RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

PAPIERS NUMÉRIQUES

September 2021

PAPIERS NUMÉRIQUES

September 2021

ACKNOWLEDGEMENTS

ANSSI would like to thank all those interviewed who enabled the content to be produced:

External interviews
Jean-Yves Le Drian
Minister for Europe and Foreign Affairs
Karel Řehka
Director of NÚKIB (Czech Republic)

ANSSI interviews
Guillaume Poupard
Director-General of ANSSI

Antoine Berthier
Sector coordinator responsible for telecommunications
Anne-Charlotte Brou
Head of the Press, crisis and international communication office
Chloé Chabanol
Head of the CERT-FR unit
Jean-Baptiste Demaison
Chairman of the ENISA board of directors, responsible for public innovation at ANSSI
Agathe Favetto
European and international political affairs policy officer
Jonathan Gimenez
Cyber Security Act implementation officer
Aude Le Tellier
Head of the European and international political affairs office
Célia Nowak
Cyber crisis management policy officer
Amélie Perron
Deputy head of the European and international politicalaffairs office
Sylvie Pigeon
Deputy head of the International coordination division
Louis Rouxel
CERT-FR cooperation activities manager
Anne Tricaud
Head of the International coordination division
Yves Verhoeven
Head of Strategy Department

COLOPHON

Papiers numériques – September 2021
Published by the French National Cyber Security Agency (ANSSI)

Editorial director
Guillaume Poupard

ANSSI coordination
Aline Barrault (project, interviews and writing)
Marc Renaudin (graphic supervision)

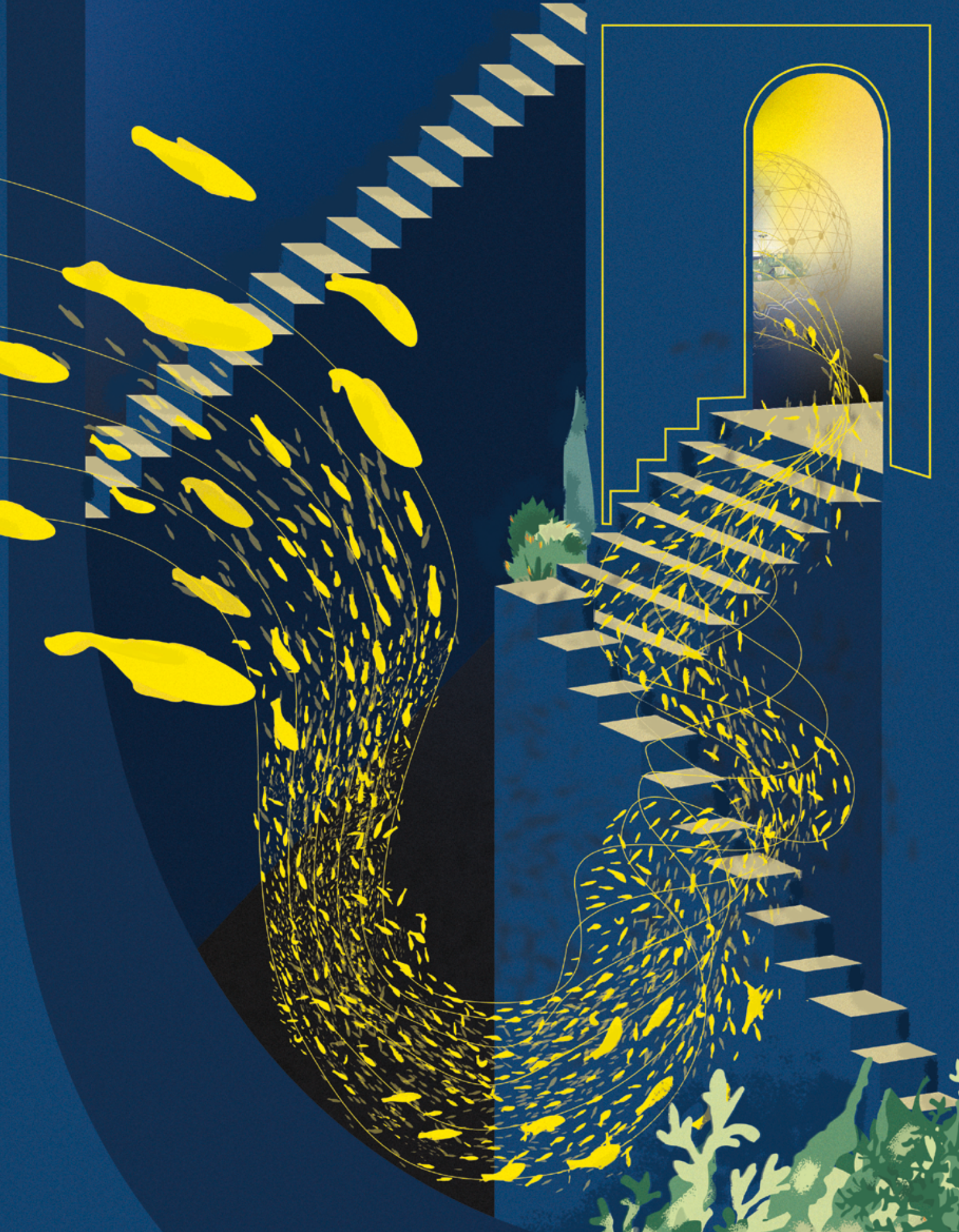
Artistic direction, layout and illustrations
Cercle Studio (www.cerclestudio.com)

