Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

FRENCH NATIONAL DIGITAL SECURITY STRATEGY

France is fully committed to the digital transition. Boasting a highly connected population, buoyed by sustained growth in its digital economy, France draws on talents and strengths on the cutting edge of European and global innovation.

Yet, the digital universe is also a locale for competition and confrontation. Cyberspace has become a new domain for unfair competition and espionage, disinformation and propaganda, terrorism and criminality.

The 'Actions to promote the digital Republic' planned by the French government are intended to promote our values, our economy and protect our citizens. By reinforcing digital security, we favour the development of a cyberspace that provides a sustainable source of growth and opportunities for French companies, thus asserting our democratic values and safeguarding our citizens' digital lives and personal data.

I have high ambitions in this regard. The national digital security strategy must be founded, in particular, on training and international cooperation. It must be supported by the entire national community: the government and the public sector at national and local levels, businesses, and, more broadly, all our countrymen. This is each and all of us' concern.

Meeting the security challenges of the digital world is a key to our collective success. I hope that this national digital security strategy will launch a new dynamic that will simultaneously provide better protection and unfetter our energies.

Manuel Valls
Prime minister

Courtesy translation. Foreword from Manuel Valls, Prime Minister of France, French national digital security strategy

FRENCH NATIONAL DIGITAL SECURITY STRATEGY

The digitalisation of French society is accelerating, with relentless growth in digital services, products and jobs. This has become a national issue. The digital transition favours innovation and growth, yet it simultaneously carries risks for the State, economic stakeholders and citizens. Cybercrime, espionage, propaganda, sabotage and excessive exploitation of personal data threaten digital trust and security, thus calling for a collective, coordinated response based on five strategic objectives.

 # Fundamental interests, defence and security of State information systems and critical infrastructures, major cybersecurity crisis.

By developing autonomous strategic thinking, supported by world-class technical expertise, France will ensure the ongoing defence of its fundamental interests in cyberspace. In parallel, France will continue to reinforce the security of its critical networks and its resilience in case of a major cyberattack by expanding cooperation with private stakeholders at national and international levels.

 # Digital trust, privacy, personal data, cybermalevolence.

For cyberspace to remain safe for businesses of all sizes and for individuals, protective measures and remedial actions will be adopted. Protection will be based on public authorities' heightened vigilance regarding the use of personal data and the development of a range of digital security products tailored to the general public. Remedial actions will be structured around aid to victims of cybermalevolence, providing technical and legal assistance.

 # Awareness raising, initial training, continuing education.

Individuals still lack sufficient awareness of the risks associated with the digitalisation of society. This is why steps will be taken to raise the awareness of schoolchildren and students. In addition, to meet increasing demands from the public and private sector regarding cybersecurity, training of experts in this domain will be enhanced.

 # Environment of digital technology businesses, industrial policy, export and internationalisation.

The growth of digital markets worldwide, together with the associated security imperatives, constitutes an opportunity to differentiate French digital products and services that have a security level adapted to their uses. By supporting investment, innovation and exports, but also via public procurement, the State will develop a favourable environment for French companies in the digital sector offering secure products and services.

 # Europe, digital strategic autonomy, cyberspace stability.

The regulation of international relations in cyberspace has become a major issue. France, along with like-minded Member States, will promote a road map for European digital strategic autonomy. France will also fortify its influence in international bodies and provide support to the least-protected countries, with their consent, to build their cybersecurity capabilities, thereby contributing to the overall stability of cyberspace.

Digital security underpins the digital Republic project. In this regard, the State plays a major role in elaborating this strategy and in launching a dynamic that must now be maintained by digital-sector professionals, public and private decision-makers and citizens.

INDEX

INTRODUCTION

France is going through its digital transition. Networks are omnipresent in the functioning of the State, economic activity and the daily lives of citizens.

Digital technology engenders new uses, new products and new services and is therefore a factor of innovation. It leads to transformation in most trades. It transforms sectors of activity and businesses giving them more flexibility and competitiveness. Boosted by digital support, these sectors are simultaneously more exposed to digital threats.

Doing without digital technology or the lack of access to it results in a form of economic and social exclusion. Similarly, the sovereignty of a State that does not have the autonomy required in the digital sector would be threatened.

For digital technology to remain an area of freedom, exchanges and growth, trust and security must be established and defended. Only through a collaborative and coordinated effort can this objective be attained.

* *
*

An initial cybersecurity strategy was developed in France in early 2010 and was published in early 2011 shortly after the discovery of a cyberattack, the intention of which was to spy on the economic and finance ministries. The attackers, who had been acting for several months, had taken control of the core of one of the ministerial networks and were regularly collecting political, economic and financial information.

This type of cyberattack targets many French businesses of all sizes in all sectors of activity. Businesses are also the target of all types of fraud such as malware infection that makes the business' files unusable until a ransom is paid by means that are difficult to trace.

In parallel, computer system intrusions aimed at stealing personal information (identity, identification data on commercial websites and bank details) are on the rise. Most of the times, it concerns criminals committing crimes that are identical to those known in the material world such as theft, fraud and blackmail, but in an industrialised manner, with less risk of being identified and prosecuted. Organised crime has seized the opportunity provided by electronic communication networks. Their technical capabilities are increasing to the point where they are now capable of carrying out acts of sabotage or taking production tools hostage, for themselves or through subcontracting by hybridisation.

Harassment campaigns are developing on social networks, such as cases of fraud victimisation whereby gullible subjects are persuaded to transfer money abroad.

The defacement of many websites, notably those belonging to territorial authorities, following the attacks of January 2015 and the cyberattack a few weeks later on a French international media have demonstrated the intention and ability of organised groups to cripple information system resources that support our daily lives.

What was recognised as «the state of threat» established in 2010, therefore turned out to be accurate. At present, the threat is intensified by the increase in the capabilities of attackers, the proliferation of techniques

of attack and the development of organised crime in cyberspace.

But another type of challenge has arisen; that posed by the appropriation of digital wealth by a business oligopoly using their dominant position to interfere with the arrival of new businesses and to harness the added value of this budding economy, which will exploit data intended to invent new services, improve our daily lives or make public services more accessible. At the forefront of these data is our personal data; including those related to our privacy. Control of this mass of data opens the way to economic destabilisation and to sophisticated forms of propaganda or ways to mislead people's judgments and habits. In this respect, this threat is a matter for national defence and security, because of its national extent and strategic issues.

* *
*

In light of these risks, which unfortunately are already established, much has already been accomplished.

As was announced in the 2008 French White Paper on Defence and National Security, a national agency was created as of 2009 to address cyberattacks and to protect the State information systems and critical infrastructures.

An industrial policy in favour of the national cybersecurity industry is notably supported by the future investments programme and in the framework of the «Future industry» plan.

