RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

2024 ANNUAL REVIEW

The rise of the cyber ecosystem

Table of Contents

Vincent Strubel's Editorial

2024 was a remarkable year for the French Cybersecurity Agency (ANSSI) and its teams, whose exceptional involvement in the protection of our nation I would hereby like to commend. Indeed, this year was marked by a collective success, as we turned the 2024 Paris Olympic and Paralympic Games into a celebration. Though both ANSSI and France's cybersecurity team have, over two years, been ceaselessly working to prepare for this event, the Games are also the consecration of a French cybersecurity model which has been years in the making. This success solidifies France's place amongst the world's leading cybersecurity nations. The knowledge gleaned from this experience will, moving forward, help us face high-intensity crises.

The Olympic and Paralympic Games, however, were not the only major event of 2024. Indeed, the national cyberdefence framework implemented by the Agency has also been put to the test during this year's European and legislative elections, at a time when actors are seeking to destabilise pivotal moments in our democracy. ANSSI has, moreover, continued to work on the transposition of the NIS 2 Directive, which has brought about significant changes in its organisation, methods, and means of interacting with its partners and beneficiaries. In this context, and in the context of an evolving

cyber regulatory framework, the new Control and Supervision Mission is an important tool for the Agency.

2024 was also marked by great European advances, including the adoption of the Cyber Resilience Act – which we supported, and which represents a significant step towards the general elevation of cybersecurity in the European Union. Additionally, the year was marked by technical advances for ANSSI, with the evolution of standards, international cooperation in the transition towards post-quantic cryptology, and significant investment in future technologies such as AI, to promote rational discourse based on scientific data. Lastly, this year was also the first year during which ANSSI officially operated from four locations. This meshing in the French cyber ecosystem is an undeniable asset in our day-to-day activities.

This exceptional year has paved the way for ANSSI to begin a new chapter, embodied in its strategy for 2025-2027 (available in French). From here on out, we will not only need to identify developments in the cyber field, but also in our broader environment. To that end, we will require the assistance of France's cybersecurity team.

Vincent Strubel
General Director of ANSSI

ANSSI's Missions

Created in 2009 as part of the Prime Minister's Office and under the authority of the Secretary General for Defence and National Security, the French Cybersecurity Agency (ANSSI) is the national authority in matters of cybersecurity and cyberdefence. The French cybersecurity model relies on the strict separation of defensive and offensive missions at the state level and, within this framework, ANSSI is responsible for coordinating the defence and protection of information systems.

As such, the Agency's primary objective is, at the interministerial level, to construct and organise the protection of the country from cyberattacks and to contribute to the stability of cyberspace. Its activities are part of the State's sovereign duties, in the general interest of public security policy and of administrative, economic, and broader societal resilience.

ANSSI's work revolves around five main missions:

- → **Defending** critical information systems and the victims of large-scale cyberattacks;
- → **Knowing** the state of the art in cybersecurity and cyberspace threats;
- → **Sharing** knowledge, recommendations, and expertise in digital safety;
- → **Assisting** the national and international ecosystem;
- → **Regulating** cybersecurity organisations, goods, and services.

The Agency is organised into four sub-directorates and one mission, guided and coordinated by the General Directorate:

- → **The Expertise Sub-Directorate** devises and promotes good cybersecurity practices and works on improving product offerings, to assist in securing organisations.
- → **The Operations Sub-Directorate** ensures the exercise of ANSSI's authority in the defence of digital systems of national interest, and functions as France's national and governmental incident-response centre (CERT-FR).
- → **The Resources Sub-Directorate** is responsible for the planning and implementation of activities pertaining to the management of financial and human resources, of movable and immovable property, of expertise, and of ANSSI's legal support.
- → **The Strategy Sub-Directorate** oversees ANSSI's contribution to the elaboration and implementation of public policy promoting cybersecurity at the national, European, and international level.
- → **The Control and Supervision Mission** devises and implements ANSSI's control and supervision policy, in accordance with European (NIS Directive, CSA and eIDAS regulations) and national (SAIV, certification) regulations.

↘ Since 2023, an Agency operating from four different locations

Previously spread across three different sites in the Paris region, ANSSI inaugurated in November of 2023 a fourth location in Rennes: ArteFact. These different locations allow the Agency to grow closer to its beneficiaries, to develop rich partnerships with its partners, and to strengthen synergies between public and private actors. In order to accommodate the environmental challenges which come with operating from multiple locations, ANSSI has developed its professional practices: deployment of video conferencing tools to limit traveling, dematerialisation of processes to limit the transmission of physical documents, arranging for constant on-site support, appointing correspondents (security or human resources). These developments are intended to help reduce ANSSI's carbon emissions. The question of working conditions is also being considered, and particular attention is given to the travel time between locations when organising in-person meetings. Created in 2023, a service specifically dedicated to the management of sites and their buildings was further developed in 2024 to accommodate the needs and requirements associated with their administration. It guarantees the smooth running of each location, in the interest of the personnel working therein, addressing issues pertaining to infrastructure and working conditions, and ensuring the equal treatment of personnel across all locations. ●

Cyber Ecosystem

↘ Institutional actors

Public and private investment actors (Bpifrance, SGPI, etc.)
Supervisory authorities (ARCEP, autorité de la concurrence, CNIL, etc.)
Sectoral authorities (ACPR, AMF, etc.)
Local governments
Professional federations
Ministries (DGA, DGE, DINUM, DITP, etc.)
Standardisation bodies (AFNOR, ETSI, etc.)

↘ Regulated actors

Administrations
ECO: Electronic Communications Operators
OIV: Operators of Vital Importance
Regulated operators
OSE: Essential Service Operators

↘ Political authorities

Local elected officials
Government
Parliament
Prime Minister
President of the Republic
SGDSN: General Secretariat for Defence and National Security

↘ Cyberdefence actors

C4: Cyber Crisis Coordination Centre (ANSSI, COMCYBER, DGA, DGSE, DGSI, MEAE)
Private CERTs: Private Cyber Incident Response Centres
CRC: Cyber Resource Centres
Ministerial CSIRTs: Ministerial Cyber Incident Response Centres
Sectoral CSIRTs: Sectoral Cyber Incident Response Centres
Territorial CSIRTs: Territorial Cyber Incident Response Centres
Gendarmerie
GIP ACYMA: Public interest group acting against malicious cyber activities
InterCERT France: First CERT community in France
National Police

↘ International partners

CERT-EU: Cyber Incident Response Centre dedicated to European Institutions
CSIRTs Network: The European Union's network of Cyber Incident Response Centres
ECCC: European Cybersecurity Competence Centre
ENISA: European Union Agency for Cybersecurity
EU-CyCLONe: European Cyber Crisis Liaison Organisation Network

European and international counterparts
NCC: Centres de coordination nationaux
OCDE: Organisation for Economic Co-operation and Development
NATO: North Atlantic Treaty Organisation

↘ Scientific and technical community

Research actors (CEA, CEA-Leti, CNRS, INRIA, etc.)
ANSSI's Scientific Council
SecNumedu and SecNumedu-FC qualified entities: Labels for higher education courses and continuous cybersecurity training programmes
Grandes écoles
Training organisations
Universities

↘ Cybersecurity suppliers

National and regional Cyber Campuses
CESTI: Information Technology Security Assessment Centres
Incubators
Trusted providers (PACS, PAMS, PASSI, PDIS, PRIS, PVID, SecNumCloud providers, trusted eIDAS service providers, EBIOS Risk Manager providers, CC suppliers, CSPN suppliers, MIE suppliers)
Cybersecurity solution providers

2024 in Figures

29,6
millions euros budget (excluding salaries)

4,386
security events[2]
+15% in comparison with 2023

59,191
automated audit reports (ADS and SILENE)
+56% in comparison with 2023

1,361
incidents[3]
+18% in comparison with 2023

68
SecNumedu certified training courses

117,856
SecNum*académie* certificates
+21% in comparison with 2023

35
SecNumedu-FC certified training courses

1,696
personnel trained by the CFSSI[4]

[1] Civilian personnel, excluding interns and apprentices.
[2] Events which have been brought up with ANSSI, and which have required the intervention of its operational teams.
[3] Security events where ANSSI has confirmed a malicious actor's successful attack on the victim's information system.
[4] Cybersecurity training centre (*Centre de formation à la sécurité des systèmes d'information*).

2024 Highlights

JANUARY

January 16th
Publication of a corpus of guides on the remediation of cybersecurity incidents

January 31st
Adoption of the EU Cybersecurity Certification (EUCC) scheme, based on common criteria

FEBRUARY

Certification by ANSSI of the Ministry of the Interior and Overseas Territories' electronic identification tool, *France Identité*, at the highest level of the eIDAS regulation

Deployment amongst ministries of the *Jecliqueoupas.cyber.gouv.fr* file analysis platform

MARCH

Publication of the results of the second instalment of the SME and cloud start-up support system, towards greater eligibility for SecNumCloud qualification

APRIL

April 11th
Establishment of the European framework pertaining to digital identity

April 24th
Restitution of consultations with professional federations regarding the transposition of the NIS 2 Directive

April 29th
Publication of a guide on the security of generative AI systems

MAY

May 3rd
Restitution of consultations with associations of elected representatives regarding the transposition of the NIS 2 Directive

May 8th
Olympic flame's arrival in mainland France, and the beginning of ANSSI's mobilisation in the context of the Paris 2024 Olympic and Paralympic Games

May 10th
Entry into force of the 2024-2030 military programming law's implementing decree, enabling ANSSI to exercise the new capabilities with which it has been entrusted

May 15th
Renewal of the mutual recognition agreement between ANSSI and its German counterpart, BSI (*Bundesamt für Sicherheit in der Informationstechnik*), concerning ANSSI's CSPN and BSI's BSZ certifications

May 22nd
Officialisation of the Agency's contribution to the "Trust" pillar of the AI Action Summit scheduled for 2025

JUNE

June 29th and 30th
First round of the French legislative elections. During these elections, ANSSI assists the Ministry for Europe and Foreign Affairs in the implementation of online voting for French citizens abroad

JULY

July 9th
Publication by the Agency of recommendations on the hosting of sensitive information systems in the cloud

First "PACS" qualification of cybersecurity providers (providers of assistance and consulting in the security of information systems) by ANSSI

July 26th
Olympics opening ceremony

AUGUST

August 11th
Olympics closing ceremony

August 28th
Paralympics opening ceremony

SEPTEMBER

September 8th
Paralympics closing ceremony and the end of ANSSI's mobilisation

September 12th
Launch by ANSSI of a call for projects on the "Support of SMEs and start-ups for the reinforcement of their capabilities in the field of cybersecurity", in the context of the Agency's role as the French National Coordination Centre for cybersecurity (NCC-FR), with the General Secretariat for investment (SGPI) and Bpifrance

September 30th
Participation in the International Counter Ransomware Initiative (CRI) Summit, alongside 67 other countries

OCTOBER

October 15th
Presentation before the Council of Ministers of a bill on the resilience of vitally important activities, on the protection of critical infrastructure, on cybersecurity, and on the operational resilience of the financial sector – whose II title, "Cybersecurity", endeavours to achieve the transposition of the NIS 2 Directive

NOVEMBER

November 20th
Publication of the Cyber Resilience Act (CRA), regarding the cybersecurity requirements applicable to products containing digital elements

November 20th
Launch of the MonAideCyber platform, allowing for the federation of cyber helpers community

