NATIONAL CYBERSECURITY STRATEGY

2019

GOBIERNO DE ESPAÑA
PRESIDENCIA DEL GOBIERNO

Catálogo de publicaciones de la Administración General del Estado
htttp://publicacionesoficiales.boe.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES E IGUALDAD

NIPO (printed edition): 042-19-028-9
NIPO (online edition): 042-19-0129-4
Depósito Legal: M-16844-2019
Edition date: June 2019
Printer: GRAFOX IMPRENTA, S.L.

NATIONAL CYBERSECURITY STRATEGY

2019

National Cybersecurity Strategy 2019 has been approved by the National Security Council.

The following bodies participated in the process: The Ministry of Foreign Affairs, European Union and Cooperation; the Ministry of Justice; the Ministry of Defence; the Ministry of the Treasury; the Ministry of Home Affairs; the Ministry of Public Works; the Ministry of Education and Vocational Training; the Ministry of Industry, Trade and Tourism; the Ministry of the Presidency, Parliamentary Relations and Equality; the Ministry of Territorial Policy and Public Function; the Ministry of the Economy and Business; the Ministry of Health, Consumption and Social Well-being; the Ministry of Science, Innovation and Universities; the National Intelligence Centre; the National Security Department and a Committee of Experts from professional associations, companies and the academia.

DSN

The fourth industrial revolution—the digital revolution—has, for years, coexisted with times of economic crises and social and political after-effects from which we are still recovering. Therefore, despite the undeniable opportunities and advances the digital world has to offer, many of our citizens are apprehensive and uncertain about all things related to the digital technological disruption. And it is here, in the fight to change that perception, that we in the public administrations must focus our priority efforts. What is at stake is society's trust in democratic institutions and in our own capacity to face the future in the certainty that we are making progress.

In the midst of an era of transformations and of uncertainties, we must offer a solid moral and material horizon, and to this end, it is increasingly essential to have cybersecurity that is equipped for the new times and the new threats. Cybersecurity that is capable of addressing the different challenges, and of doing so with public-private cooperation and with the support of a citizenry that is aware of the changing reality and committed to the solutions to these challenges.

This National Cybersecurity Strategy, in line with the 2017 National Security Strategy, seeks to contribute to this. And it seeks to do so with a clear goal as its guide: ensuring that these times of changes are not a source of cultural discontent and of economic and labour regression, but, rather, an opportunity to increase Spain's competitiveness and the well-being of Spaniards, as well as that of our European partners. This work has also taken into account our current geopolitical situation, which makes it more urgent and necessary to build and strengthen the European Union's strategic autonomy.

In all of this, Spain has a lot to say and to contribute. After all, ours is one of the most interconnected countries in the world. It only takes a glance at the daily news to realize how common and how dangerous the cyber threats we are facing really are. From fake news on social networks, to cyber espionage or the funding of terrorism—the digital realm is increasingly influencing and shaping reality. Moreover, other new technologies, such as artificial intelligence, robotics, big and smart data, and blockchain are already part of the daily activity of citizens, companies and public administrations. These new technologies have paved the way for ground-breaking instruments to obtain information, generate knowledge, and share data.

This influence will grow even further with the current implementation of what is known as 5G for the new connectivity of the internet of things. Being more interconnected and more dependent on said infrastructures will allow us to advance in many important fields, from achieving the United Nations Sustainable Development Goals, to combating the effects of climate change.

But it also makes us more vulnerable to hostile actions against—and coming from—said new infrastructures. Threats are becoming increasingly sophisticated and complex, and cyberspace is a weakly regulated area with no clear borders or jurisdictional demarcations, where the traceability of criminal actions, and the identification of state or non-state perpetrators, is difficult.

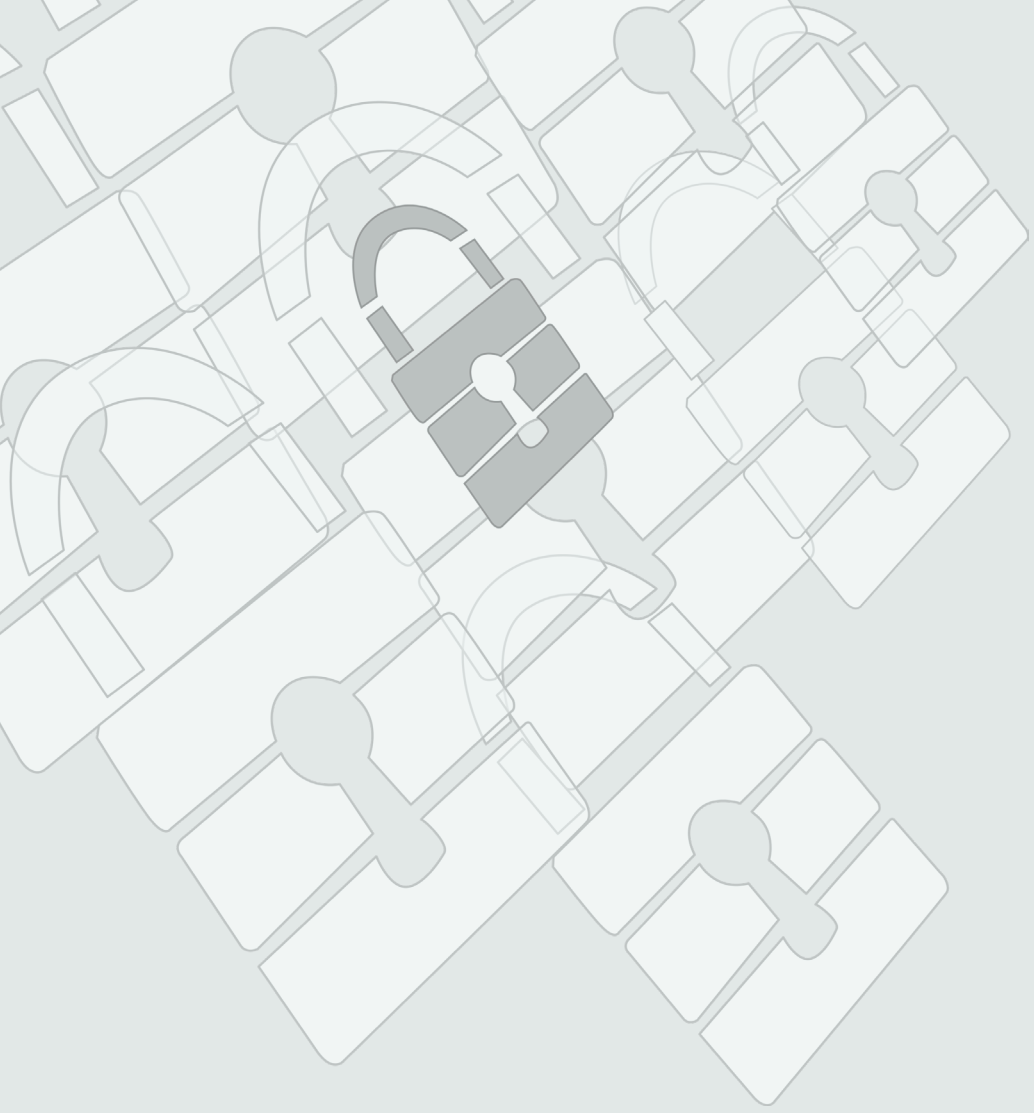
The challenge is enormous and multidisciplinary. Our professionals in the diverse areas involved in cybersecurity have well-deserved prestige and will be able to rise to the challenge. But cybersecurity requires commitment from us all. It is our responsibility, at the public administrations, to lead this commitment and to offer a framework of certainty to companies and citizens, who must also share this commitment. Once again, this is not only to avert the dangers and threats, but to make the most of the many opportunities to the benefit of all.

Cybersecurity protects assets, but it also protects essential values for a free society such as ours. We are not going to relinquish these principles in this era of global transformation. The technical challenges involved in cybersecurity are varied and complex, but something else is at stake. Something that refers to moral and cultural values related to our way of seeing and understanding the world, to what best defines us. Our freedom, well-being and democracy ultimately depend upon our success in designing an effective Cybersecurity Strategy. I am convinced that, with this document, we have taken a key step towards successfully addressing uncertain, but at the same time fascinating, years.

Pedro Sánchez Castejón

President of the Government of Spain

SUMMAY



Executive Summary

Executive Summary

The National Cybersecurity Strategy works with forecasts from the 2017 National Security Strategy in the cybersecurity field, considering general goals, the field's specific goal and lines of action laid down to achieve them.

The document is divided into five chapters. The first, entitled "Cyberspace, beyond a common global space", provides an overall understanding of the cybersecurity field, progress made in it since approving the Strategy in 2013, reasons behind drawing up the 2019 National Cybersecurity Strategy, plus the main features of its development.

Activities in cyberspace are fundamental for current society. Cyberspace technology and infrastructures are strategic elements, running across all fields of activity, making cyberspace vulnerability a major risk for our development as a nation.

For this reason, cyberspace security is a priority goal on government agendas to guarantee National Security and a State competence to create a trust-based digital society.

Helping promote secure and reliable cyberspace, from a multidisciplinary focus, moving beyond purely technical aspects, is a task that should stem from knowing about and understanding any threats we might face, including new and emerging threats.

The **second chapter**, entitled "Threats and challenges in cyberspace" determines the main threats to cyberspace stemming from its definition as a common global space, highly technified and widely connected, that amplifies the impact of any attack. It classifies these threats and challenges in two categories: on the one hand, threats to cyberspace assets; and on the other, threats that use cyberspace to carry out all types of malicious and illicit activities.

The **third chapter**, entitled "Proposal, principles and goals for cybersecurity" applies the governing principles of the 2017 National Security Strategy (Action unit, Anticipation, Efficiency and Resilience) to five specific goals. Its development is mentioned in the **fourth chapter,** entitled "Lines of action and measures", setting seven lines of action and identifying measures to develop each one.

