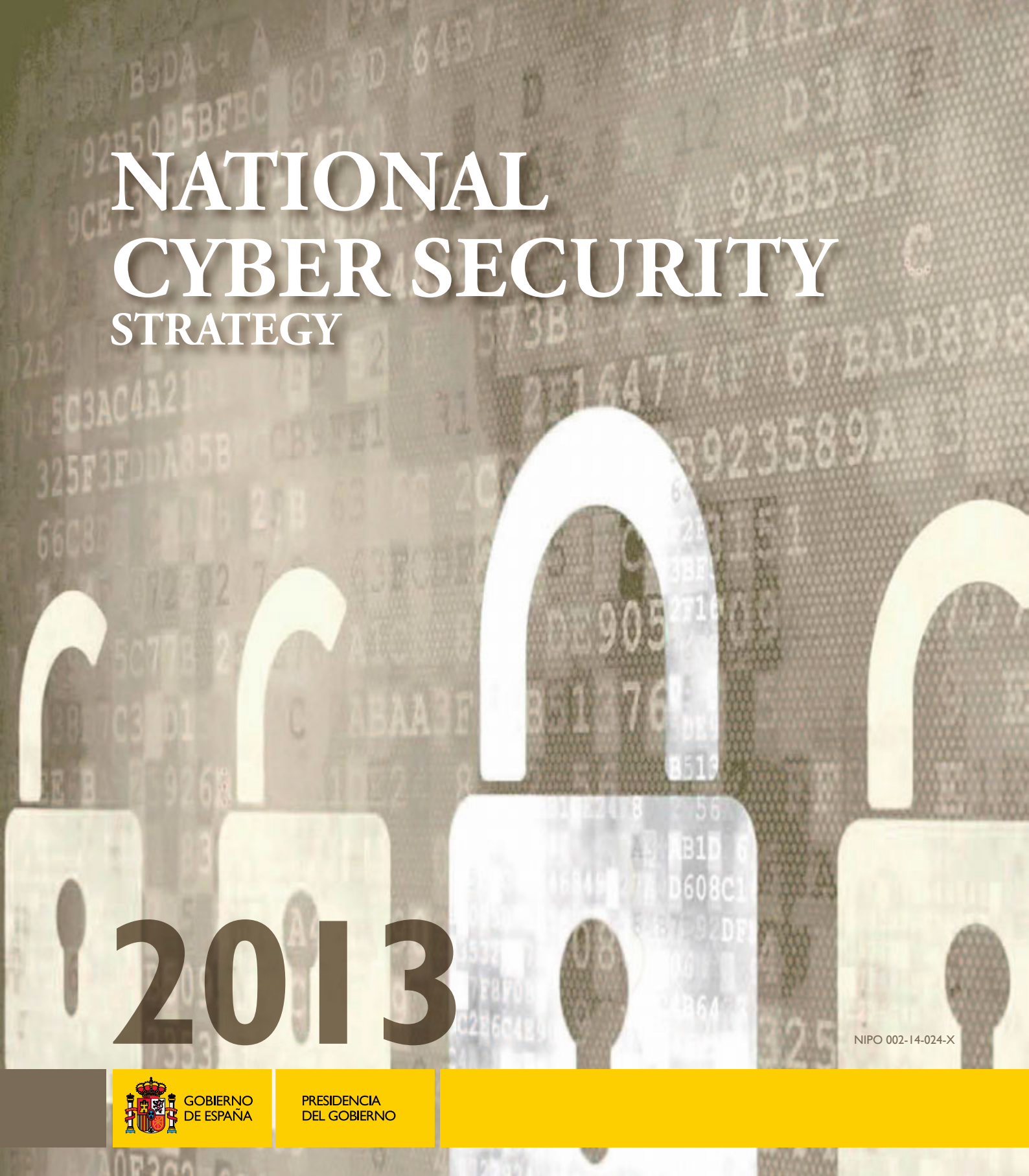


NATIONAL CYBER SECURITY STRATEGY

2013

NIPO 002-14-024-X

GOBIERNO DE ESPAÑA

PRESIDENCIA DEL GOBIERNO

NATIONAL CYBER SECURITY STRATEGY

The use of Information and Communications Technologies has become widespread in daily life in our country. This new scenario of possibilities offers unprecedented development in the exchange of information and communications, but at the same time it entails serious risks and threats which can affect National Security.

Several factors contribute to the proliferation of criminal actions in cyberspace: the profitability of exploiting it in economic, political or other terms, the ease and low cost of employing the tools used to stage attacks, and the ease with which attackers can hide make it possible to carry out these activities anonymously and from anywhere in the world, with cross-cutting impacts on the public and private sectors and on citizens themselves.

The different attacker profiles exploit technological vulnerabilities in order to glean information, steal highly valuable assets and threaten basic services that are essential to our country's normal functioning. The peaceful enjoyment of certain fundamental rights enshrined in our Constitution and in international law can be seriously compromised as a result of actions of this kind.

Fully conscious of the importance of the matter and committed to the development of the Digital Society, the National Security Council has promoted the drafting of the National Cyber Security Strategy in order to provide a response to the huge challenge entailed by protecting cyberspace from the risks and threats hovering over it.

The National Cyber Security Strategy is adopted under, and aligned with, the National Security Strategy of 2013, which includes cyber security in its twelve areas of action.

The adoption of the present strategic document highlights the collective capabilities and the commitment of a nation determined to guarantee its security in cyberspace. For Spain, advances in the field of cyber security furthermore contribute to enhancing our economic potential, as they promote a more secure environment for investment, job creation and competitiveness.

The National Cyber Security Strategy is the frame of reference of a comprehensive model based on the involvement, coordination and harmonisation of all the State actors and resources, and on public-private collaboration and citizen participation. Likewise, as cyber security is transnational, cooperation with the European Union and other international organizations with responsibilities in this field is an essential part of this model.

To achieve its objectives, the Strategy establishes an organisational structure that is integrated into the framework of the National Security System. This structure will underpin the single action of the State in accordance with principles shared by the actors concerned and in an appropriate institutional framework.

This dependence on cyberspace requires us to devote all the necessary means to placing our capabilities at the service of cyber security. The environment is dynamic and we face many uncertainties and challenges. Only if we are firmly committed to the security of cyberspace will the competitiveness of our economy and Spain's prosperity be a possibility.