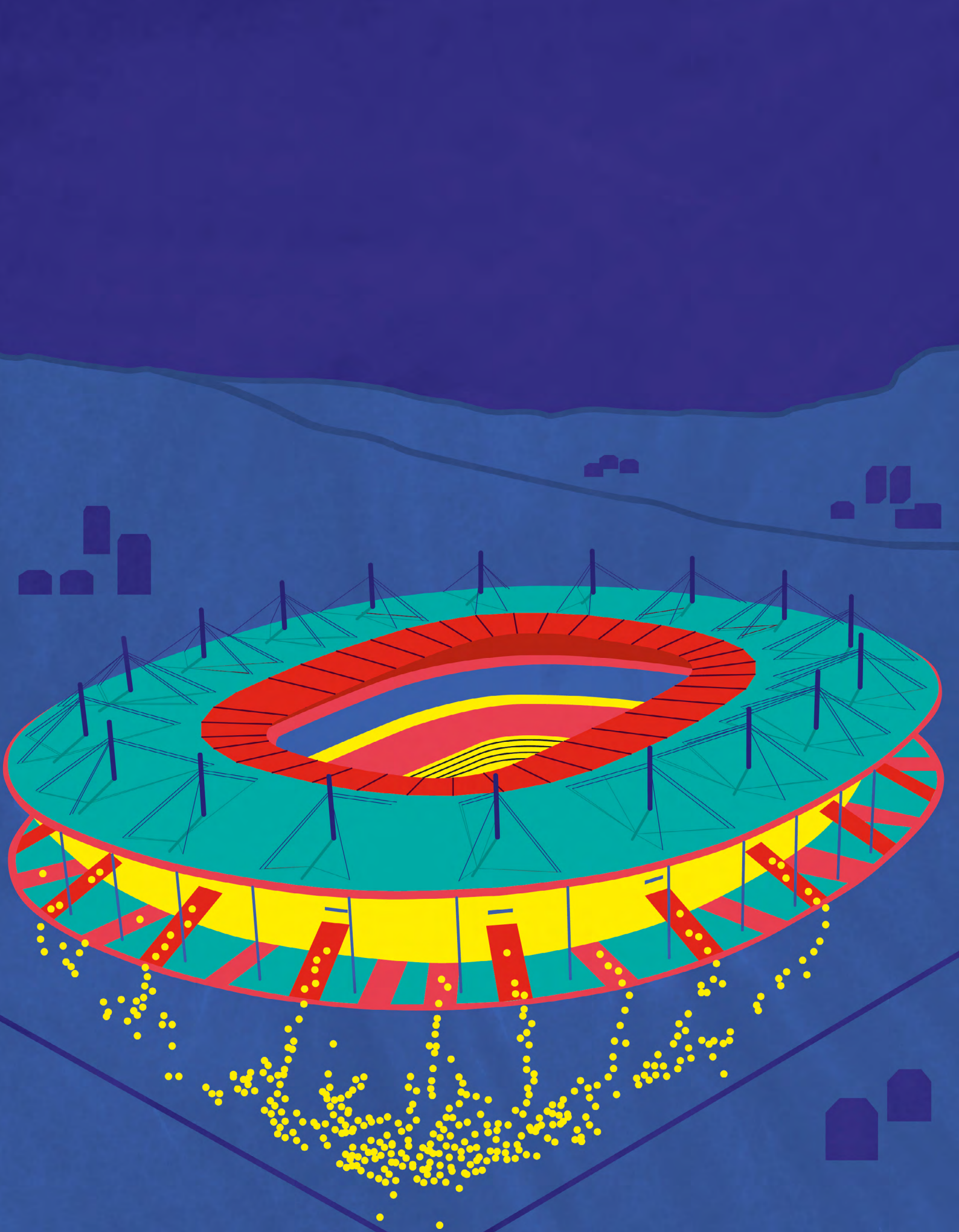
November 27th
Publication, with the BSI, of *Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography*

November 29th
Publication of the newest versions of requirement repositories, allowing for the qualification of Information Systems Security Auditing Service Providers (PASSI) and of Security Incident Response Providers (PRIS)

DECEMBER

December 17th
Launch of 17Cyber, providing online assistance to victims of digital infractions (individuals, enterprises, and local governments)

December 18th
Publication, with the BSI, of *Guaranteeing the Cybersecurity of Major Sports Events Through Cooperation with the Private Sector*



The 2024 Paris Olympic and Paralympic Games: A Collective Success

On the 20th of July 2022, following the Prime Minister's decision, ANSSI was entrusted with leading the cyberattack-prevention strategy during the 2024 Paris Olympic and Paralympic Games. By virtue of their global exposure and of the financial flows they generate, the Games are an appealing target for attackers with various motivations. In its evaluation of the threats faced by large-scale French sporting events published on the 17th of April 2024, ANSSI recalled that previous Olympic Games had been targeted by large-scale cyberattacks: distributed denial-of-service attacks (DDoS[5]) in Rio de Janeiro, sabotage in PyeongChang, and espionage in Tokyo were indeed observed. The Agency assessed the risks facing the Games, anticipating an elevated level of extortion-motivated threat (scams, data thefts), a significant level of threat aimed at destabilisation (sabotage, DDoS, website defacement), and a medium level of threat geared towards espionage (targeting of foreign delegations or of subcontractors in possession of sensitive data).

Responsible for managing the "cybersecurity" aspect of the 2024 Paris Olympic and Paralympic Games, ANSSI worked alongside every entity involved in the organisation of the event – including the Interministerial Delegation for the Olympic and Paralympic Games (DIJOP), the Ministry of the Interior and Overseas Territories (MIOM), the Olympic and Paralympic Organising Committee (Paris 2024). The established framework was founded upon five main pillars: understanding the threat, securing critical information systems, protecting sensitive data, raising awareness across the ecosystem, and intense operational preparation. ●

[5] Distributed Denial of Service: Action which prevents or severely limits a system's ability to provide the expected service. The action may be malicious or may be the result of the incorrect sizing of the service. We speak of a "distributed denial of service" when the attack mobilises a network of (often compromised) devices to interrupt the targeted service(s).

Preparing for the Games: the establishment of an ecosystem

The implementation of this strategy began with the identification of the Games' ecosystem, achieved with the support of the Ministry of the Interior and Overseas Territories' National Coordination for the Security of the 2024 Olympic and Paralympic Games (CNSJ) and of Paris 2024. ANSSI was able to target close to 500 entities involved in the Games, categorised on the basis of their criticality, during the deployment of a preventive security strategy in the run-up to the event. In order to provide adequate support, the Agency specifically sought to better understand the activities and professions associated with the Games – accreditation, ticketing, venue access management, audio-visual broadcasting, accredited transportation, anti-doping, etc. – and the security challenges they must face, to develop its knowledge of the entities it was set to assist and defend.

> "The goal was to discuss cybersecurity thoroughly enough prior to the Games to not have to discuss it as much during the event itself."
>
> Vincent Strubel, Director General of ANSSI

The preventive security strategy had four main objectives: the first one consisted in making a diagnosis and in identifying, via over a hundred cybersecurity audits, the vulnerabilities impacting information systems so that security plans might be drawn up. 80 entities also had access to the Agency's automated audit services.

Cyber Threat Intelligence (CTI) was additionally shared with approximately 130 entities, and assistance in the detection of vulnerabilities was also offered to a dozen major entities. The "securing" objective entailed the provision of technical support for the majority of audited entities. The "control" objective concerned several dozen entities, including competition venues, which underwent control audits intended to ensure the proper implementation of security measures. The last "detection" objective consisted in the deployment, for a couple of particularly critical entities, of a cyberattack detection service made up of a managed EDR (End Point Detection and Response) and industrial probes.

From 2023, an awareness-raising plan was concurrently implemented across the ecosystem of the Games. This plan informed entities of the cyber threats facing large-scale sporting events, and facilitated the dissemination of cybersecurity recommendations and good practices. It entailed the conduct of awareness-raising activities by ANSSI's territorial representatives and sectoral coordinators, and the organisation of a seminar at the Cyber Campus on the 5th of July 2023. The implementation of this plan also involved a thematic e-mail campaign and the distribution of several reports addressing the evolution of the threat. ●

2,000

hours of security expertise dedicated to the support of a dozen critical entities, to the benefit of the MIOM, of Paris 2024, of its major partners, and of State actors.

↘ Training itself and the ecosystem through cyber-crisis drills

ANSSI undertook a range of actions intended to assist the main public and private actors working on the Games in securing their information systems and ensuring the resilience of their organisations in the event of a cyberattack. Several crisis drills were organised in 2023 and 2024, to collectively prepare for potential cyberattacks during the Games. Additionally, ready-made drill kits were offered to actors of the Olympic and Paralympic ecosystem – host territories, public authorities, service providers, competition venues – looking to train with scenarios tailored to their specific maturity level. Organisations were able to choose from a total of 12 different drill formats (broken down into three maturity levels, adapted to four different types of sector). Hundreds of entities participated in drills tailored to their specific context, thereby improving their incident-response capabilities and ensuring the continuity of essential services during the Games. ●

Cyber-coordination led by ANSSI

In collaboration with the different State departments involved in the preparation of the Games, the Agency implemented an enhanced system of cyber-incident watchkeeping, alerting, and handling. This exceptional interministerial coordination framework was materialised in the National Strategic Command Centre (CNCS), and involved a specific posture intended to accommodate heightened operational activity. ANSSI was identified as the sole entry point for cyber-related reports, enabling the centralisation of information and the optimisation of the incident-handling process. All identified cybersecurity events were therefore reported to the Agency, through Paris 2024, Ministries, or the Olympic ecosystem, with the idea of maintaining a single consolidated view of the Games' cyber-situation.

Close coordination with the event's organiser was also sustained, via the presence of one of ANSSI's liaison officers with Paris 2024's cyber teams, to facilitate the report and qualification of cybersecurity events. In the run-up to the Games, the Agency's national and international partners were also regularly consulted and mobilised to ensure effective cooperation over the course of this international event. During the Games, cyber information related to the event was regularly shared with international partners, bilaterally and within dedicated frameworks. Much information was notably shared with the International Cooperation Centre (ICC), the European crisis management network EU-CyCLONe, and the European Union's CSIRT network. From an operational standpoint, given the risk of large-scale cyberattacks and of attacks targeting multiple locations across the country, procedures were implemented to allow for emergency reinforcements from other State administrations (more particularly from the MINARM[6] and MIOM, with whom ANSSI had signed conventions). ●

[6] The French Ministry of the Armed Forces.

↘ An increasingly accessible CERT-FR

In the run-up to the Games and with the intention of facilitating the report of cybersecurity events to the CERT-FR, the Agency continued to develop its services and communication channels. Designed to streamline procedures and exchanges with beneficiaries, they endeavour to provide optimised assistance during crises. These efforts continued beyond the Games, and until 2025:
→ The new short call number, 3218, provides simple and resilient 24/7 access to the CERT-FR.
→ The Internet Club SSI portal was remodelled and rolled out in November of 2024. In 2025, the portal will be enhanced with the addition of new services such as the pre-registration of future entities subjected to the NIS 2 Directive. ●

"A response cannot be improvised in the thick of a catastrophe. Preparation, tooling, and training are all key to ensuring the continuity of activities in the event of a cyberattack. That is what we did with the Paris Olympic and Paralympic Games, and it worked."

Cédric Mullot, Cyber-training mission Officer, Operations Sub-Directorate

The Games: a success for both the Agency and the ecosystem as a whole

The culmination of two years' worth of work, the prevention strategy planned by the Agency over the long term bore fruit. The preparation of the ecosystem and the operational framework put in place prevented any cyber event from interrupting the Games and their opening and closing ceremonies. Though a total of 548 cybersecurity events were recorded by ANSSI between May 8th (the day of the flame's arrival in Marseille) and September 8th 2024 (the day of the Paralympic Games' closing ceremony), they had little to no impact on the targeted entities. These cybersecurity events can be broken down into 465 reports[7] and 83 incidents. Close to half of reported cybersecurity events resulted in the non-availability of services, and a quarter of these were caused by DDoS attacks. The rest of the events were characterised by the report of vulnerabilities, by data leaks, or by attempted or successful compromises. Unsurprisingly, the most targeted sectors of activity were governmental, sports, entertainment (competition venues and Paris 2024), and telecommunications entities.

