RÉPUBLIQUE
FRANÇAISE

Liberté
Égalité
Fraternité

NATIONAL CYBERSECURITY STRATEGY 2026 — 2030

PREFACE

There are silent upheavals that disrupt world order more surely than the crashes of history. The digital revolution is one of them.

At a time when our lives, our economies and our democracies are woven together through networks and algorithms, when the line between sovereignty and dependence can be drawn with a single line of code, cybersecurity has become a prerequisite for freedom. A vital requirement. A strategic imperative.

For the digital space is now a theatre of power, reflecting and relaying physical confrontations. A place where nations, interests and ideologies clash. A field of operations where decisive battles for the independence of our states, the security of our citizens and the strength of our institutions are often fought silently.

France cannot be a spectator. It will be a sovereign power, with strength, method and ambition.

This 2026-2030 national cybersecurity strategy sets our course. It extends and gives concrete form to the guidelines of the National Strategic Review, to make our country a major hub for global cybersecurity.

We will train thousands of talented individuals, because tomorrow's war is being won today, in schools, laboratories, start-ups and campuses. We will protect our infrastructure, our businesses and our communities by combining innovation and regulation, boldness and vigilance.

We will strengthen our resilience to the shocks of an increasingly fragmented world by preparing the entire nation – both public and private actors – to face crises, limit their impact and emerge stronger.

And we will deter attacks by asserting a clear, credible doctrine that respects international law but is capable of defending our interests firmly and effectively.

We will not do this alone. This fight for sovereignty is a fight for the entire European Union. It calls for increased cooperation, the pooling of expertise and an ambitious industrial agenda. Together, as Europeans, we must build a secure, open and democratic cyberspace that is faithful to our values.

That is why I would like to take this opportunity to commend the commitment of all those – civil servants, technicians, engineers, researchers, digital warriors and entrepreneurs – who bring this strategy to life on a daily basis. Their demanding and often invisible work is essential to our future.

The twenty-first century is already a digital century; with each and every one of you, it is up to us to make it a century of trust and freedom.

Emmanuel Macron

CONTENTS

For world-class cyber resilience – p.5

PILLAR 1

Making France the largest pool
of cyber talent in Europe - p.7

PILLAR 2

Strengthening the nation's cyber resilience – p.11

PILLAR 3

Halting the expansion of cyber threats – p.15

PILLAR 4

Maintaining control over the security of our digital
foundations – p.19

PILLAR 5

Supporting the security and stability of cyberspace
in Europe and internationally – p.23

Multi-stakeholder governance
in the service of national resilience - p.29

A growing threat

The digitisation of everyday activities brings many benefits to French citizens, both in their professional and personal lives and as citizens, and to businesses, for which it is a driver of innovation and new business opportunities. However, by weaving a complex web of interconnections and generating increased dependence on critical infrastructure, digitisation has profoundly disrupted the foundations of society and exposed entire sections of the daily lives of citizens and organisations to increasingly sophisticated cyber attacks.

Cyberspace has become an arena for competition, contestation and sometimes even uninhibited confrontation, mirroring geopolitical tensions and international rivalries.

Like many countries around the world, France faces an intense cyber threat that extends across the entire economic and social fabric, whether it comes from states, cybercriminals or activists, or is the result of a combination of actions by these different actors.

Whether motivated by economic, political, military or ideological considerations, these cyberattacks can cause considerable damage, disrupting the functioning of society and threatening national security. They can also have significant economic repercussions for victims, causing considerable financial losses and disrupting supply chains.

From espionage to sabotage, extortion and subversion, this constant pressure takes many forms. It manifests itself in particular through the rise of a cybercrime market and the proliferation of cyber-intrusive tools.

It affects all digital infrastructures, even the most critical ones, such as cloud services that host a growing proportion of sensitive data and critical applications. The rise of disruptive technologies such as artificial intelligence systems and the potential emergence of quantum computers capable of defeating current cryptographic security mechanisms, which are widely deployed to secure digital infrastructures, amplify these risks.

France's strategic vision

Faced with the major challenges posed by this threat, France has been resolutely committed to strengthening its cybersecurity for more than a decade. This area is a national priority.

