POSITION PAPER

INITIATIVE SOUVERAINETÉ

INSTITUT CHOISEUL

Cybersecurity, a prerequesite for European economic sovereignty

A call for new private and public leadership in cybersecurity

June 2022

The Sovereignty Initiative (l'*Initiative Souveraineté*), launched in January 2022, is the Institut Choiseul's platform dedicated to the stakes of sovereignty and resilience. This Initiative aims to identify and promote pragmatic and concrete measures to strengthen the strategic autonomy of France and Europe. Through regular meetings bringing together leading economic players and recognised experts, and through the production of summary analyses and guidance papers emanating from the different ecosystems brought together, the Institut Choiseul intends to take part in the debate on the necessary national and European sovereignty in fields ranging from defence to industry, the food sector and transports.

The first *Sovereignty & Resilience Meeting* was held in May 2022 with leading actors sharing their testimonies, prospective vision and best practices: Daniel Le Coguic (Alliance pour la Confiance Numérique & Atos), Elena Poincet (Tehtris), Cédric Sylvestre (Olvid) and Michel Van Den Berghe (Campus Cyber).

Introduction

Cybersecurity is the prerequisite for a European strategic autonomy

Cybersecurity makes it possible to ensure the integrity and security of all physical entities using information systems, data or software. It guarantees the functioning of administrations, companies and of essential or critical infrastructures. An effective cybersecurity is a prerequisite for a full and complete digital sovereignty.

The ecosystem's main goal must be to enable the development of French and European companies specialising in cybersecurity and to guarantee the excellence of their solutions. This will facilitate their promotion and their massive and systematic use by the greatest number of public and private players. The focus must be put on raising awareness on the need and opportunity to acquire and trust European products, with equal characteristics and performance.

A European private and public leadership in cybersecurity to transform the culture of the business community and public sector

The increase in cyberthreats should make all stakeholders aware of the phenomenon and encourage them to adopt a global roadmap.

The cybersecurity industry needs a surge of leadership and awareness from decision-makers, both within the major players as well as in small companies, and at the highest level of the French and European political level.

The responsibility for the choice of digital tools cannot be borne solely by the Information Systems Management or the Chief Information Security Officer (CISO). Decisions must be taken and assumed at the highest level, by the general management of companies and administrations. Cybersecurity and technological sovereignty choices must permeate down in organisations from the highest level of governance. The transformation of the cultures of companies and administrations can only be achieved through a strong will in the first place at the decision-making level. A "cyber culture", understood as existential and transversal in nature, must be instilled in European companies and administrations, guided by the example of the salutary dynamic that has been mobilised the last fifteen years around CSR issues.

The Institut Choiseul calls for cybersecurity to be placed at the heart of a renewed sovereignty strategy

Institut Choiseul
12 rue Auber 75009 Paris, France - www.choiseul.info - +33 (0)1 53 34 09 93

Cybersecurity has become everyone's business

The global dimension of the cyberspace has led to an increase in the number of threats and a diversification of the parties concerned: citizens, states and companies, whatever their size.

The ultra-connectivity of societies and economies and the exponential digitalisation of production chains are leading to a continuous increase of the attack surface. Cybersecurity is becoming a transversal issue extremely linked to national sovereignty.

The cybersecurity industry is becoming a lever of global competitiveness for France and Europe

In France, cybersecurity is a highly export-oriented industry, with €14.1 billion in turnover generated internationally and €5 billion in export turnover. It creates €7.1 billion in added value and employs 70,500 people. According to the French Senate's report of the 10th of June 2021, "*Not only is the security industry the fastest growing industrial sector with the highest rate of added value (nearly 43%), but cybersecurity is the segment of this sector that is driving the sector's dynamics*".

Cybersecurity offers the opportunity to place European digital confidence players among the world leaders in the field

French players in cybersecurity - and digital confidence in the broader sense - are recognised worldwide for the reliability of their solutions and their innovativeness. A solid base exists of leading players who have the necessary size to compete on the international scene, such as Orange Cyberdéfense, Thales, SopraSteria, Airbus CyberSecurity, Tehtris or YesWeHack. This base constitutes the submerged part of a lively and innovative ecosystem made up of numerous SMEs, start-ups and scale-ups.