In 2013 the French Parliament voted for the measures recommended by the Government aimed at reinforcing the cybersecurity of operators of vital importance and of those who participate in their most critical information systems.

France's positions are supported within all international bodies, and notably the United Nations (UN) which acknowledged the application of international law to cyberspace in 2013. In addition, bilateral operational relations with several countries have been initiated by the State's services.

The ministries have become aware of the political and technical impact of information technologies on their missions and administration activity and are becoming equipped with coordinators in charge of digital issues and the security aspects thereof. A State Information Systems Security Policy was developed and is progressively being implemented.

In the coming years it should be possible to reap the benefits of the measures taken and to extend the scope of public action and stakeholders. It must now be acknowledged and made known that the defence and security of digital technology depends on the national community and not only on the action of the State.

* *
*

Up until the past few years, our defence and national security depended on the expertise, behaviour and decisions of men and women with access to the most sophisticated, protected and secret installations and equipment. But with the emergence of a society that is massively connected, this responsibility is now partially shared by all French people. One connected object or one service that is inadequately secured by its developers, negligence by one information systems' security decision-maker, dangerous behaviour by one service provider or by one employee who carelessly mixes private life and professional life can lead to losses in availability, confidentiality or integrity of essential information, suspensions in activity and economic losses, industrial accidents and losses of human lives or ecological catastrophes and disturbances in public order, capable of affecting the life of the entire nation.

In fact, never has the stability of our future, supported by digital technology, been so dependent on each person's responsibilities and on the collective responsibilities of three communities of stakeholders.

The first community is responsible for recommending and implementing technologies, products and services equipped with the level of security that is adap-

ted to the uses and capable of mitigating the identified risks. The main stakeholders in this community are researchers, product and service inventors and integrators, cybersecurity businesses, electronic communications network operators, internet service providers and remote data processing services.

The second community is responsible for protecting the nation from digital pirates. Besides the implementation of cybersecurity policies, an aggressive policy to develop the required technical competences should be adopted, and an environment of trust should be established that supports the society's digital transformation by defending citizens, our values and our interests in cyberspace. This responsibility obliges the bearer to express his position in favour of qualified security solutions and to promote national industry, also in relation to export. This community consists of elected officials, the Government, central and territorial administrations and trade unions.

The third community is responsible for using the available services and technologies in a well thought-out manner, making rational choices and avoiding high-risk behaviours in actions related to digital life. This community consists of all users, companies' managers, participants in civil society and citizens.

These are synallagmatic commitments made by each stakeholder that enable France to fully benefit from the contributions of digital technology, transform the choices related to digital security into national competitive advantages – which are often currently experienced as an economic and behavioural constraint – and to promote our values, products and services.

The role of the State in cyberspace is to ensure France's freedom of expression and action as well as the security of its critical infrastructures in case of a major cyberattack (objective 1), to protect the digital lives of citizens and businesses and combat cybercriminality (objective 2), to ensure the education and training required for digital security (objective 3), to contribute to the development of an environment that is conducive to trust in digital technology (objective 4) and to promote cooperation between Member States of the European Union (EU) in a manner favourable to the emergence of a European digital strategic autonomy, a long-term guarantor of a cyberspace that is more secure and respectful of our values (objective 5).

FIVE STRATEGIC **OBJECTIVES**

1

#FUNDAMENTAL INTERESTS, DEFENCE AND SECURITY OF STATE INFORMATION SYSTEMS AND CRITICAL INFRASTRUCTURES, MAJOR CYBERSECURITY CRISIS

STAKES

France is the target of cyberattacks that damage its fundamental interests.

Today, when an attacker targets the State, operators of vital importance or strategic businesses, the aim is for long-term installation in the information system in order to steal confidential data (political, diplomatic, military, technological, economic, financial or commercial). In the future, an attacker could take control of connected objects, remotely interrupt an industrial activity or destroy its target. Since 2011, about one hundred major cyberattacks have been addressed, most often in complete confidentiality, by competent administrations and service providers.

In parallel, the positions taken by France on the international scene, its military operations and certain public debates are followed by cyberattacks aimed at marking public opinion. For example, the defacement of many websites after the terrorist attacks that targeted France in the beginning of 2015 had a technically low but symbolically high impact desired by the attackers. Similarly, the cyberattack that led to the interruption of an international French media was also aimed at making a strong impression and contributes to the radicalisation that leads to terrorist acts. This attack also demonstrated the capacity of attackers determined to disrupt the functioning of a highly symbolic infrastructure.

For several years now many States have implemented their political will and considerable human, technical and financial means to carry out large-scale cyberspace operations against us.

Whether they are known through publicly disclosed documents or revealed during the treatment of cyberattacks, the excesses of such practices harm the credibility of some of these States on the international scene and destroy the trust that would be naturally attributed to their businesses' digital products and services.

Therefore, the cyber risk, which was placed in third position for major threats to France by the 2013 White Paper on Defence and National Security, is now reinforced and constitutes a major challenge facing France.

« the excesses of such practices harm the credibility of some of these States on the international scene and destroy the trust that would be naturally attributed to their businesses' digital products and services. »

OBJECTIVE

France will ensure the defence of its fundamental interests in cyberspace. It will reinforce the digital security of its critical infrastructures and do its utmost to ensure that of its essential operators to the economy.

ORIENTATIONS

> **Having the scientific, technical and industrial capabilities required to protect sovereign information, ensure cybersecurity and develop a trustworthy digital economy.**

An Expert Panel for Digital Trust will be created, under the aegis of the State Secretariat for Digital Technology and the National Authority for the Security of Information Systems.

The Expert Panel for Digital Trust will very regularly unite the competent administrations of the Prime Minister, the Ministries of National Education, Higher Education and Research, Justice, Defence, Social Affairs, Health and Women's Rights, Economy, Industry, and Digital Technology and the Ministry of the Interior, the General Commission for Investment, the National Research Agency and the research organisations concerned. The panel can include stakeholders from the

private sector and qualified key figures in their work.

The mission of this panel will notably be to identify the key technologies for which in-depth knowledge is required for cybersecurity professions and in general for the development of a trustworthy digital environment. It will evaluate the initial and continuing education needs, will monitor Research and support its development, participate in improving support for young PhD holders. In the field of digital technologies, it will contribute to setting the strategic goals of systems for financing and supporting research and industrial development. This work will be implemented in consistence with that of the structures that have already been established such as the French Security Industries Sector Association (CoFIS).

In general, the choice of major private stakeholders in terms of economic or technological model, which are sometimes external to any normalisation framework, or simply certain innovations in digital uses, can consolidate trust or incite mistrust. The Expert Panel for Digital Trust will organise technological and economic monitoring through which evolutions of digital related issues can be anticipated. If necessary, adapted measures will be recommended to support or supervise these changes. These measures could, for example, concern the protection of the Nation's scientific and technical potential or the control of foreign investments in critical national businesses.

