French Republic

PARLIAMENTARY OFFICE FOR SCIENTIFIC AND TECHNOLOGICAL ASSESSMENT

Digital safety and risks: issues and opportunities for businesses

Rapporteurs: Mrs Anne-Yvonne Le Dain, Deputy, and Mr Bruno Sido, Senator.

*At the time of the digital omnipresence and the continual development of its tremendous possibilities, **businesses need to rely on secured digital tools**. Yet, each day, on all sides, evidences of new vulnerabilities multiply.*

*The escalation between known flaws and the solutions to fix them seems to be endless, considering that **the origin of these weaknesses lies in numerous thoughtless human behaviours** and the slowness of the essential understanding.*

*Further to the hearings of over a hundred people, and a precise analysis of the assets and weaknesses of digital messages and their diffusion channels, the Parliamentary Office for Scientific and Technological Assessment firstly proposes **about thirty general recommendations** (digital culture, sovereignty, cooperation among actors, EU data protection rules). Then, the Office proposes **a** **vade-mecum** **on digital safety for the use of businesses** that will endeavour to a considered and evolving construction on which depends their future prosperity.*

Facing the digital globalisation, the elaboration of efficient solutions turns out to be individual and national in order to prevent French businesses from deliberately assenting to the plundering of their data by spreading them openly.

I. THE INTERNATIONAL CONTEXT OF BUSINESSES' DIGITAL SAFETY

A. The technical governance of the Digital issue at the global scale

The web that surrounds the world, the Net, the Internet, concerns all human activities. The understated rules of its implementation and organisation benefited commercial businesses and their home State, while the global population was lending itself with ardour and recklessness to this global stranglehold on minds and objects.

The organisation of the governance of the Internet (allocation of IP addresses and DNS domain name, and other operating elements of the Internet protocol) **does not result from any international text**.

In 2014, in São Paulo, **the European Union has advocated a single, open, free, safe, reliable and non-fragmented Internet**.

However, **whereas the law ought to enact the rule, ratio of power among digital giants, governments, businesses and citizens prevail over.**

B. The global management of digital safety incidents

Connected to the United States Department of Commerce, the *National Institute of Standards and Technology (NIST*), in charge of **promoting businesses competitiveness face to the use of complex technologies**, expanded its scope to the **normalisation of information technologies**.

The *NIST*, which hosts and manages the *National Vulnerability Database*, is the origin of the use and development of most norms for safety monitoring purposes (*OVAL*, *CVE* & *CVSS* reports).

The understanding of most vulnerabilities is concentrated on the *Safety Content Automation Protocol* (*SCAP*), a *NIST* platform assuring the networking of safety knowledge among the scientific and industrial research. **The *SCAP* centralises and spreads safety events considered as dangerous in order to favour cooperation at the national and international level.**

The United States also created the *Computer Emergency Response Team Coordination Centre* (*CERT/CC*), that **spreads these vulnerabilities to the general public through bugtraq, as it *de facto* puts software developers on notice to fix their flaws. The *CERT/CC* daily releases for free a list of vulnerabilities and the attached detailed analysis.**

The CERT/CC developed a worldwide network in order to federate knowledge on scientific and industrial safety and **provides a service to users all around the globe. Each State or entity asking for joining this network has to be certified by the CERT/CC.**

In France, there are about twenty CERT, including public ones such as the *ANSSI*.

The emergence of these monitoring services express the anxiety of States, of the European Commission and of the Atlantic Alliance regarding digital data. **The awareness of the riskiness of the threats on the Internet and**

through the modern electronic ways of exchanging constitutes the main issue of the coming decade.

C. The Transatlantic Trade and Investment Partnership project

European and international guarantees have to be established regarding personal data protection and the Internet governance prior to the adoption of some clauses related to the digital in the Transatlantic free-trade agreement.
Besides, the digital should not be incorporated in the trade agreement, as the digital embraces commerce, and not the other way round. The digital could justify a digital exception in the manner of the cultural exception. Hence, this sector would be excluded from commercial negotiations.

D. Towards a coherent digital Europe?

During the European Council on the digital economy in October **2013**, **France has defined three priorities**: to develop a European industrial strategy on the digital allowing the **emergence of innovative European actors**; to guarantee an **open access for the services and the users of the Internet**; **to reinforce the rules on the protection of the European citizens' privacy** (controlling the transfer of data in the direction of third state, single counter of defence of individuals and businesses rights, cooperation among national control authorities about the decisions on the treatment of personal data).

E. Sovereignty and digital technology

Considering the possible extent of the damages caused by digital attacks, **States have to devise the protection of the crucial infrastructures of the society: protection of essential operators, such as of citizens crucially linked to these operators.** The notions of **vulnerability identification** and **resilience**, facing or after a digital attack, are essential.