While the Agency and its national partners did assist several victims in the resolution of incidents, all of the cybersecurity events which occurred during this period had a rather minor impact. The effective prevention of major cyber crises was the culmination of several years of work for ANSSI and the Olympic ecosystem, and it allowed France to both demonstrate its cybersecurity resilience and reinforce its position on the international stage. The work undertaken also enabled the implementation of a stable framework for the management of major crises. Joint action and coordination across the national cyber ecosystem were consequently reinforced. Ultimately, the Games were not only a success for the Agency, but also for the ecosystem as a whole. ●

[7] Security events of cyber origin which have had a limited impact on the victims' information systems, thus only requiring minor interventions by the Agency.

"Much like Olympic athletes, the cybersecurity of the Olympic and Paralympic Games required lengthy preparation which began long before their kick-off. And behind every performance, there is an entire team working to keep the wheels turning."

Julien Garcin, Governance Officer, Resources Sub-Directorate

548

cybersecurity events affecting entities involved in the organisation of the Paris 2024 Olympic and Paralympic Games were reported to ANSSI between the 8th of May and the 8th of September 2024:

465 reports

83 incidents

An evolving regulatory framework to elevate the general level of cybersecurity

In 2024, efforts to secure cyberspace continued at the national and European levels. The different regulatory and legislative projects to which ANSSI had contributed over the past few years thus progressively came to fruition.

The Agency's involvement in the transposition of the NIS 2 Directive

The NIS 2 (Network and Information Security) Directive was one of the major challenges tackled by the Agency in 2024, and will remain so for years to come. This directive aims to reinforce the cybersecurity level of EU member States' administrative and economic fabrics. While the first NIS Directive sought to protect the EU's major economic actors, this new directive broadens the range of concerned entities and sectors and, in view of the evolving cyberthreat, also introduces new requirements. The requirements set out by the European directive will incite several thousand entities to strengthen their cyberdefence mechanisms, with the aim of promoting more secure structural operation, greater trust in their stakeholders, and enhanced competitiveness for enterprises. In France, ANSSI is responsible for handling the transposition of the directive and ensuring its implementation.

> "CRA, REC, NIS 2, CSA, LPM... These acronyms all embody the general objective of raising national and European levels of cybersecurity, and of defending our sovereignty and the interests of both enterprises and citizens."
>
> Adeline Lescaut, Head of Expertise and Legal Support Division, Resources Sub-Directorate

The NIS 2 Directive is applicable to State administrations, local governments, and medium-sized and large companies involved in 18 different sectors of activity. It distinguishes between two categories of regulated entities: essential entities (EE) and important entities (IE). The directive presents three main actions whose associated requirements, following the transposition into French law, shall be proportional to the entity type (essential or important) and to the risks they face: providing updated information to the national authority, implementing legal, technical, and operational measures to manage challenges to the security of their networks and information systems, and reporting significant security inci-

dents to the national authority. The NIS 2 Directive therefore commits and redefines the Agency's roles by adding, to the support and defence of beneficiaries, prerogatives of control and supervision over all concerned entities.

Significantly dimensioning for ANSSI, this transposition has demanded extensive effort over the past few months, beyond the simple drafting of the cyber segment of the bill on the resilience of vital activities, on the protection of critical infrastructure, on cybersecurity, and on the operational resilience of the financial sector, presented to the Parliament for consideration on the 15th of October 2024. The "Resilience" bill's title II, "Cybersecurity", endeavours to transpose the NIS 2 Directive and to adapt national law to accommodate the eIDA (Electronic Identification and Trust Services[8]) and CSA (Cybersecurity Act[9]) regulations following their entry into force.

In a logic of co-construction, ANSSI organised consultations with involved professional federations, associations of local elected officials, and ministries. These consultations were had to gain a greater understanding of the realities and needs of future regulated entities and thus guarantee a successful transposition. The Agency coordinated, at the European level, the elaboration of the bill and negotiations related to the NIS 2 implementing regulation[10].

ANSSI is developing its support strategy and offers a range of dedicated services through its *Monespacenis2.cyber.gouv.fr*, platform which, though still in its beta version, allows entities to take a test to figure out which category they belong to, and whether or not they are subject to the directive. This informative platform complements the communication and awareness-raising efforts already implemented to acquaint entities with future requirements and thus facilitate compliance. The Agency is preparing to assist several thousand entities in their registration as regulated entities, simultaneously adapting and equipping itself to receive reports and cooperate with territorial and international partners. ●

"The NIS 2 Directive is the key to our collective resilience when confronted with cyber challenges. It ushers in major developments in terms of both digital security and our own sovereignty."

Mathieu Couturier, Head of Security Management Division, Strategy Sub-Directorate

↘ The creation of the Control and Supervision Mission

Given the multiplication of regulations in the field of information system security, notably at the European level, ANSSI geared up for a monitoring and supervisory role. In 2022, it initiated a project to revise its internal organisational framework and facilitate the exercise of its new functions. These efforts led to the creation, in early 2025, of the Control and Supervision Mission – a separate structure from the Sub-Directorates which reports directly to the Agency's General Director. The Mission will be responsible for monitoring, in accordance with the Activities of Vital Importance Security (SAIV) framework established by the military programming law of 2013, with the eIDAS regulation, and with the Cybersecurity Act (CSA), in respect to European cybersecurity certification. It is also involved in preparatory work for future supervisory and control activities under the NIS 2 Directive. The responsibility of preparing the corrective measures to be implemented by ANSSI in cases of non-conformity to these texts also lies with the Mission. ●

[8] Regulation concerning electronic identification and trusted electronic transaction services within the internal market.

[9] Regulation concerning ENISA (European Union Agency for Cybersecurity) and the cybersecurity certification of information and communications technologies.

[10] See *digital-strategy.ec.europa.eu*

"To digital solution providers, the Cyber Resilience Act is the counterpart to the NIS 2 Directive. It was designed to mirror NIS 2 and to allow for the equitable division of efforts, between digital solution providers and organisations subject to NIS 2, in the elevation of European cybersecurity levels."

Sylvain Leroy, Head of Security Products and Services, Expertise Sub-Directorate

The Cyber Resilience Act, complementary to the NIS 2 Directive

While NIS 2 sets the objective of securing the networks and information systems of EU administrations and enterprises, the Cyber Resilience Act (CRA) endeavours to secure the digital products used by organisations and the general public in the EU. Published on the 20th of November 2024, this European regulation sets out minimum cybersecurity requirements for products on the European market which contain digital elements. The CRA will be entirely applicable from the 11th of December 2027.

In 2024, the Agency contributed towards the successful conclusion of regulation negotiations at the European level, and subsequently initiated the implementation of the CRA. In this context, ANSSI embarked on a project to organise the report of vulnerabilities and incidents, to define the necessary evaluation processes, and to specify the national organisational framework. The Agency also plans to assist the ecosystem in the implementation of this new regulation. ●

Revisiting the European eIDAS regulation, to develop a trusted framework for digital identity

The eIDAS regulation on electronic identification and trusted electronic transaction services within the internal market endeavours to promote the security of cross-border digital transactions and to develop a trusted framework for digital identity and authentication. Following the publication of the first version of regulation n°2024/1183 in June of 2024, the European Commission initiated a revision of the text with the intention of enhancing its effectiveness, developing its day-to-day usage, more broadly involving the private sector, and promoting trusted digital identity for all European citizens.

In support of the French Interdepartmental Directorate of Digital Affairs (DINUM) leading negotiations, ANSSI contributed to the revision of the European regulation. The Agency called for greater consideration of cybersecurity issues and assisted the European Commission in the technical implementation of the regulation. The eIDAS revision text – which seeks to allow all European citizens to possess a digital identity by 2030 – thus entered into force on the 20th of May 2024.

One of the major innovations brought about by the text has been the introduction of European digital identity wallets. By November of 2026, member States will need to have provided European digital identity wallets recognised across the EU to all of their citizens. These wallets will make it possible for users to store identification information (first name, last name, date and place of birth, etc.) or documents related to their identity (mailing address, diplomas, etc.), to share them with other users on demand, and to use them to access public or private services across Europe, both on and off-line. The text also allows for the elaboration and update of the wallets' "ARF" reference architecture.

The perimeter for trusted services has also been broadened to include four new services, now eligible to qualification: the provision of electronic attribute attestations, electronic archival, electronic registries, and the remote management of qualified signature and electronic seal creation tools. In France, ANSSI is the primary supervisory body responsible for qualifying trusted service providers, and for drawing up and updating the "trusted list".

Lastly, the revision has initiated the creation of a new transverse European cooperation forum to assist the Commission in its work and monitor the implementation of the regulation: the European Digital Identity Cooperation Group (EDICG). Alongside DINUM, ANSSI will participate in this new cooperation group to ensure that adequate consideration is given to cybersecurity issues. ●

The EUCC: first European cybersecurity certification scheme

On the 31st of January 2024, the European Commission announced the adoption of the EUCC (EU Common Criteria[11]) – the first European certification scheme of its kind to conform to European cybersecurity regulations. The EUCC entered into force in February of 2024 and was expected to issue its first certificates a year later. The EUCC scheme provides certification rules and procedures – harmonised at the EU-level – for communication and information technology products, and reproduces the features of existing national certification schemes from the Senior Officials Group – Information Systems Security (SOG-IS) mutual recognition agreement. As representative of France in the European Cybersecurity Certification Group (ECCG), ANSSI has actively contributed to the elaboration of this scheme – developed in compliance with the European Cybersecurity Act (CSA).

In October of 2024, ANSSI applied with the French Accreditation Committee (COFRAC) to become the national certification centre responsible for issuing EUCC certificates. Once it has obtained the accreditation, the Agency will become the national cybersecurity certification authority (NCCA) in charge of issuing high-level certifications and overseeing the implementation of the EUCC scheme in France. Existing SOG-IS certificates will be re-evaluated as EUCC certificates once the new requirements have been met. This scheme will also provide substantial support for the implementation of recent developments in the European framework on cybersecurity. These requirements are consistent with those set out by the NIS 2 Directive and by the revised eIDAS regulation. ●

[11] The European Common Criteria-based cybersecurity certification scheme.

↘ The 2024-2030 Military Programming Law (LPM): new operational capabilities for ANSSI

The Paris 2024 Olympic and Paralympic Games were a successful "test" case of operational rescaling, owing in part to the new capabilities with which ANSSI was entrusted under the 2024-2030 Military Programming Law (LPM), promulgated on the 1st of August 2023. The implementing decree of articles L. 2321-2-1 to L. 2321-4-1 of the Defence Code and of articles L. 33-14 and L. 36-14 of the Posts and Electronic Communications Code, along with the associated tariff orders, was published on the 10th of May 2024. On the 19th of July 2024, it was followed by the publication of the decree on the automated processing of personal data. This entry into force was the culmination of close to three years of work to grant ANSSI additional operational capabilities in the anticipation, characterisation, and neutralisation of threats. More specifically, these efforts allowed the Agency to gain a greater understanding of cyberattackers' intrusion sets, to better remedy the effect of their attacks and to more effectively inform victims of incidents or of threats to their information systems. ANSSI was thus able to develop its capabilities in the prevention and characterisation of threats, via Domain Name System (DNS) filtering, DNS cache collection, or the considerably improved collection of data. The enhanced handling of product vulnerabilities also now requires vendors to report significant vulnerabilities to ANSSI and to its clients. ANSSI has worked on the operationalisation of the abilities granted by the LPM 2024-2030, upholding a logical coherence with the mechanisms already put in place by operators, hosts, and DNS resolver providers. In the context of its supervision of ANSSI's activities, the means implemented were presented to the Electronic Communications, Posts and Print Media Distribution Regulatory Authority (ARCEP). These new mechanisms were deployed in stages; the initial operational capacity was established prior to the Games, ensuring the prevention of threats and vulnerabilities during the event. This deployment will continue until 2026, with the progressive integration of new capabilities and of new solicited actors. ●

↘ The national cybersecurity strategy: towards first-class cyber resilience

In 2018, the Prime Minister entrusted the Secretary General for Defence and National Security (SGDSN) with the production of a strategic review of cyberdefence – the first extensive work of strategic synthesis in this field. This document introduced a new strategy based on the hardened protection of information systems belonging to the State and to critical organisations, and on the reinforcement of the digital security of citizens, institutions, and actors contributing to France's economic, industrial, social, and cultural dynamism. In 2024, ANSSI actively contributed to the implementation of France's cybersecurity strategy, led by Bruno Marescaux, deputy to the Chief of the Armaments General Directorate (DGA) and the SGDSN's secretariat. This strategy charts a new course in the development of collective cyber resilience – including technological investments, national security reinforcement, and the assertion, at the international level, of our cyber power as one that is both responsible and supportive. ●

Using the Agency's expertise to anticipate upcoming technological challenges

The development of technologies provides new opportunities for both defenders and attackers. Whether they concern data cloud-hosting, the development of artificial intelligence (AI), or post-quantum cryptography, ANSSI's activities aim to ensure the mastery of its beneficiaries' technical environment, and to anticipate the impacts of new technologies on the security of information systems.