The ministerial coordinators for cyberspace issues in collaboration with the General Secretary of Defence and National Security will come together in an Expert Panel Commission for the subjects that fall within its competence.

This Expert Panel will also give an annual report to the Prime Minister on its activities.

> Ensuring active monitoring of the security of technologies and uses for the State, businesses and citizens.

In anticipation of major technological developments, such as the 5th generation of mobile telecommunications (5G) or «software-defined networks», France will remain attentive to the type and capabilities of equipment and software installed within these electronic communication networks, to protect the privacy of correspondences, that of its citizens and the resilience of these infrastructures, and will continue to adapt its regulatory framework to new emerging technologies.

The National Authority on Information Systems Security will regularly inform the ministries, businesses, territorial authorities and citizens, by means adapted to the target community, of factors that might present a danger in terms of digital use. These information will have been consolidated beforehand with the competent administrations.

> Accelerating the reinforcement of State Information Systems Security.

Since 2010, several measures have been taken to raise the level of security of State information systems. A State Information Systems Security Policy (PSSIE) was developed, an inter-ministerial electronic communications network is in rapid growth and the roll-out of secured mobile terminals has been initiated. These measures, like those aimed at producing the security equipment to protect sovereign information, mobilise human and budgetary resources. They will be pursued in order to provide to the Government and our military capabilities with the level of security adapted to long-term preservation of France's autonomy in making decisions and taking action.

The application of the State Information Systems Security Policy and the effectiveness of the measures adopted will be evaluated annually. An annual confidential report will be transmitted to the Prime Minister and the Parliament will be informed by means of indicators.

With the same objective of informing the Parliament, as of 2016, bills will have a section in their impact assessment dedicated to digital technology which will also include cybersecurity, established under the auspices of the senior civil servants in charge of the quality of regulation. More broadly, senior civil servants in charge of the quality of regulation will ensure that the

issues related to the reinforcement of the security of information systems is taken into account in the steering of the normative process.

> Preparing France and the multilateral organisations to which it belongs to face major cybersecurity crises.

Reinforcement of the security of the most sensitive information systems of operators of vital importance, which was announced in the 2013 White Paper on Defence and National Security, was the subject of legislative measures (Articles 21 and 22 of law n° 2013-1168 of 18 December 2013). The work started with these operators will continue over the long term, notably by routine updating of regulatory texts. This work will be progressively extended, as is specified by the law, to public and private operators who participate in these sensitive information systems.

This choice made by France will have made it possible to actively participate in the development of the orientations of the European Directive concerning measures to ensure a high common level of network and information systems security across the Union and to anticipate its transposition. At the right moment, France will specify the operators who are essential to its economy according to the orientations of the Directive and will participate in the European initiatives intended to reinforce their digital security.

Over time, cybersecurity crises management exercises carried out at the national level will progressively concern the entire territory and vitally important activity sectors. The Ministry of Defence, in collaboration with the National Authority on Information Systems Security, will continue to implement a cyberdefence reserve for operational purposes to face major information technology crises.

In parallel, France will continue to contribute to the emergence of an environment of voluntary cooperation for cybernetic crisis management at the European level, by supporting the work of the European agency ENISA (European Union Agency for Network and Information Security) in particular.

It is up to the CERT-EU (Computer Emergency Response Team of the European Union (EU) institutions, bodies and agencies) and to the NCIRC (Computer Incidence Response Capability) within the North Atlantic Treaty Organization (NATO) to ensure the cyberdefence of their respective institutions. France, which is active during cybersecurity crisis management exercises organised by these organisations, and which is highly represented in proceedings that orient EU and NATO choices concerning secured digital technologies, will continue to provide its support to these institutions and their members according to their respective competences.

France will also contribute to reinforcing the cybersecurity of other international organisations to which it belongs, on a political and technical level, notably those hosted on the national territory that benefit from the national technical environment.

> Developing an autonomous way of thinking that is in line with our values.

The strategic choices made by France immediately after the Second World War led to the emergence of an autonomous way of thinking and the development of a doctrine that gave France a unique place on the international scene and today still permeates its diplomacy and the concepts behind the use of its armed forces.

Although digital technology fundamentally changes our societies, its impact on other realities such as those of sovereignty, national territory, currency or the fundamental interests of the Nation is yet to be measured and the organisation and means of public action to make the law apply to it or to ensure their protection must be reconsidered. A discussion, coordinated by the General Secretary of Defence and National Security, will be held to develop an intellectual corpus related to cyberspace.

2

#DIGITAL TRUST, PRIVACY, PERSONAL DATA, CYBERMALEVOLENCE

STAKES

Although in general the French trust in digital technology, they are wary of its impact on their daily lives and especially their personal lives. But despite being generally careful in the use and preservation of their personal data, they entrust them to platforms for which the conditions of use are one-sided to users' detriment.

The technique noted during certain cyberattacks against businesses or administrations also shows a real difficulty separating private and professional life when using equipment and services.

The objective of cyberattacks against individuals is usually financial gain. By taking control of the personal equipment used (computers, tablets, smartphones), usurping identity and stealing users' banking or commercial website credentials, starting a friendly virtual relationship that ends with a request for a money transfer, or encoding data without the user's knowledge resulting in the payment of a ransom, racketeering is today widely practised by a criminal element that has become organised and increasingly efficient.

While no special technique of attack is used, harassment, which is facilitated and amplified by electronic communication networks, is a digital aggression against people with results that are sometimes tragic.

Although the National Cybersecurity Agency (ANSSI) is the identified State contact in case of serious cybersecurity incidents that affect the administrations and operators of vital importance, there is far less clarity regarding the public offer for assistance to victims of cybermalevolence for the other stakeholders, whether it concerns intermediate-sized enterprises, small and medium-sized enterprises, liberal professions, territorial authorities or individuals.

Victims of cybermalevolent acts are encouraged to file a complaint with the police or gendarmerie services which have adapted to the treatment of such disputes. Nevertheless, the response with which they are provided in this framework is focused on the identification of those suspected of the cybermalevolent acts and on the commitment, if applicable, to filing proceedings against these suspects. Victims must be able to reach a service that is competent in the treatment of the cybersecurity incidents as these incidents are often the source of the cybermalevolent acts.

Digital platforms, including social networks, can shape opinion more insidiously and are often vectors of values that are not those of the French Republic. In certain cases, they can be used for purposes of disinformation and spreading propaganda to French citizens, in particular the youngest ones. The opinions that are disseminated are therefore against France's fundamental interests and are an attack on defence and national security which is sanctioned by law.