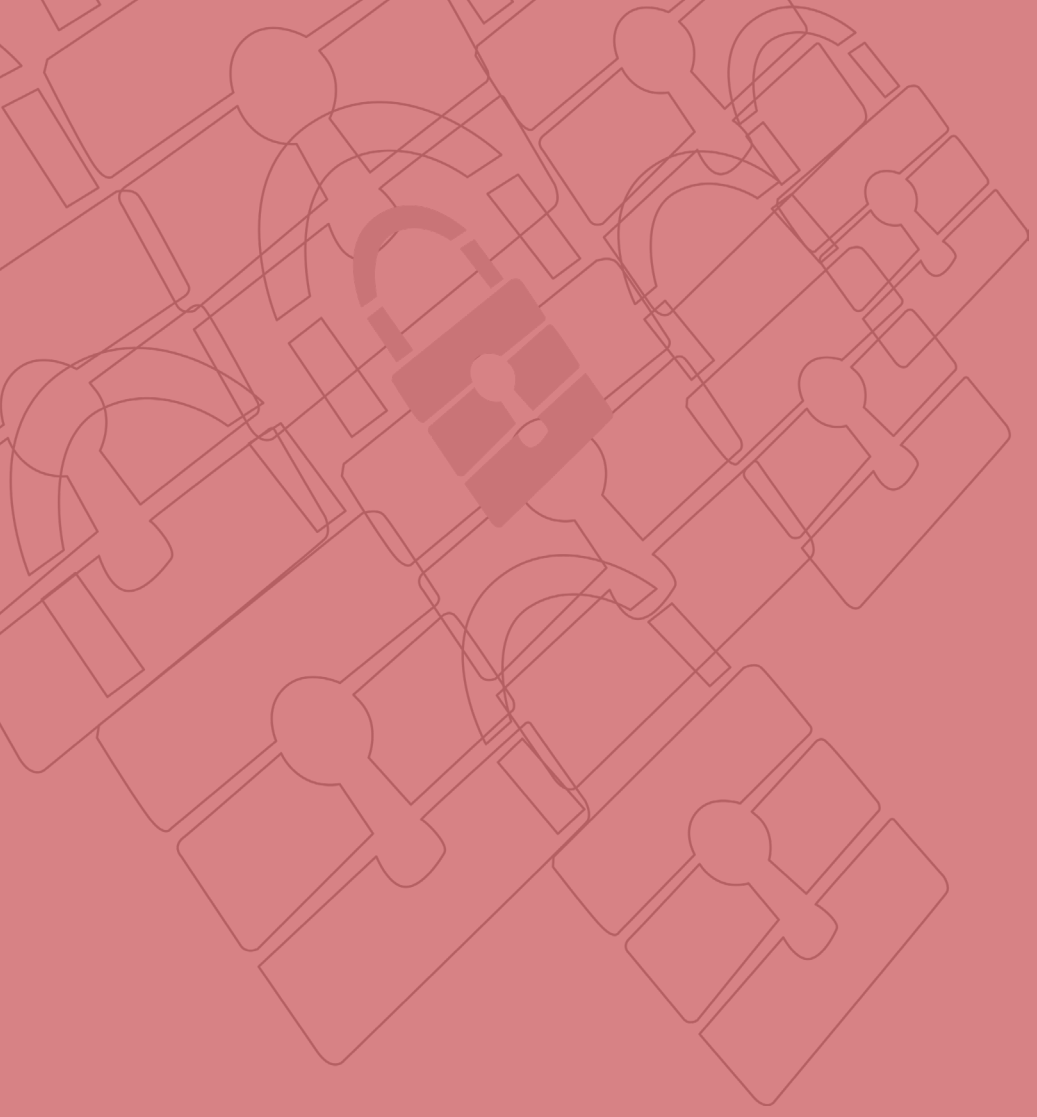
These lines of action aim to: strengthen skills to fight threats from cyberspace; guarantee strategic asset security and resilience for Spain; boost cybersecurity for citizens and companies; strengthen skills to investigate and prosecute cybercrimes, guarantee citizen security and protect rights and freedoms in cyberspace; boost cybersecurity for citizens and companies; bolster the Spanish cybersecurity industry and encourage and retain talent, strengthen digital autonomy; contribute to international cyberspace security, promoting open, plural, secure and reliable cyberspace supporting national interests and developing a cybersecurity culture to contribute to the Comprehensive National Security Culture Plan.

The **fifth chapter,** entitled "Cybersecurity in the National Security System" defines cybersecurity's organic architecture. Led by Spain's Prime Minister, the structure is divided into three authorities: the **National Security Council,** as the Government's Delegate Commission for National Security; the **National Cybersecurity Council,** that supports the National Security Council and helps the Prime Minister manage and coordinate National Security policy on cybersecurity, and promotes coordination, collaboration and cooperation among Public Administrations and between these and

the private sector, and the **Specialised Situation Committee** that, with support from the National Security Department, will support crisis situation management in any field that, because it crosses disciplines or due to its sheer size, might overwhelm the response capabilities of the usual mechanisms.

This system is completed by the **Standing Committee on Cybersecurity,** that eases inter-ministerial coordination at an operational level in the field of cybersecurity, as the authority assisting the National Cybersecurity Council on aspects relating to technical and operational evaluation of risks and threats to cybersecurity; the competent public authorities and the national CSIRT (Computer Security Incident Response Team) and it includes setting up a new public-private joint-project, the **National Cybersecurity Forum**.

In addition, this last chapter makes some final conclusions and outlines mechanisms to update and assess the Strategy.



Introduction

Introduction

The 2019 National Cybersecurity Strategy establishes Spain's position in the light of a new understanding of cybersecurity within the framework of the National Security Policy.

Spain's first National Cybersecurity Strategy was approved in 2013. The document set directives and general lines of action to tackle the challenge that cyberspace vulnerability represented for the country. Furthermore, the strategy designed the governance model for national cybersecurity. In the intervening period, Spain has also continued moving forward in a bid to contribute to secure, reliable cyberspace.

One of its mainstays, dating back to 2014, is the National Cybersecurity Council, an authority supporting the National Security Council. Since its first meeting, the National Cybersecurity Council has assumed the task of coordinating nationally-competent organisations plus developing the National Cybersecurity Plan and its

offshoots. Consequently, Spain today can boast specialist cybersecurity organisations and an outstanding position not only in Europe but throughout the world.

The legal framework has also been considerably adapted. To keep on top of its evolution and use experience accumulated over these last few years, the National Security Framework modification was published in 2015 to guarantee security for Public Sector systems. On the other hand, bringing into force the Royal Decree-law 12/2018 of 7 September, on information network and system security, that transposes Directive (EU) 2016/1148 (known as the NIS Directive) to Spanish legal order, represented an important milestone in our country's cybersecurity improvements, extending the scope of this Directive in an attempt to improve cybersecurity among all strategic sectors.

Law 36/2015, of 28 September, on National Security was extended to boost a project representing one of the government's greatest responsibilities, National Security. The National Security Law considers cybersecurity as a special interest field.

Without the shadow of a doubt, cybersecurity has modernised National Security, as this field has made the greatest progress to date. This dynamic should stay on the same track.

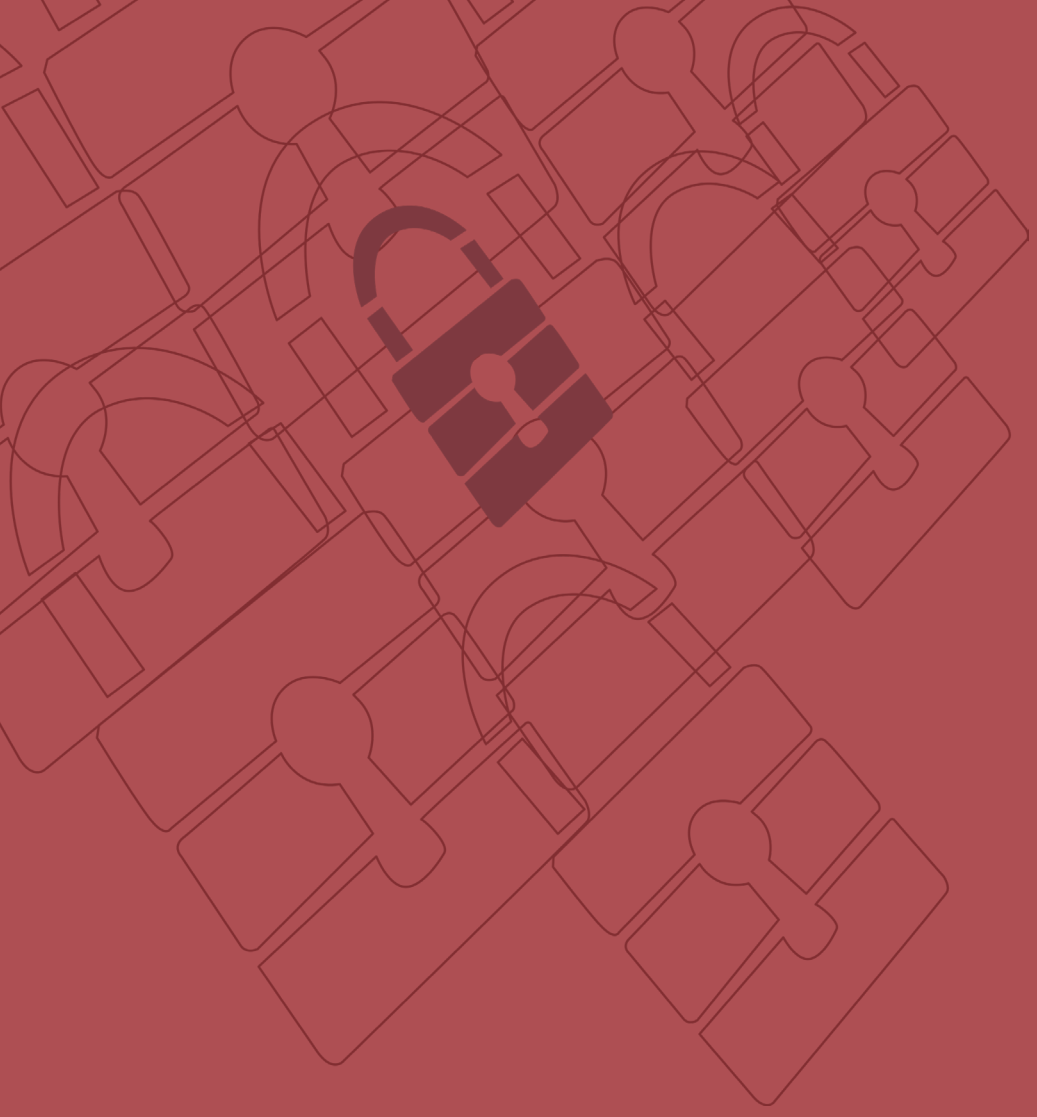
The 2017 National Security Strategy was a turning point in national strategic thinking, giving cybersecurity its own differential space.

One of the global trends identified in the Strategy, digitalisation, is shown to drive change with implications for security. The Strategy sets a new framework, with five general goals running across all fields. Crisis management, National Security Culture, global common spaces, technological development and international projection for Spain shape a strategic grid where cybersecurity is used to open up new paths leading to Spain's present and future security model.

New cybersecurity spreads beyond the mere sphere of protecting technological patrimony and delves into political, economic and social fields.

In addition to actions that affect digital systems, cyberspace should be considered as a strategic communication vector that can be used to influence public opinion and how people think by manipulating information, disinformation campaigns or hybrid actions. Its potential application in a very wide range of situations, including electoral processes, makes it extremely complex.

This renewed outlook in a field that is understood to have spread functionally, and where public-private collaboration is key, calls for a new approach in the form of a new national cybersecurity strategy.