In addition, major industrial players attached to the sovereignty of their production and to the security of their value chain are developing their own cyber responses. They create specific programs adapted to their activities starting at the design stage and upstream development.

France can count on strong public players and ambitious institutionalised initiatives:

- The French National Cybersecurity Agency (ANSSI) has become a reference in raising awareness, alerting, training and fighting against cyberattacks;
- The "Security Industries" strategic committee brings together the Directorate General for Enterprise (DGE) and industrial security players under the aegis of the national industry council;
- The "Campus Cyber" is now a model for getting all the players in the sector to work together for the attractiveness of an entire profession.

Buyers, both public and private accounts, are themselves in demand of so-called "sovereign" technological solutions, developed in France and certified by the ANSSI, such as the MACTAN detection solution developed by Sopra Steria or the Olvid solution, instant messaging used by many companies and ministries including the Ministry of the Interior. ■

Cybersecurity in a nutshell

4th *France is the 4th most affected country in the world by number of inhabitants*

Attacks targeting companies of all sizes have been multiplied by 4 between 2020 and 2021 in France **x4**

70,500 people
are employed in the cybersecurity sector in France

€ 5,700 bn
The needs for cybersecurity are estimated at 5,700 billion euros worldwide

The European cybersecurity market worth was estimated in 2021 at **€ 34 bn**

Weaknesses - Limitations - Threats

The challenges of strategic autonomy specific to cybersecurity are not yet unanimously shared and the resort to foreign solutions is still too significant

On a daily basis, public and private actors in Europe often use digital tools of non-EU origin. These technologies are governed by the law of the country in which the solutions are developed, which undermines the principle of sovereignty

Major public and private purchasers do not sufficiently choose European Cyber solutions in their purchasing policy, even though 30% of the CISOs of CAC 40 companies are already convinced of the risks associated with foreign solution providers.

Strong contradictions prevail between policy objectives and the actions deployed

Many projects illustrate the gap between the stated objectives of public authorities and their implementation.

The choices made in public procurement also show strong contradictions. This is the case, for example, of the European Commission's recent choice to select a British company, British Telecom, to manage confidential communications between Member States, at the cost of 1.2 billion euros.

The professional attractiveness and the training programs don't yet reach the goals

The cyber sector relies on a pool of talent: analysts, consultants, and especially developers, engineers and technicians.

However :

- prospective studies agree on a future shortage of talent. In France, nearly 15,000 open positions in this field are not currently filled;
- the younger generation is not sufficiently aware of cybersecurity professions and the shortcomings in the teaching of mathematics and, more generally, of computer sciences are strongly felt.

Proposals - Guidelines - Actions

Make public and private spending a lever for strengthening the European Cyber offer and technological independence 1

Guide public procurement towards European players: a preference for "Made in Europe" solutions based on a Buy European Act.

Encourage large private buyers to direct part of their IT orders to European companies offering trusted cybersecurity solutions.

Strengthen the European capability through a revision of the European regulatory framework 2

Incorporate trusted European technology in critical and economically essential infrastructures: introduce systematically in all legal texts under discussion (e.g. revision of the Network and Information Security Directive, Cyber Resilience Act) the origin of products and services as a criterion of trust in the proposed solutions.

Make initiatives converge through a unified and coherent network of standards: ensure that the revision of the eIDAS Regulation, which aims to increase trust in electronic transactions within the internal market, is carried out in coherence with the revision of the NIS Directive.

Democratizing useful skills and rethinking career paths for tomorrow's cybersecurity talents 3

Introducing children to the basics of software development from an early age. The programming at school, and simultaneously of cybersecurity issues, has become a necessity.

Strengthen public training in software development by making it more accessible. Certifications or diplomas in applied mathematics should no longer be a criterion for benefiting from these courses and the range of continuous education programs should be increased, thus opening the way to more professional conversion in cybersecurity.

Clarify private higher education possibilities and establish a European label.