Another area of concern is the recent and simultaneous developments of new uses and new data storage and processing techniques which contribute to the emergence of risks of economic imbalance and attacks on individual and national security. For example, the desire to introduce the free flow of data, including personal data collected by connected objects, through commercial treaties, does not successfully mask the intent to appropriate these data by oligopolies whose values and practices do not correspond with the French or European concept of privacy or with its legal framework. Massive and illicit appropriation of certain types of personal data, for example, health-related data, can actually affect individual and collective security, or simply result in abusive commercial exploitation (resale to insu-

« Digital platforms, including social networks, can shape opinion more insidiously and are often vectors of values that are not those of the French Republic. »

« Digital technology development cannot be sustainable in a cyberspace where States do not respect the good practices required for a balanced digital transition that is beneficial to all nations »

rance companies, for example).

Digital technology development cannot be sustainable in a cyberspace where States do not respect the good practices required for a balanced digital transition that is beneficial to all nations and where a few economic players monopolise the wealth that constitutes digital data, notably personal data, true resources for future generations.

OBJECTIVE

France will develop cyberspace use that is in line with its values and will protect the digital lives of its citizens. It will increase its combat against cybercrime and its assistance to victims of cybermalevolence acts.

ORIENTATIONS

> Advocating and defending our values on electronic communication networks and in international proceedings.

Individual rights are applicable in the same way «on-line» and «off-line». Cyberspace should therefore remain a place of free expression for all citizens, where abuses can only be prevented within the limits set by the law and in line with our international agreements. In international proceedings, France advocates this approach aimed at preserving a free and open cyberspace.

It is the State's responsibility to inform citizens of the risks of manipulation and propaganda techniques used by malicious players on the Internet. After the terrorist attacks against France in January 2015, the Government established an information platform on the risks related to Islamic radicalisation via the electronic communication networks : « Stop-djihadisme.gouv.fr ». This approach could be extended to respond to other phenomena of propaganda or destabilisation. The competent defence and security services are responsible for detecting these phenomena and providing the Government with recommendations for implementing these measures.

> Providing local assistance to victims of cybermalevolent acts.

Co-piloted by the Ministry of the Interior and the National Agency for Information Systems Security, with the support of the Department of Justice, the Ministries of Finance and Public Accounts, Defence, Economy and Industry, and Digital Technology, a national system will be established as of 2016 to provide assistance for victims of cybermalevolence.

This system will also be aimed at increasing awareness of the challenges of protecting digital privacy and of prevention which, on a local level, will be based on measures taken by prefects and State services. ANSSI's territorial network, the regional economic intelligence delegates and the competent economic security departments of the Ministry of the Interior, the «digital transition» network and that of the Bank of France (which could in the long run, integrate a criterion related to the consideration of the cyber risk in its company listing) will participate in this mission. An appeal will be made to the Chambers of Commerce and Industry, the Guild Chambers and in general all the professional networks.

The system will have a legal form and an organisation that will enable it to benefit from the contribution of economic stakeholders from the cybersecurity sector; software editors, digital platforms and solution providers. Thanks to the technologies implemented, the system should provide victims with technical solutions supported by local stakeholders and facilitate administrative procedures, notably to encourage the lodging of complaints.

> **Measuring cybercrime.**

The inter-ministerial work initiated by the Ministry of the Interior since 2013 has led to the conclusion that there are currently no reliable statistics specifically related to digital delinquency or cybercriminality since most of the offences concerned are registered under a classification that does not take into account this dimension, which is currently absent from the reference systems used.

The absence of such statistics is detrimental to the elaboration by the public authorities of policies continuously reassessed and to the implementation of adequate measures. This is why the Ministry of the Interior will implement new instruments to monitor the development of cybercrime in order to guide public action. The National Delinquency and Penal Solutions Monitoring Agency will also contribute to it by dedicating a section of its work to the statistical examination of cybercrime. This section will integrate data transmitted by the National Authority on Information Systems Security and by the system for the assistance of victims of cybermalevolent acts, which have contributed to its elaboration.

> **Protecting the digital lives, privacy and personal data of the French people.**

With the prospect of the European Regulation on electronic identification (eIDAS - Electronic Identification and Trust Services), France will equip itself with a clear road map for digital identity delivered by the State. This road map will be established before the end of 2015 under the aegis of the Ministry of the Interior and Secretaries of State in charge of Digital Technology and State Reform, supported by the Departments of the Prime Minister, and should include a section that will define a framework of reference to the benefit of the territorial authorities to use digital identity delivered by the State.

This road map will take into account the Government's digital strategy which provides for the roll-out of federated identity systems to enable the use of the same digital identity to authenticate the same person on different services. Thanks to these systems, digital identities can be provided by different entities as long as the third party responsible for managing the federated identity is capable of determining the level of

trustworthiness associated with the identity.

Subject to compliance with the security requirements adapted to the uses and threats, these systems are intended to increase users' trust in their digital world and contribute to its smooth flow while minimising the risk of unwanted processing of their personal data. For more sensitive use, such as that which concerns democratic life or international exchanges related to the law, high levels of trustworthiness of the systems and services will be systematically enforced. These high levels of trustworthiness will rely on the national industrial make-up and the established security certification scheme.

France will protect its citizens' privacy and personal data. The right to privacy and individual and collective control of personal data will be reaffirmed whenever necessary and notably during commercial negotiations between States, whether bilateral or multilateral.

To inform the French people on the use made of their data entrusted to digital services, an identification system adapted and shared with the participating States and consistent with the European work carried out in the framework of the European Regulation related to the protection of personal data will be established during 2016. This identification system will make it possible to view the essential characteristics and conditions of use for digital platforms and services or means of payment used.

> Recommending technical solutions aimed at securing digital life and which are accessible to all businesses and the general public.

The competent State services will label securing solutions for personal terminals. An identification system that is consistent with the one recommended above will enable users to be informed of the potential transmission of information to third parties in the framework of this protection. Once created, the system for the assistance of victims of cybermalevolent acts mentioned above, as part of its mission of prevention, will advocate these systems to the public concerned.

In addition, and since it was possible to initiate this by the future investments programme, the offer of accessible and adapted solutions to secure the digital lives of small and medium-sized enterprises will be supported.

Support for the development of French solutions will be provided as well as for the free software communities that develop security solutions.

> Reinforcing the operational mechanisms of legal international mutual aid and universalising the principles of the Budapest Convention on Cybercrime.

The Budapest Convention, which was adopted in 2001 in the framework of the Council of Europe, has become a reference instrument that enables States of the five continents to cooperate in the combat against cybercrime. Ratified by 46 States, including 7 non-members of the Council of Europe, this instrument now unites 125 States for one reason or another (signatories, States invited to become members, States receiving technical assistance in view of future membership, States that have adapted their internal law to the model of the Convention).