Chapter 1

Cyberspace: beyond a global common space

Cyberspace: beyond a global common space

This chapter presents the opportunities and challenges of cyberspace and digital infrastructure, outlines the inherently international aspect of its security approach and describes the broad strokes of Spain's new understanding of cyberspace.

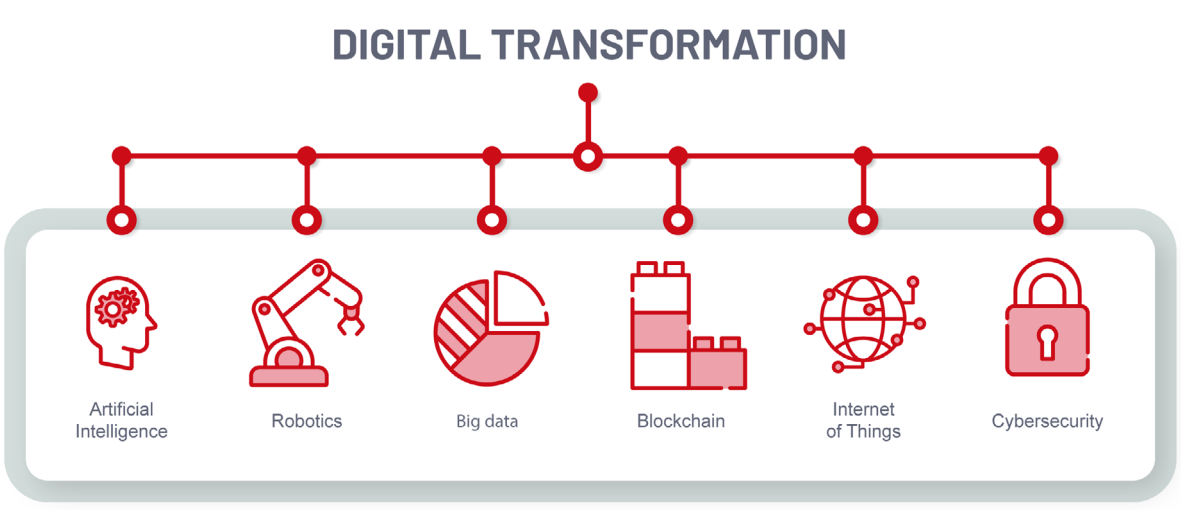
Cyberspace: opportunities and challenges

Cyberspace is a global common space characterised by its functionality and dynamism. Lack of sovereignty, its weak jurisdiction, ease of access and difficulty to attribute actions within it define a scenario with a wide range of future opportunities while also posing some serious

security challenges.

On the one hand, cyberspace makes universal connectivity possible and eases free flow of information, services and ideas. It is thereby a field that stimulates entrepreneurship, strengthens socio-economic progress and creates new opportunities every day in all business sectors. The change caused by digital transformation of production processes is demonstrated globally at an unprecedented rate. Artificial intelligence, robotics, big data, blockchain and the Internet of Things are already with us, although the real transforming power is still to be unleashed. Its implications go beyond technology, extending to new social models and delving into personal relations and ethics.

On the other hand, digitalisation transforms security and lays down some serious challenges. Cyberspace is structured as a battleground where information and data privacy are high-value assets in an environment with greater geopolitical competition, reorganisation of power and individual empowerment. Consequently, booming connectivity and greater dependence on networks and systems, not to mention digital components, objects and devices, create vulnerabilities and make it hard to protect information properly.



Digital infrastructure

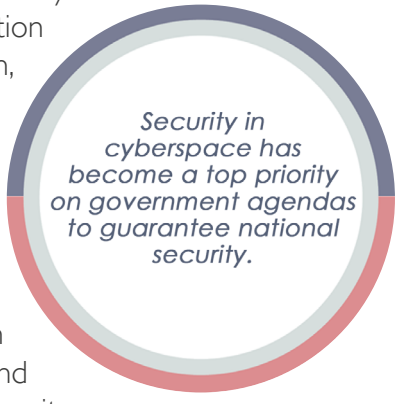
Cyberspace is not only virtual, but also sustained by physical and logical elements. Devices, components and systems within information and communication networks and systems can be exposed to malfunctions that stop them working correctly and deliberate actions with malicious intentions that jeopardise correct operation of critical infrastructures and essential services that depend on the associated digital systems and networks.

This risk is amplified by the importance of commercial criteria over security criteria in hardware and software product design, not to mention systems and services, which complicate certification processes and might compromise the supply chain.

All these aspects, along with mounting interconnectivity between systems, can bring about cascade effects with unpredictable results.

International plan: security in cyberspace

Security in cyberspace has become a top priority on government agendas to guarantee national security and create a trust-based digital society. In this context, Spain defends it outlook and interests as a nation and works with the international community by backing open, plural and secure cyberspace.

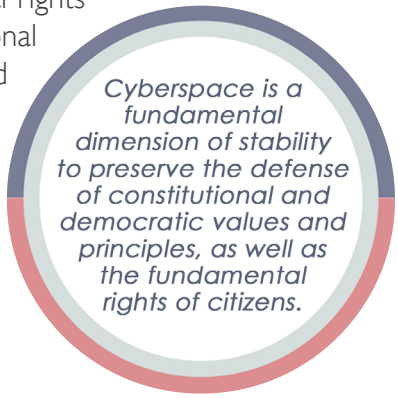


Spain maintains its active role in all institutions where cybersecurity takes centre-stage, particularly within the European Union, the Atlantic Alliance and the United Nations, thereby proving its commitment to partners and allies. Ties are also maintained with third-party States through bilateral cooperation mechanisms that ease understanding and mutual trust based on fluid relationships in the field of cybersecurity, in an attempt to build on our skills.

Aware of the importance of a multilateral approach, in addition to International Law and non-binding standards for responsible behaviour among States, we might highlight the role of the United Nations Charter as the reference principle for conflict prevention, cooperation and stability in cyberspace. Forging agreements and trust-building measures are the basis for its application and implementation, as well as International Treaties and Agreements that Spain has joined.

A new conception of cyberspace

A fundamental dimension of stability involves continued defence of constitutional and democratic values and principles plus citizens' fundamental rights in cyberspace, particularly in terms of protecting their personal data, privacy, freedom of expression and access to truthful, good quality information.



Good understanding of this approach requires a multidisciplinary focus, moving beyond purely technical aspects, using centralised management principles and coordinating its performance, assigning cybersecurity to National Security as a State competence.

Firstly, the private sector plays a relevant role as administrator and owner of Spain's digital assets, meaning that the country's cybersecurity skills largely lie in its companies. This thereby means that cybersecurity needs support, promotion and investment to become more competitive and boost economic growth, whilst providing a secure and reliable digital environment.

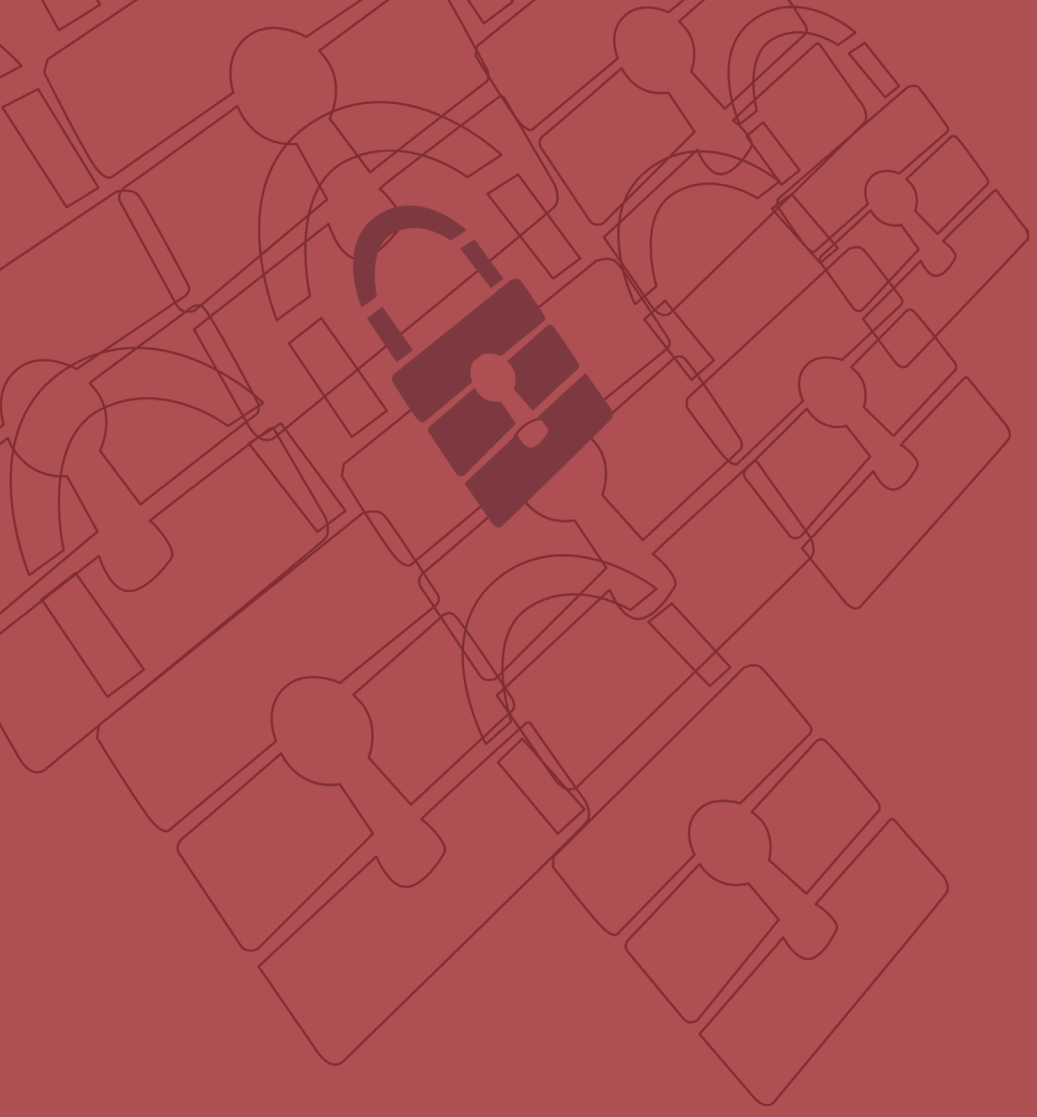
On the other hand, we should aspire to increasing technological autonomy by encouraging a national industrial base for cybersecurity, R+D+i and technological talent management. Human resources remain a critical factor. A gaping chasm has opened up between the number of highly specialised jobs in information technologies,

particularly cybersecurity, and availability of workers with the required level of knowledge or training.

Secondly, transition from a preventive and defensive cybersecurity model to a more dissuasive framework falls into line with a global context demonstrating greater geopolitical competence. Use of cyberspace as a field of confrontation, independently or as part of a hybrid action, is widely recognised. Dissuasion in cybersecurity requires obtaining and strengthening cyberdefence skills, as a fundamental element of the State's action.