Since 2008 and the publication of the *White Paper on Defence and National Security*, France's strategic vision for cybersecurity has been consolidated, enabling the country to develop a strong culture in this area and gradually increase its level of cyber resilience. It has laid the foundations for a robust and internationally recognised national model, separating defensive and offensive cyber defence missions.

This momentum, embodied in the 2018 *Strategic Review of Cyber Defence* and supported by strong public investment, has enabled France to develop skilled human resources, excellent research capabilities, a cutting-edge economic sector, a rich ecosystem of public and private actors engaged in cybersecurity, and defensive and offensive capabilities that enable it to

protect its interests and its place on the international stage.

However, developments in cyber threats make it necessary to develop a new national cybersecurity strategy to adapt France's capabilities to this new context. The country now faces a continuum of more tightly intertwined cyber attacks, involving both state actors and cybercriminals in a more unstable geopolitical context.

The national cybersecurity strategy is part of the *National Strategic Review*, which sets France the goal of achieving world-class cyber resilience. It develops a structured approach based on five pillars to achieve this goal by 2030:

PILLAR 1 | MAKING FRANCE THE LARGEST POOL OF CYBER TALENT IN EUROPE

PILLAR 2 | STRENGTHENING THE NATION'S CYBER RESILIENCE

PILLAR 3 | HALTING THE EXPANSION OF CYBER THREATS

PILLAR 4 | MAINTAINING CONTROL OVER THE SECURITY OF OUR DIGITAL FOUNDATIONS

PILLAR 5 | SUPPORTING THE SECURITY AND STABILITY OF CYBERSPACE IN EUROPE AND INTERNATIONALLY

PILLAR 01

MAKING FRANCE A MAJOR POOL OF CYBER TALENT

France's ability to develop and attract talent in the field of cybersecurity is essential to achieving world-class cyber resilience. That is why this ambition is the priority focus of this strategy.

The digital sector in general, and cybersecurity in particular, are experiencing a global labour shortage. This phenomenon is exacerbated by a lack of career guidance for people from disadvantaged social backgrounds and women towards the IT sector, which has been growing rapidly and continuously for many years.

In response to this shortage, this pillar aims to invest heavily in guiding young people towards these professions from an early age and supporting training and attractiveness plans in this field. In close collaboration with the private sector, France will implement an ambitious human resources policy aimed at making France a major breeding ground for cyber talent.

OBJECTIVE 1
Develop an inclusive culture of cybersecurity from an early age

Young people are the future of the nation and therefore the foundation of the country's collective resilience. This objective therefore responds to a twofold challenge: to spread a culture of cybersecurity from an early age and to create a pool of talent for tomorrow.

Persistent prejudices – "a male-dominated, solitary, essentially technical profession accessible only to those with a high level of education" – are hindering the attractiveness of this promising field. France will therefore strive to take ambitious action to attract people to cybersecurity professions who currently face barriers to entering this field.

These efforts will be undertaken in the fields of education and culture. They will take the form of targeted support measures for studies and a specific mentoring programme for young girls, capitalising on the feedback from existing initiatives. France will also integrate cybersecurity into its civic engagement programmes for young people.

OBJECTIVE 2
Invest in all areas of cybersecurity training

To promote cybersecurity training and careers, France will create a national platform to guide people towards these careers by bringing together the efforts of public and private sector players.

In a constantly evolving field, France will also support the development of continuing education for cybersecurity professionals and retraining programmes for careers in cybersecurity. With this in mind, France will encourage French and European digital and cybersecurity sectors to develop their training offerings.

In addition, to reach all sectors of society, the development of self-training tools (MOOCs, etc.) on digital security issues will be promoted.

Finally, to ensure that cybersecurity remains central to the French and European scientific and technological landscape, France will implement "bridge strategies" between different cyber and non-cyber scientific and technological disciplines. These bridges will promote the cross-fertilisation of expertise, thereby strengthening the position of France and the European Union (EU) in this strategic field. Career paths within the public sector and between the public and private sectors will also be encouraged.