English translation
Acolad (www.acolad.com/fr)

Dépôt légal
August 2021

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
51, boulevard de la Tour-Maubourg
75700 PARIS 07 SP

www.ssi.gouv.fr
communication@ssi.gouv.fr



EUROPEAN CYBER SECURITY: HISTORY OF A CULTURAL TRANSFORMATION

In the first half of 2022, France will hold the presidency of the Council of the European Union. An opportunity which, in terms of cyber security, offers the prospect of increasing the momentum started in the last few years. In preparation for this time, certain key words can be heard at ANSSI: ambition, scaling up, cooperation, solidarity, digital sovereignty. Just a decade ago, such intentions didn't come so naturally. Let's take a look back at an area which, year on year, has become considerably "Europeanised".

When, at the start of the 2010s, the bodies of the European Union (EU) suggested to the member states a draft European regulation for IT security, many were interested, yet also... cautious.

Cautious because, at the time, cyber security and cyber defence were mainly perceived as sovereign affairs, the competence of the states. The idea that external bodies could have the right to be heard on these sovereign subjects therefore seemed counter-intuitive to those with an interest in the domain.

Although issues of national sovereignty remain relevant today, the way in which "cyber" subjects are handled at the EU level has changed considerably. In a decade, exchanges between states and bodies of the Union have been ramped up, resulting in regulations, cooperation groups, recommendations, benchmarks, common stances and large-scale projects. All blocks laid down in just a few years, and now testimony to the inestimable value of European cooperation. Because when it comes to cyber issues, things move at great speed.

To prevent the emergence of a two-speed Europe in terms of security, with varying levels of vulnerability among states, the implementation of protection mechanisms at the EU level was in fact inevitable. All the more so since in cyberspace, "borders" are porous: an attack affecting the information systems of an operator within one State can have a rebound effect and impact the services it provides in other countries. When we talk about IT protection, the interests of the various parties involved often overlap.

DEVELOPING NATIONAL CAPACITY

The proposed directive issued therefore pursued a laudable and necessary objective: to defend an area of common economic and societal interest, the EU. But how? "When the subject of building a European cyberdefence emerged, the first reaction was to say that we had to do on a European scale what we were doing on a national scale", recalls Guillaume Poupard, Director General of ANSSI. "We were somewhat opposed to that. Not out of mistrust, but out of pragmatism."

↓
WHEN WE TALK ABOUT IT PROTECTION, THE INTERESTS OF THE VARIOUS PARTIES INVOLVED OFTEN OVERLAP.
↑

Let's put things into perspective. "The most emblematic part of ANSSI's work, historically, is to stop computer attacks against the most critical information systems and to help repair the damage", recalls Anne Tricaud, head of the International coordination division. "If a European body had taken on these tasks, it would have had to intervene in the sensitive networks of critical operators - ministries, large companies, etc. - of states". A very sovereign area, in other words.

The question of the sovereignty of member states was not the only objection raised at the time. "We were not convinced of the effectiveness of a single operational team having to manage crises across the continent," concedes Anne Tricaud. "We therefore asked ourselves how to build a European cyber defence that would be beneficial for national cyber defence", continues Guillaume Poupard. "For us, there was one priority: for each State to develop its own capacity to detect and react to incidents."

↓
"FOR US, THERE WAS ONE PRIORITY: FOR EACH STATE TO DEVELOP ITS OWN CAPACITY TO DETECT AND REACT TO INCIDENTS."
↑

GUILLAUME POUPARD
Director-General of ANSSI

For three years, France, the member states and the EU institutions negotiated what was to become the *Network and Information Security* (NIS) directive, with the development of state capacity as a central principle. In particular, the directive provides for the designation of cybersecurity authorities within each state.

FOCUS ON ESSENTIAL OPERATORS

But the ambition of NIS does not end there. From the first exchanges, the desire expressed is to enact, at European level, security requirements for certain critical operators.

While this subject is emerging at European level, in France, the protection of sensitive operators against computer attacks has already been studied by the Secretariat General for Defence and National Security (SGDSN) and ANSSI. Choosing to act through the Military programming law (LPM), France effectively added in 2013 a "cyber" component to an existing system: the security of activities of vital importance (SAIV). Put simply, this requires the application, for a set of public or private entities whose activity is considered essential to the survival and stability of the Nation, of security measures for their protection.

For those in the know, we refer to operators of vital importance (OVI). Several hundred organisations are divided across twelve sectors. Transport, military activities, health, water management or even energy: we can quickly imagine - well in fact, we'd prefer not to imagine - the potentially dramatic consequences of an attack against such organisations. In addition to setting out a number of security measures for the most critical information systems[1], the LPM requires OVIs to report any cyber incident to ANSSI, the national authority in the matter.

Following on from these developments in France, or comparably in Germany, it is at the European level that the desire to use regulatory lever to protect sensitive organisations from a growing cyber threat is then being carried forward. Within the terminology of the directive, we do not refer to OVIs but to OESs: operators of essential services.

So the stakes are high for France, dedicated to protecting the ambitions of its national law. "There was a real divide", comments Anne Tricaud, head of the International coordination division. "We had two texts intended to provide a framework for the security of critical infrastructures. The two therefore needed to be connected, especially since cybersecurity was considered to remain a matter of national security."