II. THE NATIONAL FRAME FOR THE IMPLEMENTATION OF DIGITAL SAFETY

A. Digital technologies and liberties

The French *Conseil d'État* (the highest level of the administrative jurisdiction) **recommends the development of a soft law** (**recommendations**, **guides of good practices**, approval of **professional codes of conduct**, **certification** or **mediation**), an adjustable and reversible law according to the use.
The European Union intends to assure its values without imposing rules penalising its citizens or businesses, and so setting the territoriality of the norm.

B. The operational implementation of the digital safety

It is assured by the conjunction of the means of the technical service ***Maîtrise de l'information*** of the French **Directorate-General for Armaments** (a department of the Ministry of Defence), of the ***Centre d'analyse de lutte informatique défensive*** **(CALID)**, of the ***brigade d'enquêtes sur les fraudes aux technologies de l'information*** **(BEFTI)** of the French *Gendarmerie Nationale*, of the ***Agence nationale de la sécurité des systèmes d'information*** **(ANSSI), and of the industrialists (ICASI, CIGREF, etc.)**.

C. Organisation of the digital safety

Regarding cyber-criminality, a great difficulty results from the lack of link between the place of the breach and its perpetrator. Indeed, Locard's exchange principle (the use of tracks as evidences) does not apply to cyber-criminality: the attacker can have taken action as on the place of the breach as disguising himself through different sites, servers and countries. **The loss of the geographical link requires cooperation among international police forces.**
As for **insurers and reinsurers**, **they are reluctant to take on the market of digital risk** (prior risks not allowing to forecast future risks; as the calculation of the insurance premium being almost impossible: has a company implemented all the possible digital safety measures?).

D. The essential operators (*Opérateurs d'importance vitale* – OIV)

Digital safety of the more than two hundred essential operators listed in France (half of them belong to the private sector) **requires a methodical anticipation (cartography of digital risks, annual plan for the safety of information systems** including the management information systems, the industrial management systems – control systems or SCADA, applications and users).The telecommunications sector as the energy sector favour their response capacities (wise organisation into short decision cycles, involved and pragmatic directors and partners), **a protection devised in profundity** and a **rapid share of all the information during crisis situations**. Strong reluctances exist face to the cloud computing to which only secondary data can be entrusted.

III. THE COMPLEXITY OF THE DIGITAL TECHNOLOGY MAKES SAFETY DIFFICULT TO DEVISE FOR BUSINESSES

A. Towards a representation of the digital technology in order to facilitate understanding

Digital technology, network of the networks (including all the objects and tools linked to it) **is vast, dynamic and omnipresent, implied in all the human or**

technological exchanges. **Digital technology does not have a finite form**. Nevertheless, **regarding safety matters, the representation of the system is an essential condition to a responsible use,** that supposes **to question the way computers and networks are interlinked** from a continent to another, and the way information are dispatched, etc. **Digital safety is cross-disciplinary and blends the military and the civilian area, professional and personal.**

B. Digital infrastructures

Infrastructures of domain names, routing, messaging services, browsing (on search engines), of digital cloud – based upon the Internet network (unreliable) and implying applications, sometimes business applications, are exposed to **cyberattack risks**.

IV. Strength and weaknesses of a business' information system

A. The three levels of a company

A company operates from systems of decision, information and communication, and production.

B. Critical analysis of the information system of a company

Digital technology has deeply modified and improved each of these systems (local network of the company, wireless or not) while bringing it **weaknesses, which are not always perceived and even less corrected**. The multiplication of sensors as well as the confusion between personal data storage spaces and professional data storage spaces and the undistinguishable share of data announce numerous **possibilities of undesired uses**. Moreover, **the world of the industrial computing and the one of general computing, more and more interconnected, increase thus the volume of inputting into the industrial system**.

V. Securing the information system of a company

A. Safety principles of the of an information system

The pragmatic and massive extension of digital equipment within businesses has not been accompanied by the implementation of a monitoring by design.

However, an information system has to assure and maintain the proprieties of **availability, integrity and confidentiality (AIC)** as from the implementation of **prevention, monitoring, analysis, reaction, investigation and repression functions** in the frame of a **continuous improvement process of safety, anticipating attacks or in reaction to it**.

In this confrontation between individuals and cybernetics, **inventiveness characterises human beings**. **For lack of mastering the introduction of machines in this spiral, the risk of a complete loss of control of the information system exists.**

Digital safety policies implemented by businesses have to be incorporated within the framework of the *Politique de Sécurité des Systèmes d'Information de l'État - PSSIE* (State Safety Policy on Information Systems) – the July 17th, 2014 circular from Prime Minister. The *PSSIE* is founded on: **trustworthy operators**, a **risk analysis**, the **planning of resources** for securing, a **strong authentication**, the **endorsement of the computing products by the *ANSSI*, and the localisation on the national territory of sensitive data**.