Thirdly, fast evolving cyberthreats require a more proactive approach from cyberintelligence. Its integration in the overall cybersecurity framework is key to provide knowledge of the situation and the necessary early warning that can anticipate actions from potential opponents through knowledge of their skills, techniques, tactics and intentions. In addition, it is necessary to encourage the use of mechanisms and means that allow appropriate investigation and prosecution of perpetrators to increase possibilities of attribution.

All the above can be added to the need for greater implication from all society by encouraging a cybersecurity culture, to evolve from awareness of the commitment, in the understanding that citizens have joint-responsibility for national cybersecurity.



Chapter 2

Threats and challenges in cyberspace

Threats and challenges in cyberspace

This chapter examines the main threats and challenges that Spain faces in cyberspace.

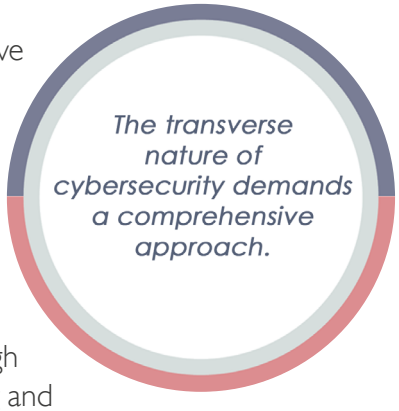
Promoting a secure, reliable environment is a task that should work from knowledge and understanding of the challenges and threats, including new and emerging aspects, that affect cyberspace. The 2017 National Security Strategy differentiates between cyberthreats and actions that use cyberspace as a medium for malicious or illicit activities.

Cyberthreats

Cyberthreats are malicious disruptions or manipulations that affect technological elements. They encompass a wide range of actions. Cyberthreats are characterised by their diversity in terms of both capacity and motivation. They affect practically all fields of National Security, such as National Defence, economic

security or protection of critical infrastructures, among others, and they do not respect borders.

This transverse nature means that cybersecurity covers a comprehensive perspective that includes Public Administrations, the public and private sector and society as a whole, so there might be simultaneous implications on a wide range of aspects such as sovereignty, fundamental rights, defence, the economy and technological development.



In this scenario, defences can evolve continually to adapt to a dominating threat that is multiplied by the pull effect caused by its high degree of impunity. At the same time, the defence ground is expanding and becoming more complicated every day.

In this respect, providing security in information networks and systems requires improving prevention, detection and response measures, encouraging security through design and by default. It should be incorporated both into developing technological products and services and their updates or how they are used.

Actions that use cyberspace for malicious purposes

Digital technologies open up new activities and ways of doing business that have to be duly regulated as they might affect stability and our rights and freedoms, presenting substantial threats and challenges for National Security. In the same way, the same qualities that help cyberspace drive progress can be exploited for harmful purposes when combined with how exceptionally easy it is to remain anonymous, steal identities and amplify effects.

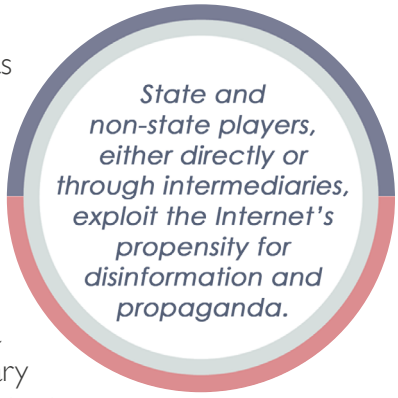
Thanks to the Internet revolution, States, organised groups, collectives and even isolated individuals can attain a so-far unprecedented level of power and capability to influence. Digital connectivity means that

global social movements take on strategic importance that has been underestimated until now.

The actions that cyberspace uses to carry out malicious or illicit activities include cyberespionage and cybercrime.

Cyberespionage is a relatively cheap, fast method with fewer risks than traditional espionage, given the difficulty of attributing authorship. The greatest capabilities are mainly held by State players (intelligence or military organisations), that fundamentally operate via what are known as Advanced Persistent Threats (APT). This type of threat means that the opponent has sophisticated knowledge levels plus resources and infrastructures so that, by deploying multiple types of attacks, they can interact on their targets over a long period of time, adapt to defence strategies, and maintain the interaction level to meet its end.

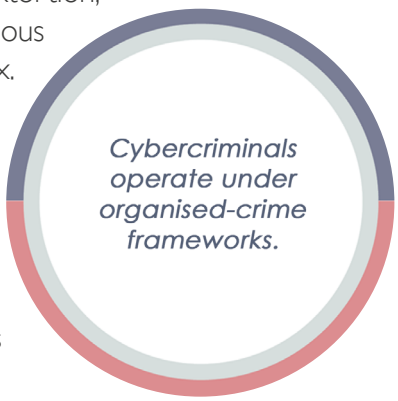
In addition, a growing trend is now seen in what are known as hybrid threats, coordinated and synchronised actions aiming to deliberately attack systemic vulnerabilities in democratic states and institutions, through a wide range of media, such as traditional military actions, cyberattacks, information manipulation operations or elements of economic pressure. State and non-state players, either directly or through intermediaries, exploit the Internet's propensity for disinformation and propaganda and a generalised interest in obtaining and developing military capabilities to operate in cyberspace, including offensive capacities in many cases.



Cybercrime, in turn, is a top-level citizen security issue, representing one of the widest-spread and generalised threats, continuously arising and increasingly victimising thousands of institutions, companies and citizens. The term Cybercrime refers to illicit activities in cyberspace, targeting elements, computer systems or any other legal property, whenever its planning, development and performance is determined by use of technological tools; depending on the nature of the actual punishable act, authorship,

motivation, or damage inflicted, this might refer to cyberterrorism, cybercrimes or, when appropriate, hacktivism.

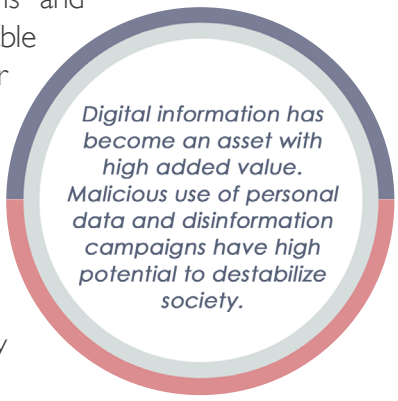
Use of new financial and economic transaction methods, such as cryptocurrency, for illicit trafficking and trading of goods and providing services or extortion, fraud and forgery of non-monetary means of payment, poses a serious security challenge because they are both sophisticated and complex. They can be used for money laundering and tax evasion and they represent a source of income for organised crime; therefore, they facilitate other activities such as financing terrorism, making the most of how difficult it is to monitor these new techniques.



Cybercriminals operate under organised-crime frameworks and incessantly explore techniques for building low-risk lucrative business models, sheltered by the fact their actions are difficult to trace.

Terrorist groups attempt to make the most of cyberspace vulnerabilities to launch cyberattacks or activities to radicalise individuals and collectives, for financing, disseminating techniques and tools to commit a terrorist attack, and for recruitment, training or propaganda. Intimately linked to this, there is the threat against critical infrastructures, with the clear chance of using networks to bring about a collapse as essential services fall like dominoes.

Hacktivist groups carry out cyberattacks for ideological reasons and sometimes, making the most of products, services and tools available in cyberspace, they seek to develop attacks with a major media or social impact.