According to Jean-Baptiste Demaison, head of negotiations at ANSSI at the time: "Complementarity was achieved by distinguishing between the types of operators regulated by the two texts. The French law concerned OVIs, critical for national security. The NIS directive, meanwhile, referred to OESs, the protection of which aims to secure the internal market." For Yves Verhoeven, head of strategy department, this outcome marks a major milestone in cybersecurity: "At a time when there were heated debates on the role of NATO in this matter, it recognised, for Europe, the primarily civilian nature of cybersecurity issues for essential operators, which mainly come under the private sector."

STRENGTHENING COOPERATION

In addition to the development of member states capacities and the protection of critical structures, the European directive brings a third pillar: the development of cooperation networks. Here again, the stakes are high, as cooperating on highly technical, intrinsically national and often confidential activities requires a certain amount of inventiveness.

WHAT IS A CSIRT?

A *Computer Security Incident Response Team* (CSIRT) or *Computer Emergency Response Team* (CERT; registered trademark) is a centre for reporting and responding to computer attacks.

There are three main types: CERTs internal to organisations, CERTs of commercial service providers and governmental and/or national CERTs.

The tasks of the French Government and national CERT (called CERT-FR, formerly CERTA) are carried out by ANSSI's Operations department

2004
Creation of ENISA

2009
Creation of ANSSI

2011
First level security certification **plan** (CSPN) for security products in France

2013
Military programming law (LPM)
Protection of operators of vital importance (OVI) in France

2016
European *Network and Information Security* (NIS) directive
Development of national capacities, protection of operators of essential services (OES), creation of the CSIRTs Network and the NIS Cooperation Group

2019
Cyber Security Act
Adoption of a permanent mandate for ENISA and a European certification framework

2021
Regulation establishing the European cyber competence centre and the Network of national coordination centres

2022
French presidency of the Council of the European Union

[1] We then talk about information systems of vital importance (SIIV).

However the idea is not new: several exchange mechanisms[2], both informal and voluntary, already bring together national and governmental CSIRTs (see box). And at ANSSI, we know how useful they are: the example often used here is that of the *WannaCry* global wave of infections in 2017, during which multilateral exchanges significantly contributed to limiting the damage in France.

Based on the principle that encouraging cooperation between States would increase the Union's overall level of security, the NIS directive creates the CSIRTs Network: the first network for cooperation and sharing of technical information between government and national CERTs. "Specifically, we exchange technical markers used to anticipate or even stem attacks, as well as advice in terms to develop a CSIRT", explains Chloé Chabanol, head of the CERT-FR unit at ANSSI.

Beyond the member states, European institutions also have their own dedicated CERT: CERT-EU. Yves Verhoeven explains: "Faced with the sophisticated threat, it became clear that European institutions had to organise themselves to ensure a common capacity to respond to incidents."Created in 2011 at the initiative of several partner states, including France, it is also involved in the CSIRTs Network.

A few years after its launch, the European network is well-established and successful. Plenary meetings, platforms, *mailing-lists*, dedicated *chat*, etc. The network is operational and constantly developing. Louis Rouxel, CERT-FR cooperation activities manager, confirms: "All states

[2] For example the Forum of Incident Response and Security Teams (FIRST), the International Watch and Warning Network (IWWN) or the European Government CERT Group (EGC).

↓
"ALL STATES ARE MATURING AND DEVELOPING THEIR CAPACITY TO COOPERATE. THE EXCHANGE OF INFORMATION REALLY IS IN OUR DNA."
↑

LOUIS ROUXEL
CERT-FR cooperation activities manager

are maturing and developing their capacity to cooperate. The exchange of information really is in our DNA."

FROM A TECHNICAL TO A STRATEGIC LEVEL

It is with this well-crafted directive that, what Anne Tricaud calls the "European transformation" of the agency, begins. "We were able to see that the NIS directive enabled us to strengthen the level of security throughout the Union, to protect more players, to coordinate with our partners ... and thus to help strengthen national security. So we started to think that dealing with cyber matters on a European scale... that was a very good idea!"

Especially since NIS also allows the creation of a strategic cooperation group. Initially designed to discuss the implementation of the directive, the forum has evolved to accommodate broader topics, such as securing 5G technology. A subject which knows all too well the interests of the major world powers, sometimes opposing positions, against which Europe must adopt a consistent stance. Antoine Berthier, sectorial coordinator responsible for telecoms at ANSSI, takes stock: "We have reached a balanced position by focusing on technical and safety issues. Each country has conducted its risk analysis to bring out a set of recommendations." For Yves Verhoeven, the creation of this instrument is a dual success: "Firstly, because it is the result of intelligent cooperation between the Commission and the member states in the face of a great technological challenge of our time. And secondly, because it constitutes a first illustration of what European digital sovereignty can be: neither naive nor autarkic."

More recently, the group served as an incubator ... for CyCLONe.[3] Dedicated to crisis management, this fledgeling network brings together the European counterparts of ANSSI's Director-General. "In 2018, the organisation of a crisis management exercise at European level highlighted the need for cooperation at a more strategic level than the CSIRTs Network, which has more of a technical vocation", explains Agathe Favetto. In addition to this observation was the desire expressed by Guillaume Poupard to be able to prepare for a major crisis with his European counterparts. The Blue OLEx event, organised in Paris in 2019, then allowed a first meeting and, subsequently, the formal creation of CyCLONe.