Raising awareness, within the ecosystem, of cybersecurity challenges associated with artificial intelligence (AI)

ANSSI has been working on securing AI systems and on identifying the opportunities and challenges they represent for cybersecurity. The development of AI raises cyber issues (cybersecurity of AI; by AI; against AI) which ANSSI must include in its action plan. The Agency wishes to act in compliance with the national strategy for AI, which endeavours to make the most of AI in terms of cybersecurity by supporting the development, in France, of trusted, secure, and responsible AI which might prove more beneficial to cyberdefence than to cyberattackers.

To this end, ANSSI promotes a risk-based approach, the enforcement of existing cyber rules, and the elaboration of new regulation adapted to the specific characteristics of AI systems. In 2024, ANSSI's AI-related activities aimed to address the challenges raised by such technology: rapid adoption of AI by the Agency's beneficiaries, entry into force of the European regulation on AI, the progressive emergence of international governance on the topic of AI, and the need for specific cybersecurity recommendations and dedicated certification schemes within the AI and cyber ecosystem. The Agency has also been involved in defining the national AI strategy (funded by "France 2030"), to support the maturation of start-ups and research projects in this field.

The publication of the *Security Recommendations for a Generative Artificial Intelligence System* guide on ANSSI's LinkedIn account garnered

4,470
reactions

1,045
reposts
and

15,947
clicks making it the most successful of the Agency's publications on this platform in 2024

"ANSSI endeavours to raise the ecosystem's awareness of challenges associated with AI, to support the deployment of trusted AI on the market, and to provide expertise, at the European level, in the implementation of regulation and the elaboration of dedicated certification schemes."

Hugo Mania, AI Project Leader,
Expertise Sub-Directorate

The growing interest in generative AI products and services – some of which have become readily available to the general public – has sparked conversations within public and private organisations seeking to assess the potential increase in productivity they may engender. While this technology does provide new opportunities, its deployment and integration into existing information systems must be approached with caution. In April of 2024, as part of its scheme to raise the ecosystem's awareness of the cybersecurity challenges associated with the use of AI, ANSSI published its *Security Recommendations for a Generative Artificial Intelligence System* guide. This document addresses the process of securing generative AI system architecture and endeavours to raise awareness, amongst administrations and enterprises, of the risks associated with such tools. It promotes good practices to implement from the design and training phase of an AI model, until its deployment and use.

In October of 2024, ANSSI and its German counterpart, the BSI, published their *security recommendations for AI programming assistants*. This joint document presents both the opportunities and the risks associated with the use of AI programming assistants, drawing particular attention to the challenges posed by mutualised services' exposure to the internet. Its publication is intended to promote the responsible and secure use of these tools, providing a range of security recommendations for managers and developers.

Post-quantum cryptography: a major security challenge

The potential development of a quantic computer capable of challenging the fundamental properties of asymmetrical cryptography could engender the collapse of the security of public-key cryptography, broadly deployed to secure digital infrastructure. Given the threat of retroactive attacks (dubbed "store now, decrypt later"), this risk must be addressed now – before it is even known if such a computer can be developed.

Post-quantum cryptography (PQC) consists of a set of cryptographic algorithms comprising key establishment and digital signatures, and ensuring security against the quantum threat – in addition to warding off conventional attacks. To ANSSI, post-quantum cryptography represents the most promising path towards quantum threat prevention. This transition to post-quantum cryptography will last several years and is bound to impact the entirety of the digital ecosystem. Its success on the national and European level will represent a major challenge for the next decade.

From 2024, the Agency has been working on offering realistic and actionable transitional guidelines. The Agency has defined two strategic areas of focus: the first of these is to guarantee the availability of trusted PQC product offerings – more specifically, to support the development of a security product offering which integrates cryptographic algorithm capable of resisting against the quantic computer; the second is to assist in the migration of beneficiaries' information systems.

Regarding the first area of focus, in late 2024 ANSSI published data from a survey of 18 developers of cybersecurity products integrating cryptography.

> "To protect itself from the quantum threat, France will need to speed up the development of its trusted product offering integrating post-quantum cryptography."
>
> Samih Souissi, Chief of Staff of the Expertise Sub-Directorate

This study (available in French) enabled the identification of several technical and organisational hurdles to be addressed during the transition: a lack of technological maturity, a lack of standard software components, performance concerns, the absence of an immediate market, the limited number of experts, etc. For ANSSI, each of these hurdles represents an area of action to be addressed. In addition to this, ANSSI has worked alongside Information Technology Security Evaluation Centres (CESTI) to ensure that they will be able to instruct on the topic of post-quantum cryptography in products set to be submitted to them for evaluation. The National Certification Centre (CCN) initiated the very first pilot evaluation projects and updated its cryptographic licencing doctrine. Lastly, to develop the technical doctrine, ANSSI has initiated studies on the integration of post-quantum cryptography in protocols, and reflections on recommendations regarding crypto-agility[12].

With respect to the second area of focus, ANSSI published *a survey* (available in French) on PQC assistance and consulting services in France. The survey involved about thirty providers, shedding light on their needs and expectations as well as on the challenges they might face. For the public sphere, the Agency also consulted around fifty ministries and strategic companies set to deploy products comprising post-quantum cryptography, with the intention of assessing their knowledge on the subject. Since early 2024, to allow ANSSI's beneficiaries to better grasp this challenge, the Agency's CFSSI offers a training course specifically dedicated to post-quantum cryptography. Lastly, a quantic risk analysis was initiated with the aim of prioritising use cases and sectors which will need to be involved in the transition.

The Agency is also working in conjunction with its European counterparts on the topic of post-quantum cryptography. In January of 2024, ANSSI published a *position paper on quantic key distribution (QKD)* alongside its German (BSI), Dutch (the Netherlands National Communications Security Agency), and Swedish (the Swedish National Communications Security Authority) counterparts. This publication aimed to assist decision-makers and political leaders in making an informed judgement about the potential benefits and limits of QKD. It concluded that the migration to post-quantum cryptography must be clearly prioritised in order to face the quantum threat. The Agency additionally co-signed *an important joint declaration* with 17 other EU member States, calling for the prioritised and immediate deployment of hybrid post-quantum cryptography solutions. Alongside its German and Dutch counterparts, ANSSI furthermore co-chairs the PQC workstream of the NIS coordination group, which endeavours to define a roadmap for the transition towards post-quantum cryptography within the European Union.

[12] Crypto-agility refers to a device's ability to evolve to update its cryptographic algorithms

↘ Data-Centric Security (DCS): a new approach to securely accessing data

The "Data-Centric Security" approach aims to reinforce the security of data itself with the idea that, wherever it may be stored, information must be secured. Guided by modern uses such as mobility or by technologies such as cloud-hosting, this new approach leads to the revision of conventional information system architecture. In 2024, ANSSI and the French National Research Institute in Computer Science and Automation (INRIA) initiated technical exchanges on this topic, with the aim of identifying cryptographic mechanisms capable of meeting the specific security needs of these new architectures. ●

↘ Securing the hosting of sensitive information systems in the cloud

Cloud hosting represents a major challenge in the protection of sensitive information systems and data. The current state of the threat suggests that attackers have, for several years now, identified cloud solution providers and their infrastructure as prime targets for cyberattacks. In line with the State's "cloud at the centre" doctrine – and to meet the particular needs shared by its beneficiaries – ANSSI published a series of security recommendations for the hosting of sensitive information systems in the cloud. Confronted with the rise of cloud computing technologies, the Agency wished to provide recommendations on the sort of cloud offer to favour depending on the type of information system concerned, on the sensitivity of the data hosted therein, and on the level of threat faced. These recommendations specify use cases for which the Agency encourages the use of SecNumCloud-qualified solutions, which guarantee high technical, operational, and legal standards. ANSSI's recommendations take the form of *a booklet*, supplemented by *an FAQ* (both available in French), and constitute a useful decision-making tool for entities considering a transition towards cloud-hosting for restricted information systems, sensitive information systems belonging to operators of vital importance and to operators of essential services, and information systems of vital importance (SIIV). ●

Working alongside the cyber ecosystem to assist a growing number of beneficiaries

Faced with the systemic evolution of the cyberthreat across our economic and social fabrics, several new cyberdefence measures have been enacted in France and Europe over the past few years – and many of these were implemented in 2024. The means available to both ANSSI and the State have been reinforced via a range of different regulations (LPM 2024-230, NIS 2, CRA, CSA, eIDAS, etc.). The cyber ecosystem plays a critical role in this change of scale, notably by assisting thousands of entities subject to the NIS 2 Directive in France. It is itself supported by ANSSI, in its role as coordinator of the cyber ecosystem.

Further developing trusted cybersecurity offerings

Given that uses are constantly evolving, organisations must have access to security solutions capable of effectively protecting their information systems and data. ANSSI's industrial policy aims to promote the development of sustainable private offerings designed to meet security challenges, to allow for the enhanced cybersecurity of the State, of local governments, and of private actors. This approach requires constant monitoring by actors in the field of cybersecurity innovation and industry, as well as coordination with the administrations responsible for advancing industrial policies, to provide effective levers for action.

The increasingly necessary link between the European and national spheres has been cemented by the National Coordination Centres ("NCCs") located in each EU member State upon which the European Cybersecurity Competence Centre (ECCC) relies. ANSSI has been designated as the French NCC (NCC-FR). This centre meets the requirements set out by the 2021/887 regulation (EU), which aims to promote expertise, research, and the development of industrial capabilities in cybersecurity at the EU level. In July of 2024, the Agency formed a consortium with Bpifrance – a public investment bank and the operator of French and European innovation programmes – to initiate the operationalisation of the NCC-FR. Financially supported by the EU, this process is expected to last 24 months and will allow the centre to reach full operational capacity by 2026. The NCC-FR has three main missions: promoting and supporting on-going European calls for projects, developing national calls for project, and animating the cyber ecosystem. The NCC-FR thus makes visible and legible the support mechanisms – including financial mechanisms – provided to the ecosystem by the European "Horizon Europe" and "Digital Europe" programmes. The centre facilitates the identification of potential public-private consortiums between suppliers/providers, research centres and regional federated bodies, in anticipation of major upcoming European projects. Bpifrance and the NCC-FR work together to assist enterprises in preparing their applications for European calls for projects. In 2024, the NCC-FR developed

a financial support programme to encourage start-ups, scale-ups, SMEs, and/or midcaps to adopt or develop digital innovations, to reinforce the security of their offering, and to enhance their capabilities. In September of that year, ANSSI, the General Secretariat for Investment in charge of France 2030, and Bpifrance launched the "Support of SMEs and start-ups for the reinforcement of their capabilities in the field of cybersecurity" project call, for a total of 2 million euros.

