies and services which will be made widely available to the business sector». Resilient secure networks* for «the entire decision-making and command chain in Metropolitan France» must be used.

- With regard to classified information*, the French strategy on security products and components has been redefined. In particular, it takes full account of France rejoining NATO integrated command.
- Within ministerial networks, the introduction of robust authentication systems based, for example, on the use of smart card technology, an area of French excellence, will have a very significant impact on the level of security.
- Government authorities now have a secure interdepartmental intranet, a high-availability telephone network that will be fully equipped with new encryption terminals by 2012, and a secure videoconferencing system mainly for use in ministerial decision-making centres. Deployment of these various networks will continue, especially in local administrations.
- With regard to the security of the information systems of operators of critical infrastructures, a public-private partnership will be set up, firstly so that these operators can benefit from the information gathered by the State on threat analysis; and secondly, to allow the State to ensure the appropriate level of protection of the infrastructures that are crucial to keep the country running properly. Such assessments will also be undertaken with equipment manufacturers.

5. Adapt French legislation

New practices introduced through the development of cyberspace can, if not enough attention is paid, threaten individual freedoms, the functioning of critical infrastructures and the stability of our companies.

Seven areas of action

Our legislative and regulatory framework must reflect recent developments in technology. Laws will be reviewed as new technologies and new practices emerge in order to strengthen the security of individuals while at the same time ensuring a balance between the desire to minimise the impact on companies' competitiveness and the need for the State to be able to intervene in the nation's best interest.

- Regarding operators of electronic communications, transposition of European directives into French law will enable the enactment of new rules to protect information systems and alert government authorities in case of incidents.
- The enforcement of the «General Security Framework» (RGS) and its development will allow public authorities to significantly raise the protection levels of their information systems, particularly in their relations with users.

6. Develop our international collaborations

The security of information systems is partly based on the quality of the data exchange between relevant services of various States. France will seek to establish a wide network of foreign partners in order to promote the sharing of essential data – e.g. information on vulnerabilities or flaws of products and services.

France will also strengthen its relationships with its partners to fight cybercrime.

Similarly, strong relations between allies form the basis of an effective cyberdefence policy. France is building a highly select circle of trustworthy partners with whom in-depth operational exchanges will be held.

7. Communicate to inform and convince

The security of information systems relies as much on personal vigilance as on the organisation, the choices and technical measures introduced by companies and the action of governments.

Given the potential consequences of a major attack on information systems on the country and its citizens, we must ensure the awareness and motivation of individuals and organisations.

In France, information and public debate on the threats posed by damage to the security of information systems and its impact on defence and national security, or simply on our daily lives, remain largely underdeveloped.

- ANSSI will provide targeted support to decision-makers in order to help them draw up measures and make the necessary decisions regarding the security of information systems that are critical to the running of their organisations and the protection of their technical, scientific, commercial and financial assets.
- In a more general sense, appropriate communication campaigns will be conducted by ANSSI targeting the general public and companies.

Glossary

Botnet

A botnet, or robot network, is a network of compromised machines controlled by a malicious individual (the master). The network is structured in a way that allows its master to transmit orders to some or all of the machines in the network and operate freely.

Comment: some networks consist of a huge number of machines (several million). They may be illegally traded or used to carry out malicious activities against other machines.

Classified information

Article 413-9 of the French Penal Code states that «processes, objects, documents, pieces of information, computer networks, computerised data or files whose disclosure or access would be prejudicial to national defence or would lead to the disclosure of a national defence secret» are subject to classification measures to restrict their distribution or access.

Cryptanalysis

The process of decrypting encrypted data, without the encryption keys.

Cryptography

The discipline that includes the principles, means, and methods for data transformation with the aim of hiding data content, preventing data modifications from remaining undetected and/or preventing unauthorised use of data (ISO 7498-2).

Cryptology

The science of both cryptography and cryptanalysis.

Cybercrime

Acts contravening international treaties and national laws, targeting networks or information systems, or using them to commit an offence or crime.

Cyberdefence

The set of all technical and non-technical measures allowing a State to defend in cyberspace information systems that it considers to be critical.

Cybersecurity

The desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible.

Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence.

Cyberspace

The communication space created by the worldwide interconnection of automated digital data processing equipment.

Flaw

Vulnerability in a computer system allowing an attacker to negatively affect its normal functioning, or the confidentiality or integrity of the data it contains.

General Security Mechanism (RGS - Référentiel général de sécurité)

Set of rules drawn up by ANSSI and stipulated in Ordinance No. 2005-1516 of 8 December 2005 «on electronic exchanges between users and the public administration and between public administrations» that certain functions contributing to the security of information must comply with. This includes, among others, electronic signatures, authentication, confidentiality and timestamps. The rules set out in the RGS are mandatory and are adjusted to reflect the level of security defined by the administrative authority concerning the security of the online services for which

it is responsible. The conditions under which they are drawn up, approved, modified and published are set out in Decree No. 2010-112 of 2 February 2010 related to the application of Articles 9, 10 and 12 of the ordinance cited on the security of information exchanged through electronic networks. (See <http://www.ssi.gouv.fr/rgs>).

Information system

Organised set of resources (hardware, software, personnel, data and procedures) used to process and circulate information.

Information systems security

All technical and non-technical protective measures enabling an information system to withstand events likely to compromise the availability, integrity or confidentiality of stored, processed or transmitted data and of the related services that these systems offer or make accessible.

Netiquette

Charter drawn up in 1995 by the Internet Engineering Task Force (IETF) introducing recommended network etiquette rules for exchanges taking place in cyberspace (see <http://tools.ietf.org/html/rfc1855>).

Operator of critical importance (OIV - Opérateur d'importance vitale)

Article R. 1332-1 of the French Defence Code states that operators of critical infrastructures are designated among the public or private operators cited in Article L. 1332-1 of the same code, or among managers of the organisations cited in Article L. 1332-2.

An operator of critical infrastructure:

- exercises activities cited in Article R. 1332-2 and included in a critical sector;
- 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.

Resilience

In the field of computing, the ability of an information system to withstand a breakdown or cyberattack and return to its initial operating state after the incident.

Security product

Hardware or software designed to protect the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that information systems offer or make accessible.

About ANSSI

The French Network and Information Security Agency (ANSSI) was created on 7 July 2009 in the form of a nationwide administrative service.

Pursuant to Decree No. 2009-834 of 7 July 2009 amended by Decree No. 2011-170 of 11 February 2011, the agency is the information systems defence and security national authority. It is directly attached to the Head of Secretary General for Defence and National Security, under the authority of the Prime Minister.

To find out more about ANSSI and its missions, please visit www.ssi.gouv.fr/en/.

February 2011

« Freely reusable public information » licence (LIP V1 2010.04.02)

French Network and Information Security Agency

ANSSI - 51 boulevard de la Tour-Maubourg - 75700 PARIS 07 SP - France

Websites : www.ssi.gouv.fr and www.securite-informatique.gouv.fr

E-mail : [communication \[at\] ssi.gouv.fr](mailto:communication@ssi.gouv.fr)