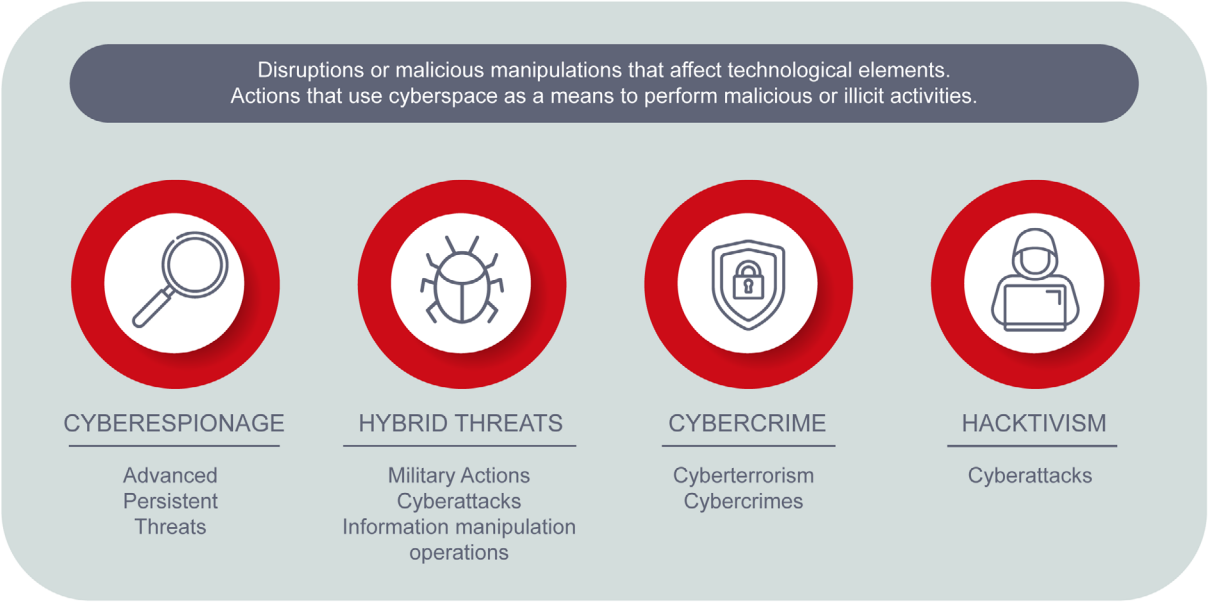


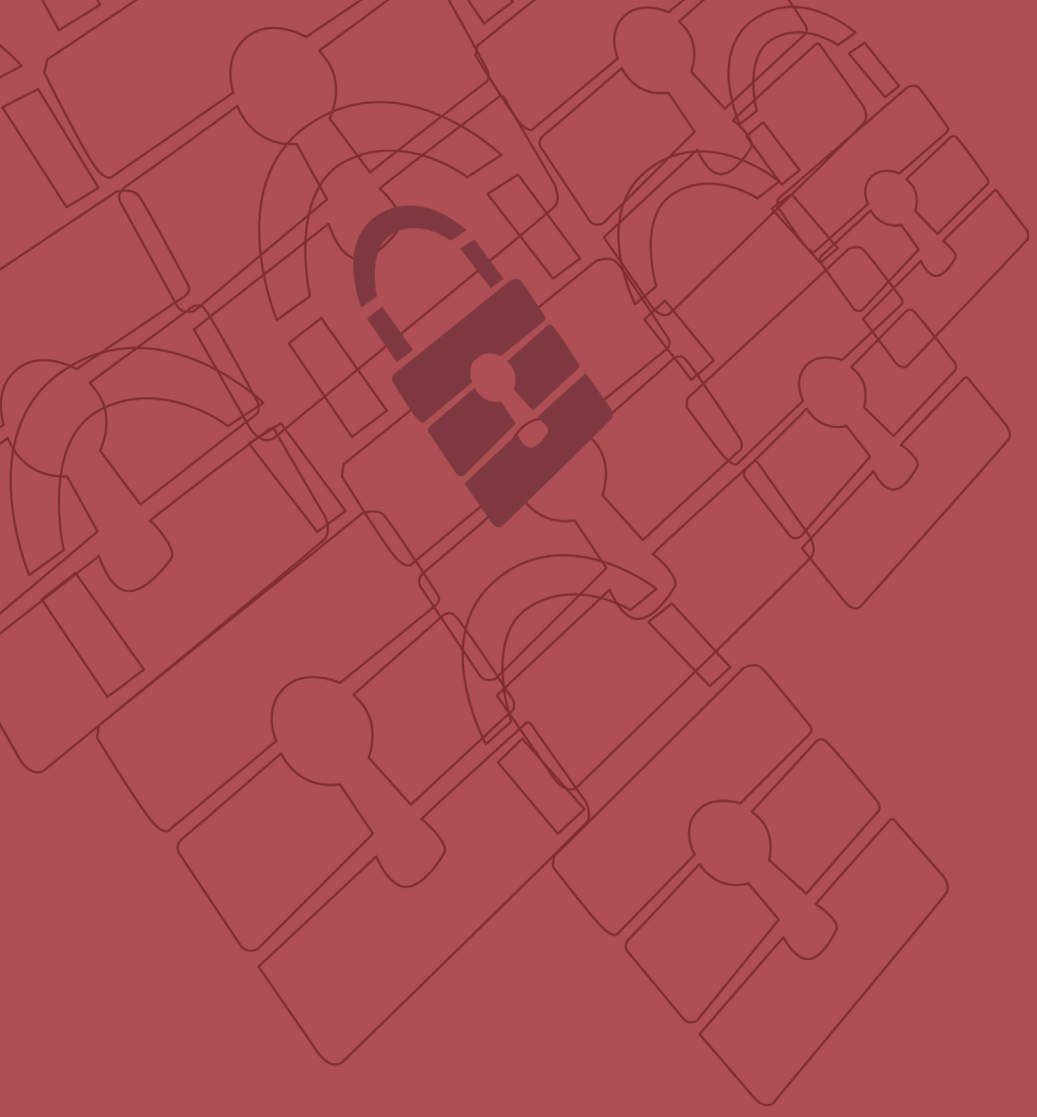
Nor can we ignore threats from the continuous surge of organisations contracting cybercriminal services to damage their competitors and their in-house technological and human resources that might be detrimental for the organisation, without forgetting all emerging threats and actions resulting from lack of cybersecurity culture.

On the other hand, digital information has become an asset with high added value. Analysis of personal data on the Net is used for a wide range of purposes from sociological studies to advertising campaigns. Malicious use of personal data and disinformation campaigns have high potential to destabilise society. Furthermore, exploiting personal data breaches represents infringement of this data's security, affecting people's privacy and their data's integrity and confidentiality.

As far as disinformation campaigns are concerned, they use elements such as fake news to influence public opinion. Internet and social media amplify the effect and scope of the information being sent out, with potential application against targets such as international organisations, States, political initiatives or public personalities or even democratic electoral processes.

CYBERTHREATS AND ACTIONS THAT USE CYBERSPACE FOR MALICIOUS PURPOSES





Chapter 3

Proposal, principles and goals for cybersecurity

Proposal, principles and goals for cybersecurity

This chapter outlines the proposal and principles governing the Strategy, plus one general and five specific goals.

Proposal

As the 2017 National Security Strategy established, Spain must guarantee secure, responsible use of information and communications networks and systems by strengthening capabilities for prevention, detection and response to cyber-attacks, developing and adopting specific measures to promote secure and reliable cyberspace

Therefore, the 2019 National Cybersecurity Strategy proposes to outline general directives for the cybersecurity field so as to meet 2017 National Security Strategy goals.

To do this, Spain must continue **strengthening skills** to tackle cyberthreats and malicious use of cyberspace. Consequently, measures will be sought that help guarantee our nation's

security, paying particular attention to the public sector and essential services, in a more coordinated framework featuring improved cooperation structures.

On the other hand, promoting **cybersecurity culture** should be one of the central themes being developed to make society aware of these threats and challenges. The right to secure, reliable use of cyberspace and contributing to this situation are shared responsibilities.

In addition, cybersecurity means progress, so singular **support and encouragement are required for the Spanish cybersecurity industry,** promoting an environment that nurtures research, development and innovation, plus participation from the academic world. On the other hand, our society prioritises attaining and maintaining **knowledge, skills,** experience and technological and professional capabilities because they are essential to tackle major cybersecurity challenges.

Cyberspace's transverse and global nature also demands cooperation and compliance from International Law, as well as utmost respect for the principles of the Constitution and the United Nations Charter; in coherence with the National Security Strategy and initiatives developed within European, regional and international frameworks, where national interests prevail at all times.

Governing Principles

The National Cybersecurity Strategy is upheld and inspired by the governing principles of National Security: action unit, anticipation, efficiency and resilience.

1. **Action Unit**: Any response to an incident in the cybersecurity field that might implicate different State agents will be strengthened if it is coherent, coordinated and resolved quickly and effectively. These qualities can be attained through careful preparation and appropriate organisation of the State's action unit.

Centralised management of cyberspace-related crises helps maintain full understanding of the threat situation and frees up available resources more quickly, efficiently, coherently and completely.

2. **Anticipation**: The specific nature of cyberspace and the players involved requires anticipation mechanisms in specialised organisations to guide State Action in crisis situations, where the private sector should also get involved.

   Anticipation prioritises preventive actions over reactions. Effective systems, with shared information as close as possible to real time, grant appropriate knowledge of the situation. This factor is essential to minimise response times which can be critical to reduce the effects of threats

3. **Eficiency:** Cybersecurity requires the use of high-value, multi-offer systems featuring a high level of technology, that are associated with very demanding needs and high costs derived from their development, purchase and operation, plus the need for advance planning and the high complexity of sustaining it.

   Furthermore, current and future scenarios are affected by economic austerity that, along with social responsibility to squeeze maximum performance from available resources, means that Spain should focus on optimisation and efficiency of resources devoted to cybersecurity, increasing the importance of the action unit, sharing information and integrating these resources for maximum efficiency.

4. **Resilience**: Resilience is a fundamental feature for systems and critical infrastructures. The State must ensure availability of elements considered to be essential for the nation, improving their protection against cyberthreats. A special mention should be given to the reinforcement required for information and communication networks against cyberthreat activities or illicit use of cyberspace.

GOVERNING PRINCIPLES

General Goal

New cybersecurity challenges have meant adapting the general goal to become more integrating, inclusive and less technified.

> In line with the 2017 National Security Strategy and broadening the cybersecurity goal mentioned in it, Spain will guarantee secure, reliable use of cyberspace, protecting citizens' rights and freedoms and promoting socio-economic progress.

Based on this general goal, a series of specific goals are explained below to guide the State's action in this field.

Goal I

> Security and resilience of information and communication networks and systems for the public sector and essential services.

A coherent, integrated national framework should be consolidated to help guarantee protection of information handled by the public sector and essential services, their systems and services, as well as the networks that support them. This framework will make it possible to develop and implant increasingly secure and efficient services.

To do so, security measures should be implemented, focussing on improving capabilities for prevention, detection and response to incidents, developing new solutions, reinforcing coordination and adapting the legal system accordingly.

Actions against cyberespionage particularly deserve a special mention as this ensures protection of Spain's Technological Patrimony, understood as the material or immaterial

assets that uphold the current business sector's intellectual and industrial property and condition future development.

The public sector and essential service operators should get actively involved in a continuous improvement process to protect their Information and Communication Technology systems based on constantly monitoring their threat exposure. These agents should act as a model for **cybersecurity management best practices.**

Applying the principle of shared responsibility, the public sector should work closely with companies that manage the relevant Information and Communication Technology Systems for national interests, exchanging knowledge that encourages appropriate coordination between the two and effective cooperation within the cybersecurity environment.

Strengthening cybersecurity requires systematic knowledge of the impact of potential interruption or destruction of the networks and systems that provide essential services, as well as security level metrics for these systems that help make the right decisions according to exposure levels.

Goal II

Secure and reliable use of cyberspace to ward off illicit or malicious use.

Cyberspace plays an increasingly important role in committing illicit or malicious acts and investigating them to encourage citizen trust. It is necessary to guarantee suitable prosecution of criminal phenomena that are taking place in it.

Fighting cybercrime can be divided into three fields: (i) cyberspace as the direct target of criminal acts, or the threat; (ii) cyberspace as the key medium for committing the crime; and (iii) cyberspace as the medium or direct investigation target for any type of illicit behaviour.

Based on solid and effective regulation that reinforces and guarantees fighting cybercrime, it is necessary to strengthen legal and police cooperation, both nationally and internationally, and assign sufficient resources to competent bodies on this matter and skills training for professionals working in this area.

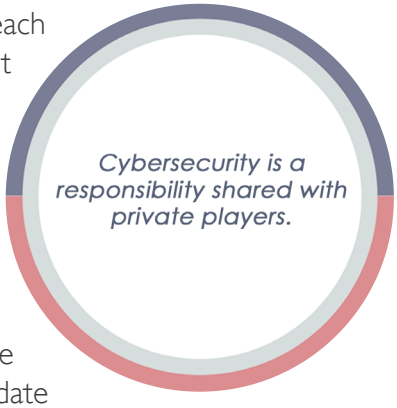
In the same way, citizen collaboration and participation must be encouraged, facilitating procedures to access and transmit information that might be of legal or police interest and identifying aspects that require improving capabilities among police institutions and competent legal organisations

Protecting the business and social ecosystem and citizens.

All persons and organisations have the right to use cyberspace securely. It is therefore the State's responsibility to promote and encourage measures to attain and maintain sufficient cybersecurity, particularly protecting the most vulnerable sectors of society and allowing proper socio-economic development for Spain.

Cybersecurity is a responsibility shared with private players that can affect them by action or omission; cybersecurity is not possible without their participation. Therefore, measures to be promoted should encourage cooperation to ensure common security.

Defending citizens, self-employed people and companies should reach beyond self-protection measures, so it is advisable to implement measures for their active cyberdefence. At the same time, all cyberspace users should demonstrate responsible use of the technology available to them.



Society's accelerated enthusiasm for emerging technologies makes risks evolve. Consequently, constant knowledge exchange with all players and monitoring mechanisms to protect the business and social ecosystem will be instruments to keep the Government informed and help it make the right decisions to update and adapt the actions taken as a result of this strategy.