OBJECTIVE 3
Support the development of cyber human resources at European level

France will support the emergence of a common set of cybersecurity skills at European level to bolster European cybersecurity capabilities and promote collaboration between Member States.

To this end, it will encourage the creation of harmonised and recognised training courses in all EU countries, as well as the mobility of professionals within European institutions and between Member States.

PILLAR 02

STRENGTHENING THE NATION'S CYBER RESILIENCE

Since the *White Paper on Defence and National Security*, resilience has been defined as the willingness and ability of a country, society and public authorities to withstand the consequences of an attack or major disaster and then quickly restore their ability to function normally, or at least in a socially acceptable way. Russia's war of aggression in Ukraine demonstrates the vital need for a country to be collectively prepared for large-scale attacks, including in the field of cybersecurity. The nature of the cyberattacks likely to affect France in the coming years calls for the strengthening of the nation's cyber resilience.

Faced with a threat that now affects all sectors of the economy and society, France will roll out an ambitious plan to raise the overall level of cybersecurity across the entire economic and social fabric, including the state's IT infrastructure, and train the nation to respond to crises caused by cyberattacks. This plan will be based on enhanced synergy between the State, local authorities, businesses, research stakeholders and civil society.

OBJECTIVE 4
Prepare the nation for crises caused by cyberattacks

To achieve collective resilience, awareness of the threats and risks involved must be shared and maintained over time. To this end, France will step up its policy of prevention and awareness-raising on cybersecurity risks. This policy will be based in particular on a national digital risk prevention brand to promote awareness campaigns, modelled on road safety campaigns.

France will also strengthen its preparedness and response capacity in the face of multiple cyberattacks and the resulting systemic crisis. In particular, it will promote a culture of cyber crisis management that is accessible to all across all sections of the economy and society. A programme of crisis exercises will be developed to test the coordination and efficiency of all of France's response capabilities. This approach will be implemented at the territorial, sectoral, national, European and international levels. France will place capacity-building at the heart of its planning and investments, with the option of drawing on new public and private response capabilities.

OBJECTIVE 5
Raise the overall level of cyber protection for the nation

Raising the level of cyber protection will be based on a proportionate approach. The nation's most vital services and infrastructure, starting with those of the State and its critical operators, will continue to be brought up to a very high level of security, capable of withstanding the most sophisticated threats. This will involve consolidating the State's shared digital infrastructure and focusing significant cybersecurity efforts on it.

France will also deploy proportionate cybersecurity obligations across a wide range of entities, in line with the requirements of the European NIS2 Directive[1]. With this in mind, France will increasingly mobilise public and private representatives from regulated sectors to act as relays for this change of scale and support the entities subject to this regulation. It will also support cybersecurity support programmes for entities that are less mature in terms of cybersecurity.

Finally, this approach will be complemented by incentives for all other businesses, local authorities and associations, which will be encouraged to raise their security levels to a sufficient level to withstand less sophisticated attacks. A trust label will be implemented to enable these players to promote their security efforts to their partners, clients and investors.

OBJECTIVE 6
Facilitate the path to better cyber security

To make cybersecurity more accessible, France will implement a process to simplify the regulatory framework and support its harmonisation at European and international level.

In order to support a wide audience, a national portal for everyday cybersecurity will be created to provide various audiences, particularly citizens, with clear information, direct them to the resources available to them, and guide them in their cybersecurity efforts. France will also support the development of a range of cybersecurity services and products that are accessible and tailored to different stakeholders. It will promote this offering through the many sectoral and regional cybersecurity relays.

Finally, France will establish a smooth support process tailored to the status or nature of each victim, involving victim support actors at the national and regional levels, in particular sectoral and regional incident response centres. With this in mind, the 17Cyber platform will serve as a public service desk for individuals and entities that are victims of cyber malicious activity, beyond entities subject to specific cyber regulations, and will be directly integrated into the national portal.

[1] European Directive on the security of network and information systems.

PILLAR 03

HALTING THE EXPANSION OF CYBER THREATS

France is facing a growing threat of cyber attacks that is undermining its interests. On the one hand, it has seen the emergence, in sectors that had previously been spared, of increasingly intense methods of attack by perpetrators who no longer hesitate, often for criminal purposes, to paralyse critical national infrastructure, such as hospitals. On the other hand, it has observed an increase in the pressure and sophistication of espionage, destabilisation and sabotage operations targeting the nation's fundamental interests.