The Agency is also committed to enhancing coordination and synergy between the different actors of the ecosystem. As such, the work carried out and the interactions had with the French cyber community have multiplied over the past year, capitalising on the Agency's expertise and on its institutional and industrial networks. ANSSI's interlocutors notably include French administrations promoting industrial or innovation policies, product suppliers and cybersecurity service providers and their professional federations, the Cyber Campus, regional service platforms, research centres, and users. The Agency facilitates the dissemination of knowledge and good practices across the community, and the continuous improvement of the cybersecurity solutions available on the market. •

Developing and improving ANSSI's security Visa offering

In 2024, in the field of certifications and qualifications – measures intended to designate, via a security Visa, trusted cybersecurity offerings – ANSSI qualified the first five assistance and consulting providers in the security of information systems (PACS). Published in 2023, the PACS repository is intended to assist chief information system security officers and their teams in their mission to protect information systems – notably in security accreditation, risk management, the conception of secure architecture, and cyber crisis management preparation.

In the interest of continuous improvement, ANSSI published on the 29th of November 2024 new versions of the requirement repositories on the basis of which security system audit providers (PASSI) and security incident response providers (PRIS) undergo qualification. Initiated in 2022, the process of updating these requirements involved consultations with actors of the ecosystem (service providers, sponsors, evaluation centres), to learn their needs and take note of their proposals. In this context, several thematic working groups and two public requests for comment were organised. These new versions significantly improve the rendering of services by providing greater flexibility and giving greater consideration to operational constraints. They introduce different levels of qualification, allowing providers to deliver services which are either substantially or highly qualified. In comparison to the substantial level, a high level of qualification provides greater guarantee of the provider's capabilities, of their trustworthiness, and of their ability to protect the concerned data and devices. The updated versions of the PASSI and PRIS repositories will be translated so that they may be promoted within the European Commission, which, under the European Cybersecurity Act, is currently considering the opportunity of implementing PASSI and PRIS certification schemes at the European level.

The SecNumCloud certification, responsible for identifying trusted cloud providers, was also further developed in 2024. Indeed, a list of the 27 laureates of the second instalment of the programme to support SMEs and start-ups in enhancing their security and eligibility to the SecNumCloud qualification has been published. SecNumCloud-qualified offerings have multiplied: by the end of 2024, they comprised 14 solutions from 7 different providers. Simultaneously, 8 companies initiated the SecNumCloud qualification process. •

[13] Security incident detection providers.

[14] Administration and security maintenance providers.

↘ Animating a community of qualified cyber providers

In 2024, the Agency consolidated and intensified its efforts to animate communities of providers in possession of ANSSI security Visas. These communities endeavour to preserve the quality, the capabilities, and the accessibility of trusted offerings. In this context, the workshops organised by ANSSI sought to enhance the capabilities of such communities and to co-construct initiatives alongside them. For the time being, this endeavour only concerns trusted cybersecurity service providers (and more specifically PASSI, PACS, PRIS, PDIS[13], and PAMS[14] qualified providers). In 2024, 10 consultations and 16 workshops were organised with these providers and the industrial ecosystem. These exchanges provided material for the update of ANSSI's repositories, permitted the co-construction of recommendations and the dissemination of existing best practices, and enabled the reinforcement of capabilities in the fields of incident response, consulting, auditing, and remediation. Additionally, the workshops facilitated the integration of the principles and requirements set out by ANSSI's repositories. The number of PRIS providers doubled over the course of one year, and the new PACS repository received more than 15 applications in 2024. ●

↘ A corpus of guides dedicated to the remediation of cybersecurity incidents

In 2022, given the necessity to enhance the cyber ecosystem's post-incident remediation capabilities, ANSSI began working on this subject alongside a large number of experts. The preparation of a corpus of guides divided into three parts (technical, operational, and strategic) involved a request for comments issued within the cyber ecosystem in 2023. This inquiry ensured greater consideration of the feedback submitted by providers and beneficiaries prior to the official publication, in January of 2024, of the first version of the three guides. The corpus is set to be regularly updated. This publication kickstarted a genuine attempt at animating the community of remediation actors. Over a year and a half, six workshops have been organised with PRISs with the intention of sharing best remediation practices, and of preparing future publications to be included in the corpus. Simultaneously, ANSSI participated in a number of cyber events and working groups, to disseminate the principles set out in these guides. ●

CSIRT relays: an essential support network

Established as part of the 2021 France Relance framework, with the support of ANSSI, territorial CSIRTs (Computer Security Response Teams) are cyber incident response centres located in the territories. These centres are responsible for handling assistance requests from actors in their territories, linking them up with local providers: incident-response providers, and State partners. Progressively deployed over the past few years, territorial CSIRTs locally provide free, top-level incident response services to supplement those rendered by providers, via the Cybermalveillance.gouv.fr platform and the 17Cyber framework, and through the CERT-FR's services.

CSIRTs assist recipients in the judicialisation of their incidents, guiding them to file a complaint with the police or gendarmerie and to submit a statement to the National Commission on Electronic Data Processing and Freedoms (CNIL) when the situation calls for it. They are also involved in prevention and awareness-raising activities, and are tasked with assisting actors across their territories in the process of their maturation. This proximity service provides humane responses catering to the specific cybersecurity challenges faced by the territories. Territorial CSIRTs are conscious of the specific needs and particularities of their local ecosystem, and work in con-

junction with the actors and with national mechanisms. They report every incident occurring on their territory to the CERT-FR. CSIRTs also act as relays for initiatives such as "MonAideCyber" and "Cyber PME".

Between the 1st of January and the 18th of December 2024, 12 territorial CSIRTs located in mainland France reported close to 700 cybersecurity events to ANSSI – 400 of which were qualified as incidents. Some of these incidents significantly hindered the activities of the affected entities. This has notably been the case with ransomware attacks, which made up a quarter of all reported events in 2024. The rest of the events involved 300 reports relating minor impacts on the targeted entities, with no detected intrusions on the information systems (phishing, denial of service, etc.). The types of victims most affected by reported cybersecurity events in 2024 were SMEs/small businesses/midcaps (37%) from every sector of activity and local governments (29%). In 2024, ANSSI reported to territorial CSIRTs a total of 102 cybersecurity events which occurred in their respective territories.

ANSSI has also worked alongside CSIRTs to assist them in their cyber maturation and to promote their visibility across the national cybersecurity ecosystem. 2024 was notably marked by the reinforced operational synchronisation of the CERT-FR and territorial CSIRTs. CSIRTs were furthermore integrated into the CERT-FR's interactive vocal server. Lastly, in 2024 the Agency supported the creation of three Cyber Resource Centres in the DROM-COM (Réunion, New Caledonia, and French territories of America). Their inauguration in the last quarter of 2024 enabled them to handle their first incidents. A consolidated overview of the 15 territorial CSIRTs and CRCs (Cyber Resource Centres) in mainland France and overseas territories should be achieved as early as 2025.

At present, there exist fifteen territorial CSIRTs located in:

- Bourgogne-Franche-Comté, with the Bourgogne-Franche-Comté CSIRT;
- Brittany, with Breizh Cyber;
- Centre-Val de Loire, with CybeRéponse;
- Corsica, with the CyberCorsica CSIRT | Centre de cybersécurité Corse;
- Grand-Est, with Grand-Est Cybersécurité;
- Hauts-de-France, with the Hauts-de-France CSIRT;
- Île-de-France, with Urgence Cyber Île-de-France;
- Normandy, with Normandie Cyber;
- Nouvelle-Aquitaine, with the Campus régional de Cybersécurité et de Confiance numérique;
- Occitania, with Cyber'Occ;
- Pays de la Loire, with Pays de la Loire Cyber Assistance;
- the Sud Provence-Alpes-Côte-d'Azur region, with Urgence Cyber région Sud;
- the French territories of America (the Guadeloupe region, the territorial authority of Guiana, the Saint-Martin, Saint-Barthélemy, and Saint-Pierre and Miquelon territorial overseas collectivities), with the CSIRT-ATLANTIC;
- La Réunion, with the Réunion CSIRT;
- New Caledonia, with the Centre Cyber du Pacifique.

As with territorial CSIRTs, the rise of ministerial CSIRTs is supervised and supported by ANSSI, who assists them in the process of their automation in the field of detection and supervision while continuing to ensure effective interministerial detection. In 2024 a technical committee common to both the CERT-FR and ministerial CSIRTs was established. Initiated in January of 2024, the incubation of the 10 major ministerial CSIRTs was completed in late April – signalling their progressive maturation. Operational exchanges have already been initiated and are set to further multiply. Indeed, the CERT-FR is already receiving incident reports from CSIRTs and regularly shares threat markers with them. ●

"CSIRT relays play a central role in streamlining user journeys, rendering them accessible to all. They provide humane, personalised support that is grounded in local and sectoral realities."

Jeanne Fournis, Project Leader, Operations Sub-Directorate

A service offering co-developed to increase cyber support

In order to assist an increasing number of beneficiaries, ANSSI continuously revisits its working methods and tools. 2024 abounded with developments and with the deployment of new digital services, initiated in collaboration with key actors of the cyber ecosystem. This trend is set to persist and intensify in 2025. Service offerings take the form of different platforms which collectively embody the rescaling necessary to the implementation of the NIS 2 Directive. These platforms enable the Agency to further multiply its activities and allow its messages to more efficiently reach beneficiaries.

MonAideCyber, for instance, enables the federation of a community of "cyber helpers", to allow them to better assist their beneficiaries in their respective cybersecurity reinforcement efforts. This community notably includes State representatives (Police, gendarmerie, customs, General Directorate of Internal Security (DGSI), Intelligence and Defence Security Directorate (DRSD), prefectures, etc.), administrations, local governments, public interest groups, consular and union councils, associations (cyber campuses, public digital service operators (OPSN), sectoral, digital, or economic development associations). Launched by ANSSI, this innovation is free and supported by the Ministry of the Interior and Overseas Territories, Cybermalveillance.gouv.fr, and the CNIL. MonAideCyber was deployed nationally after a trial period of two years, but functionalities are still continuously being reworked to take into consideration user feedback. Over 1,000 "cyber helpers" are already registered, and MonAideCyber has thus far assisted over 1,450 "helpees".

In this same perspective of pedagogy and with the intention of providing a "turnkey" service, ANSSI and the CNIL continued to develop MonServiceSécurisé. Available since 2022, this platform was created by the Agency in accordance with the principles of the BetaGouv method. MonServiceSécurisé is accessible to all public servants: municipalities, communities of municipalities, cities, public digital service operators (OPSN), mixed unions, departmental councils, universities, ministries – whatever their level of cybersecurity. Initially intended to assist in securing public entities' online services, the platform hastens the

"We cannot wait for the transposition of the NIS 2 Directive to assist in securing the entities concerned. ANSSI is therefore working alongside its beneficiaries to innovate, and notably employs methods derived from design to come up with solutions adapted to their needs."

Solène Bellego, Head of Design, in the Innovation Laboratory, Strategy Sub-Directorate

security registration process and helps public entities to conform to regulation. In 2024, the number of users on the platform reached 6,063 – which represented a 100% increase compared to the previous year, covering 3,403 secure services. Over the past year, MonServiceSecurisé helped user entities patch a total of 81,986 vulnerabilities. In 2024, for the second time since its creation, the platform received the State start-up acceleration fund allocated by the Interdepartmental Directorate of Digital Affairs.

Also intended for public servants to supplement the security measures implemented by the ministries, the *jecliqueoupas.cyber.gouv.fr* platform was likewise deployed in 2024, developed by the company Glimps as part of a public procurement initiated by ANSSI. This tool conducts file analyses to easily and rapidly assess the safety of any given document, providing an alternative to the freely accessible online services offered by foreign companies whose use of collected data is unregulated.

In 2024, a beta version of *monespacenis2.cyber.gouv.fr* was also inaugurated. Developed by ANSSI, the platform is geared towards any entity wishing to find out if they are concerned by the NIS 2 Directive. It provides a test designed to allow entities to figure out which category (essential or important) they belong to, and whether or not they are subject to the directive. The service will also make it possible to register with ANSSI, to learn more about the requirements set out by the directive, and to subscribe to a dedicated newsletter.