Goal IV

Culture and commitment to cybersecurity and strengthening human and technological skills.

To tackle cybersecurity challenges, Spain should have technical and human resources to give it the necessary technological autonomy and appropriate skills training for secure use of cyberspace, making cybersecurity the key enabler for an entrepreneurial nation.

To do this, it must improve collective cybersecurity, diffusing cybersecurity culture with the help of public and private organisations and the media, strengthening information mechanisms and help for citizens and promoting spaces for encounters between civil society, administrations and companies.

It should also contribute to secure and responsible use of Information and Communication Technologies by promoting appropriate skills training on cybersecurity for professionals according to job market demands, stimulating professionals' development with their own skills, boosting specialised training and qualification, plus skills to generate knowledge, **develop R+D+i activities in cybersecurity and encourage use of certified products and services**.

In addition, special attention should be paid to protecting technological patrimony and industrial and intellectual property. To promote technological sovereignty and make the most of digital transformation opportunities, the Spanish cybersecurity industry should be encouraged and boosted hand-in-hand with good practice on development and implementation of information and communication systems.

International cyberspace security.

Spain will promote open, plural, secure and trustworthy cyberspace both in its bilateral relations and in multilateral, regional and international organisations, and in forums and conferences, where cyberspace plays a leading role.

It will advocate setting up an international framework for conflict prevention, cooperation and stability in cyberspace, applying principles from the whole United Nations Charter, International Law, Human Rights and Humanitarian Rights in War, as well as non-binding standards on responsible behaviour for States.

Aware of the importance of multilateralism, the United Nations' role is considered relevant to move forward building consensus that, along with adopting and setting in motion measures to promote trust, collaboration and participation from all players involved (States, private sector, civil society, users and academia), constitutes the groundwork to achieve security and stability in cyberspace and work towards regulation.

In line with our European partners, this goal will strengthen trust in the internet, digital transformation and development of new technologies, helping to consolidate a secure European cybernetic ecosystem that boosts progress towards the single digital market. To do this, it will defend an interoperative, neutral, open and diverse internet, a reflection of international cultural and linguistic plurality, based on a system of democratic, representative and inclusive governance resulting from agreement and consensus. In addition, it will provide access to global and generalised internet, thereby helping meet Sustainable Development Goals.

In this way, belonging to the European Union (EU) means that we have to strengthen security and European strategic autonomy by seeking synergy, technical, operative, strategic and political cooperation; to strengthen our resilience, our capacity to respond

to a crisis and the complementary nature of civil and military fields as EU partners and allies of the North Atlantic Treaty Organisation (NATO).

Based on the above, Spain will continue to take an active role in the EU and NATO; in the United Nations and in its offshoot forums such as the Internet Governance Forum (IGF); the Organisation for Security and Cooperation in Europe (OSCE), development and implementation of Confidence-Building Measures; the Organisation of American States (OAS). As well as the Global Forum on Cyber Expertise (GFCE) and the Freedom Online Coalition FOC, without forgetting our presence in the European Centre of Excellence to counter-attack Hybrid Threats (Hybrid CoE) plus the NATO Cooperative Cyberdefence Centre of Excellence (CCD CoE).

In addition, it will reinforce international bilateral cooperation on cybersecurity, promote fluid and trustworthy relations in this field, work jointly on building skills in third-party countries, paying particular attention to women and young people and promoting setting up information channels and experience exchange, boosting bilateral and multilateral agreements in this field.

STRATEGY GOALS

GENERAL GOAL

In line with the 2017 National Security Strategy and broadening the cybersecurity goal mentioned in it, Spain will guarantee secure, reliable use of cyberspace, protecting citizens' rights and freedoms and promoting socio-economic progress.

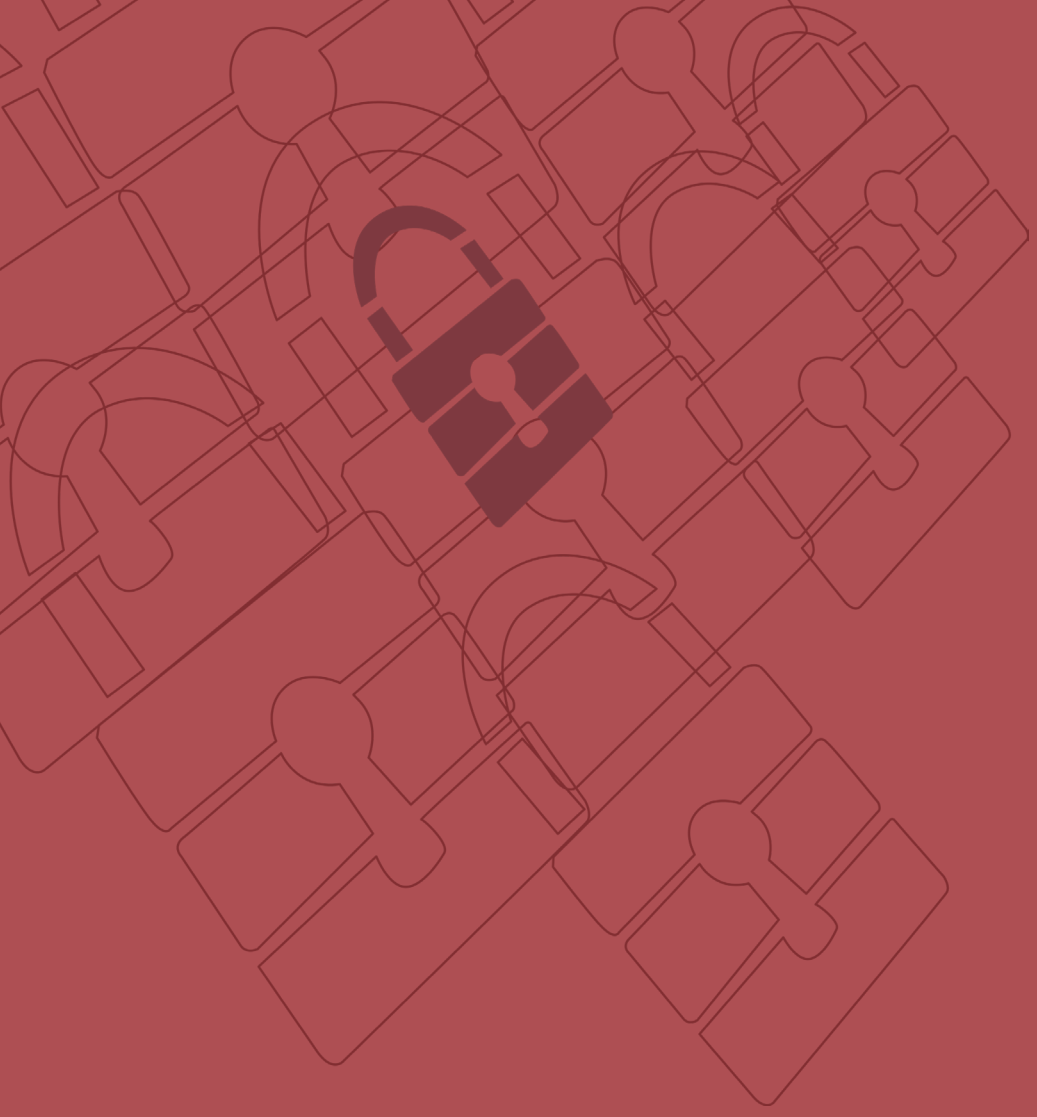
Goal **01** Security and resilience of information and communication networks and systems for the public sector and essential services.

Goal **02** Secure and reliable use of cyberspace to ward off illicit or malicious use.

Goal **03** Protecting the business and social ecosystem and citizens.

Goal **04** Culture and commitment to cybersecurity and strengthening human and technological skills.

Goal **05** International cyberspace security.



Chapter 4

Lines of action and measures

Lines of action and measures

This chapter sets the lines of action to achieve the goals.

LINE OF ACTION 1

Strengthen capabilities to deal with threats from cyberspace.

This line of action meets Goal 1 in the Strategy.

MEASURES

1. Extend and improve cyberthreat detection and analysis skills to be able to identify attack procedures and origins; also draw up the necessary intelligence for more effective protection, attribution and defence.

2. Encourage centres of excellence and research facilities to work together to tackle cyberthreats.

3. Strengthen creation, dissemination and application of best practices and standards for cybersecurity.

4. Ensure technical and operational coordination of organisations with cybersecurity responsibilities, companies and society.

5. Develop and update standards, procedures and instructions to respond to cybersecurity incidents, ensuring inclusion in the National Security System.

6. Strengthen cyberdefence and cyberintelligence capabilities.

7. Promote participation from companies on sector-based platforms for information exchange and analysis, and to measure sector-based risk, and suggest actions to mitigate this, alongside the legal requirements that regulate them.

8. Strengthen and support developments in the Spanish CSIRT network.

9. Boost development for notification platforms, exchange of information and coordination to improve sector-based cybersecurity.

10. Develop instruments for prevention, detection, response, return to normality and assessment focussed on crisis management for the cybersecurity field within the framework of National Security.

11. Guarantee coordination, cooperation and exchange of information on cyberincidents and intelligence on cyberthreats between the public sector, private sector and competent international organisations, encouraging prevention and early warnings.

12. Implanting active cyberdefence measures in the public sector to improve response capabilities.

LINE OF ACTION 2

Guarantee security and resilience for Spain's strategic assets.

Esta línea de acción responde al Objetivo I de la Estrategia.

MEASURES

1. Broaden and strengthen capabilities for prevention, detection, response, recovery and resilience against cyberattacks aimed at the public sector, essential services and strategic companies.

2. Strengthen development of the critical infrastructure protection standard, reinforcing security for information networks and systems that support them.

3. Ensure full implementation of the National Security Framework, the Critical Infrastructure Protection System and compliance and harmonisation of the critical infrastructure protection standard and essential services with a risk-based priority focus.

4. Within their competences, strengthen progressive implication and creation of cybersecurity infrastructures in Autonomous Regions, Autonomous Cities, Local Entities and in their affiliated or dependent organisations that will cooperate and be coordinated with national structures to improve national cybersecurity.

5. Develop the Spanish Central Administration Cybersecurity Operations Centre that improves prevention, detection and response skills and boosts regional and local development of cybersecurity operations centres.

6. Strengthen the implementation of telecommunications infrastructures and services and common horizontal information systems, also shared by Public Administrations, bolstering use and their security and resilience skills, whilst ensuring coordination with the former when common infrastructures and services are not used.

7. Boost development of a metrics system for major cybersecurity variables that allows competent authorities to determine security levels and how they might evolve.

8. Commit the public and private sector to supply chain risk management, particularly when affecting essential service provision.

9. Develop catalogues of qualified, certified products and services, for use in public sector contracting processes and essential services.