Mariano Rajoy Brey
Prime Minister of Spain

Contents

Executive Summary

Executive Summary

Executive Summary

The **National Cyber Security Strategy** is the strategic document that provides the Spanish Government with a basis for developing the provisions of the National Security Strategy on the protection of cyberspace in order to implement cyber threat prevention, defence, detection, response and recovery actions against cyber threats

The Strategy consists of **five chapters. The first,** entitled Cyberspace and its security, outlines the characteristics that define cyberspace, the opportunities it provides and the security implications of depending on it. This chapter shows how the particular characteristics which are common to cyber threats and the high dependence of the economy and essential services on cyberspace result in an increase in risks and threats with a potentially serious impact on National Security.

The **second chapter** deals with the *Purpose and guiding principles of cyber security in Spain.* It establishes as a purpose the setting of general guidelines for the secure use of cyberspace through a comprehensive vision that involves the coordination of the Public Authorities, the private sector and citizens and channels international initiatives in this field, respecting domestic and international law and in line with other national and international strategic documents.

The *guiding principles* of cyber security are *national leadership and the coordination of efforts; shared responsibility; proportionality, rationality and efficiency; and international cooperation* as an extension of the basic principles of the National Security Strategy. These principles underline the need for development planning of the current context, with special emphasis on protecting the constitutional values as an element common to all four principles.

In the **third chapter,** the Strategy examines the *Cyber security objectives* in greater detail. An overall objective is to *ensure that Spain makes secure use of the Information and Telecommunications Systems, strengthening cyber-attack prevention, de-*

fence, detection, analysis, investigation, recovery and response capabilities. The National Cyber Security Policy must serve this purpose.

The Strategy goes on to set up **six specific objectives:** 1) *for the Public Authorities,* to ensure that the Information and Telecommunications Systems used by them have the appropriate level of security and resilience; 2) *for companies and critical infrastructures,* to foster the security and resilience of the networks and information systems used by the business sector in general and by operators of critical infrastructures in particular; 3) *in the judicial and police field operations*, to enhance prevention, detection, response, investigation and coordination capabilities vis-à-vis terrorist activities and crime in cyberspace; 4) *in the field of sensitisation,* to raise the awareness of citizens, professionals, companies and Spanish Public Authorities about the risks derived from cyberspace; 5) *in capacity building,* to gain and maintain the knowledge, skills, experience and technological capabilities Spain needs to underpin all the cyber security objectives; and 6) with respect to international collaboration, to contribute to improving cyber security, supporting the development of a coordinated cyber security policy in the European Union and in international organisations, and to collaborate in the capacity building of States that so require through the development cooperation policy.

Chapter four lays down the *Lines of Action of National Cyber Security.* Interdependently, and in connection with the objectives established in the previous chapter, the Strategy guides the action aimed at achieving the objectives set out.

The **fifth and last chapter** is devoted to Cyber security in the National Security System and establishes the organisational structure at the service of cyber security. Under the direction of the Prime Minister, the structure is comprised of three bodies. One already exists – **the National Security Council** as the Government Delegated Commission for National Security – and two are new: **the Specialised Cyber Security Committee,** which will support the National Security Council by assisting the direction and coordination of the National Security Policy in cyber security matters and by fostering coordination, cooperation and collaboration among Public Authorities and between them and the private sector; and **the Specialised Situation Committee** which, with the support of the Situation Centre of the National Security Department, will manage cyber security crisis situations which, on account of their cross-cutting nature or extent,

exceed the response capabilities of the usual mechanisms. The two Specialised Committees will act in a complementary manner.

Cyberspace and its security

Chapter 1
Cyberspace and its security

Chapter 1
Cyberspace and its security

The development of Information and Communications Technologies (ICT) has given rise to a new space in which relations are conducted and in which the speed and ease with which information and communications are exchanged have overcome the barriers of distance and time. Cyberspace, the name given to the global and dynamic domain composed of the infrastructures of information technology – including the Internet – networks and information and telecommunications systems, has blurred borders, involving their users in an unprecedented globalisation that provides new opportunities but also entails new challenges, risks and threats.

Our society's degree of reliance on ICT and cyberspace is growing daily. Knowledge of its threats, managing the risks and building an appropriate prevention, defence, detection, analysis, investigation, recovery and response capability are essential elements of the National Cyber Security Policy.

"The development of ICT has given rise to a new space in which relations are conducted and in which the speed and ease with which information and communications are exchanged have overcome the barriers of distance and time"

The attacks derived from these threats, known as cyber attacks, generally share a number of common characteristics:

Characteristics of cyber attacks

Low Cost

- many of the tools used by attackers can be obtained free of charge or at a very low cost.

Ubiquity and ease of execution

- the execution of attacks is independent of the location of the aggressors, and in many cases considerable technical knowledge is not necessary.

Effectiveness and impact

- if the attack is well designed, it may achieve its desired objectives. The absence of cyber security policies, insufficient resources and lack of awareness and skills can facilitate this adverse outcome.

Reduced risk for the attacker

- ease of concealment means that it is not easy to attribute a cyber attack to its real perpetrator or perpetrators. This, coupled with a disparate or non-existent legal framework, makes it difficult to prosecute the action.