It is now essential to universalise and consolidate the base of norms as well as the tool of cooperation that this text is composed of.

In addition, France will advocate the definition of a system of simplified legal cooperation between Member States within the European Union in order to accelerate the transmission of data and put an end to illegal activities.

3

#RAISING AWARENESS, INITIAL TRAINING, CONTINUING EDUCATION

STAKES

France is late in comparison to its partners in terms of raising the awareness of its population to the risks associated with the use of digital technologies and in cybersecurity training.

In general, the French neglect good practices when using electronic communication networks.

In private use of electronic communication networks, children and adolescents confronted with unsuitable content, exposed to harassment or predation, are the primary victims. In order to break the silence and enable legal proceedings, the youngest subjects should be taught how to proceed when they are victims of digital malevolence.

Raising the awareness of everyone is a required prerequisite for elected officials, administrative or business leaders to be able to take «cyber risk» into account at the right level and to choose measures capable of protecting the citizens whom they represent or the organisations that they run, in light of the threats of information or intellectual property theft, violation of personal data, or even exposure to breakdowns in activity and production accidents, with the technological or environmental impacts to which they are potentially exposed.

Besides raising the awareness of the youngest subjects, training in digital technology professions should provide future professionals in the field with extensive information systems security skills, which remains currently absent from many higher education programmes.

In addition, the content and number of initial training and higher education programmes for cybersecurity professions do not meet the needs of businesses and administrations.

OBJECTIVE

France will raise children's awareness of digital security and responsible cyberspace behaviours as of school age. Initial higher education and continuing education will include a section dedicated to digital security adapted to the sector under consideration.

ORIENTATIONS

> **Raising the awareness of all French people.**

An ambitious awareness-raising programme for all French people should be initiated.

Under the command of the Ministry of National Education, Higher Education and Research and the State Secretariat for Digital Technology, with the support of the Government's Information Department and the National Agency for Information Systems Security, a call for a show of interest in the creation of educational content for the general public will be launched.

The Ministry of the Interior will continue the «Internet Licence» operation which was initiated in 2014 by the Gendarmerie in collaboration with a private foundation, and taken over by the National Police since the beginning of 2015. This operation makes it possible to raise the awareness of risks and to give advice to more than 300,000 sixth-year students to protect their Internet browsing.

The visibility of the "A digital education for all" portal of the CNIL will be reinforced.

The associations will be invited to develop advertising campaign projects aimed at increasing trust in digital technology and which could become a part of a «great national cause».

> Integrating cybersecurity awareness into all higher and continuing education programmes.

The Ministry of National Education, Higher Education and Research, with the assistance of the University Presidents' Conference, the Grandes Ecoles Conference and the competent administrations, will encourage the establishment of cybersecurity awareness corresponding to the educational field in all initial higher education programmes as of the start of the 2016 academic year.

The Ministry of Social Affairs and Employment, supported by the competent cybersecurity State administrations, will initiate the consultations required for the organisations that provide continuing education to integrate cybersecurity issues adapted to the training in the curriculum as of 2016.

Finally, the State Secretariat in charge of Digital Technology, along with the ministries concerned and the support of ANSSI, will coordinate the initiation of the awareness programme for the professional categories in which an inculcation of cybersecurity issues is particularly necessary in relation to their societal responsibilities. These categories will be specified by the Strategic Committee for Digital Trust.

> Integrating cybersecurity training into all higher education that includes some information technology.

The «CyberÉdu» initiative launched in 2013 confirmed that teachers involved in the higher education curricula for information technology professions are interested in the subjects related to information systems security. This initiative should be reinforced.

The Ministry of National Education, Higher Education and Research, with the assistance of the University Presidents' Conference, the Grandes Ecoles Conference, the administrations and competent professional organisations, will ensure that information systems security training adapted to the field and which covers issues related to digital technology is provided in all initial higher education programmes as of the start of the 2016 academic year. The priority should be to integrate these security elements in the existing courses and in a pertinent manner in the broader context of each field that is taught. It would be useful to base these steps on the educational contents being developed, in close collaboration with the teaching community, in the framework of the CyberEdu project.

The Ministry of Decentralisation and Public Service will ensure that training programmes for public service functions include elements of cybersecurity training. In collaboration with the Ministry of the Interior, it will ensure that the recruitment examination for the civil servants corps of information and communication systems engineers regulated by Decree n° 2015-576 of 27 May 2015, as well as the training that will be provided for the members of the corps will have a cybersecurity section.

In light of a growing demand from our partners, whenever possible, a part of the training and education offer should be adapted to an international public, notably by providing programmes in the English language.

> Recording and anticipating the initial and continuing education needs.

Under the aegis of the Expert Panel for Digital Trust, the short, medium and long-term initial training needs will be established in collaboration with all the stakeholders concerned in the administration and the private sector.

The professional trade unions will be called on to develop and implement continuing education programmes adapted to the needs of employees and businesses.

4

THE ENVIRONMENT OF DIGITAL TECHNOLOGY BUSINESSES, INDUSTRIAL POLICY, EXPORT AND INTERNATIONALISATION

STAKES

« The development of an offer of cybersecurity products and services by national businesses in the digital technology sector should also be seen as an essential factor of competitiveness for these businesses. »

Cyberspace is under rapid growth. 100,000 new objects connect to the Internet every hour. Many French businesses participate in international shows and the success of the «French Tech» initiative for example, shows a real dynamism of French innovation in digital products and services. However, this reality should not hide a certain loss of control and real technological dependence.

Large equipment that ensures the functioning of electronic communication networks with infrastructures located in France, is often designed, developed and managed from centres located outside Europe. The same goes for most of the communications and data security equipment of our operators of vital importance. The operation of an increasing number of businesses is based on the use of applications and data processing hosted in uncontrolled virtual spaces, supported by physical infrastructures located outside the national territory and not subject to European law.

With the increase in the number of connected objects or the concentration of on-line service platforms in the hands of only a few stakeholders for example, current developments both in technology and in economic models magnify this loss of control in the national cyberspace. In the event of an international crisis, access to entire sections of cyberspace could be contested.

The answer to this issue of sovereignty requires first and foremost the maintenance of a strong and competitive national and European industry in the specialised field of cybersecurity products and services. In general, it requires the development, in France and Europe, of a digital equipment and service offer that provides clients with the guarantees of security and trust adapted to the issues and uses.

Users do not have the means to ensure the level of security of digital objects and services themselves. The promotion of security in marketing arguments by suppliers is becoming widespread without, however, allowing for an objective evaluation of the level of security actually achieved. The development of greater clarity in terms of security in the digital offer based on objective elements that can be verified by a third party, constitutes a major challenge for ensuring trust in the digital economy.