"We have not yet had to put it to the test" states Guillaume Poupard, reassuringly. "But the preparation work we are doing today will save so much time when the moment comes." More able to take a step back from technical incidents, to have an overview of the impacts and to provide political advice, CyCLONe continues to improve, also by developing its interactions with the CSIRTs Network.

A UNIFYING AGENCY

We can say that NIS paved the way for all the initiatives that followed for the construction of genuine European cybersecurity. That with the solid foundations it laid, all the blocks that have been put together since then can't help but fit together naturally.

But let's take a little step back. A first stone was, in fact, laid several years before the turning point of the famous European directive, almost as if to mark the place where it was to be built. As early as 2004, an institution was conceived as a means to strengthen cooperation between the states of the continent; a European cybersecurity agency: ENISA[4].

Several years before the acceptance of the very concept of European cybersecurity and the first steps in this

[3] Cyber Crisis Liaison Organisation Network

[4] European Union Agency for Cybersecurity

"France has, since the early days of the implementation of the European digital strategy, been promoting a vision at the heart of which lies digital sovereignty."

JEAN-YVES LE DRIAN

Minister for Europe and Foreign Affairs

How does cooperation between the ministry for Europe and Foreign Affairs (MEAE) and ANSSI help to promote French interests in cybersecurity?

The MEAE and ANSSI work closely together to lead our country's international action in the field of cybersecurity. Firstly, we are working together to strengthen cooperation with our partners. The MEAE and ANSSI also participate in bilateral strategic dialogues we hold with the most significant states on major cybersecurity issues. Secondly, ANSSI supports the MEAE in defining French positions in multilateral fora, particularly at the United Nations, to defend our vision of an open, safe, stable, accessible and peaceful cyberspace. We also support the French conception of the role of private players in the governance of cyber space, in particular to the Organisation for Economic Co-operation and Development. Finally, at EU level, ANSSI and the MEAE promote the aim of European digital sovereignty based in particular on enhanced cyber security.

To what extent does the French presidency of the Council of the European Union represent an opportunity to develop cyber priorities?

Cyber issues are one of the digital priorities of our presidency of the Council of the EU. The first step will be to foster the capacity of member states to show solidarity in the event of a large cyber incident or attack. For this to happen, building up the capacity and the resilience of both the EU and member states is essential. That is why we will place special emphasis on strengthening the security of EU networks. Regarding the Union's external action plan, we intend to propose a review of the EU's strategy in terms of capacity building for third party countries, in order to better coordinate the actions carried out. European research and industrial innovation in the cyber domain also need to be developed. These actions will be fully in line with the implementation of the Union's cybersecurity strategy.

How does France intend to support the construction of a secure, trusted and prosperous digital space on a European scale?

The key to building a digital Europe lies in defining a common understanding of the objectives responding to the major challenges posed in this domain. This is why France has, since the early days of the implementation of the European digital strategy, been promoting a vision at the heart of which lies digital sovereignty. By this we mean the promotion of a model based on our values, which is neither inward-looking nor representative of a desire for supremacy, but which will on the contrary promote the opening of the Union to the world, whilst ensuring its independence and the protection of its interests. It must promote cyber security, innovation, responsible standards and the protection of the main common digital objectives. We support current and future European initiatives, aimed at making this agenda a reality, and we are in favour of the adoption of these instruments that reflect this state of mind. ●

direction, this rather pioneering agency was like a UFO. However, within a decade, ENISA has developed missions that have proven essential. First on the list: organising the Cyber Europe exercise, held every two years, simulating cyber crises and testing states' capacity to cope with them. And in 2019, fifteen years after its creation, the adoption of the *Cyber Security Act* moved ENISA on to a new dimension.

This regulation gives ENISA a permanent mandate and clearly defined missions. For Jean-Baptiste Demaison, chairman of the board of directors at the European agency since 2016, "ENISA plays an essential coordinating role. Within the framework of the various groups and networks bringing together the member states on cyber issues, it is quite naturally ENISA which coordinates and summarises the work."

Beyond this first role, ENISA has the crucial task of providing information on good practices and raising awareness. "This is undoubtedly the field in which it has proven most essential", comments Jean-Baptiste Demaison, "with its training, its guides, its exercises and the coordination of the European cybersecurity month (editor's note: known as Cybermoi/s in France). It has also gained legitimacy in European public policies, where it can be consulted for the production of guidelines. Lastly, it can on request advise states victims of incidents."

Far from the initial uncertainties, ENISA is now demonstrating just how important it is. "It is a great ally in the European cyber ecosystem, which is extremely varied and complex. Without a coordination body, there would be a real risk of everything being fragmented", concludes Jean-Baptiste Demaison.

ENSURING TRUST IN THE ECOSYSTEM

And the *Cyber Security Act* gives ENISA another fundamental role. Because the 2019 regulation takes things to a new level by creating a European framework for safety certification (see box). A real turning point for security and digital trust in Europe.

The principle: harmonise the certification practices of the member states to allow mutual recognition within the EU. A certified Swedish service would therefore also be certified, for example, in Portugal or Hungary.
The development of a European industrial network capable of delivering trusted services is a central subject here. "Certifying services requires considerable resources from suppliers", states Amélie Perron, at the heart of the negotiations for this section of the *Cyber Security Act*. "Developing access to a European market therefore encourages them to embark on this process. And through a domino effect, this serves our objective: to raise the overall level of security."