Other products were introduced in 2024 to supplement the Agency's service offering. Produced by ANSSI in collaboration with the France InterCERT, incident response guides were published on the website of the CERT-FR, *cert.ssi.gouv.fr*. Made up of practical guides and quick action sheets, these publications were designed to help detection and/or incident response teams efficiently handle security incidents. The goal was to provide concise and operational resources to help enhance reactivity in the face of cyberthreats. Contributions were also made in open-source on GitHub, indicating a desire to share ANSSI's tools amongst professionals of the cybersecurity community. These contributions are primarily made for CSIRTs by security teams and providers, and generally concern information system security, automated auditing, or digital investigation tools. ●

81,986

patched vulnerabilities

3,403

services secured *via MonServiceSécurisé*

↘ AlerteCyber and *cybermalveillance.gouv.fr*: a system to alert entities of all sizes

Launched in July of 2021 at the initiative of the GIP ACYMA and a collective of professional organisations, AlerteCyber was designed to help entities of all sizes face cyberthreats, to inform them, and to encourage them to implement the necessary protective measures. AlerteCyber is activated whenever a threat or serious breach is detected and qualified as such by ANSSI and *Cybermalveillance.gouv.fr*. It is more specifically intended for hardware or software solutions deployed by the GIP's target public, primarily used by individuals or structures which do not possess an information system – such, for instance, as small businesses or governing bodies.
In 2024, two AlerteCyber campaigns were conducted:

→ February 26th: Critical security breach impacting Microsoft Outlook
→ May 6th: Critical security breaches impacting QNAP products

Given the increase in vulnerabilities observed by ANSSI, AlerteCyber effectively contributes to the prevention of attacks and to the notification of victims. ●

Assessment of the regulatory frameworks implemented by ANSSI

This section provides an assessment of the main regulatory frameworks – qualification and certification schemes excluded – implemented by ANSSI in 2024. Enshrined in the Defence Code and in the Posts and Electronic Communications Code, these frameworks allow ANSSI to carry out the duties with which it has been entrusted under Decree n°2009-834, dated July 7th 2009.

They may be classified according to their purpose:

- → protecting whistleblowers,
- → alerting victims,
- → detecting State or cybercriminal threats,
- → countering a threat to national security,
- → protecting privacy and the confidentiality of correspondences,
- → maintaining the security of 5G networks and of future generations.

2024 was marked by the entry into force of the 2024-2030 LPM's new operational measures, made legally binding *via* the publication of decrees and implementing orders.

In order to identify victims of cyberattacks, an initial set of capacities had been provided by the previous LPM. Prior to the Games in 2024, ANSSI successfully implemented its first framework under the supervision of ARCEP and the CNIL. The additional capacities for action provided by the new LPM are progressively being rolled out, in cooperation with all of the private and public actors concerned. Ultimately, these capabilities will facilitate the prevention and characterisation of threats (DNS filtering, DNS cache collection, collection of data), and enable more effective handling of product vulnerabilities – by requiring vendors to report significant vulnerabilities to both ANSSI and its clients, for instance.

Protecting whistleblowers

Ⓐ Any individual who discovers a security breach or vulnerability may report it to ANSSI under article L.2321-4 of the Defence Code.

PRESENTATION OF THE FRAMEWORK

This legal framework ensures that any individual who, in good faith, reports discovered vulnerabilities only to ANSSI will see their identity protected by the Agency. Indeed, this framework dispenses ANSSI's agents with their obligation to inform the Public Prosecutor's Office, as is required under article 40 of the Code of Criminal Procedure.

2024 ASSESSMENT

In 2024, the Agency received 236 reports under article 2321-4 of the Defence Code. Half (49%) of these reports concerned vulnerabilities affecting websites. Such vulnerabilities may lead to the exposure of data, and even to the partial or complete hijacking of the website. Whether they are caused by vulnerabilities or by faulty configuration, data exposures represent 37% of all reports. Only 11% of reports received by ANSSI concerned vulnerabilities affecting software (generally professional solutions).

The Agency has thus far never been confronted with a notifier who was not acting in good faith. As such, it has not made any declarations to the Public Prosecutor's Office under this framework.

It is important to note that, in many cases, notifiers include the concerned entities as recipients of their reports – thus waiving their own anonymity. ●

Ⓑ ANSSI may receive and handle whistleblowers' reports under decree n°2022-1284, dated October 3rd 2022 and drawn from law n°2022-401 of March 21st 2022, which endeavours to strengthen the protection of whistleblowers.

Under this decree, ANSSI was tasked with receiving and handling reports made by whistleblowers in the field of information system and network security (ISS) – and more particularly those of critical operators. As such, it is possible for whistleblowers to petition the Agency in cases of non-compliance to regulatory provisions:

- → violation of NIS 1 or eIDAS implementation schemes, or of measures pertaining to the security of information systems employed in activities of vital importance (SAIV)[15];
- → non-compliance to regulatory frameworks for the qualification and certification of products or services;
- → violation of regulatory control, including that which is associated with the protection of correspondence confidentiality;
- → non-compliance to the regulatory obligations imposed on electronic communications operators (ECO) providing operational support to ANSSI[16], such as the unavailability of detection abilities for the identification of victims or the characterisation of a proven threat, or the failure to inform ANSSI should a security incident be observed on one of their own networks.

2024 ASSESSMENT

No cases of non-compliance to regulatory frameworks dedicated to the security of information systems were reported to ANSSI. ●

[15] For more information of the NIS regulation and the SAIV framework: *cyber.gouv.fr/les-directives-nis-nis-2-et-le-dispositif-saiv*

[16] Under article D.98-5 of the Posts and Electronic Communications Code (CPCE), article L.33-14, para.2, of the CPCE, article L.33-14, para.5, of the CPCE, and article L.2321-2-1 of the Defence Code.

Alerting victims

Ⓐ ANSSI may conduct alert campaigns amongst electronic communications operators, under article L.33-14 para.5 of the CPCE.

PRESENTATION OF THE FRAMEWORK

This framework allows ANSSI to rely on ECOs of vital importance in the transmission of compromise or vulnerability reports to the concerned entities.

2024 ASSESSMENT

In 2024, 9 vulnerability alert campaigns – involving 15,900 IP addresses – were conducted with subscribers of these operators. 8,731 of these vulnerabilities were identified. All of the affected ECOs participated in the campaigns.

The *Cybermalveillance.gouv.fr* website hosts the vulnerability report webpage through which clients of these operators are encouraged to keep track of alerts. In the context of these campaigns, the webpages were consulted a total of 438 times. ●

Ⓑ ANSSI may request victims' identifiers from electronic communications operators, under article L.2321-3 para.1 of the Defence Code.

PRESENTATION OF THE FRAMEWORK

This article defines the cases in which ANSSI may request information from ECOs. The first paragraph provides that, in the interest of the security of information systems belonging to operators of vital importance (OIV), to essential service providers (OSE), or to public authorities, the Agency may request that ECOs convey the identity, physical address and e-mail address of users or proprietors of vulnerable, threatened, or attacked information systems. The objective is to alert said users and proprietors of the vulnerability or attack detected on their information systems.

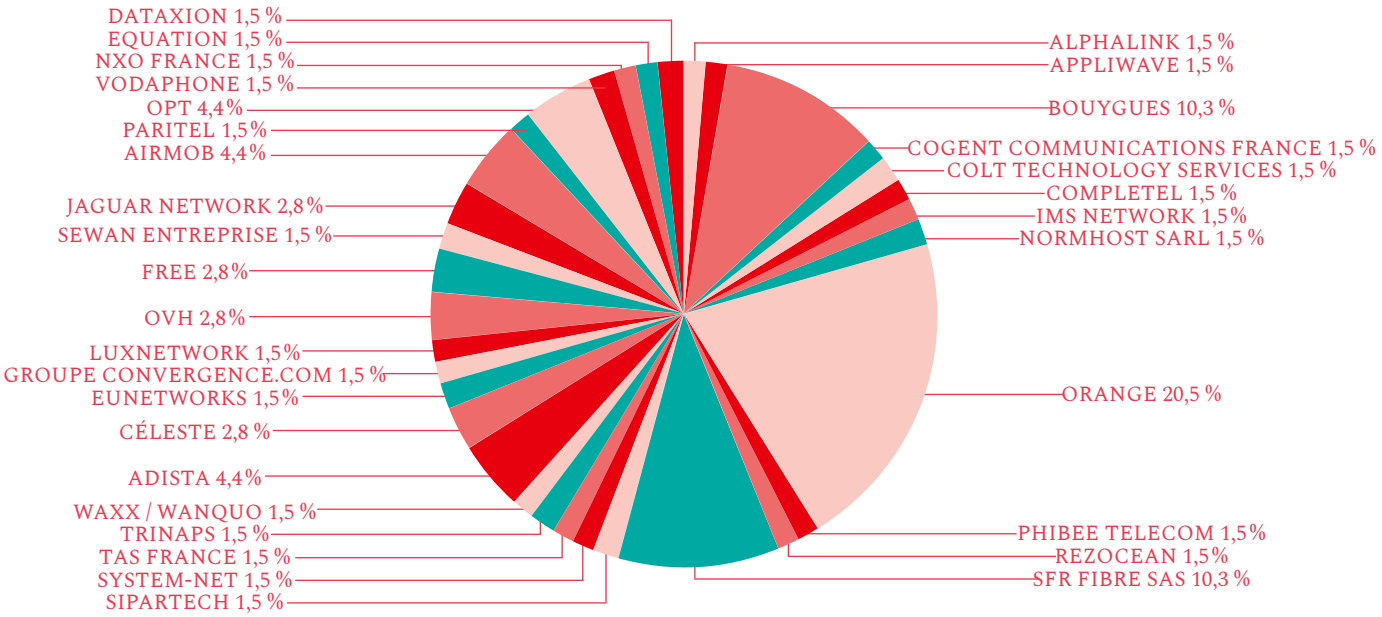
This identification process responds to the need of regulated operators to enhance the security of their systems.

2024 ASSESSMENT

In 2024, 68 identification requests – concerning 978 IP addresses – were submitted by ANSSI to 34 different electronic communications operators. As the primary providers of OIVs, OSEs, and public authorities, Orange, SFR, and Bouygues were the recipients of close to half of these requests.

Article L.2321-3 para.1 of the Defence Code is a core pillar of ANSSI's awareness-raising missions, supplementing the rest of the tools at its disposal. Before it has recourse to this framework, the Agency searches for potential victims on all of the bases to which is has access – and these have, over the years, grown more numerous and precise. ●

BREAKDOWN OF VICTIM IDENTIFICATION REQUESTS MADE UNDER ARTICLE L.2321-3 PARA.1 OF THE DEFENCE CODE, BY ELECTRONIC COMMUNICATION OPERATOR



© Article L2321-4-1 of the National Defence Code requires vendors to notify ANSSI of any significant vulnerabilities detected on products distributed in France.

PRESENTATION OF THE FRAMEWORK

Article L2321-4-1 of the National Defence Code was devised under the LPM 2024-2030. It introduced a new obligation for vendors: the requirement to report significant vulnerabilities to users and to ANSSI.

The article ensures that vulnerabilities are adequately taken into consideration until they are patched, and facilitates communication with users in order to better protect their information systems. This new disposition provides for greater coordination between ANSSI and interested parties in the handling of significant vulnerabilities. Should an editor fail to fulfil this obligation to communicate with users, ANSSI has the capacity to order them to disclose the vulnerability – publicly or not – and to publish the injunction in the case of repeated failures to comply.

This new obligation is only applicable when the following conditions have been met[17]:

- The vulnerability is affecting a software vendor: within this framework, the term "software vendor" refers to "any natural or legal person responsible for designing, developing, or requesting the development of software, supplying it to users either freely or against payment."

[17] An FAQ is available on ANSSI's website: *https://cyber.gouv.fr/sites/default/files/document/FAQ_decret_LPM-2024-2030_consultations.pdf*

- The vendor supplies its software:
- On French territory;

→ To companies whose headquarters are located on French territory;

→ Or to companies controlled, under article L. 233-3 of the Commercial Code, by companies whose headquarters are located on French territory.