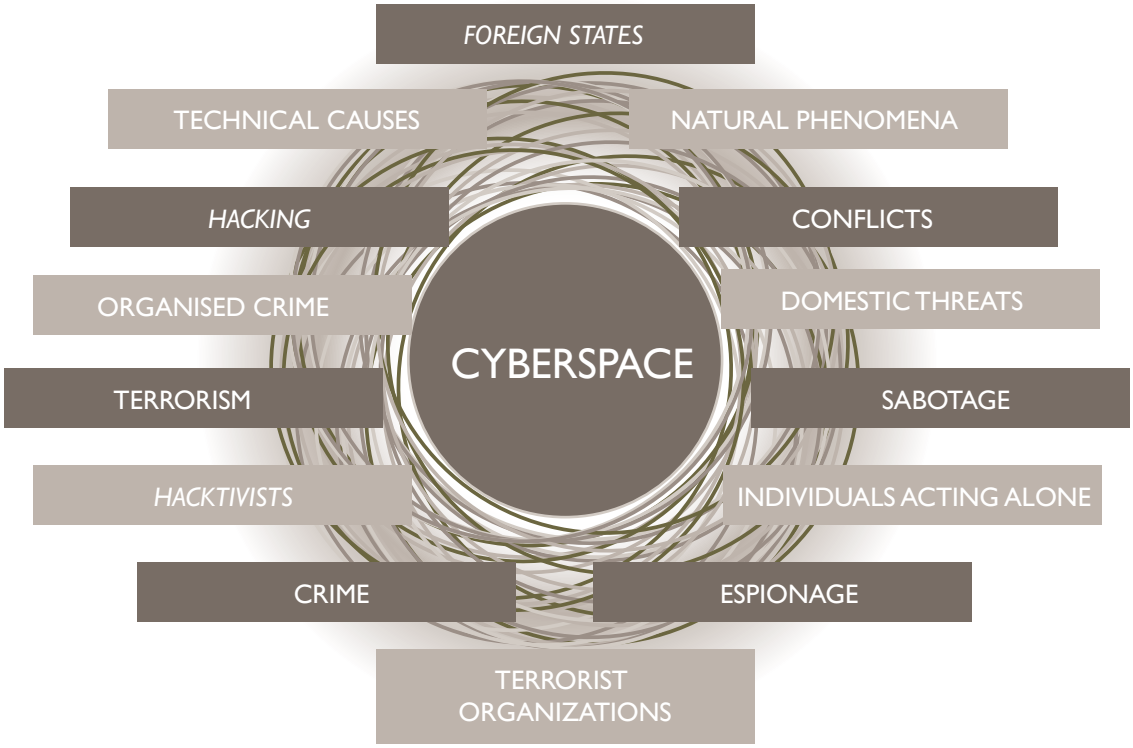
The host of potential attackers increases the risks and threats that can seriously jeopardise the services provided by the Public Authorities and the Critical Infrastructures and the activities of companies and citizens. Furthermore, there is evidence that certain countries have military and intelligence capabilities to carry out cyber attacks that place National Security at risk.

Cyber security is a necessity of our society and our economic model. Given the influence of Information and Telecommunications Systems on the economy and public services,

"Cyber security is a necessity of our society and our economic model"

Spain's stability and prosperity largely depend on the security and reliability of cyberspace – qualities which can be jeopardised by technical causes, natural phenomena or deliberate aggressions.

Risks and threats to national Cyber Security



Purpose and guiding principles of cyber security in Spain

Chapter 2

Purpose and guiding principles of cyber security in Spain

Chapter 2
Purpose and guiding principles of cyber security in Spain

Spain requires secure and reliable Information and Telecommunications Systems, both for its physical infrastructure (equipment and networks) and the intangible component (computer programmes, models or procedures). These systems, while allowing citizens and companies access to cyberspace, store valuable information and support strategic services for our nation that are essential to the correct functioning of our society.

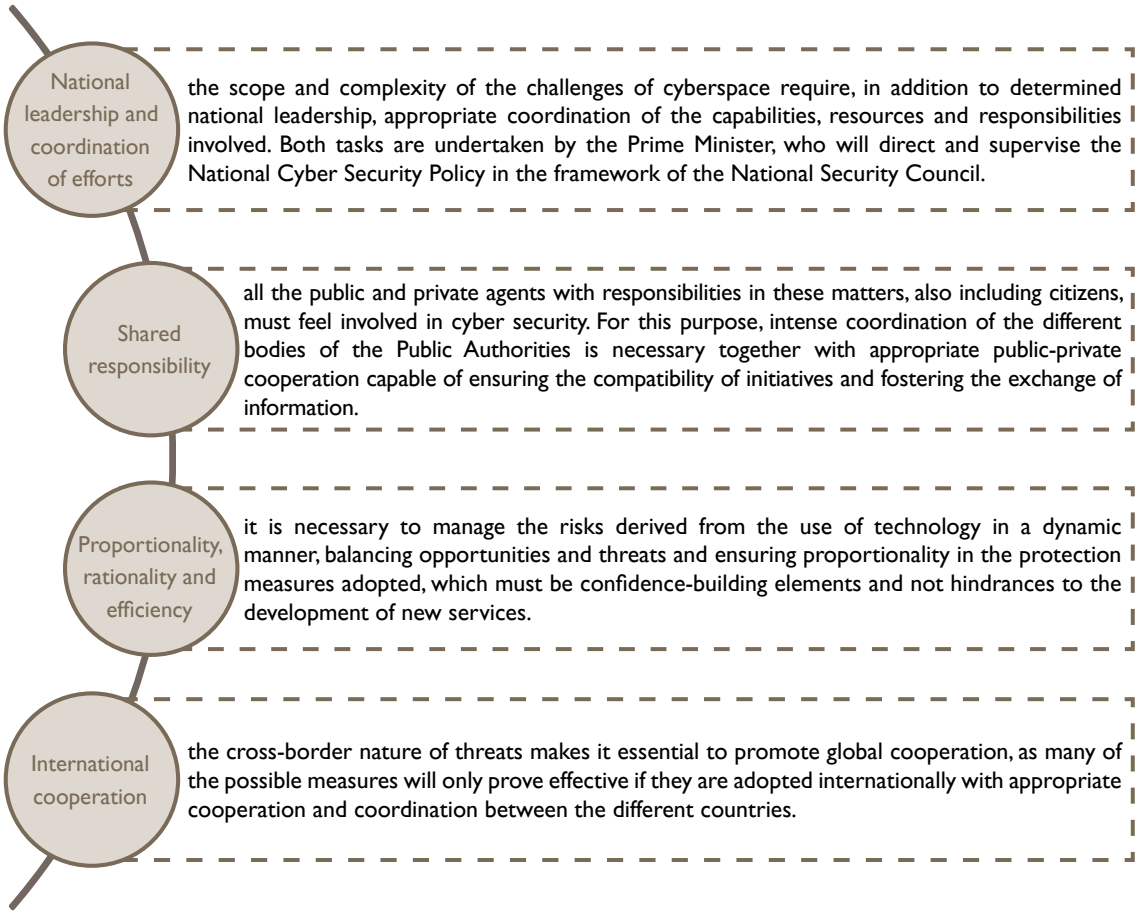
The purpose of the **National Cyber Security Strategy** promoted by the **National Security Council** is to establish general guidelines for the secure use of cyberspace, encouraging a comprehensive vision, the application of which helps guarantee our nation's security and progress through appropriate coordination and cooperation among all the Public Authorities and with the private sector and citizens, with utmost respect for the principles enshrined in the Constitution and in the provisions of the Charter of the United Nations on the peace keeping and international security; and in consonance with the National Security Strategy and initiatives developed in the European, international and regional framework.