The project is therefore an ambitious one. "For ANSSI, the aim was to prevent the homogenisation of practices from becoming synonymous with a race to the bottom", continues Amélie Perron. To avoid this risk, the regulation ensures thorough knowledge of the process by specialists within the member states. National certification authorities[5] are therefore designated and networked[6]. In France, this role is performed by ANSSI.

It should be noted that in itself, the *Cyber Security Act* defines a framework and governance, without specifying the certification rules. The products, services and processes to be certified will successively be the subject of plans around a set theme. This therefore looks set to be an ongoing adaptation performed by the member states, guided by ENISA.

One of these plans, currently under negotiation, concerns a well-known and emblematic subject: the *cloud*. On this subject, a major issue concerns immunity to non-European extraterritorial laws. A technical expression that conceals a fundamental issue: protection against access by foreign powers, thanks to their own regulations and under certain conditions, to data hosted by their *cloud* service providers. This includes when the servers in question are located in EU territory.

The French SecNum*Cloud* qualification - which will eventually be replaced by the equivalent European certification scheme - already incorporates this "immunity" by ensuring its users the exclusive application of European law and control over the hosted data. By integrating this provision across the continent, after the General data protection regulation (GDPR), the EU would once again demonstrate its intention to take action to protect the data of European organisations and citizens. "Not doing so would condemn European users to a lack of control over their data", states Amélie Perron.

WHAT IS CERTIFICATION?

Certification is the confirmation of robustness of a security process, product or service. In France, high-level certification is issued under the name "Security visa" following a rigorous verification process, under ANSSI's authority

In France, the LPM requires OVIs to call on organisations holding an ANSSI visa for certain services. Certification gives users trust in the level of security of the services requested and allows suppliers to access new markets.

[5] We refer to National Cybersecurity Certification Authorities (NCCA).

[6] Through the European Cybersecurity Certification Group (ECCG)

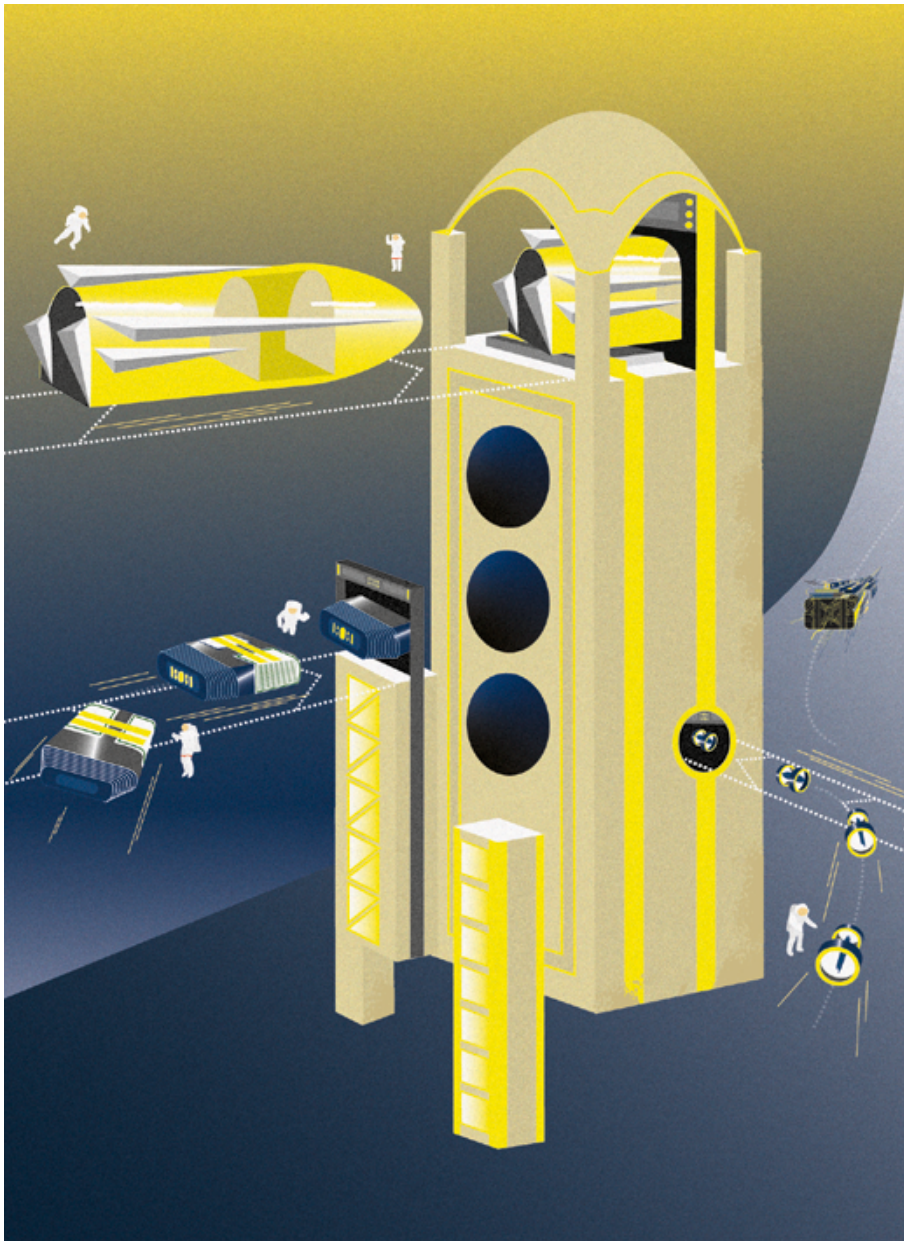
Anne Tricaud concludes: "It is a real matter of European sovereignty."