France is determined to halt the expansion of this cyber threat. It will mobilise all the levers at its disposal to significantly increase the financial, human and reputational cost for potential adversaries who could harm its economy, the stability of its democracy, or the security of property and people on its territory, and to discourage them from attacking France and its partners.

OBJECTIVE 7
Activate all levers to deter cyber attacks

France is determined to halt the growth of cyber threats. It will mobilise all the levers at its disposal – judicial, technical, diplomatic, military and economic – in a coordinated manner to increase the costs and risks for those who undermine its economy, its democratic institutions or the security of its citizens.

This approach includes better use of sanctions, the deterrent capacity offered by national cyber offensive capabilities in strict compliance with international law, intelligence gathering capabilities (including financial) and a stronger judicial response.

Under the aegis of the General Secretariat for Defence and National Security (SGDSN), the Cyber Crisis Coordination Centre (C4), composed of the National Information Systems Security Agency (ANSSI), the Cyber Defence Command (COMCYBER), the Directorate-General for Armament (DGA), the Directorate-General for External Security (DGSE), the Directorate-General for Internal Security (DGSI) and the Ministry for Europe and Foreign Affairs, currently plays a central role in responding to cyberattacks. By bringing together, beyond this circle alone, all the state actors capable of mobilising a response to a cyberattack, it will ensure a broader activation of the most relevant response measures and propose options to the political authorities – public attribution will be one of them.

Finally, France will strengthen coordination with its European partners and fully support the implementation of the European Union's cyber-diplomatic toolbox, in particular its sanctions regime.

OBJECTIVE 8
Mobilise private players in the cyber defence of the nation

The internet relies on private operators who, by virtue of their position, play a structuring role in global cybersecurity. In partnership with these actors, France will put in place a set of protective measures to detect and characterise attacks as early as possible, and potentially block them.

France will also deploy a cybersecurity filter for the general public, aimed at preventing access to malicious websites.

France will also strengthen the sharing of technical information on threats between government services and private actors. This networking will be based in particular on the development of InterCERT France, the leading community of incident response centres in France, in its coordinating role. France will also take action to strengthen this sharing at European and international level in order to amplify its effect.

PILLAR 04

MAINTAINING CONTROL OVER THE SECURITY OF OUR DIGITAL FOUNDATIONS

The functioning of the economy and society relies on a set of essential digital technologies, such as communication networks, operating systems, the cloud and software applications. These technologies are the target of cyberattacks and their vulnerability can have serious and lasting consequences for the nation's digital infrastructure.

France has set itself the clear ambition of controlling its technological dependencies and maintaining its autonomy of judgement and freedom of action in cyberspace. To this end, it will sustain and develop its mastery of critical cybersecurity technologies and autonomous assessment capabilities, and will support the consolidation of world-leading cyber industrial players at European level.

This effort will be based on continued government investment in innovation as part of the France 2030 plan, and on enhanced dialogue between stakeholders – research and innovation players, economic sectors, financing players and industrial public policy leaders – in order to mobilise all industrial policy levers and best direct financial investments.

OBJECTIVE 9
Invest in the security of digital technologies

France will support suppliers in implementing the European Cyber Resilience Act (CRA), which extends essential cybersecurity requirements to all digital products. To this end, it will strengthen its national policy for coordinated vulnerability management, in consultation with the relevant stakeholders, and will support best practices in software development and research into the security of open source products.

It will also invest in research into the risks and opportunities associated with disruptive technologies. For artificial intelligence, this action will be supported in particular by the National Institute for the Evaluation and Security of Artificial Intelligence (INESIA). At the same time, France will support a transition plan to post-quantum cryptography at national and European level.

In the field of cloud computing, it will support the public and private sectors in their migration, adopting an approach proportionate to the sensitivity of the data and IT systems concerned. It will continue to support the emergence of a trusted cloud offering and promote this proportionate approach at European level.