"The purpose of the National Cyber Security Strategy promoted by the National Security Council is to establish guidelines for the secure use of cyberspace"

It likewise encourages Spain's presence in international organisations and forums by channelling international initiatives and efforts to protect cyberspace.

Guiding Principles

The **National Cyber Security Strategy,** in tune with the basic principles of the National Security Strategy and as an extension of them, is underpinned and inspired by the following Guiding Principles:



They all respect and strengthen the protection and full enjoyment of the fundamental freedoms enshrined in our Constitution and in international instruments as important as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention for the Protection of Human Rights and Fundamental Freedoms. The Spanish Government undertakes to develop policies which, by improving the security of the Information and Telecommunications Systems used by citizens, professionals and companies, preserve the fundamental rights of them all, especially in the most underprivileged sectors.

Objectives of cyber security

Chapter 3
Objectives of cyber security

Chapter 3
Objectives of cyber security

OVERALL OBJECTIVE

To ensure that Spain uses Information and Telecommunications Systems securely by strengthening prevention, defence, detection and response capabilities vis-à-vis cyber attacks.

To achieve a secure cyberspace, a National Cyber Security Policy will be promoted by developing an appropriate regulatory framework and fostering a Structure that brings together and coordinates all the institutions and agents with responsibilities in this area. This Structure will be based on the principle of efficiency and sustainability in the use of resources, guaranteeing the optimal prevention, defence, detection, analysis, investigation, recovery and response capabilities of the Information and Telecommunications Systems vis-à-vis possible cyber attacks.

"To achieve a secure cyberspace, a National Cyber Security Policy will be promoted by developing an appropriate regulatory framework and fostering a Structure that brings together and coordinates all the institutions and agents with responsibilities in this area"

The strengthening of cyber security will provide the Public Authorities, the industrial and business sector, the scientific community and citizens in general with greater **confidence** in the use of ICT. For this purpose the public organisations responsible will work in coordination with the private sector and citizens themselves to guarantee the security and reliability of the systems that underpin the so-called Information Society.

Also, in defence of national interest, the National Cyber Security Policy will be aligned with initiatives similar to those of the countries in our neighbourhood and with the European and international organizations with responsibilities in this area, particularly the EU Cyber Security Strategy.

Finally, in order to ensure the protection of the systems and the resilience of the services of the Public Authorities and Critical Infrastructures, as well as the availability of reliable products, it will be necessary to bolster, give impetus to and strengthen the national cyber security research and development capabilities of the ICT.

In this connection Spain, continuing with its policy of technological diversification and neutrality, will endeavour to use components that are certified as conforming to internationally recognised standards.

The considerations of this overall objective will apply to the rest of the objectives.

OBJECTIVE I

To ensure that the Information and Telecommunications Systems used by the Public Authorities have an appropriate level of cyber security and resilience

A considerable part of the ICT systems of the Spanish Public Authorities, the information contained in them and the services they provide constitute strategic national assets.

It is therefore essential to foster the implementation of a coherent and comprehensive national framework for policies, procedures and technical standards that help ensure the protection of public information and its systems and services, and of the supporting networks. This framework will be a key to developing and implementing services that are increasingly secure.

"It is essential to foster the implementation of a coherent and comprehensive national framework for policies, procedures and technical standards that help ensure the protection of public information"

Adapting the systems of the Public Authorities to this reality involves establishing security services in them, improving and exercising their ability to prevent, detect, respond to and recover from incidents, developing new tools and keeping the legal system up to date.

Likewise, in addition to improving the capabilities of the military, Defence and intelligence systems, it is necessary to bolster the security of the strategic Information and Communication Systems, adapting them to the new risks and threats of cyberspace.

The Public Authorities will be actively involved in a process of continuous improvement with respect to protecting their ICT systems. The authorities are required to set an example in the management of cyber security.

OBJECTIVE II

To foster the security and resilience of the Information and Telecommunications Systems used by the business sector in general and the operators of Critical Infrastructures in particular

When applying the principle of shared responsibility, the Public Authorities must maintain close relations with the companies that manage Information and Telecommunications Systems relevant to national interests, exchanging knowledge in order to facilitate appropriate coordination between both and a mutual understanding of the cyber security environment.

"Ensuring the Protection of Spain's Technological Heritage"

In this connection special mention should be made of actions aimed at ensuring the Protection of Spain's Technological Heritage, which is taken to mean those tangible or non-tangible assets which underpin the intellectual and industrial property of the business sector, shape our present and condition future development.

It is also interesting to determine the impact that potential interruption or destruction of the networks and systems that provide essential services to society may have on Spain. As the private sector owns a good many of these systems, the measures adopted in cyber security must be aligned with the requirements laid down in the regulations on the Protection of Critical Infrastructures in order to achieve a comprehensive set of measures to be applied to the relevant sectors.

OBJECTIVE III

To enhance prevention, detection, reaction, analysis, recovery, response, research and coordination capabilities vis-à-vis terrorist activities and crime in cyberspace

"It is essential to strengthen international judicial and police cooperation, establishing appropriate instruments for collaboration and the exchange of information and the harmonisation of national legislation"

ICT are a means, an end or a combination of both, used by terrorist and criminal organisations to achieve their objectives. To this should be added the growing possibility of using cyberspace as an objective in itself to perpetrate attacks against essential services or Critical Infrastructures. In both cases it is necessary to bolster the prevention, detection, reaction, analysis recovery, response, investigation and coordination mechanisms relating to these kinds of crimes.

The police and judicial action of the State in cyber security matters must be adapted to the patterns of conduct and types of crime committed by terrorists and criminals in cyberspace, whose objectives – but not methods – usually coincide with traditional ones.

To effectively address these threats, which often extend beyond States' borders, it is essential to strengthen international judicial and police cooperation, establishing appropriate instruments for collaboration and the exchange of information and the harmonisation of national legislation, and developing and maintaining sound and effective regulations.