- The vulnerability affecting the software is significant: the significance of the vulnerability is assessed by the vendor on the basis of said vendor's understanding of the software, of its users, of its uses, and of its environment, drawing on the criteria set out in article R2321-1-16 of the Defence Code:

→ The number of users impacted by the vulnerability or by the incident affecting the product;

→ The number of products into which the affected product has been integrated;

→ The technical, potential, or actual impact of the vulnerability or incident on the expected functioning of the product. Depending on the product's specific features, this impact is assessed on the basis of security criteria such as availability, integrity, confidentiality, or trackability;

→ The type of product, taking into account its uses and the environments in which it is deployed;

→ The impending or proven exploitation of the vulnerability;

→ The existence of technical proof of exploitation or of an exploitation code.

2024 ASSESSMENT

Since its entry into force on the 1st of June 2024, ANSSI handled one significant vulnerability within the scope of article L.2321-4-1 of the National Defence Code. ●

Detecting state and cybercriminal threats

Ⓐ Electronic communications operators must employ detection mechanisms and exploit the technical markers provided by ANSSI, under article L.33-14 para.1 and 2 of the CPCE supplemented by article L.2321-3 para.2 of the Defence Code.

PRESENTATION OF THE FRAMEWORK

Given the interconnexions they generate between the information systems of their clients, electronic communications operators play a crucial role in the detection of cyberattacks.

In its second paragraph, article L.33-14 of the CPCE stipulates that ANSSI should provide markers for ECOs to exploit in their detection systems. These markers should allow for alerts to be triggered and, ultimately, for victims to be identified and alerted.

2024 ASSESSMENT

Operators are now able to implement the Agency's markers using components from their infrastructure which were not initially designed to address this need. In 2024, ANSSI conducted a campaign on the basis of these capabilities.

Since the publication of decree 2024-421 on the 10th of May 2024, this system has been imposed upon operators of vital importance and the deployment of detection mechanisms has even been financially compensated. The Agency is assisted by the Commission for Electronic Defence Communications (CCED) to ensure the deployment of capacities capable of supporting it in its endeavour to meet the needs of operators and fulfil the mission with which it has been entrusted by law. ●

Ⓑ ANSSI may deploy detection mechanisms on the devices owned by electronic communications operators and hosts which are subjected to the control of attackers, under article L.2321-2-1 of the Defence Code.

PRESENTATION OF THE FRAMEWORK

Introduced under the LPM 2019-2025 and reinforced by the LPM 2024-2030, article L.2321-2-1 of the Defence Code enables ANSSI to implement data collection mechanisms for electronic communications operators or hosts, to keep devices controlled by attackers under observation.

Closely monitored by ARCEP, this mechanism is specifically intended to address threats against national security and defence or against critical operators (OIVs, OSEs, public authorities). It has facilitated the identification of victims of cyberthreats, both in France and abroad.

2024 ASSESSMENT

In 2024, four operations were conducted with hosts, and two operations initiated in 2023 were prolonged beyond their initial period of three months in order to keep track, over the longer term, of a threat against national security.

The year was notably marked by internal efforts carried out alongside hosts to operationalise the new capacities provided by the LPM 2024-2030. In the latter half of the year, these efforts led to a first data collection operation – as permitted by the extended capacities provided by the LPM. ●

Ⓒ The transmission of technical data from DNS cache servers to ANSSI: article L.2321-3-1 of the Defence Code.

PRESENTATION OF THE FRAMEWORK

This new disposition requires that domain name resolution system providers regularly communicate the cache data stored on their systems to ANSSI. This non-identifying data makes possible the association of domain names to their IP addresses and is used for analyses and threat characterisation.

The disposition aims to raise awareness of the offensive actors likely to threaten national security whose methods involve using domain names to carry out cyberattacks – notably by facilitating the identification of other components of their attack infrastructure, or by shedding light on the chronology of attacks. "DNS cache" data is fundamental to threat analysis and, in some cases, may also be obtained from commercial sources.

2024 ASSESSMENT

Dialogue has been initiated with different electronic communications operators to facilitate the implementation of this measure. An initial proof of concept has been produced in cooperation with an ECO; nonetheless, this measure with require significant adjustments within the Agency and within the infrastructures of operators. Exchanges have been initiated with the CCED in order to facilitate these technical adjustments. ●

Countering a threat impacting national security

PRESENTATION OF THE FRAMEWORK

Article L.2321-2-3 of the Defence Code empowers ANSSI to request the filtering of domain names used by attackers. Should national security be threatened, ANSSI may – under the strict supervision of ARCEP – prescribe gradual domain name filtering measures to DNS resolvers, registrars, and the Registration Office.

Amongst the different dispositions, ANSSI may request the blocking or suspension of domain names to prevent their malicious use. For more advanced threats, however, such a measure would not durably impede the attacker's efforts. In such cases, the Agency may request the redirection or transfer of domain names in order to observe the queries addressed to them and, subsequently, to identify victims. Once they have been alerted by ANSSI, victims may implement measures to durably contain and remediate the attack.

2024 ASSESSMENT

Prior to the Paris 2024 Olympic and Paralympic Games, the Agency developed domain name blocking and redirection capabilities in cooperation with the Ministry of the Interior and Overseas Territories and with major ECOs. The Agency uses an exchange platform introduced by the ministry to send out automated blocking and unblocking requests to operators. The mutualisation of this platform made the implementation of this measure much more cost-effective in terms of both financial and human resources. ●

Protecting privacy and the confidentiality of correspondence

In France, the commercialisation and exploitation of technological devices or mechanisms capable of undermining the privacy of users or the confidentiality of correspondence are closely supervised.

ANSSI is responsible for this supervision, exercised within the bounds of a system of prior administrative authorisations established under articles 226-3 and 226-7 of the Penal Code.

PRESENTATION OF THE FRAMEWORK

In order to protect user privacy and the confidentiality of correspondences, articles 226-3 and 226-7 of the Penal Code prescribe the obtention of prior authorisations for the production, importation, acquisition, possession, exposition, offering, renting, or sale of certain devices.

This system concerns both manufacturers, resellers, and users of the devices. As such, the authorisation required for "production, importation, acquisition, possession, exposition, offering, renting, or sale" under article 226-3 of the Penal Code must be distinguished from the authorisation required under article 226-7 of that same code, for "acquisition and possession".

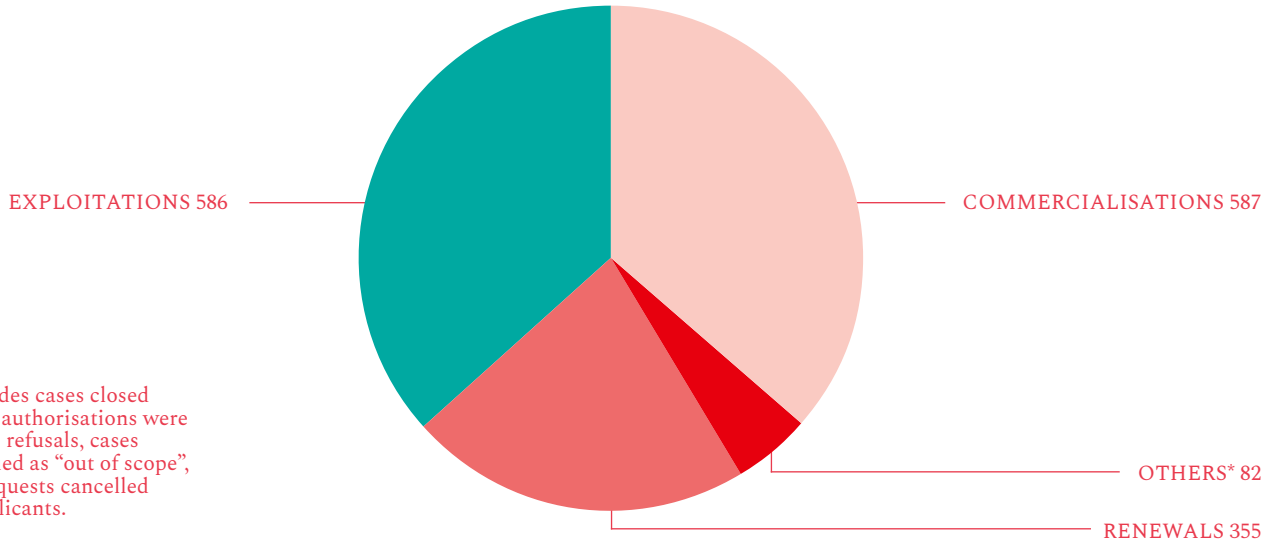
Authorisation requests are advised by the Agency, which has been tasked with ensuring that the system serves a legitimate purpose in compliance with French law, that it is adequately secure, and that it cannot be hijacked for illegitimate use. Requests are then reviewed by the consultative commission, headed by ANSSI's Director General and made up of representatives from the concerned administrative bodies (Ministry of Justice, of the Interior and Overseas Territories, of the Armed Forces, of Customs, of the Industry, of Telecommunications, National Frequencies Agency, National Commission for the Control of Intelligence Techniques).

In addition to the duration – which can vary between one and six years – authorisations may specify the number of devices concerned and subject their use to conditions in order to prevent their misuse.

2024 ASSESSMENT

In 2024, ANSSI issued 1,610 decisions – including 52 refusals. The number of commercialisation authorisations (intended for manufacturers) roughly matches the number of possession authorisations (intended for users), given that the two generally go hand in hand. ●

VOLUME OF DECISIONS MADE UNDER ARTICLES 226-3 AND 226-7 OF THE PENAL CODE



* Includes cases closed before authorisations were issued, refusals, cases classified as "out of scope", and requests cancelled by applicants.

Ensuring the security of 5G networks and of future generations

Since 2019, ANSSI has been monitoring the equipment used to deploy 5G networks in order to guarantee their security. This monitoring is conducted under article L.34-11 of the CPCE.

PRESENTATION OF THE FRAMEWORK

In the interest of national defence and security, article L.34-11 of the CPCE subjects to the Prime Minister's authorisation the exploitation, on French territory, of hardware or software which enables the connection of end-user devices to 5G networks and which may represent a threat to the permanence, integrity, security, and availability of the network, or to the confidentiality of correspondences[18].

This framework – whose implementation is ensured by the General Secretariat for Defence and National Security – concerns fifth-generation "5G" networks and will also apply to future generations.

It seeks to take into consideration the risks posed by the new capacities of mobile infrastructure on national security and defence. In this sense, it is a response to the fundamental changes engendered by the deployment of 5G technologies, which could not adequately be taken into consideration within the "R. 226" framework presented in the previous section:

- ➔ the emergence of a multiplicity of new uses, such as telemedicine, transportation, or connected industry, and the convergence within public 5G networks of use cases which had previously been confined to specific or isolated networks. In this context, the compromised integrity or unavailability of 5G networks could have severe consequences on the security of goods and individuals and on the continuity of the State's activities;
- ➔ the development of radioelectric network infrastructure towards primarily software-based applications, driven by generic computing technologies, in lieu of the highly-specialised technologies used in previous generations. This development grants the operators of such infrastructure greater freedom for configuration, but also exposes them to the threats and vulnerabilities inherent to these generic technologies;
- ➔ by virtue of the central role they play in the majority of digital uses, 5G networks are strategically very important and may therefore be exposed to interference attempts by third States which may seek to exert pressure on operators or their suppliers and service providers.

The types of devices subjected to authorisation are defined by order. The first of these are base stations – meaning the antennas set up across the territory to provide connectivity to user terminal equipment. The second are a set of functions considered to be critical to network cores, central infrastructures of mobile networks.