SCALING UP

However, as the head of the International coordination division reminds us, "We talk a lot about the *cloud*, but certification goes way beyond that." Especially since the European framework provides for three levels of certification: basic, substantial and high. Although the last of these corresponds more or less to the historical spectrum of ANSSI in this area, the addition of the first two levels makes a big difference. At ANSSI, there is even talk of a "revolution": certified services will be aimed at small businesses, associations, communities and citizens ... far removed from the traditional OVIs and OESs! A new scenario which therefore involves a change of method. "At the high level, ANSSI approves assessment laboratories (editor's note: CESTIs[7]), validates the reports and declares the certification itself", explains Jonathan Gimenez, responsible for the implementation of the *Cyber Security Act*. "To scale up at basic and substantial levels, ANSSI will authorise private organisations to issue certifications under certain conditions."

And, while "certification" historically relates above all to security products (smart cards, VPN, encryptors, etc.), it will increasingly encompass digital products which need to be secured *by design*, as well as services or processes essential to the construction of a secure digital space. Testimony to this is the upcoming work around connected objects or even secure development processes. There is a very wide and extremely promising range of possibilities for digital trust on the continent. "We wondered at the start what subjects deserved to be put before the Union", says Guillaume Poupard.

[7] Information technology security assessment centre. See glossary.



↓
"FOR ANSSI, THE AIM WAS TO PREVENT THE STANDARDISATION OF PRACTICES FROM BECOMING SYNONYMOUS WITH A RACE TO THE BOTTOM."
↑

Amélie Perron
Deputy head of the European and international political affairs office

"In fact, when we talk about certification, we can see that it makes a lot more sense to work with our European partners rather than alone, in our Gaulish village."

PREPARING THE NEXT STEPS

Regarding the development of the cyber industrial network, another major step has just been taken. Because while there are, within the EU, numerous centres of expertise in cyber research and innovation, a new regulation has just been adopted to ensure their coordination. "It's a question of establishing a common roadmap to allow all these players to work on the basis of identified priorities", explains Aude Le Tellier. "This will avoid the use of funds for projects that do not result in solutions on the market, or that do not meet the needs of users." To do this, the regulation provides for coordination mechanisms at State level but also at European level. A cyber competence centre located in Bucharest could therefore organise calls for projects itself. "This regulation promises to be fundamental for the strategic autonomy of the EU."

Under consideration for the future of European cybersecurity, there is also and above all the revision of the NIS directive. A "V2" that Anne Tricaud expects to bring about major changes: "Through this new directive, we could be required to regulate a much wider field of operators. Many companies and organisations would be involved." A necessary change of dimension, given the observed threat. The scale, however, will mean a real "cultural change" for ANSSI, which will need to update its methods as it has done since its creation. A bit like the changes made for scaling up certification.

↓
CERTIFIED SERVICES WILL BE AIMED AT SMALL BUSINESSES, ASSOCIATIONS, COMMUNITIES AND CITIZENS ... FAR REMOVED FROM THE TRADITIONAL OVIS AND OESS!
↑

Finally, beyond strengthening the level of security of member states and their critical operators, the security of EU institutions bodies and agencies will probably be set out in new protective regulations.

Coordination efforts for a European cybersecurity model are bearing fruit, triggering a new dynamic and demonstrating the benefits of making "cyber" issues a strategic and political subject. But while this orchestration is essential, the purely technical considerations remain central. Certain founding principles, such as the use of encryption, also need to be implemented across Europe. "For twenty-five years, we have seen an increasing use of cryptographic solutions everywhere", recalls Guillaume Poupard. Everyone can, in their daily lives, judge the consequences of this evolution which has made it possible, in particular, to secure the many means of communication that we constantly use, like with end-to-end encrypted messaging applications[8]. The Director-General continues: "Since then, there have been debates around the world about how this could hinder investigation services". To which ANSSI has always reiterated the importance of these mechanisms for digital security. Implementing a systemic solution (aimed, for example, at prohibiting or weakening encryption) would make potentially catastrophic attack scenarios possible. As for the

[8] See glossary.

"We must make sure the EU remains at the cutting edge of technological change, but at the same time, we must not compromise on security."

KAREL ŘEHKA

Director
of the National Office for Cyber and Information Security (NÚKIB)
Czech Republic

The Czech Republic and France concluded The Strategic Partnership Agreement back in 2010. Ever since then, we have enjoyed an increasingly fruitful cooperation, including the area of cyber security. I am grateful to have this opportunity to reflect on the many good years of mutual engagement, and as we approach our respective presidencies in the Council of the European Union, to indicate in a few words where we see the next big issues we can address together in EU cyber politics.