The development of an offer of cybersecurity products and services by national businesses in the digital technology sector should also be seen as an essential factor of competitiveness for these businesses. The field of payment methods (smart cards, payment terminals, etc.) is the archetype of an economic sector in which an adapted level of security against threats which can be verified by third parties constitutes a first-line marketing argument. Several national businesses hold a competitive international position in this sector that is largely due to the excellence that they were able to develop and demonstrate in the field of security.

The increase in cyber threats and the growing awareness of the reality of these threats will lead to making security an essential purchase criterion in many other sectors a few years from now. Acting now to improve the security and transparency of the national offer for digital solutions also means preparing their future competitiveness.

In 2015, the share of French businesses, and especially SMEs, that widely use digital technology is only within the average of the European countries. Catching up from behind should be accompanied by improved security of the digital lives of businesses starting with better security of their information systems. This is essential for our competitiveness and therefore our jobs.

The challenge for French businesses is to reconcile the search for productivity, savings and

profitability with the use or development of digital products and services that do not endanger their competitiveness or security, those of their partners or their clients.

Most digital equipment, objects and services that are currently available on the market do not have the level of data security that enables them to avoid an incident: data leakage, malfunction or break in service. For French businesses, ergonomics, the protection of personal data and the level of security of digital products and services that they develop and produce, in the short term should become a differentiator, a competitive advantage for them and in return, for the nation.

In addition, although counterfeiting does not directly fall under information systems security, counterfeit cybersecurity products can endanger the activity of organisations that purchase them.

In terms of the internationalisation of businesses and export, considering the environment of extreme international competition in which our partners provide solid and structured support to their industry, the State services should become sustainably organised to support French cybersecurity businesses.

The mobilisation and coordination of all the public and private resources available are essential to increase the visibility and competitiveness of the French offer on an international level and to pool knowledge and feedback and thereby contribute to the sharing of information between the different stakeholders in the field.

« For French businesses, ergonomics, the protection of personal data and the level of security of digital products and services that they develop and produce, in the short term should become a differentiator, a competitive advantage for them and in return, for the nation. »

OBJECTIVE

France will develop an environment that is favourable to research and innovation and will make digital security a factor in competitiveness. It will support the development of the economy and the international promotion of its digital products and services. It will ensure that digital products and services with levels of ergonomics, trust and security adapted to the uses and cyber threats are available to its citizens, businesses and administrations.

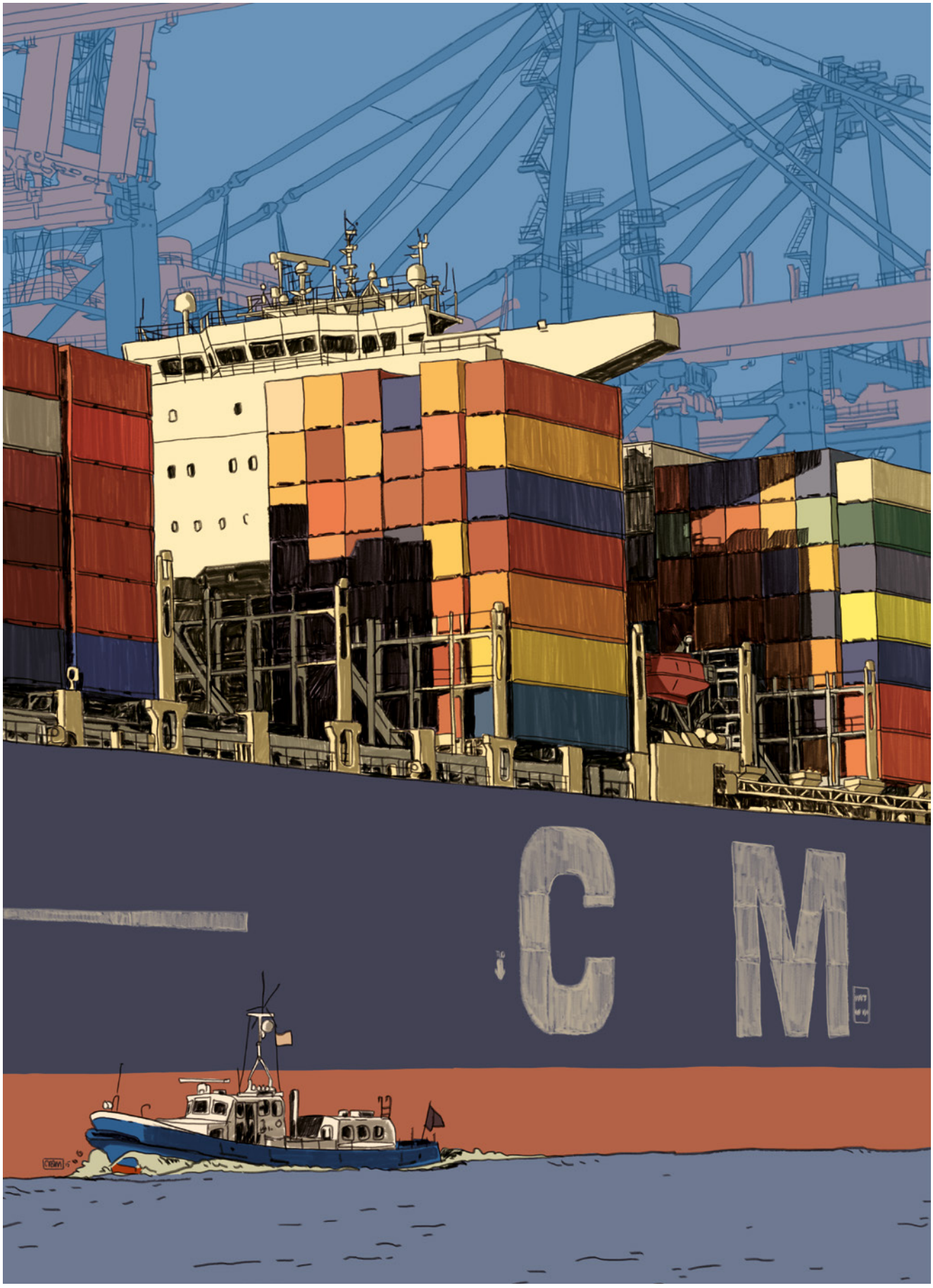
ORIENTATIONS

> Developing and accentuating the national and European offer of security products and services.

In collaboration with the competent administrations of the Ministry of Economy, Industry and Digital Technology and the Ministry of Defence, in 2012 the National Agency for Information Systems Security initiated an industrial policy to develop the national fabric of businesses that develop cybersecurity products and services.

The launch of the New Industrial France «cybersecurity» plan in 2013, now included in the «Digital Trust» solution, and the support of the General Commission for Investment and of BpiFrance made it possible to organise the sector and issue requests for proposals aimed at creating an offer for trustworthy equipment to detect cyberattacks, essentially for operators of vital importance, and secured mobile products for all businesses.