Likewise, it is necessary to foster citizen collaboration, facilitating procedures for the access to and transmission of information of interest to the police.

Success in combating terrorism and crime in cyber space requires putting in place the mechanisms needed to improve the capabilities of the police institutions and relevant judicial bodies.

OBJECTIVE IV

To raise the awareness of citizens, professionals, companies and Spanish Public Authorities about the risks derived from cyberspace

The Spanish Government, recognising the importance of building and maintaining confidence in the Information and Telecommunications Systems used by citizens, professionals, companies and public sector bodies, will undertake the information and sensitisation actions needed to ensure that they are all aware of the risks of operating in cyberspace and have knowledge of, and access to, tools that make its protection possible.

"Companies must be aware of the responsibility of ensuring the security of their systems, the protection of their clients' and suppliers' information and the reliability of the services they provide"

At the same time, companies must be aware of the responsibility of ensuring the security of their systems, the protection of their clients' and suppliers' information and the reliability of the services they provide. Maintaining consumer confidence is essential to the success of the digital economy. The same is true of the Public Authorities and their relationship with citizens.

Therefore, an essential function is to promote a sound cyber security culture which provides all actors with the necessary awareness and confidence to maximise the benefits of the Information Society and reduce to a minimum their exposure to the risks of cyberspace by adopting reasonable measures to guarantee the protection of their data and the secure connection of their systems and equipment.

The effective management of the risks derived from cyberspace must be built on a sound culture of cyber security. This requires users to be sensitive to the risks entailed by operating in this domain, and to be familiar with the tools for protecting their information, systems and services.

OBJECTIVE V

To gain and maintain the knowledge, skills, experience and technological capabilities Spain needs to underpin all the cyber security objectives

Given the strategic importance of security in cyberspace, an absolute priority is to have qualified personnel at all levels: government, management, operational, technical and judicial bodies.

"It is necessary to foster and effectively maintain R&D&I activity in cyber security"

Furthermore, it is important to foster and boost the technological capabilities required for reliable national solutions that enable systems to be adequately protected from different threats.

To achieve this confidence, it is necessary to foster and effectively maintain R&D&I activity in cyber security. For this purpose the group of agents involved in ICT must be appropriately coordinated, facilitating collaboration between companies and public research bodies and promoting projects for the evaluation and certification of security.

The qualification of the personnel in charge of the direction, management and implementation of cyber security is a fundamental objective, especially in the Public Authorities and Strategic and Critical Infrastructures of national interest. What is more, the use of verified security products is a significant additional element of protection.

OBJECTIVE VI

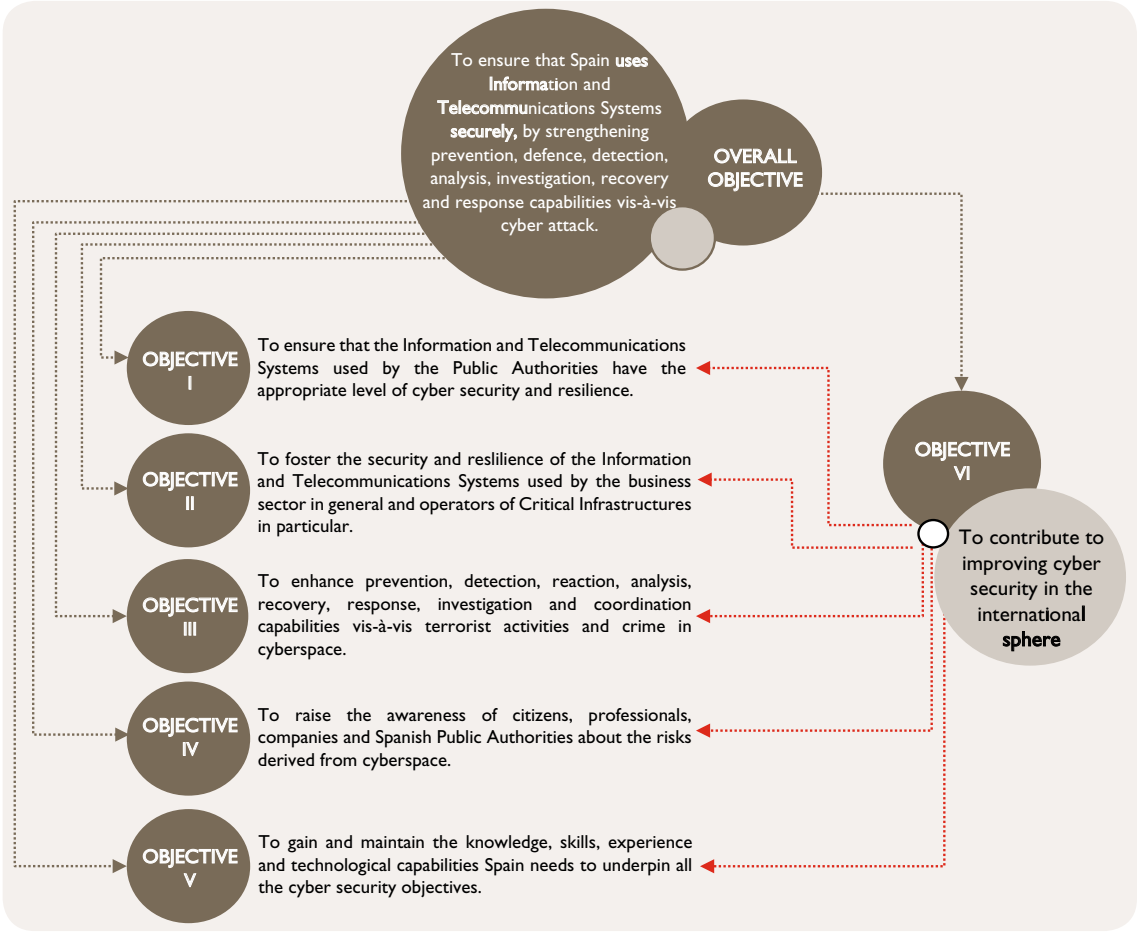
To contribute to improving cyber security in the international sphere

The development of a coordinated cyber security policy in the European Union and in the international Security and Defence organisations in which Spain takes part will be fostered and supported, and collaboration will be carried out in capacity building of States that so require through the development cooperation policy, helping them to implement a cyber security culture.