10. Reinforce security structures and surveillance capacity for information systems that handle classified information.

11. Promote cyberexercises and cybersecurity assessments, particularly in areas that affect National Security, Public Administration, essential services and sought-after companies.

12. Ensure protection of Singular Scientific-Technical Infrastructures and R+D+i reference centres.

LINE OF ACTION 3

Reinforce capabilities for investigation and prosecution of cybercrime, to guarantee citizen security and protect rights and freedoms in cyberspace.

This line of action meets Goal II in the Strategy.

MEASURES

1. Reinforce the legal framework for an effective response to cybercrime, relating to both defining types of crime and regulating the right investigation measures.

2. Promote citizen collaboration and participation, articulating instruments to exchange and transmit information that might interest the police and promoting cybercrime prevention campaigns aimed at citizens and businesses.

3. Reinforce actions to strengthen investigation, attribution and prosecution skills and, when appropriate, criminal action, against cybercrime.

4. Promote transfer of the criminal jurisdiction of information relating to criminal security incidents to competent organisations, particularly any that affect or might affect essential service provision and critical infrastructures.

5. Obtain access to information and material resources for legal operators that ensure better application of the legal and technical framework for fighting

cybercrime, giving them greater skills to investigate and judge the corresponding illicit acts.

6. Promote exchange of information, experience and knowledge among personnel with responsibilities cybercrime investigation and prosecution.

7. Ensure legal professionals and State Security Forces access to human and material resources, giving them the necessary knowledge to best apply the associated legal and technical framework.

8. Boost investigation coordination on cybercrime and other illicit uses of cyberspace among the different bodies and units with competence in this field.

9. Strengthen international legal and police cooperation.

LINE OF ACTION 4

Boost cybersecurity for citizens and companies.

This line of action meets Goal III in the Strategy.

MEASURES

1. Offer citizens and the private sector an integrated public cybersecurity service, which is good quality and easy to access, and that stimulates demand for cybersecurity business sector services.

2. Boost cybersecurity in SMEs, microSMEs and among self-employed workers by articulating public policies on cybersecurity, particularly developing resilience.

3. Promote cybersecurity to guarantee privacy and protection for personal data within the framework of citizen's digital rights in accordance with the legal system, promoting "digital identity" protection.

4. Create agile, secure complaint mechanisms for the private sector and citizens.

5. Stimulate cooperation between public and private players, particularly promoting commitment from Internet Service and Digital Service Providers to improve cybersecurity. National regulation will be boosted in this respect and measures will be implemented for active cyberdefence of citizens and SMEs.

6. Develop mechanisms to measure accumulated risk and how it changes, both for citizens and companies, to prioritise cybersecurity measures and keep society appropriately informed.

7. In the business sector, boost implementation of recognised cybersecurity standards. Working with national and international standardisation entities, stimulate creation, diffusion and application of sector-based cybersecurity best practices, including different certification frameworks.

8. Boost implementation of reliable electronic identification systems and trusted electronic services.

9. Promote setting up the National Cybersecurity Forum that incorporates representatives from civil society, independent experts, private sector, academia, associations, non-profiting-making organisations, among others, to strengthen and set up public-private synergies, particularly generating knowledge on security opportunities and threats in cyberspace.

LINE OF ACTION 5

Strengthen the Spanish cybersecurity industry and its capacity to nurture and retain talent, to bolster digital autonomy.

This line of action meets Goal IV in the Strategy.

MEASURES

1. Boost R+D+i support programmes in digital security and cybersecurity in SMEs, businesses, universities and research centres, facilitating access to national and international incentive programmes and through innovative public purchasing programmes.

2. Revitalise the industrial and cybersecurity services sector, providing incentives for measures supporting innovation, investment, internationalisation and technology transfer, particularly in the case of microSMEs and SMEs.

3. Increase national activities to develop cybersecurity products, services and systems, and security right from design, specifically supporting any that uphold national interest needs to strengthen digital autonomy, and intellectual and industrial property.

4. Promote standardisation activities and cybersecurity requirements in the Information and Communication Technologies products and services, facilitate access to products and services that meet these requirements, promoting

compliance assessment and certification, and providing support for drawing up catalogues.

5. Update or, when appropriate, develop competence frameworks in cybersecurity that meet the job market's needs.

6. Identify needs for professional skills in cybersecurity, promoting collaboration between educational and training institutions by boosting continuous training, employment training and university education, promoting professional credential and certification systems.

7. Include professional cybersecurity profiles in public sector job descriptions.

8. Detect, encourage and retain talent in cybersecurity paying particular attention to the research field.

9. Boost specific R+D+i programmes in cybersecurity and cyberdefence.

LINE OF ACTION 6

Contribute to cyberspace security internationally, promoting open, plural, secure and trustworthy cyberspace, supporting national interests.

This line of action meets Goal V in the Strategy.

MEASURES

1. Strengthen and reinforce Spain's presence in the organisations, conferences and regional and international forums to which it belongs and where cybersecurity is a substantial part of its mandate, and support and participate actively in different initiatives, coordinating the position of the different national agents involved.

2. In the sphere of the United Nations, promote the search for consensus to fully abide by the United Nations Charter and application and implementation of International Law and States' rules for responsible behaviour. Likewise, move forward in adopting and implementing Confidence-Building Measures in cyberspace.

3. Take an active part in the European Union in terms of developing a secure European ecosystem that encourages progress and consolidation of the single market, and Europe's security and strategic autonomy, seeking complementary aspects and cooperation between the European Union and NATO.

4. Promote bilateral dialogue, cooperation and information and experience-exchange systems, and early warning devices to develop a coordinated focus on fighting cyberthreats with other countries, promoting negotiation and signing international agreements.

5. Promote development of technological skills and internet access in third-party countries to thereby aid compliance with Sustainable Development Goals.

6. Work with surrounding countries to develop greater awareness on Hybrid Threats, limiting impact on our countries' sovereignty and integrity.

LINE OF ACTION 7

Develop a cybersecurity culture.

The measures included in this Line of Action will contribute to the National Security Culture Plan and meet goal IV of the Strategy.

MEASURES

1. Increase awareness-raising campaigns for citizens and companies and provide them with useful information that is suitable for each profile, particularly in the field of self-employed workers and small and medium-sized companies.

2. Strengthen actions that bring about an surge in joint-responsibility and obligations from society regarding national cybersecurity.

3. Boost initiatives and plans for digital literacy in cybersecurity.

4. Promote the spread of cybersecurity culture as a best business practice and acknowledge companies' implication in improving collective cybersecurity as corporate social responsibility.

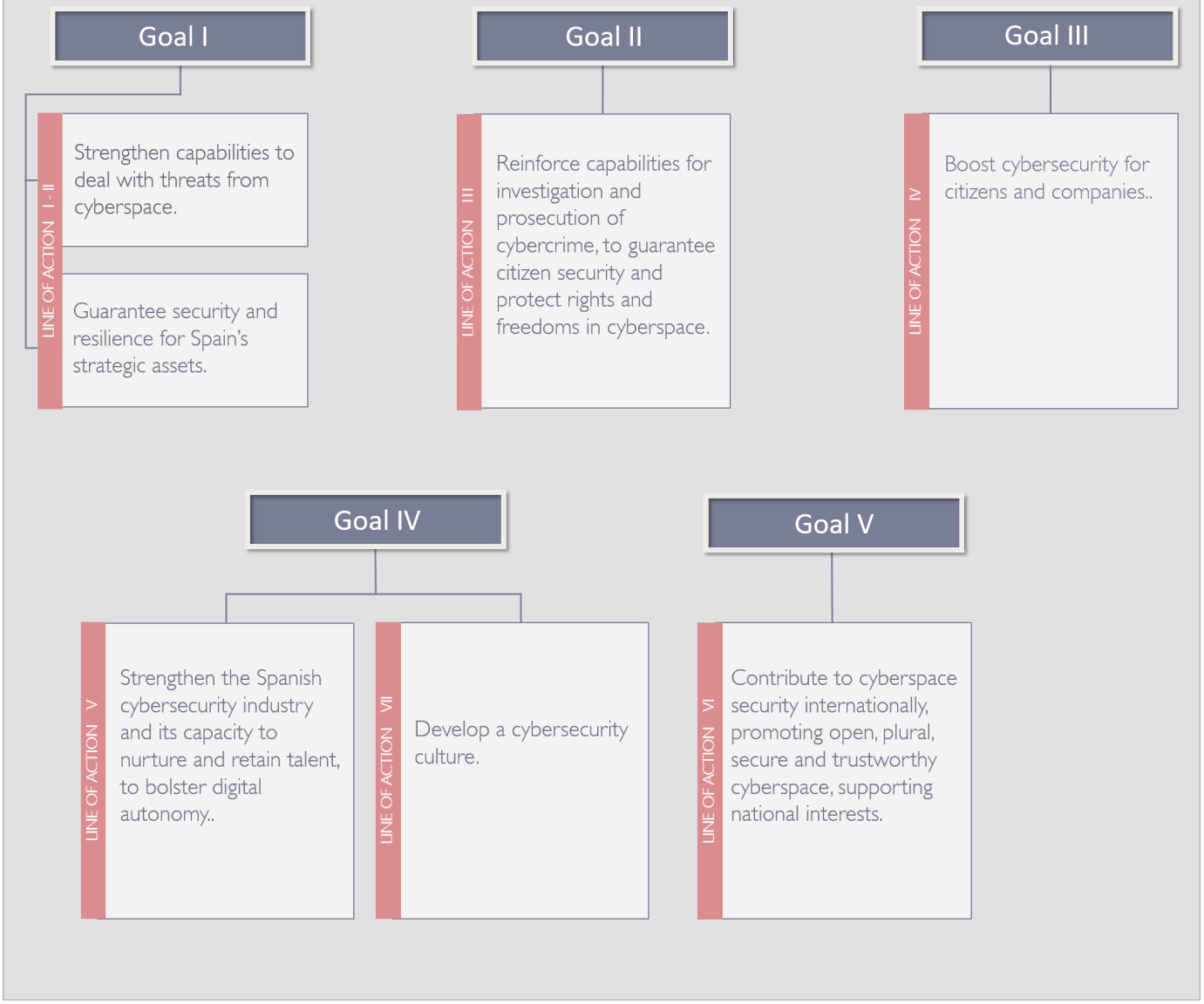
5. Promote a critical spirit in favour of truthful, high quality information that helps pinpoint fake news and disinformation.