Develop a competitive and industrial vision of cybersecurity supported by funding mechanisms for the players that can meet the challenges 4

Adopt and share a vision of conquering digital sovereignty in order to seize the opportunities of the cybersecurity market, and not give in to an overly protective vision of sovereignty that would lead to a loss of competitiveness.

Encourage the growth of industrial companies involved in cyber issues, not only in IT for solution providers but also in OT for business companies involved in cyber by design to transform their industrial processes with their own European or national solutions.

Scale up the use of private funding to address the entire European digital ecosystem, by :

- encouraging the emergence of new investment funds with a European scope and capable of deploying their capital in Growth level fundraising (Series B, +€10M);
- setting up more Corporate Venture Capital funds dedicated to the entire sovereignty perimeter (defence, space, intelligence, etc.).

Allow private players to benefit from non-European funding to scale up and exceed a critical size in the markets. Subject to the conservation of control, and to a series of criteria on the technologies used, their countries of origin and the countries where employees and decision-making centres are located, it is important to show pragmatism in order to counterbalance the lack of European funding. It is also important to welcome foreign investments that do not question the decision-making and operational independence of sovereign players to enable them to conquer new international markets.

Double the total funding planned (from 1 to 2 billion euros) in the context of 'France 2030' for the cybersecurity acceleration strategy by innovating with private public funding.

Consolidate a made in Europe cyber offer as a high-level alternative to foreign solutions and a long-term competitive advantage 5

Establish a common set of principles and criteria for «sovereign» cybersecurity solutions that stand out at the global level: respect for the framework of public liberties, traceability of financial flows and compliance with anti-terrorism and money laundering regulations, data respect and GDPR, use of European solutions, having a majority of Europeans as developers and in technical teams, etc.

Build a catalogue of recognised and widely shared sovereign cybersecurity solutions, accessible to all players who need to use these solutions. There are many initiatives aimed at referencing French cybersecurity solutions or capability catalogues that constitute a foundational compendium. Following the referencing of "qualified products and services" carried out by the ANSSI and the launch of the "Cybersecurity Made in Europe" label, it is recommendable to pool the sources of referencing in a reference catalogue, to promote it and to make it accessible to the greatest number of people, particularly for small and medium-sized companies. A concrete link between the technical opinion and operational use in companies and administrations could be made by completing the list of references with use cases. This new catalogue could be produced by involving legitimate players who compile solutions committed to sovereignty, such as the Comité Richelieu, the Alliance pour la Confiance numérique or the Institut Choiseul, under the guidance of the ANSSI. The utility of such a catalogue has moreover been clearly identified by GICAT's (the French land defence and security industry association) soon-to-be-created Digital Cyberspace Commission, which has identified this referencing as one of its areas of work.

Adopt new standards and practices for greater efficiency and trust 6

Implement Security by design in the development of IT products and solutions.

Develop crowdsourced security that ensures a high level of security by encouraging company employees to report incidents and vulnerabilities that they may discover. Vulnerability disclosure policies that share the severity and extent of flaws, while legally protecting researchers, are thus central to fostering confidence in information systems and future technologies.

Implement mandatory vulnerability scanning programmes similar to those developed in the United States (Hack DHS or Operational Directive 20-01). ■

About us

The Institut Choiseul

The Institut Choiseul is an independent, non-partisan and non-profit think and do tank. It is dedicated to deciphering the major economic issues and to uniting the young economic generation.

To fuel public debate and embody current economic dynamics, the Institut Choiseul produces Strategic Notes, occasional studies, and rankings of young leaders. To federate and animate its communities, it organizes high-level events combining convivial networking, testimonies of experts and practitioners as well as exchanges on prospective subjects, in different territories and across economic topics, in France, Europe and Africa.

At the crossroads between a business community and a think tank, the Institut Choiseul offers a platform for private and public economic decision-makers to identify each other, network, promote their initiatives and reflect on the major economic trends of tomorrow.

The Sovereignty Initiative's partners

The Institute is supported by a core group of founding partners, all French or European actors, who take an active part in the discussion and in the formalisation of recommendations:

INSTITUT CHOISEUL

Institut Choiseul

12, rue Auber 75009 Paris
+33 (0)1 53 34 09 93

www.choiseul.info