Cooperation will be fostered in the framework of the EU and with international and regional organisations such as the European Defence Agency (EDA), the European Union Agency for Network and Information Security (ENISA), the European Cybercrime Centre attached to EUROPOL, the United Nations (UN), the Organization for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), and the Organization for Economic Cooperation and Development (OECD), among others.

"The development of a coordinated cyber security policy in the European Union and the international Security and Defence organisations will be promoted and supported"

Together with the countries belonging to our strategic environment, efforts aimed at achieving a secure and reliable cyberspace will be promoted by strengthening international collaboration, creating confidence relationships for the exchange of essential cyber security information and data and the development of cooperation and development initiatives. Actions designed to promote the adoption of international cyber security standards and their progressive raising will likewise be carried out.


To ensure that Spain **uses Information** and **Telecommunications Systems securely,** by strengthening prevention, defence, detection, analysis, investigation, recovery and response capabilities vis-à-vis cyber attack.
OVERALL OBJECTIVE
OBJECTIVE I
To ensure that the Information and Telecommunications Systems used by the Public Authorities have the appropriate level of cyber security and resilience.
OBJECTIVE II
To foster the security and reslilience of the Information and Telecommunications Systems used by the business sector in general and operators of Critical Infrastructures in particular.
OBJECTIVE III
To enhance prevention, detection, reaction, analysis, recovery, response, investigation and coordination capabilities vis-à-vis terrorist activities and crime in cyberspace.
OBJECTIVE IV
To raise the awareness of citizens, professionals, companies and Spanish Public Authorities about the risks derived from cyberspace.
OBJECTIVE V
To gain and maintain the knowledge, skills, experience and technological capabilities Spain needs to underpin all the cyber security objectives.
OBJECTIVE VI
To contribute to improving cyber security in the international **sphere**

Lines of action of National cyber security

Chapter 4

Lines of action of National cyber security

Chapter 4
Lines of action of National cyber security

The **National Cyber Security Strategy** for achieving the above objectives is based on the following Lines of Action:

LINE OF ACTION 1

Capability to prevent, detect, respond to and recover from cyber threats

Increase prevention, defence, detection, analysis, response, recovery and coordination capabilities vis-à-vis cyber threats, placing particular emphasis on the Public Authorities, Critical Infrastructures, military and Defence capabilities and other systems of national interest.

The Spanish Government will adopt the relevant measures in this line of action, including:

- Broaden and improve capabilities to detect and analyse cyber threats in order to enable attack procedures and origins to be identified and the necessary intelligence to be gathered for a more effective defence and protection of national networks.
- Broaden and strengthen capabilities to detect and respond to cyber attacks directed against national, regional or sectorial targets, including citizens and companies.
- Guarantee the coordination, cooperation and exchange of information between the Central Government, the Autonomous Regions, Local Authorities, the private sector and the EU and international bodies with responsibilities in this field in order to ensure continuous awareness raising, training and response capability through the System for the Exchange of Information and Reporting of Incidents.

- Ensure the cooperation of organisations with responsibilities in cyber security, especially between the Government CERT of the National Cryptology Centre (CCN-CERT), the Armed Forces Joint Cyber Defence Command (MCCD), and the CERT for Security and Industry. The CERTs of the Autonomous Regions, those of private institutions and other relevant cyber security services must be coordinated with the above-mentioned depending on the responsibilities of each one, establishing the appropriate instruments for this purpose.

- Develop prevention and detection instructions and keep them updated, including procedures for responding to crisis situations and specific contingency plans vis-à-vis cyber security incidents that are national in scope, ensuring they are integrated into the National Security System.

- Develop and implement a Programme of Simulation Exercises for Cyber Security Incidents, in order to assess and improve the actions carried out in this field.

- Broaden and continuously develop the Cyber Defence capabilities of the Armed Forces allowing them to appropriately protect their Networks and Information and Telecommunications Systems, as well as other systems which affect National Defence. The implementation of the Joint Cyber Defence Command will be consolidated and it will be encouraged to cooperate with the different bodies with the capability to respond to cyber incidents in aspects of common interest.

- Boost military and intelligence capabilities to deliver a timely, legitimate and proportionate response in cyberspace to threats or aggressions that can affect National Defence.

LINE OF ACTION 2

Security of the Information and Telecommunications Systems that underpin the Public Authorities

Ensure the implementation of the National Security Scheme, strengthen detection capabilities and improve the defence of classified systems.

This line of action covers the initiatives needed to protect the Information Systems of the Central Government, the Autonomous Regions, the Local Authorities and bodies related or attached to them, as well as the Information and Telecommunications Systems and infrastructures common to them all.

For this purpose, the Spanish Government will adopt the following measures, among others:

- Ensure the full implementation of the National Security Scheme and establish the necessary procedures for being regularly apprised of the state of the main security variables of the systems involved.
- Broaden and improve the capabilities of the Government CERT CCN-CERT and particularly of its Detection and Early Warning Systems.
- Strengthen the security structures and surveillance capability of Information Systems, particularly those that handle classified information.
- Optimise the model whereby the Spanish Government bodies interconnect with public voice and data networks, maximising their efficiency, availability and security.
- Strengthen the implementation and security of the common and secure infrastructure in the Spanish public administration system (SARA network), boosting its use and its security and resilience capabilities.
- Develop new secure horizontal services in accordance with the guidelines of the Directorate for Information and Communication Technologies of the Central Government, the body responsible for coordinating, directing and rationalising the use of ICT in the Central Government.
- Step up national activities aimed at developing and evaluating products, services and systems in order to obtain their certification by specifically supporting those which underpin national security needs.
- Give impetus to the creation, dissemination and application of Best Practices in Cyber Security matters within the domain of the Public Authorities.

LINE OF ACTION 3

Security of the Information and Telecommunications Systems that underpin Critical Infrastructures

Foster the implementation of the regulations on the Protection of Critical Infrastructures and of the necessary capabilities for protecting essential services.

It is necessary to increase the resilience of Spain's Critical Infrastructures to prevent potential disruptions to the normal functioning of the essential services, which could affect Spanish people's daily activity.