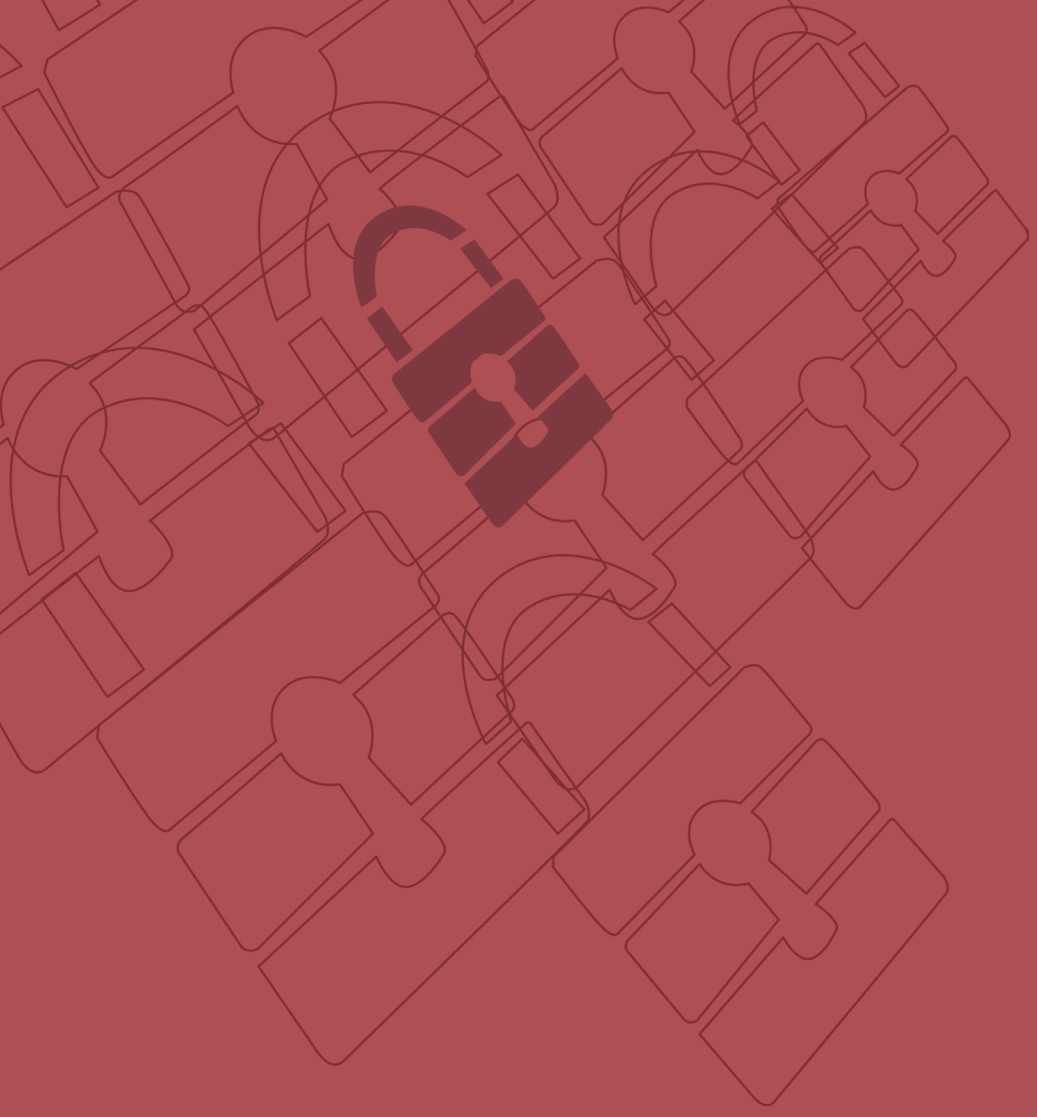
6. Raise awareness among organisations' executives so that they can free up the necessary resources and promote cybersecurity projects as required by their entities.

7. Promote awareness-raising and training on cybersecurity in schools, adapted to all training levels and specialities.

8. Seek and recognise media collaboration and participation, to give citizen campaigns further reach, particularly among young people.

LINES OF ACTION





Chapter 5

Cybersecurity in the National Security System

Cybersecurity in the National Security System

This chapter considers how cybersecurity is incorporated into the current National Security System.

The 2013 National Cybersecurity Strategy and subsequent approval of the National Security Law in 2015, created a specific organic structure for cybersecurity. This 2019 Strategy boosts initiatives that complement further progress in the national governance model with European policies

Within the National Security System, the cybersecurity structure comprises the following components:

1. The National Security Council.
2. A single Specialised Situation Committee for the whole National Security System in crisis situations.
3. The National Cybersecurity Council
4. The Cybersecurity Standing Committee.
5. The National Cybersecurity Forum.
6. Competent public authorities and the national CSIRT.

The National Security Council

The National Security Council, as the Government's Delegate Commission for National Security, is the body which helps the Spanish Prime Minister to manage National Security Policy.

The National Security Council acts through the National Security Department as a single point of contact, as a link, and guarantees cross-border cooperation with other countries in the European Union

The Situation Committee

There is just one Situation Committee for the whole National Security Council and, supported by the National Security Department, it acts according to political-strategic guidelines dictated by the National Security Council on crisis management.

The National Cybersecurity Council

The National Cybersecurity Council helps the National Security Council meet its functions, particularly helping the Spanish Prime Minister manage and coordinate National Security Policy in the field of cybersecurity.

Its functions include reinforcing coordination, collaboration and cooperation between Public Administrations with competences in cybersecurity, and between public and private sectors, and easing decision-making for the actual Council by analysing, studying and suggesting initiatives and evaluating risks and threats, analysing possible crisis scenarios, studying how they might evolve, drafting and updating response plans and formulating directives for crisis management exercises in the field of cybersecurity and assessing their performance results, all in coordination with directly competent bodies and authorities.

The Cybersecurity Standing Committee

The Cybersecurity Standing Committee is set up to ease inter-ministerial coordination on an operational level in the field of cybersecurity. Presided over by the National Security Department, it comprises the bodies and organisations represented within the National Cybersecurity Council with operational responsibilities. This body helps the National Cybersecurity Council on aspects relating to technical and operative assessment of cybersecurity risks and threats.

The Commission's operation falls within the crisis management procedure in the field of cybersecurity. This procedure establishes its functions aimed at detecting and assessing risks and threats; eases the decision-making process and ensures an optimum, coordinated response from the State. Furthermore, it includes the National Security System's different activation levels plus instructions to manage public communication.

To provide a relevant response, in proportion to situations of special relevance in its functions, it will improve the definition of its skills and responsibilities.

National Cybersecurity Forum

It will act on strengthening and creating public-private synergies, particularly generating knowledge on opportunities, challenges and threats to security in cyberspace.

Setting up the **National Cybersecurity Forum**, and harmonising its operation with existing bodies, will require approval of the necessary standard-based provisions,

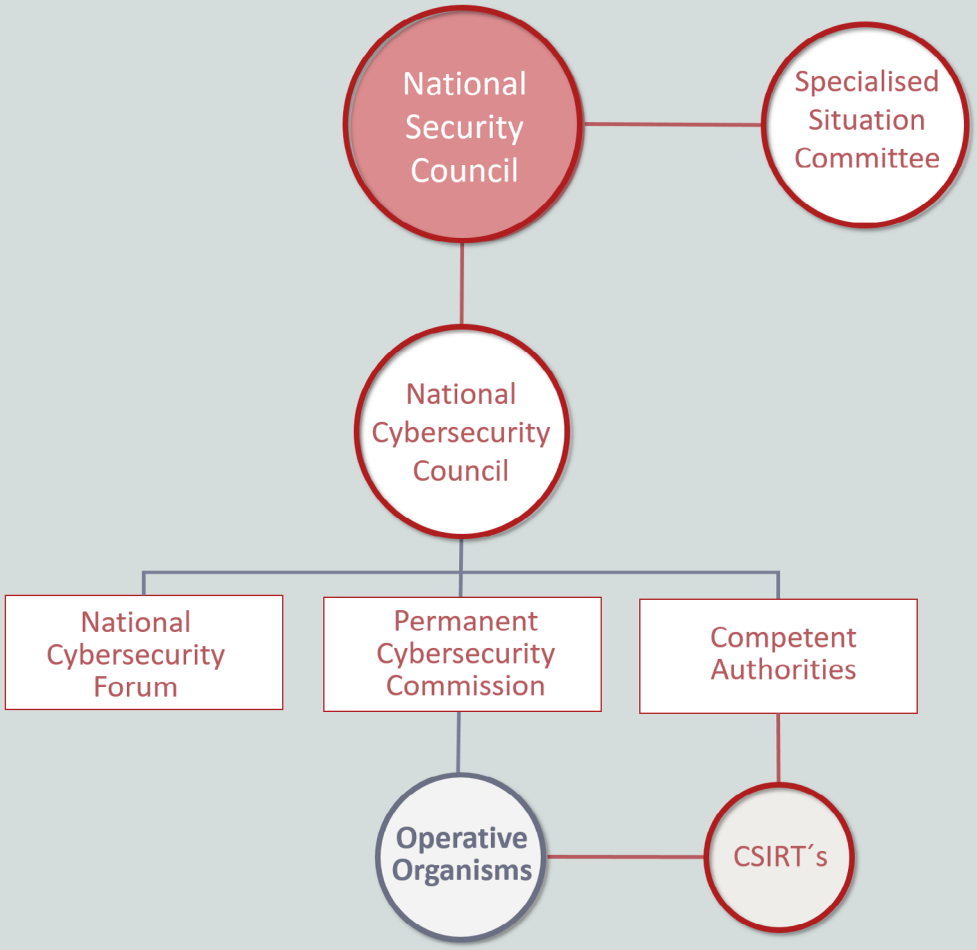
so that these components might be coordinated and run efficiently in the National Security System.

Competent public authorities and the national reference CSIRT

Cybersecurity's strategic, institutional framework is complemented by the competent public authorities on security in information networks and systems and the national CSIRTs that are compiled in the national legal framework.

In addition, CSIRTs from the Autonomous Regions and Autonomous Cities, from Local Entities and their affiliated or dependent bodies, from private entities, the CSIRT. es network and other relevant cybersecurity services should be coordinated with the above, depending on each one's competences. In the same way, working with regional and private CSIRTs, national CSIRTs will encourage initiatives that help meet national strategy goals

CYBERSECURITY IN THE NATIONAL SECURITY SYSTEM



Final considerations and evaluation

Thanks to experience from the 2013 National Cybersecurity Strategy, this document can express and update the ever-changing threats and challenges that we are facing. To adapt to this new, shifting scenario, Lines of Action are proposed plus more dynamic measures that, when necessary, allow the national cybersecurity ecosystem to adapt quickly, based on a considerably mature governance model, which should include active participation from the private sector and the rest of civil society.

In this respect, the Strategy is conceived as a living document that has to be adapted to gradual changes in cybersecurity, so it should be continuously revised, along with specific, sector-based plans derived from it. An annual assessment report will be drafted on the Strategy that will show how much it has been followed and if its goals have been met.

On the other hand, in the light of increasing cybersecurity threats and challenges as faced by countries around us, it is increasingly urgent to equip ourselves with economic, human and material resources to tackle them. One particularly relevant action here is to make sure that the Spanish Central Administration Cybersecurity Operations Centre is properly equipped.

DSN

www.dsn.gob.es