Allow me first a short trip down the institutional memory lane. What started off as a courtesy bilateral engagement in 2013 – when my predecessor first met the director of ANSSI – had already shifted gears by 2017, with the exchanges on cyber security, PRS Galileo, cryptography and TEMPEST capacities. In 2018, we added *cyber threat intelligence* to the mix. I am glad these interactions have grown steadily over the years, be it on matters of technology or exchanges on threat actors. Recognizing this special relationship, NÚKIB has designated a cyber attaché to nurture bilateral relations with France in 2020.

As we near 2022 – the year you and then we take on the role of Presidency of the Council – I know the bond we share can only get stronger. We have a full schedule ahead of us. We will stand by your side (or, more precisely, sit by your side) as you take forward the negotiations on the revised NIS directive, with every best wish for you to take the file to a successful conclusion. We will in turn pick up the mantle where you leave off in making sure EU institutions, bodies and agencies can rely on resilient cyber security, and a robust mechanism for a coordinated response in case their defences fail. As we rebuild from the COVID-19 pandemic, we will aim to make sure we underpin our digital efforts with a renewed focus on the security and continued availability of technologies, including those that are seemingly still emerging, but have in numerous instances already rounded the corner. We must make sure the EU remains at the cutting edge of technological change, but at the same time, we must not compromise on security as we aim to make new technologies available. This includes engaging in conversations about secure and resilient supply chains. To this end we look forward to welcoming you again, both this year and next, at the Prague 5G Security Conference. As in the first two years, I am sure your support will be of paramount importance. ●

integration of *backdoors*[9], this would create master keys which would, inevitably, end up in the hands of attackers. "Especially since these measures would probably not be useful to the investigation services: wrongdoers would still find a way to use other tools. Everything that has been considered so far to allow systematic bypassing of encryption has proven ineffective and dangerous", notes Guillaume Poupard.

To find a solution that is both viable in terms of digital security and effective for investigation services, ANSSI is in favour of specific, ad hoc and targeted mechanisms. "One can imagine, with *over-the-top*[10] (OTT) service providers, intermediary options that respect private data, but allow access to certain data upon request from a judge", suggests the Director-General of ANSSI. "For example by allowing access to certain information related to the content of communications, in cases that require it." Solutions which, in order to constitute an alternative to the contrary thoughts emerging elsewhere around the globe, undoubtedly deserve to be developed in a concerted manner on a European scale.

THINKING WITH SOLIDARITY

In the first half of 2022, France will hold the presidency of the Council of the European Union. The opportunity to provide major guidance in terms of cybersecurity. "We are facing a growing threat with major incidents,alongside increasingly significant and cross-border impacts. We therefore need ambitious measures", believes Agathe Favetto. Anne Tricaud agrees: "The idea is to move towards increased solidarity. Now, we just need to propose effective mechanisms."

Because in practice, if a crisis exceeds the capacities of a Member State, how do we react? "We do not believe that the ideal solution is to create a permanent European team", warns Guillaume Poupard. To establish European solidarity, ANSSI is more inclined to favour well-defined mutual assistance mechanisms that respect the specific needs of the states.

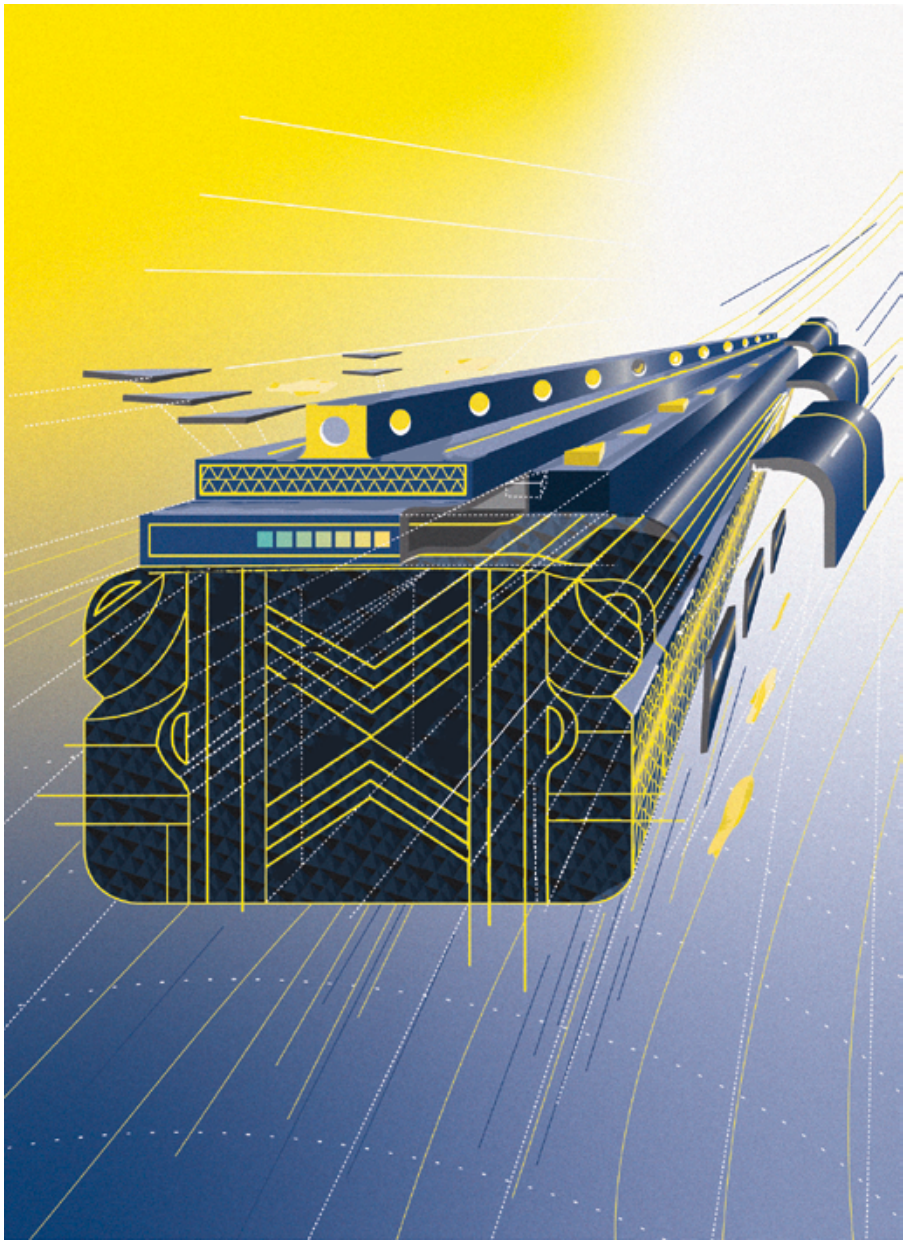
> ↓
> "EVERYTHING THAT HAS BEEN CONSIDERED SO FAR TO ALLOW SYSTEMATIC BYPASSING OF ENCRYPTION HAS PROVEN INEFFECTIVE AND DANGEROUS."
> ↑
>
> GUILLAUME POUPARD
> *Director-General of ANSSI*

