NOTE DE SYNTHÈSE

RÉPUBLIQUE FRANÇAISE

CYBER DEFENCE AN INTERNATIONAL ISSUE, A NATIONAL PRIORITY

Committee on foreign affairs, defence and armed forces

Information report n°. 681 by Mr Jean-Marie BOCKEL, senator for Haut-Rhin

A major cyber attack on **Bercy** on the eve of the French presidency of the G8 and G20, cyber espionage in companies as in the case of **AREVA**, disruption of institutional websites like that of the **Senate**: **attacks on information systems** have **multiplied in France**, as they have right across the world in recent years. Even **the Elysée** has recently been the victim of several cyber attacks.

In addition, revelations concerning the United States' probable involvement in the design of the **STUXNET** virus, which destroyed about a thousand uranium enrichment centrifuges, thus delaying Iran's military nuclear programme by several months or several years, or further, the recent discovery of the twenty times more powerful virus **FLAME**, could be the harbinger of new "*cyber weapons*", of still largely unknown capabilities.

With the development of the Internet, and their growing interconnection, information systems are our societies' true "nerve centres", without which they could not function.

In this context, **is France sufficiently organised and prepared to deal with a cyber attack?**

Attacks against information systems: a strategic threat that has materialised and increased in recent years

From Tallinn to Teheran: now no country is safe from cyber attacks

Since the widespread cyber attacks that hit Estonia in 2007, practically not a week goes by without an announcement that somewhere in the world, there has been **a major cyber attack** against a large public or private institution.

France is not spared by this scourge

In France, administrative authorities, companies and vital service operators (energy, transport, health, etc.) are victims **daily** of **several million** cyber attacks.

Whether it is a matter of a "denial of service attack" designed to saturate a public website with a great number of requests thus making it inaccessible, like what happened to the Senate's website, attempts to penetrate systems for spying purposes in particular via "spyware" introduced by a "Trojan horse", like the Bercy or AREVA attacks, or further, real "computer bombs" designed to destroy data contained in information systems, like STUXNET, **the threat is specific and multifaceted**.

These cyber attacks may be carried out by computer hackers, activist groups, criminal organisations, as well as by competitor companies, or even by other States. The finger of suspicion often points towards China or Russia, even if it is very difficult to identify the authors of these attacks precisely.

Certainly, it is not a matter of claiming absolute protection. This would be fairly illusory. The distinguishing feature of cyber attacks is that they exploit weaknesses, they go where defences have not yet been put in place. But the **security of the most sensitive networks and infrastructure** can be **strengthened and their resilience** improved.

JULY 18 2012

A threat now recognised at international level

1. Better armed allies

- **The United States**

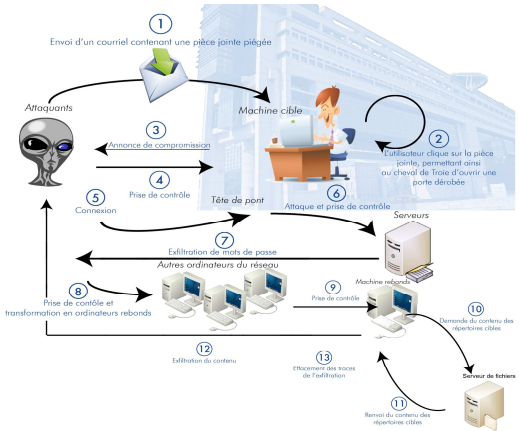
President Barack Obama is firmly committed to the subject and has qualified cybersecurity as being a **strategic priority**. There are several bodies, within the department responsible for national security or the Pentagon, which operate in this area, like the National Security Agency (NSA) or *Cybercommand*. From 2010 to 2015, the United States plans to devote **50 billion dollars** to cyber defence and **several tens of thousands of agents** are working on this subject.

- **The United Kingdom**

The Government adopted a new strategy in November 2011. The main body responsible is the *Government Communications Headquarters* (GCHQ), the agency responsible for technical information. About **700 agents** are occupied by cyber defence questions. Despite the budgetary context, Prime Minister David Cameron announced additional spending in 2010 of 650 million pounds (**750 million euros**) on cyber defence over the next four years.

- **Germany**

A strategy was prepared in February 2011. Coordination of this strategy is the responsibility of the Federal Interior Ministry to which is attached the federal office of information system security (BSI) located in Bonn, which has a budget of 80 million euros and over 500 agents.



2. The beginnings of international cooperation

- **The UNO**

China and Russia are the main sponsors of an international treaty and restrictive rules in cyberspace. Concerned to preserve freedom of expression on the Internet, western countries are opposed to this and are suggesting that confidence building measures should be prepared.

- **NATO**

Since the new strategic concept adopted at the Lisbon Summit in 2010, NATO approved a policy and cyber defence concept in 2011. A management authority, as well as an excellence centre, located in Tallinn, were created.