In this connection, the Spanish Government will adopt the following measures among others:

- Ensure the implementation of the regulations on the Protection of Critical Infrastructures in order to achieve a security that embraces both physical and technological aspects. To this end the incorporation of suitable cyber security measures into the different plans established will be evaluated.
- Broaden and improve the capabilities of the CERT for Security and Industry, boosting collaboration and coordination with the National Centre for the Protection of Critical Infrastructures, with the different bodies with the capability to respond cyber security incidents and with the operational units of the State Law Enforcement Agencies.
- Encourage private-sector involvement in the Programmes of simulation Exercises for Cyber Security incidents.
- Develop simulation models that allow the interdependence of the different Critical Infrastructures and the risks accumulated by them to be analysed.

LINE OF ACTION 4

Capability to investigate and prosecute cyber terrorism and cyber crime

Strengthen capabilities to detect, investigate and prosecute terrorist and criminal activities in cyberspace on the basis of an effective legal and operational framework.

This line of action is focused on combating terrorism and crime that operate in cyberspace, which plays a dual role as both an instrument that facilitates their activities and a direct target of their action. This concept also includes organisations which use technology for their own financing or for profit, making crimes and money-laundering possible.

The Spanish Government will take relevant measures in this line of action, among them:

- Incorporate into the Spanish legal framework solutions to problems that arise in connection with cyber security in order to establish types of criminal offences and the work of the departments with responsibilities in this area.
- Broaden and improve the capabilities of the bodies responsible for investigating and prosecuting cyber terrorism and cybercrime and ensure that these capabilities are coordinated with activities in the field of cyber security by exchanging information and intelligence through the appropriate channels of communication.
- Strengthen international police cooperation and foster citizen collaboration, establishing instruments for the exchange and transmission of information of interest to the police.
- Ensure that legal professionals have access to information and resources that provide them with the necessary level of knowledge in the judicial field to apply the associated legal and technical framework more effectively. In this connection cooperation with the General Council of the Judiciary, the State Lawyer's Office, the State Prosecutor's Office, the Computer Crime Prosecutor's Office and the General Council of Spanish Lawyers is particularly important.

LINE OF ACTION 5

Security and resilience of ICT in the private sector

Boost the security and resilience of infrastructures, networks, products and services using instruments of public-private cooperation.

This line of action is designed to improve the security and resilience of networks, products and services used by the industrial sector in developing its activity by strengthening public-private collaboration with the industrial sector and in particular with the ICT security sector.The participation of professional Colleges and Associations, among others, will be valued.

The Government will develop the following measures, among others:

- Foster cooperation between the public and private sectors, promoting the exchange of information on vulnerabilities, cyber threats and their possible consequences, especially in relation to protecting systems of national interest.
- Promote cooperation with the industry sectors and cyber security services in order to jointly improve detection, prevention, response and recovery capabilities vis-à-vis the security risks of cyberspace, giving impetus to the active involvement of service providers and the development and adoption of codes of conduct and good practice.
- Foster the development of standards in cyber security through the national and international standardisation and certification bodies and institutions, and promote their adoption.

LINE OF ACTION 6

Knowledge, skills and R&D&I

Promote the training of professionals, give impetus to industrial development and strengthen the R&D&I system in cyber security matters.

This line of action envisages initiatives that need to be undertaken in order to achieve and maintain an appropriate level of training in cyber security for professionals (knowledge and skills) and to boost Spanish industry and R&D&I. The Spanish Government will:

- Develop a Framework for Cyber Security Knowledge in the technical, operational and legal fields.
- Extend and broaden talent recruitment, advanced research and training programmes in cyber security in cooperation with Universities and specialised centres.
- Establish mechanisms that allow the cyber security priorities and demands of the public authorities to be identified at an early stage in order to incorporate them into previous initiatives.
- Foster the industrial development of cyber security products and services through instruments such as, among others, the State Plan for Scientific and Technical Research and Innovation and initiatives for supporting its internationalisation.
- Promote the national coordination and stimulation of the industrial and cyber security services sector in order to improve competitiveness, internationalisation, identification of opportunities, elimination of barriers and regulatory guidance, among other activities.
- Promote cyber security certification activities in accordance with the internationally recognised norms and standards, incorporating these criteria into processes for the development and acquisition of products or systems.
- Promote models and techniques for analysing cyber threats and measures for protecting products, services and systems, as well as their specification, evaluation and certification.

LINE OF ACTION 7

Cyber security culture

Raise the awareness of citizens, professionals and companies about the importance of cyber security and the responsible use of new technologies and the services of the Information Society.

The Spanish Government will adapt, foster or develop related measures, including:

- Give impetus to sensitisation activities to ensure that citizens and companies have access to information about vulnerabilities and cyber threats and about the best way of protecting their technological environment.
- Promote the development of Cyber Security Awareness-Raising programmes in collaboration with public- and private-sector agents, fostering the necessary coordination and rationalisation of efforts through bodies with responsibilities in this field.
- Foster the mechanisms for supporting companies and professionals in the secure use of ICT, bolstering knowledge in security matters, promoting the adoption of tools, the dissemination of regulations and the use of good practices.
- Advise on and support the development of education modules for sensitisation in cyber security, aimed at all levels of teaching.

LINE OF ACTION 8

International commitment

Promote a secure and reliable international cyberspace, in support of national interests.

Technological globalisation and its opportunities and risks make it necessary to align the initiatives of all countries that pursue a secure and reliable cyberspace. These international efforts must envisage the drafting and adoption of global standards, the expansion of the capabilities of the international legal system and the development and promotion of best practices in assessing the situation, warning and response to cyber incidents.

Within this line of action, the Spanish Government will develop the following measures, among others:

- Enhance Spain's presence at international and regional organisations and forums on cyber security, supporting and taking an active role in the various initiatives and coordinating the position of the national agents involved.
- Promote legislative harmonisation and international judicial and police cooperation in combating cybercrime and cyber terrorism, supporting the negotiation and adoption of international conventions on these matters.
- Foster the signing of agreements within international organisations and with principal partners and allies, in order to strengthen cooperation in cyber security and develop a coordinated approach for combating cyber threats.
- Give impetus to the establishment of international channels of information, detection and response.
- Promote the coordinated participation of public institutions and the private sector in international exercises and simulations.
- In the scope of the EU, collaborate in harmonising national legislations, implementing the EU Cyber Security Strategy and promoting an international policy in cyberspace.
- Foster cooperation with NATO in Cyber Defence, particularly with respect to responding to cyber incidents and exchanging technical information on threats and vulnerabilities, while promoting actions within the Organization aimed at highlighting Cyber Defence as one of its priorities.