Digital identity, a major lever against mass cybercrime, will be given particular attention. France will encourage the provision of trusted identification methods for individuals and organisations, and their widespread use. It will also support the harmonisation of security requirements within the European digital identity portfolio.

Finally, it will establish conditions conducive to greater consideration of cybersecurity across all industrial sectors. This will involve, in particular, the integration of cybersecurity criteria into State aid schemes, such as France 2030, and enhanced dialogue with the National Industry Council on the integration of cybersecurity considerations into sector contracts at the appropriate level.

OBJECTIVE 10
Support the structuring of a European market for cybersecurity products and services

The European Union has adopted an ambitious strategy to strengthen its cybersecurity capabilities by harmonising standards and promoting cooperation between Member States.

In the favourable context of strong growth in the European internal market for security products and services, France will mobilise all industrial policy instruments to stimulate and support consolidation in the sector, proactively contributing to **European strategic autonomy in this area**.

France will thus support the emergence of leading European industrial cybersecurity capabilities, in particular by seeking synergies between the civil and military sectors. With the support of European funds and in partnership with the private sector, it will continue to invest in the sector and support the growth of world-class companies. In particular, it will encourage the development of investment funds with appropriate strategies and support the sector in its internationalisation.

This momentum will be supported by the deployment of the European certification framework for cybersecurity products and services, to which France will actively contribute.

OBJECTIVE 11
Control technological dependencies in the field of digital security

Encryption is an essential component of the security foundation that ensures the confidentiality and integrity of communications and data storage. France will invest heavily to maintain its mastery of critical technologies in the field of cryptography. It will also support work on data protection technologies throughout their life cycle.

In addition, France will continue to invest in order to acquire a wider range of products capable of countering the most advanced threats, particularly for sovereign uses. France will also offer top-level security solutions to its European partners and allies.

Finally, France will support the development of its security evaluation sector, which is internationally recognised for its excellence. It will also promote the emergence of an autonomous security evaluation capability within the European Union.

PILLAR 05

SUPPORTING THE SECURITY AND STABILITY OF CYBERSPACE IN EUROPE AND INTERNATIONALLY

A key factor in the resilience of nations and the stability of cyberspace, international cooperation today faces many challenges: growing conflict, including in the context of hybrid strategies[2], the questioning of multilateralism and UN mechanisms, the promotion of an authoritarian vision of digital technology, the proliferation of cyber-intrusive tools, technological breakthroughs facilitating access to offensive capabilities, and the increased role of non-state actors. In this context, France will seek to maximise the impact of its international action by relying on several fundamental principles:

Respect for democratic values, promotion of the rule of law and application of international law in cyberspace. Through these principles, it advocates for a free, open, secure and non-fragmented cyberspace. It contributes fully to the development of European strategic autonomy based on multi-sector cyber resilience (regulatory, industrial, judicial, diplomatic, military), in the service of Euro-Atlantic security and the European pillar of NATO.

Adaptive international governance, combining multilateral governance (international organisations and Member States) and multi-stakeholder governance (States, private sector, research, civil society), where the rights and responsibilities of each are clearly defined. France remains particularly attached to the multi-stakeholder nature of Internet governance.

The search for consensus. With its proactive and inclusive diplomacy (Paris Call, Pall Mall Process, UN reform), France rejects the logic of geopolitical blocs, which are sources of instability and fragmentation. It defends its freedom of action in cyberspace, based on defensive and offensive cyber capabilities, implemented alone or with its partners, in accordance with international law.

Strengthened by its adherence to these principles, France will work as a responsible, cooperative and supportive power for the security and stability of cyberspace.

OBJECTIVE 12

Promote an international framework and governance guaranteeing the security and stability of cyberspace

France will root its actions as broadly as possible within a multilateral framework in order to promote and support the implementation of a normative framework capable of guaranteeing the security and stability of cyberspace. In particular, it will continue to contribute to the reform of United Nations (UN) governance through the establishment of a Global

[2] These hybrid strategies are characterised in particular by the combination of cyber-attacks, information manipulation, the instrumentalisation of law (or "lawfare") and the economy, and the use of military operations. For France, a hybrid strategy refers to the use by a foreign actor of an integrated and deliberately ambiguous combination of military and non-military, direct and indirect, legal and illegal modes of action that are difficult to attribute. Playing with the estimated thresholds for retaliation and armed conflict, this combination is designed to constrain and weaken France and its partners.