For all that, **NATO does not seem to be fully armed in the face of this threat.** The Alliance's main computer unit is not operational 24 hours in 24, and 7 days in 7. More generally, the Alliance is still to determine the attitude it should adopt in response to these cyber attacks. **Can article 5 of the Washington treaty be invoked?** There is no clear answer to this question.

- **The European Union**

The European Union has **an important role to play** because a large part of the rules governing electronic communication networks come within its competence. However, **the European Commission and a number of member countries still do not seem to have taken on board** the risks and issues linked to cyber defence.

Symbol of the Anonymous movement

Despite significant progress since 2008, our mechanism still has some major gaps

1. Real progress since 2008

The Lasborde (2006) and Romani (2008) reports concluded that France was neither sufficiently organised nor well-prepared to deal with a cyber attack.
The **2008 White paper concerning defence and national security** identified the threat and provided **real impetus** to the cyber defence policy.

In terms of organisation, it enabled this policy to be clearly identified with the creation, in July 2009, of **the National Agency for the Security of Information Systems** (ANSSI), an inter-ministerial agency which is the national authority for the defence of information systems. In February 2011 France also adopted a **national strategy**.

France has, with this strategy and with the ANSSI, major tools that can be used for cyber defence. For all that, **a lot remains to be done in this area**.

2. Our mechanism still has some major gaps

With a staff of 230 people and a budget of 75 million euros, **ANSSI still lags far behind similar departments in the United Kingdom or Germany**, which have between 500 and 700 agents.

In addition, even if the ministry of defence and armies has taken measures, the other ministries, companies and vital major operators are still **insufficiently aware** of the threat.

What would be the simplest means of causing our country major disruption via a cyber attack? A very simple means would be to attack energy distribution or health. The example of the STUXNET virus or the *Conficker* worm, that disrupted the operation of several hospitals, shows that this is no mere hypothesis.

10 priorities and 50 specific recommendations to make the protection and defence of information systems a real national priority

- **Priority no. 1:** Make **cyber defence** and the **protection of information systems a national priority**, taken **to the highest level of Government**, in particular in the context of the new White Paper. Consider the relevance of formulating a **public doctrine** concerning **offensive capacities**.

- **Priority no. 2:** Strengthen **the staff, resources and prerogatives** of the **French Network and Information Security Agency (ANSSI),** as well as providing dedicated staff and resources within **the armed forces, the French procurement agency and specialized services,** and develop **a true human resources policy.**

- **Priority no. 3:** Introduce **amended legislation** to give ANSSI the resources to carry out its missions and set up **a specialist legal function with national competence** to crack down on serious attacks on information systems.

- **Priority no. 4:** Improve recognition of **the need to protect information systems in the actions of each ministry**, improving awareness at all levels, reducing the number of gateways between networks and the Internet, and developing analysis systems that can be used to detect attacks, as well as enhancing the authority of civil servants involved in the security of information systems.

- **Priority no. 5:** Make it **compulsory** for companies and vital service operators **to declare incidents** to ANSSI should a major attack occur against their information systems and encourage them to take **protective measures** by means of incentive measures.

- **Priority no. 6:** Strengthen the protection of **critical infrastructure operator** information systems by reducing the number of gateways between their networks and the Internet, developing analysis systems, generalising audits, making it compulsory to declare processes and SCADA systems connected to the Internet and by preferring the introduction, on a sector basis, of shared detection centres.

- **Priority no. 7:** Support via **a voluntarist industrial policy**, on a national and European scale, French industrial base, in particular SMEs, specialising in the design of products and services essential to information systems security, and, more generally, the **information and communication technologies sector**, and strengthen cooperation between the Government and the private sector.

- **Priority no. 8:** Encourage **the training of engineers specialising** in the protection of information systems, develop **research** and **consultancy activities**, and emphasise **raising public awareness**, in particular through a communication campaign inspired by French road safety campaigns.

- **Priority no. 9:** Pursue **bilateral cooperation** with our main allies, support **NATO** and **the European Union's** actions, engage in **dialogue** with China and Russia and promote the adoption **at international level** of confidence building measures.

- **Priority no. 10:** **Prohibit** the deployment and use nationally and at a European level of **"routers" or other core network equipment** that present **a risk to national security, in particular "routers" and certain other equipment of Chinese origin**.

The ANSSI logo

Mr. Jean-Marie BOCKEL in Washington

Senate Committee on foreign affairs, defence and armed forces
http://www.senat.fr/commission/etr/index.html

The Committee's reports:
http://www.senat.fr/rapports-classes/cretrd.html

Chairman :

Jean-Louis CARRÈRE

The Committee's secretariat:
15, rue de Vaugirard
75291 Paris Cedex 06

Telephone: 01.42.34.38.97
Fax: 01.42.34.47.63
secretariat-affetra@senat.fr

Rapporteur :

Jean-Marie BOCKEL