B. Implementation of prevention in the information system of a company

Starting from a line of **perimeter defence (firewall)** around the network, **exclusive accesses** are defined according to the sensitiveness of the resources to protect, installed **antivirus software**, the **strong authentication** used (internals or externals), **managed identities**, implemented **cryptography**, secured **tunnels of network** (virtual networks).

If it does not exist a specific threat to the cloud computing – that already contains them all – usually, that environment increases risks.

The difficult management of connected devices, **designed without regard to serious mechanisms of securing**, constitutes a major preoccupation, all the more so as **these devices are already present on industrial sites of high criticality**.

VI. Digital flaws and attacks compromising the safety of businesses

A. A hostile environment

Vulnerabilities (including backdoors) and threats have to be disclosed and analysed so that solutions can be designed at the earliest through a **continuous monitoring** (intrusion tests). The ***CERT/CCs***, including the *ANSSI*, specialised and certified organisations, **intervene urgently on computing safety breaches**.

The analysis of risks (evaluation of impacts and probabilities of occurrence of a scenario), founded on a **cartography of the system**, tends towards making businesses activities as safe as possible, even though **a complete safety cannot be guaranteed**.

Businesses that do not have the means to carry out that type of audit would be interested in inexpensive models of IT charter.

B. Attacks against the information system

Everything cannot be considered as a digital attack; the quoted statistics regarding this are usually excessive.

As it was anecdotal few years ago, **some attacks become extremely professional and widespread. Complex attacks include preliminary phase of social engineering.**
They are not all due to highly qualified computer specialists; particularly as general public hacking software begin to spread.
The specific features of digital risk cause for a business to ignore, sometimes for years, an ongoing cyber-attack, or not to perceive the long term consequences of such an intrusion.

C. The monitoring function of society

Supervision of safety is based on **tracks analysis** coming from the systems detecting intrusions and placed on several places of the information system in order to ensure the monitoring.
The security information management system (*SIEM*) handles and interprets these tracks.
The creation of a Security Operations Centre (SOC) is only accessible for great companies, while the other businesses resort to external experts such as the *ANSSI*, the *DGA*, etc.

VII. DIGITAL CULTURE AND THE EDUCATION TO SECURE IT

A. One-beats and off-beats of digital safety

The gap between the constant resort to the budding digital tool and the lack of control of that tool leads businesses to be disconcerted, while the evolutions of this situation are incorporated to numerous and (sometimes) opposing schedules.
Time has been short for an observation, or even a reflection, all the more so for an education and the construction of a digital culture.
However, **all businesses need safe digital technology** – this is their nervous system that cannot be affected without jeopardising their existence.
The *ANSSI* and groups of companies have elaborated methods and guidelines in order to help businesses to build quickly, coherently and efficiently their digital safety **in the respect of the healthy network rules**.
Another off-beat results from the **coexistence, so far non- converging, of several priorities: global priorities** (global governance of the Internet), **international priorities** (*TAFTA* project), **European priorities** (pending regulations and directives), and **national priorities** (French law on the digital, *loi République numérique*). Given that digital technology is essential, **the question of a required affirmation of digital exception during international negotiations is asked.**

B. The actors of digital safety

In addition to the cyber-defence national plan and its *Pacte Défense cyber 2016* and *Pacte Défense PME* (related to training, research or businesses), and the cyber-security plans among the plans of *Nouvelle France industrielle* (new industrial France), the **French government** encouraged the creation of **industrial clubs of cyber-defence** and contributed to the emergence of a **national community of cyber-defence**. These achievements complete the actions of the ***CNIL*** and of the ***ANSSI***, as well as **businesses'** actions (such as ***CoFIS***, ***CIGREF***, ***CLUSIF***, etc.) contributing to **the establishment of a healthy network by combining cyber-security and cyber-defence**.

C. Make the economy running with law?

Once analysed, the digital risk can be a great opportunity with sizeable fallouts thanks to the development of French assets (regarding training, digital safety audits, cartography of risks, cryptography, sovereign probes, intrusion detector, etc.) in order to build "*France as the land of digital safety and trust*" by the means of an efficient industry regarding cyber-security
Beyond a digital science or technology imposing their binary logic, **the reduction of the digital risk also goes through awareness, education, reflex acquisition, a certain knowledge on how to behave face to the digital technology. The whole without losing sight of the swift evolution of the international context in which these progresses must be incorporated.**

To read the report:
www.assemblee-nationale.fr/commissions/opecst-index.asp
www.senat.fr/opecst

April 2015