The State services will increase their efforts to qualify and monitor cybersecurity products and services, and support the development of new security products that correspond to the changes in usage patterns. They


C M

will also support the enhancement and perpetuation of these offers through public contracting that chooses security products and services qualified at the right level, as well as by communication and educational measures for the private sector.

In addition, the State services will endeavour to disseminate the results of research and development which they finance for high-level security equipment in order to raise the security level of products for businesses and the general public.

Finally, France will endeavour to take full advantage of leverage offered by the European Union to support, promote and defend French scientific, technological and industrial competences in the cybersecurity fields. It will also discourage the EU from limiting itself to the role of consumer, and will incite it rather to stand out as an indispensable global stakeholder for the offer in this sector.

> Transferring acquired knowledge to the private sector to contribute to the handling of its cybersecurity.

For five years now France has equipped itself with the capacity to detect and respond to cyberattacks, as announced in the 2008 White Paper on Defence and National Security. Although this effort should be pursued, notably by ANSSI, it is up to the private sector to ensure its own security in the field of information technology as is the case in other fields, since the State services are only required to intervene in case of serious crisis.

Supported by the transfer of this knowledge acquired by the administrations to the private sector, labelling of competent and trustworthy service providers should enable the detection and treatment of the inevitable growth in the number of cyberattacks that businesses are subjected to.

> Preparing a safer digital world through better anticipation of uses, adapted support and stakeholders' information.

For the next five years, the priority for the competent information systems security authorities should be anticipation and prevention.

This will entail ensuring that the digital products and services or those that involve digital technology, which are designed, developed and produced in France, are among the safest in the world. To achieve this objective, the competent authorities should direct their communication efforts towards the public and private scientific community, and the innovation centres; competitive clusters, technological research institutes, incubators and «fab labs»; by devoting specific means to these areas as needed, as is the case with the Ministry of Defence, and more recently, the Ministry of the Interior.

When digital products and services store personal data or are intended for the business sectors of vital importance, the State services will provide the elements that are useful for risk analysis or the recommendations required to obtain the level of security that corresponds to the use of the product or the service being designed or developed. For uses that justify it, they will also contribute to establishing systems to independently evaluate the level of security and trustworthiness of these products and services, and to providing their potential users with adapted guarantees through labelling.

In parallel, the legal environment to accommodate new products and services should be anticipated. For example, the imminent arrival of autonomous cars should incite the regulator to prepare the conditions to ensure the security of their circulation. Cybersecurity should be taken into account in the international working groups that define the framework and control technical procedures.

For other types of products or services, an adapted identification system should inform the consumer of their essential digital features and notably the processing of the data that is collected. For certain sectors such as the health sector, systematic labelling of digital products and services will be considered.

France will endeavour to include other EU Member States in the implementation of these practices in order

to create a zone of digital trust and security. The work initiated with Germany on cloud computing or secured messaging is moving in this direction.

> Integrating the requirements for cybersecurity in public contracting and support.

For the protection of its sovereignty and notably the protection of its information concerning the national defence secret, France will preserve its financial and industrial capacity to develop solutions with the highest levels of security.

In general, the entire administration should set an example in public contracting by integrating the right level of security criteria in its choices of digital products and services.

Finally, as of 2016 any product or service that is embedded in or is based on an information system and wants to answer a call for tenders, a request for public projects, or be eligible for public funds, will benefit from a bonus factor if it is accompanied by a cybersecurity risk analysis that corresponds to the intended use of the product or service.

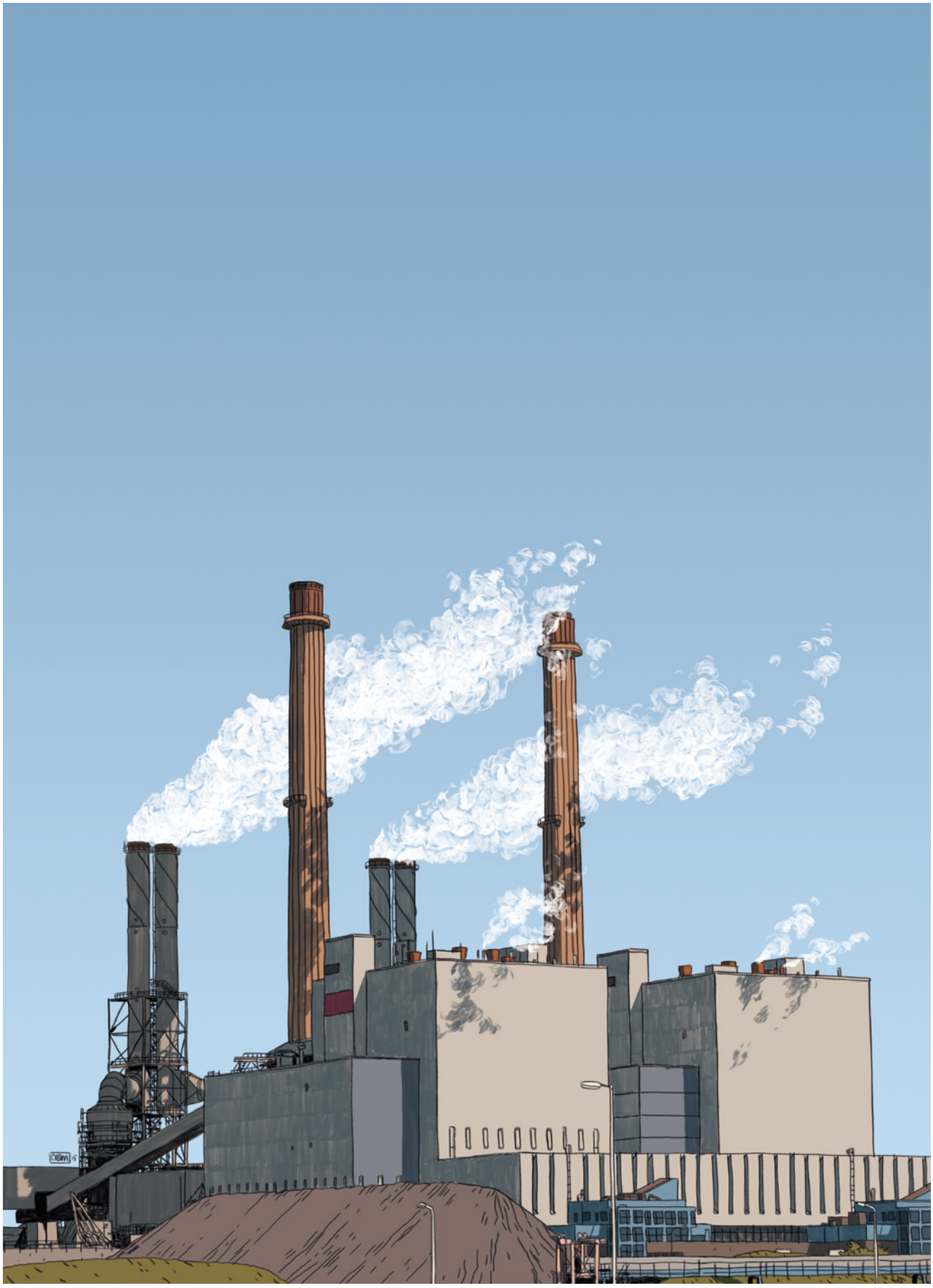
> Supporting export and internationalisation of the businesses in the sector.