2024 ASSESSMENT

Decisions pertaining to 5G antennas

In 2024, 83 decisions were issued – including 3 refusals. It should be noted that authorisation requests are typically made for groups of antennas; as such, decisions may pertain to several dozen base stations. Furthermore, given that every update necessitates a new authorisation, the number of decisions issued is not representative of the actual number of antennas on French territory: a single antenna may be the subject of successive authorisations as new software versions are introduced.

In actuality, 75% of decisions issued after 2020 have been authorisation renewals requested in the context of software updates.

Decisions pertaining to 5G network cores

Up until 2023, operators only submitted authorisation requests for base stations (antennas). Indeed, in the early days of its deployment on French territory, 5G was rolled out in a "Non-Standalone" configuration (NSA) relying on fourth-generation (4G) network nodes which do not fall within the scope of article L.34-11 of the CPCE.

With regards to "Standalone" 5G (SA), the first few requests concerning the network core section were submitted from July of 2023. Over the past year, 39 authorisations were issued for fifth-generation network nodes. ●

[18] This measure was introduced under law n° 2019-810 of August 1st, 2019. It aims to preserve France's national security and defence, in the context of the exploitation of radioelectric mobile networks.

Bibliography

GOOD PRACTICE GUIDES

→ LES ESSENTIELS
(French version of the "Back to Basics")

DevSecOps, version 1.0.
Learn more

Virtualisation, version 1.0.
Learn more

→ BACK TO BASICS

DevSecOps, version 1.0.
Learn more

Distributed Denial of Service (DDoS), version 2.0.
Learn more

Secure implementation of CMS, version 1.1.
Learn more

Virtualization, version 1.0.
Learn more

The golden rules of backup, version 1.1.
Learn more

→ FUNDAMENTALS

Sécurisation d'une infrastructure VMware, version 1.0.
Learn more

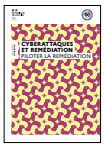
→ TECHNICAL GUIDES

Recommandations pour les architectures des interconnexions multiniveaux, version 1.0.
Learn more

Recommandations relatives aux architectures des services DNS, version 1.0.
Learn more

Recommandations de déploiement d'un service IAAS OpenStack SecNumCloud, version 1.0.
Learn more

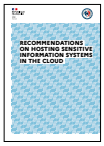
Cyberattaques et remédiation : La remédiation du Tier 0 Active Directory, version 1.0.
Learn more



Cyberattaques et remédiation : Piloter la remédiation, version 1.0.
Learn more

Cyberattaques et remédiation : Les clés de décision, version 1.0.
Learn more

Security recommendations for a generative AI system, version 1.0.
Learn more



Recommendations on hosting sensitive information systems in the cloud, version 1.0.
Learn more

SCIENTIFIC PUBLICATIONS

→ SCIENTIFIC ARTICLES PRESENTED IN CONFERENCES

Cryptology laboratory

A Not So Discrete Sampler: Power Analysis Attacks on HAWK signature scheme, Morgane Guerreau and Mélissa Rossi [⋄]. CHES 2024, vol. 4, pp. 156-178.
Learn more

A Univariate Attack against the Limited-Data Instance of Ciminion, Augustin Bariant [⋄]. Selected Areas in Cryptography (SAC) 2024.
Learn more

Fast AES-Based Universal Hash Functions and MACs, Augustin Bariant, Jules Baudrin, Gaëtan Leurent, Clara Pernot, Léo Perrin, et Thomas Peyrin. IACR Transactions on Symmetric Cryptology (ToSC) 2024, vol. 2, pp. 35-67.
Learn more

G+G : A Fiat-Shamir Lattice Signature Based on Convolved Gaussians, Julien Devevey [⋄], Alain Passelègue and Damien Stehlé. Asiacrypt 2024, pp. 37-64.
Learn more

HAETAE: Shorter Lattice-Based Fiat-Shamir Signatures, Jung Hee Cheon, Hyeongmin Choe, Julien Devevey, Tim Güneysu, Dongyeon Hong, Markus Krausz, Georg Land, Marc Möller, Damien Stehlé, et Minjune Yi. TCHES 2024, pp. 25-75.
Learn more

Quarantined-TreeKEM: a Continuous Group Key Agreement for MLS, Secure in Presence of Inactive Users, Céline Chevalier, Guirec Lebrun, Ange Martinelli and Abdul Rahman Taleb. ACM CCS 2024.
Learn more

Raccoon : A Masking-friendly Signature Proven in the Probing Model, Rafaël del Pino, Shuichi Katsumata, Thomas Prest and Mélissa Rossi [⋄]. CRYPTO 2024, pp. 409-444.
Learn more

The Algebraic FreeLunch: Efficient Gröbner Basis Attacks Against Arithmetization-Oriented Primitives, Augustin Bariant [⋄], Aurélien Boeuf, Axel Lemoine, Irati Manterola Ayala, Morten Øygarden, Léo Perrin et Håvard Raddum. CRYPTO 2024, pp. 139-173.
Learn more

Updatable Encryption from Group Actions, Antonin Leroux and Maxime Roméas [⋄]. PQCrypto 2024, vol. 2, pp. 20-53.
Learn more

[⋄] Individuals associated with ANSSI at the time of the submission or publication of the scientific article.

Security of wireless technology laboratory

Time-Memory Trade-Offs Sound the Death Knell for GPRS and GSM, Gildas Avoine, Xavier Carpent, Tristan Claverie [⋄], Christophe Devine [⋄], Diane Leblanc-Albarel, conférence CRYPTO 2024, Santa Barbara, 206-240.

Communications à grande distance avec un lecteur ISO 14443, Yoann Burny, Pierre-Michel Ricordel [⋄], SSTIC 2024, Rennes.
Learn more

Detection research and exploration laboratory

Inductive Lateral Movement Detection in Enterprise Computer Networks, Corentin Larroche, ESANN 2024.
Learn more

Protocol, network security laboratory

A Unified Symbolic Analysis of WireGuard, Pascal Lafourcade, Dhekra Mahmoud et Sylvain Ruhault [⋄]. NDSS 2024.
Learn more

Hardware and software architecture laboratory

Characterizing and Modeling Synchronous Clock-Glitch Fault Injection, Amélie Marotta, Ronan Lashermes, Guillaume Bouffard [⋄], Olivier Sentieys et Rachid Dafali, COSADE 2024.
Learn more

Évolutions dans la sécurité des modules de gestion de l'énergie, Gwenn Le Gonidec, Maria Méndez Real, Guillaume Bouffard [⋄] et Jean-Christophe Prévotet, JAIF 2024.
Learn more

Évolution des protections du moteur Javascript V8, François Jolivet [⋄]. SSTIC' 24,
Learn more

Component security laboratory

Butterfly Probes : Estimating the Derivative of the Magnetic Flux, Philippe Maurine, Jérémy Raoult, Anselme Mouette, Julien Toulemont [⋄]. EMC COMPO 2024.
Learn more

Cryptology laboratory, exploration and detection research laboratory and component security laboratory

Retour d'expérience sur l'organisation d'un CTF, Adrien Thuau, Alexandre Iooss [⋄], Emilien Court, Jérémy Jean, Matthieu Olivier, Tristan Claverie [⋄]. SSTIC 2024.
Learn more

→ ARTICLES PUBLISHED IN SCIENTIFIC RESEARCH JOURNALS

Cryptology laboratory

Masking the GLP Lattice-Based Signature Scheme at Any Order, Gilles Barthe, Sonia Belaïd, Thomas Espitau, Pierre-Alain Fouque, Benjamin Grégoire, Mélissa Rossi, Mehdi Tibouchi. Journal of Cryptoly 2024.

A Long Tweak Goes a Long Way : High Multi-User Security Authenticated Encryption from Tweakable Block Ciphers, 2. Benoit Cogliati, Jérémy Jean, Thomas Peyrin et Yannick Seurin, IACR Communications in Cryptology 2024, vol. 1.

A provably masked implementation of the BIKE Key Encapsulation Mechanism, Loïc Demange, Mélissa Rossi. Communications in Cryptology 2024, vol. 1, Number 1.

→ CONTRIBUTIONS TO SCIENTIFIC PUBLICATIONS

Security of wireless technology laboratory

Sécurité électromagnétique : panorama des modèles de menace, José Lopes Esteves [⋄], magazine *MISC*, hors-série n° 29.

An Introduction to intentional electromagnetic interference exploitation, José Lopes Esteves [⋄], Embedded Cryptography, éditions ISTE/WILEY.

OPEN-SOURCE PUBLICATIONS

Detection research and exploration laboratory

DECODE : Malicious Portable Executable (PE) file detection tool based on NTFSInfo data collected by the DFIR-ORC tool.
Learn more

Component security laboratory

Hackropole-hugo : *hackropole.fr* website engine, used to host archived challenges of the French CyberSecurity Challenge (FCSC).
Learn more

Hardware and software architecture laboratory

Chipsec-check : generation of USB stick comprising chipsec and other tools to test hardware and firmware security requirements.
Code source Github

Keysas: a prototype of file decontamination station, with a focus on the security of the station itself.
Code source Github

Lidi: software diode developed in Rust, initiated by the LSL and maintained by the LAM. Code source Github

CONTRIBUTIONS TO THIRD-PARTY OPEN-SOURCE PROJECTS

Component security laboratory

QEMU: generic emulator and virtual device; contribution in TCP plugins.
Learn more

PicoEMP: electromagnetic fault injection (EM-FI); bug fix.
Code source Github

CTFd: management of an online Capture-The-Flag (CTF) challenge; contribution following the FCSC.
Code source Github

Wireless technology security laboratory

Tamarin prover: Tamarin models of Bluetooth, Bluetooth Low Energy, and Bluetooth Mesh key establishment protocols.
Code source Github

Hardware and software architecture laboratory

Chipsec : Platform Security Assessment Framework (Intel). Maintainer for the AMD architecture, added support for USB image construction.
Code source Github

Noyau Linux: multiple vulnerability patches.
Memory corruption, type confusion

Systemd: correction of the enrollment behaviour of secure-boot keys by bootctl, in order to meet the UEFI specification.
Public contribution

THREAT AND INCIDENT REPORTS

Cyber Threat Overview 2023, February 27th 2024.
Learn more

État de la menace ciblant les grands événements sportifs en France, 17 avril 2024.
Learn more

Opération ENDGAME, 30 mai 2024.
Learn more

Failles sur les équipements de sécurité – Retour d'expérience du CERT-FR, 12 juin 2024.
Learn more

Malicious activities linked to the Nobelium intrusion set, June 19th 2024.
Learn more

Codes malveillants utilisés à des fins destructrices, 11 juillet 2024.
Learn more

État de la menace ciblant les organismes de recherche et think tanks, 02 septembre 2024.
Learn more

Exfiltration de données du secteur social – Retour d'expérience du CERT-FR, 24 septembre 2024.
Learn more

État de la menace ciblant le secteur de la santé, 07 novembre 2024.
Learn more

État de la menace ciblant le secteur de l'eau, 28 novembre 2024.
Learn more

PARTNERSHIPS

Position Paper on Quantum Key Distribution.
Learn more

Securing Tomorrow, Today: Transitioning to Post-Quantum Cryptography.
Learn more

MARKET STUDIES

État de l'offre des solutions de cryptographie post-quantique en 2023, version 1.0.
Learn more

État de l'offre de prestation d'accompagnement et de conseil en sécurité, version 1.0.
Learn more

Observatoire des métiers, L'attractivité et la représentation des métiers de la cybersécurité vues par les professionnels, version 1.0.
Learn more

REPOSITORIES

Information system security audit providers – Requirements repository Version 2.2 of August 1st 2024 (published on 29/11/24)

Security incident response providers, Requirements repository Version 3.0 of July 18th 2024 (published on 29/11/2024)

Version 1.0 – April 2025
Registration of copyright:
April 2025
ISSN 3077-8115 (online)
Open Licence Licence
(Etalab — V1)

French Cybersecurity Agency
ANSSI
51 boulevard
de la Tour-Maubourg 75
700 PARIS 07 SP
www.cyber.gouv.fr

Graphic design & illustrations:
Cercle Studio