Cybersecurity Mechanism by 2026, with the aim of operationalising the commitments made under the standards of responsible behaviour agreed by the UN in 2015. It will also continue to play an active role in implementing confidence-building measures governing how States conduct themselves in cyberspace, in both bilateral and multilateral frameworks, notably at the Organization for Security and Co-operation in Europe (OSCE).

France will also commit to involving the various stakeholders in this ambition. To this end, it will continue to lead the community that emerged from the Paris Call[3] and will support related international initiatives aimed at implementing the principles of this initiative. In this regard, France will continue its active involvement in the Pall Mall Process[4], which aims to combat the proliferation and irresponsible use of commercially available cyber intrusion capabilities.

Finally, France will continue to advocate for an effective system of judicial cooperation in criminal matters to combat cybercrime while respecting human rights and the sovereignty of States. To this end, it will ensure that the fundamental principles enshrined in the Council of Europe's Budapest Convention are preserved, particularly in the context of the implementation of the new United Nations Convention on Cybercrime.

OBJECTIVE 13
Act as an ally and cooperative and reliable partner within an international cyber community of interest

France's capacity for action and resilience in cyberspace is primarily based on a partnership approach. With its robust and unique national model, France intends to act as a reliable partner at several levels.

At the European level, France regards the EU as an essential and preferred political organisation for safeguarding its capacity for initiative and action in cyberspace. France will seek to strengthen the European Union's strategic autonomy in the areas of cybersecurity and cyber defence. It will be fully involved in European cooperation forums and crisis management

[3]Launched on 12 November 2018 by the Chairman of the French Republic, the Paris Call brings together more than 1,200 stakeholders around nine founding principles to promote an open, secure, stable, accessible and peaceful cyberspace. In particular, the Paris Call has played a pioneering role in developing regulations around the security of digital products and the phenomenon of "cyber mercenaries".

[4] The result of a Franco-British initiative at the bilateral summit on 10 March 2023, the Pall Mall Process was officially launched at a conference co-organised by France and the United Kingdom at Lancaster House in London on 6 and 7 February 2024. It aims to produce concrete recommendations for governments and industry. In April 2025, a code of best practices for governments aimed at combating the proliferation and irresponsible use of commercial cyber intrusion capabilities was adopted in Paris. In August 2025, it had the support of 27 governments.

mechanisms (CSIRT Network[5], CyCLONe[6], CYBERCO[7], MICNET[8]). In particular, it will encourage the sharing of information on threats, with the aim of achieving greater autonomy for Europeans in this area.

Within NATO, France will continue to promote the integration of cyber defence into the Alliance's missions and operations, as well as the strengthening of the organisation's cybersecurity, while ensuring complementarity with EU actions.

Beyond these frameworks, France will develop cooperation with partners who share common interests and an equivalent level of maturity in cyber defence, focusing on sharing expertise and mutually reinforcing capabilities.

In these three areas of action, France will mobilise its partnerships to improve threat awareness, prevention, protection, response to attacks and the conduct of military operations. It will also strengthen its capacity to implement joint cyber response strategies at European and international level.

OBJECTIVE 14
Develop cyber solidarity capabilities

Strengthening our national resilience requires efforts to build resilience capabilities on a global scale.

In coordination with its partners and allies, France will contribute to raising the level of cybersecurity internationally by developing targeted assistance capabilities for its most vulnerable partners, in accordance with the guidelines of the Accra Call[9].

[5] Established in 2017 by the NIS Directive, the CSIRT Network brings together the incident response teams of each EU Member State and the cybersecurity service for the Union's institutions, bodies and agencies (CERT-EU). The aim of the network is to promote information exchange between its members in order to improve the handling of cyber attacks.

[6] Created on the initiative of France in 2020 and institutionalised by the NIS2 Directive, the CyCLONe (Cyber crisis liaison organisation network) brings together the agencies responsible for cybersecurity crisis management in the 27 EU Member States. Its objective is twofold: to enable the sharing of information on national response strategies in the event of a cyber crisis and to coordinate the development of a consolidated analysis of the crisis for the benefit of policy makers at both national and European level.