LINE OF ACTION		CONTENT
1	**Capability to prevent, detect, respond to and recover from cyber threats**	Increase prevention, defence, detection, analysis, response, recovery and coordination capabilities vis-à-vis cyber threats, placing particular emphasis on the Public Authorities, Critical Infrastructures, military and Defence capabilities and other systems of national interest.
2	**Security of the Information and Telecommunications Systems that underpin the Public Authorities**	Ensure the implementation of the National Security Scheme, strengthen detection capabilities and improve the defence of classified systems.
3	**Security of the Information and Telecommunications Systems that underpin Critical Structures**	Foster the implementation of the regulations on the Protection of Critical Infrastructures and of the necessary capabilities for protecting essential services.
4	**Capability to investigate and prosecute cyber terrorism and cybercrime**	Strengthen capabilities to detect, investigate and prosecute terrorist and criminal activities in cyberspace on the basis of an effective legal and operational framework.
5	**Security and resilience of ICT in the private sector**	Boost the security and resilience of infrastructures, networks, products and services using instruments of public-private cooperation.
6	**Knowledge, skills and R&D&I**	Promote the training of professionals, give impetus to industrial development and strengthen the R&D&I system in cyber security matters.
7	**Cyber security culture**	Raise the awareness of citizens, professionals and companies about the importance of cyber security and the responsible use of new technologies and the services of the Information Society.
8	**International commitment**	Promote a secure and reliable international cyberspace, in support of national interests.

Cyber security in the National Security System

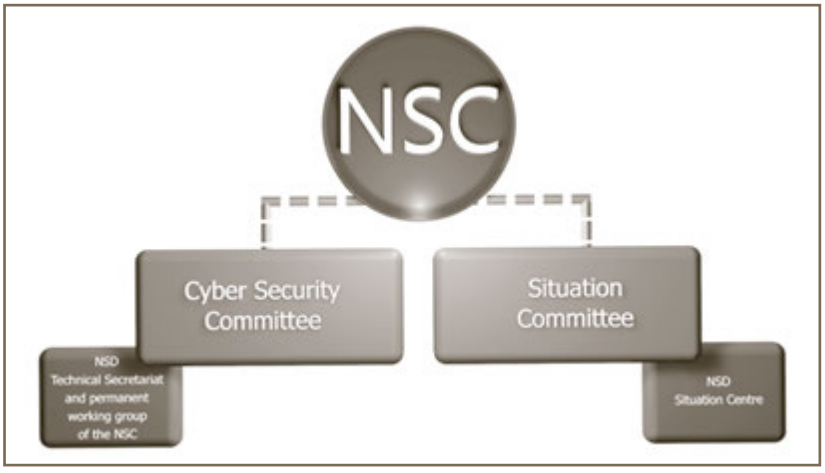
Chapter 5

Cyber security in the National Security System

Chapter 5
Cyber security in the National Security System

The comprehensive vision of cyber security enshrined in this Strategy, the detected risks and threats that affect it and the stated objectives and lines of action for providing an appropriate joint response to preserving cyber security in accordance with the principles that underpin the National Security System explain the need for an organisational structure tailed to these purposes, which will consist of the following components under the direction of the Prime Minister:

A. The National Security Council;
B. The Specialised Cyber Security Committee;
C. The Specialised Situation Committee, which is unique to the whole National Security System.



Organisational structure of cyber security

ORGANISATIONAL STRUCTURE OF CYBER SECURITY

a) National Security Council:

The National Security Council, which is the Delegated Commission of the Government for National Security, assists the Prime Minister in directing the National Security Policy.

b) Specialised Cyber Security Committee:

The Specialised Cyber Security Committee will support the National Security Council in performing its functions, particularly in assisting the Prime Minister in directing and coordinating the National Security Policy in the field of cyber security. It will furthermore strengthen coordination, collaboration and cooperation relations among the different Public Authorities with responsibilities in cyber security matters and between the public and private sectors, and will facilitate the Council's decision making by analysing, studying and proposing initiatives at both the national and the international levels.

The composition of the Specialised Cyber Security Committee will reflect the spectrum of areas covered by the departments, bodies and agencies of the Public Authorities with responsibilities in cyber security matters, in order to coordinate actions that need to be addressed jointly with the aim of raising security levels.

Other relevant private-sector actors and specialists whose contribution is deemed necessary may take part in the Committee.

In compliance with its functions, the Specialised Cyber Security Committee will be supported by the National Security Department as a Technical Secretariat and permanent working body of the National Security Council.

c) Specialised Situation Committee:

The Specialised Situation Committee will be convened to manage crisis situations in the field of cyber security which, on account of the significant cross-cutting nature or the extent and impact of their effects, exceed the effective response capabilities of the usual mechanisms, while always respecting the responsibilities assigned to the different Public Authorities in order to guarantee an immediate and effective response through a single body in charge of the strategic and political direction of the crisis.

The Specialised Cyber Security Committee and the Specialised Situation Committee will act in a complementary manner, each in its own area of responsibility, but under the same strategic and political direction of the National Security Council chaired by the Prime Minister.

"The Specialised Cyber Security Committee and the Specialised Situation Committee will act in a complementary manner, each in its own area of responsibility, but under the same strategic and political direction of the National Security Council chaired by the Prime Minister"

The Specialised Situation Committee will be supported by the Situation Centre of the National Security Department in order to ensure it is interconnected with the operational centres involved and to provide an appropriate response in crisis situations, facilitating their monitoring and control and the transmission of decisions.

To ensure the effective fulfilment of its functions of supporting the Specialised Situation Committee, the Situation Centre of the National Security Department may be reinforced with specialised personnel from ministerial departments or bodies with responsibilities in this area, who will make up the specific Coordination Cell in the field of Cyber Security.

IMPLEMENTATION

The setting up of the Specialised Cyber Security Committee and the Specialised Situation Committee and the harmonisation of their functioning with the existing bodies will be carried out gradually through the approval of the necessary legal provisions and readjustments of the existing ones, in order to achieve the coordinated and efficient functioning of these components of the National Security System.

www.lamoncloa.gob.es