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.

GENERAL RECOMMENDATIONS

I. DEVELOP A DIGITAL CULTURE: MASSIVELY INFORM AND TRAIN ALL AGE GROUPS FROM ALL SOCIAL BACKGROUNDS IN INFORMATION TECHNOLOGY

- **Teach digital technology within the educational system, from preschool until higher education, and throughout the whole life – notably through lifelong learning**:
  - ✓ Train to **understand what is the digital technology** rather than settle for learning how to use digital tools;
  - ✓ Teach the **digital symbols**, **basic coding** and **programming**, and the **principles of encryption**.
- **Educate about digital safety**:
  - ✓ Teaching computing science at school: **include the teaching of computing safety** through the healthy network rules and train in digital risk;
  - ✓ Higher education programmes: **strengthen the means of higher education regarding cyber-security** and design **training modules in computing safety**, including healthy network rules, leading to a diploma in that field;
  - ✓ **Favour as well other types of training, including experimental trainings**;
  - ✓ Create a research centre for European purposes in civil cyber-security, in addition to the military centre in Western France; the latter could rely on the *INRIA* and be designed for developing European cooperation;
  - ✓ Basic and lifelong training for civil servants and magistrates of justice and civil safety; including **awareness actions to the digital risk and digital securing**.
- Establish a license for a safe use of digital technology – a sort of **digital driving license** guaranteeing a regular update for its owners in order to face the rapid evolutions in this field (*possible economic outcomes*)
- Carry out **prevention campaigns about digital safety** towards the general public and professionals:
  - ✓ Broadcast awareness programs about digital safety on the **radio** and **television** at peak viewing times, along with a presence on the **Internet**.
- Raise awareness among digital users and accountable people, through platforms showing **cyber-attacks and resistance tests** (*possible economic outcomes*).

II. GUARANTEE THE CONDITIONS OF A DIGITAL AUTONOMY IN ORDER TO PRESERVE SOVEREIGNTY

- **Develop French hardware detecting cyber-attacks** (benefiting from the financing governmental programme "*Programme d'investissements d'avenir*") and high security laboratories (*possible economic outcomes*)
- Define circles of trust proper to digital safety.
- Formulate a **French doctrine on cyber-security for use by businesses** – cf. *vade-mecum* on digital security recommendations for use by businesses (Volume I, page 251 of the report) – and by the citizens and civil services.
- Implement a unified European framework for the **securing of European citizens' data**.

- **Create the equivalent of a European or French sovereign *Google*** – after the European *Aérospatiale* or *Ariane* – as well as China, India and Russia are currently developing their own Internet networks (for matters of language and alphabets, etc.). *Europe could benefit from possible economic outcomes.*
- **Subject to the French law companies managing servers on the national territory and the French clients of firms managing servers out of the national territory.**
- As law does not allow these days to find solutions to the problems met, for instance, during the scandal of general spying of French diplomacy and industrials, **authorise civil and military specialised laboratories to lead researches with offensive aims in the dual field of cyber-security**.
- **Reinforce teams working on IT cryptology and virology** and provide them, under the control of the ANSSI, including academic laboratories, the possibility to unleash operating systems, to unlock and disassemble software, to check computing flows, to reverse engineer software in order to have a **better understanding of the nature of the threats so as to give means to trace digital flows spreading malicious programmes.**

III. EMPOWER DIGITAL SAFETY BY A BETTER COOPERATION AMONG ACTORS

- Create a place for dialogue and exchange on digital technology, gathering **engineers, politicians and public administration in order to develop a digital culture** within the political and administrative sphere.
- Establish a cooperation among industrials, and among industrials, the defence community and the academic world so as to elaborate and implement a **national cyber-security strategy in the medium and long terms** to face attacks.
- Expand the powers of the ANSSI by granting it the **power of regulation and injunction**.
- Stimulate, on the whole national territory, the **development of trustworthy actors specialised in digital safety** (*possible economic outcomes*).

IV. FROM VIRTUOUS NATIONAL PROVISIONS AND USES, DEVELOP A SPECIFIC EUROPEAN LAW

- Modify the French *Code des marchés publics* (the code regulating public tenders) so that **propositions to invitations to tender do not reveal the information system of a company** (*possible economic outcomes*).
- **To better organise the preservation of evidences of a digital infraction.**
- Reform the French and European law in order **to decree the level of protection and the standards of security of essential operations to SMBs** linked to them (subsidiaries, suppliers, subcontractors) (*possible economic outcomes*).
- **Think a data law**, after a large public consultation, in order to:
  - ✓ **decree the respect of presumption of innocence and of objection on the Internet**;
  - ✓ **legislate the right to be forgotten and removed from a search engine for personal data**;
  - ✓ **extend the duration of prescriptions in matter of digital infraction, while damages remain**;
  - ✓ conform **the first day of the prescription of a digital infraction with the day on which the victim realises the infraction**.

V. PARLIAMENTARY ASSEMBLIES, REGIONAL AUTHORITIES AND CIVIL SERVICES

- **Raise awareness among regional authorities and civil services about digital safety**;
- **Make of the Parliament the exemplary place of awareness regarding digital vulnerabilities.**