[7] The Conference of European Cyber Commanders (CYBERCO) was created in 2022 on France's initiative. It brings together all the highest military cyber defence authorities of the EU Member States twice a year, under the leadership of the President of the Council of the European Union. The aim of the network is to build trust, exchange information on cyber threats and discuss operational cyber defence issues facing nations.

[8] The MICNET (Military Computer Emergency Response Team Operational Network) is the military counterpart of the European CSIRT network. It was created in November 2022 by 18 EU Member States, including France. It is a military cooperation initiative that aims to provide an emergency response to cyberattacks at the level of defence ministers.

[9] This Call inspired by the format of the Paris Call brings together states, international organisations, businesses and civil society organisations to strengthen international cyber capabilities. France has supported it since its adoption at the Global Conference on Cyber Capacity Building on 29 and 30 November 2023.

With this in mind, France will take action in two areas:

- **It will carry out structural cooperation (capacity building) activities**, with the aim of having a long-term impact on its partners' cybersecurity capabilities by helping them to build their capacity, in particular through advice, training and logistical support. With this in mind, France will continue its efforts to develop regional capacity-building centres and its involvement in European projects. Cybersecurity support for Ukraine will continue within the framework of the Tallinn Mechanism. Coordination and synergy with the work of state operators in the field of international technical cooperation (Expertise France, Civipol) will be sought.
- **It will also carry out operational cooperation activities** aimed at supporting a partner through specific operations, either preventively (IT system audits) or reactively (incident response). The use of the private sector for assistance will also be encouraged. France will thus support the operationalisation of the EU Cyber Reserve[10] and its extension to the European Political Community. On the military front, France will develop long-term partnerships, known as Tailored Cyber Partnerships (TCPs), which will support the armed forces of partner countries in developing their cyber defence capabilities and responding to incidents.

[10] Operational by 2026, the EU Cybersecurity Reserve will consist of incident response services provided by trusted private service providers, which can be deployed to help deal with cybersecurity incidents faced by EU Member States, EU institutions, bodies and agencies and, where appropriate, third countries associated with the Digital Europe Programme.