To support the economic development of the cybersecurity industrial sector, France will endeavour to reinforce the visibility and competitiveness of the French offer worldwide and to facilitate access of SMEs and start-ups notably to the international markets.

Inter-ministerial coordination will be structured and reinforced. An adapted French business support organisation will be established in addition to the occasional and often isolated measures that are currently led by the different ministries and State entities.

Along with the possible creation of specific support systems for the stakeholders in the cybersecurity sector, the conditions for access to the existing support systems, as well as their implementation methods will be clarified and optimised. The procedures to control exportations of cybersecurity solutions will be clarified and optimised.

In addition, as is the case with «French Tech» creations, the collaborative initiatives generated by the private sector and intended to assist SMEs and start-ups on an international level will be supported.



5

#EUROPE, DIGITAL STRATEGIC AUTONOMY, CYBERSPACE STABILITY

STAKES

Cyberspace has become a major subject for negotiation within international organisations whose work now concerns the entire digital field.

In 2013, the States acknowledged that far from being a space without rules, cyberspace was governed by existing international law. Despite this, the international normative framework is still being debated, which, without any advancement in negotiations, could harm the preservation of a stable safe cyberspace that is compliant with the fundamental laws and is appropriate for the development of a prosperous trustworthy economy in the digital era.

While an increasing number of countries are declaring themselves equipped with offensive capabilities, the level of conflict between States is increasingly being expressed in cyberspace. In addition, the massive revelations of practices and espionage techniques carried out by major States or alliances of States against other States (sometimes allies), people and businesses, have increased the political mistrust of countries that are at the origin of these practices and technical mistrust of their products and services. These revelations also contribute to the proliferation of similar technical methods.

In parallel, groups of individuals with diverse motivations and supports, mercenaries recruited worldwide and associated according to the circumstances, regularly take recourse in cyberattacks to attempt to destabilise the governing authorities of many countries or businesses that symbolise them. In addition, terrorist organisations take advantage of the audience provided by social networks to disseminate propaganda intended to attract volunteers and terrorise the populations. These different groups benefit from continuous media impact.

On the economic level, the trend at the beginning of the decade is being confirmed. A small number of businesses supported by the States which enabled their development use their technological advance, their domination on the market and their financial capacities to pre-empt digital innovation. This privatisation of cyberspace to the benefit of a few monopolies condemns the other stakeholders in digital technology to dependence and harnesses a share of the added value of digital technology that is too great for this situation to be bearable for the economies of the other countries.

« Although it supports world growth, cyberspace has become a place of conflict and often unfair competition »

Although it supports world growth, cyberspace has become a place of conflict and often unfair competition, which until now has been one of low intensity in terms of information technology, and of political destabilisation and economic hegemony.

Europe has been able to identify these issues and through dialogue and regulations is trying to provide ideas and solutions that are more respectful of sustainable digital development, both in terms of Internet governance and protection of personal data or cybersecurity of the operators who are essential to the economy. Despite having adopted a cybersecurity strategy in 2013, Europe is still struggling to assert digital strategic autonomy and equip itself with the tools required to re-balance cyberspace in its favour, even though this subject is now on the agenda for many European centres for discussions and negotiations.

Because it shares common values with other EU Member States, France and these Member States should play a driving role in digital technology.

France wants to participate in the digital transformation of Europe through alliances. Europe built itself in the past through an alliance based on raw materials. Digital Europe will build itself on alliances, trust and data control, the raw materials of the coming decades.

OBJECTIVE

Along with voluntary Member States, France will be the driving force behind European strategic autonomy. It will play an active role in the promotion of a safe, stable and open cyberspace.

ORIENTATIONS

> **Establishing a road map for European strategic autonomy with voluntary Member States.**

This road map, which is open to the European Union Member States, will determine the key factors of success of the short-term implementation of the policies that are adequate for the emergence of a European digital strategic autonomy, notably in terms of regulations, standardisation and certification, research and development, trust in digital technology — while respecting Member States' sovereignty — the protection of privacy and personal data conceived of as a public interest property.

Similarly, France will ensure that the international treaties negotiated in the name of Europe do not lead to technological or economic dependence of European stakeholders and to the alienation of the personal data of its citizens or sensitive data of its administrations, sources of destabilization of cyberspace.

This will involve making Europe the digital territory that is most respectful of the fundamental rights of individuals and implementing a zone of trust and economic prosperity, in line with the precursor work between France and Germany on Cloud computing and the encrypted exchange of e-mails between the two countries.

> **Reinforcing French presence and influence in the international discussions on cybersecurity.**

In order to reinforce trust on an international level and to explore new regulation mechanisms aimed at preventing conflicts in cyberspace, France will reinforce its contact with all the parties directly involved who are willing to engage in dialogue on the issues of cybersecurity.

Participation in multilateral negotiations on cybersecurity (UNO, OSCE) will be intensified in order to consolidate a global base of commitments to good

conduct in cyberspace for the States, in compliance with international law.

Bilateral contact will be reinforced, notably in the framework of inter-ministerial diplomatic dialogue on the issues concerning cyberspace, headed by the Ministry of Foreign Affairs and International Development.

Finally, to assert its influence, France will increase its investment in more informal international forums in which the technical and academic communities and the political decision-makers come together to discuss the future balances.

> Contributing to the global stability of cyberspace by assisting voluntary countries to establish cybersecurity capabilities.

Digital transition, the bearer of political, social and economic opportunities, is far from being uniformly controlled in all countries. This harms the security and development of States that are less protected, and weakens all digital environments on an international level.

In order to contribute to a reliable and sustainable roll-out of digital technologies in all countries, and in particular the developing ones, France owes it to itself to assist in reinforcing the capabilities of countries that would like to increase the resilience and security of their information systems, notably in terms of the protection of critical infrastructures and the combat against cybercrime.

To ensure the durability and sustainability of projects to reinforce capabilities, France will preferably act through long-term trustworthy partnerships. This action should also enable France to reinforce its own cybersecurity.