But above all, one idea stands out: the call for certified service providers on a European level. "Solidarity can only be implemented if the capacity of states is increased through trusted private service providers", states Anne Tricaud. "Even in France, the national authority cannot respond to all incidents. The trusted service provider model allows critical operators to call on service providers for audits, detection or incident response." Guillaume Poupard agrees: "Opting for this model would avoid spreading ourselves thin on one front in order to supply another. This is undoubtedly the best way to be able to adapt the available workforce in the event of a crisis, much like what is already being done on a national level."

All these avenues could be tried out during the French presidency through a crisis exercise that could link technical (with the CSIRTs Network), strategic (with CyCLONe) and political levels, with the ministers for Foreign Affairs. "This exercise would allow us to bring together these three levels and answer this question: what does European solidarity actually mean?", anticipates Célia Nowak, cyber crisis management policy officer at ANSSI.

It remains the case that through ongoing consideration on solidarity, we can reflect positively on the steps taken so far. Guillaume Poupard summarises: "First of all, we ensured that states develop their own capacities and protect their critical operators. Next, we put them into a network. We then worked on the emergence of a trusted industrial ecosystem. And now that all these foundations have been laid, we are ready to seriously get to grips with this issue of European solidarity."

[9, 10] *Ibid.*



↓
"SOLIDARITY CAN ONLY BE IMPLEMENTED IF THE CAPACITY OF STATES IS INCREASED THROUGH TRUSTED PRIVATE SERVICE PROVIDERS"
↑

Anne Tricaud
Head of the International coordination division

"Both technically and politically speaking, cyber matters are, in some aspects, a very national issue," continues Guillaume Poupard, "but in other ones, they are also deeply European. To build a coherent and effective model against the threat, it's all about putting the blocks together in the right order. So far, that's what we've done". The rest of the story just needs to be written ... ●

GLOSSARY

Backdoor
A means of accessing a computer system or encrypted data in a covert way, bypassing security mechanisms. The backdoor can be hardware or software, intentionally implemented by the designer or installed by an attacker.

CyCLONe
Cooperation network complementing the existing cybersecurity structures in the European Union. It makes the links between the technical (CSIRTs Network) and political (Integrated Political Crisis Response - IPCR) levels. It therefore allows a coordinated assessment of the impact during a crisis and consultations on national response strategies, for the benefit of policy makers.

End-to-end encryption
End-to-end encryption refers to communication systems with which only equipment located at the ends of the exchange has access to the decryption keys. In other words, service providers do not have the ability to access unencrypted data moving from user to user.

Information technology security assessment centre (CESTI)
Laboratories carrying out product security assessments. CESTIs act as a third party, independent of developers and sponsors, and must be approved by the certification organisation. As such, CESTIs are required to comply with the rules developed by ANSSI.

Operators of essential services (OES)
Operator dependent on networks or information systems providing a service, the interruption of which would have a significant impact on the functioning of the economy or society.

Operators of vital importance (OVI)
Operator carrying out one or more activity(-ies), as mentioned in article R. 1332-2 of the French Defence Code, the damage, unavailability or destruction of which would risk seriously impairing the warfare or economic potential, the security or the survival capacity of the Nation or seriously endangering the health or life of the population.

***Over-the-top* (OTT) service**
Services used for the distribution of content (messages, audio, images, etc.) via an Internet connection, without the participation of a traditional network operator.

Security of activities of vital importance (SAIV)
The SAIV system constitutes the framework for associating operators of vital importance (OVI) in the implementation of the national security strategy in terms of protection against malicious acts as well as natural, technological and health risks.
At the heart of the system, the operators of vital importance identified must therefore analyse the risks to which they are exposed and apply the protective measures incumbent on them.