MULTI-STAKEHOLDER GOVERNANCE IN THE SERVICE OF NATIONAL RESILIENCE

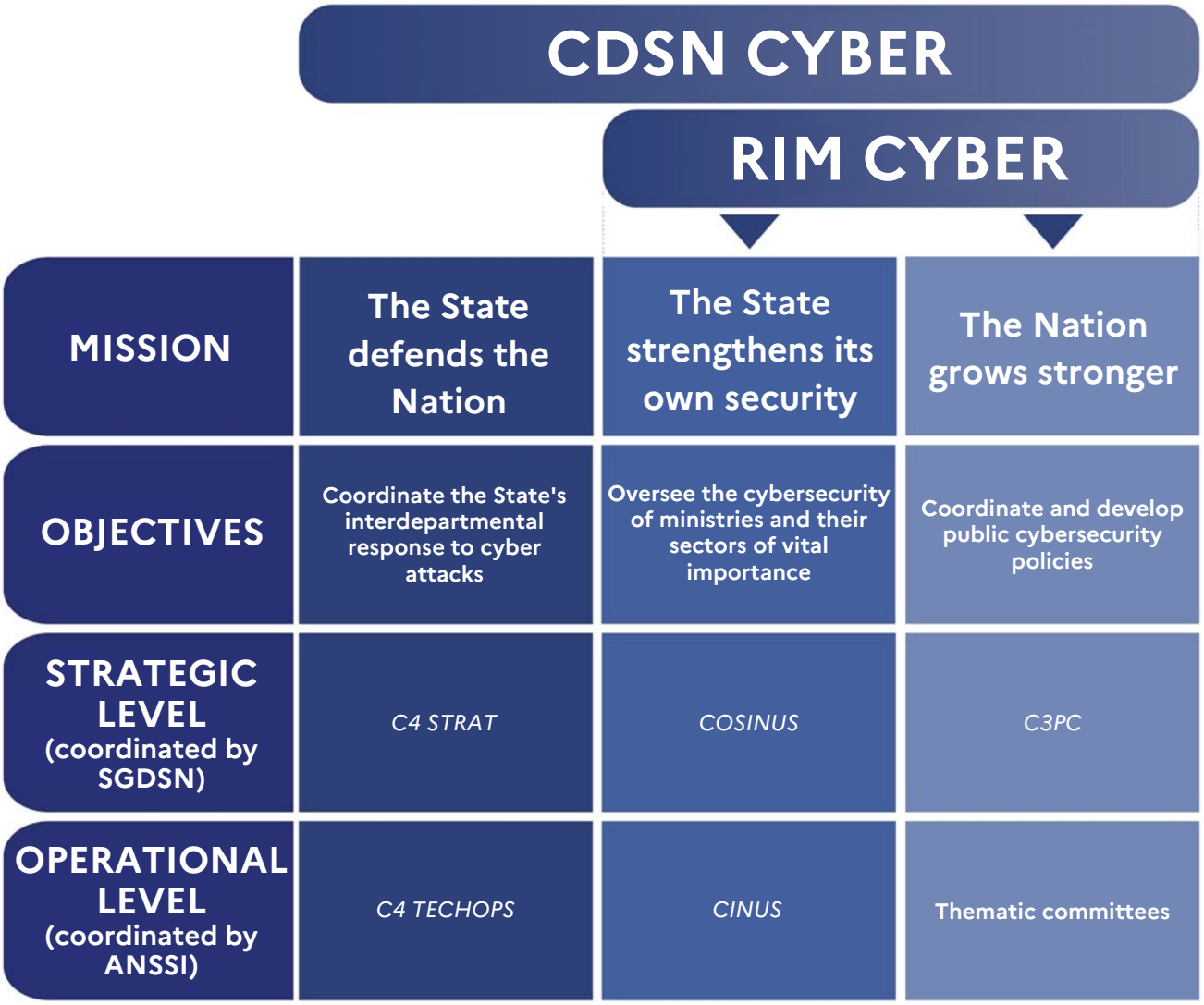
The cybersecurity organisational model adopted by France guarantees respect for civil liberties and separates defensive and offensive missions and capabilities. However, the governance system in place ensures effective coordination between these areas, guaranteeing the effectiveness of France's cyber defence.

On the defensive side, this governance is based on three missions, each involving different stakeholders:

- "The State defends the Nation": this mission aims to understand the threat and develop France's response to cyberattacks;
- "The State secures itself": this mission ensures the security of the State's IT systems and its most critical operators;
- "The Nation strengthens itself": this mission coordinates public action and private efforts to strengthen the cybersecurity of individuals, businesses, associations and local authorities.

Cyber threats now affect all areas of society, the economy and the national territory. Professional sectors, local government (local authorities, decentralised government departments, etc.), academia and civil society are now both victims of cyber attacks and essential partners in developing and implementing the response to this threat. This is why France will strengthen the integration of all these stakeholders in national cybersecurity governance, both at the national level and in its regional implementation.

France's cyber governance framework[11]



[11] *CDSN: Conseil de défense et de sécurité nationale (National Defence and Security Council)*
RIM: réunion interministérielle (interministerial meeting)
C4 STRAT: Centre de coordination des crises cyber de niveau stratégique (Strategic-level cyber crisis coordination centre)
C4 TECHOPS: Centre de coordination des crises cyber de niveau technico-opérationnel (Technical-operational-level cyber crisis coordination centre)
COSINUS: Comité stratégique interministériel de la sécurité numérique (Interministerial strategic committee for digital security)
CINUS: Comité interministériel de suivi de la sécurité numérique (Interministerial committee for monitoring digital security)
C3PC: Comité de pilotage des politiques publiques cyber (Steering committee for public cyber policies)

PREMIER
MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général
de la défense
et de la sécurité nationale

51, boulevard de La Tour-Maubourg - 75007 Paris
N 48°51'23,5" E 2°18'43,2'"
www.sgdsn.gouv.fr