National Cyber Security, a commitment for everybody

The need to evolve from a reactive culture
to one of prevention and resilience

SCSI
Spanish
Cyber Security
Institute

National Cyber Security, a commitment for everybody

The need to evolve from a reactive culture to one of prevention and resilience

Published in June 2012

Authors
Enrique Fojón Chamorro
Dr. José Ramón Coz Fernández
Ramón Miralles López
Samuel Linares Fernández

Coordinator
Miguel Rego Fernández

Editors
Gianluca D'Antonio
Nathaly Rey Arenas

Translated and reviewed by
Juan Miguel Velasco López-Urda

Index

1. Introduction

1. Introduction

Information and Communications Technology (ICT) have contributed to the welfare and progress of societies, in such a way that a large part of public and private relations depend on these technologies. Over time and throughout evolution risks have emerged that have made it necessary to manage the ICT security.

Initially cyber security was concerned with protecting information reactively, although subsequently it has evolved towards a proactive position which identifies and manages risks that threaten cyber space.

Within the framework of the SCSI (Spanish Cyber Security Institute) and ISMS Forum, a study was carried out which developed an approach to concepts of cyber space and cyber security, to known risks and threats, to the existing management in Spain, and to the need to develop a National Cyber Security System to promote the integration of all players and instruments involved, both public and private, and to make good use of the opportunities presented by new technologies, as well as to address the challenges that they present. The main conclusions obtained from the study are summarised in this document.

Organisation of the document

This document is divided into 15 Sections, including the present introductory Section.

Section 2 discusses the SCSI, Spanish Cyber Security Institute, highlighting its mission, values and principle activities.

Section 3 presents the study, explaining the need to evolve from a reactive culture to a culture of prevention and resilience, as well as the need to progress towards a comprehensive security model.

Section 4 addresses an approach to the concepts of cyber space and cyber security.

Section 5 identifies the strategic importance of cyber space as a new dimension of the operating environment.

Section 6 analyses the risk status of cyber space, describing the principle objectives of cyber attacks and the main cyber threats, along with the types and authors of these attacks.

Section 7 summarises the current status of cyber security at a national level.

Section 8 carries out a diagnosis of National Cyber Security, and lists the main causes that have prevented us from reaching a level of cyber security focused on the status of the risk.

Section 9 analyses why we need a National Cyber Security Strategy.

Section10 lists and defines the main functions that should be attributed to National Cyber Security.

Section 11 lists and discusses the enablers of cyber security, who will make it possible to operate cyber security on a national level.

Section12 proposes an organisational structure which allows National Cyber Security to be run, controlled and managed.

Section 13 sets out the main objectives for National Cyber Security for the period between 2012 and 2015.

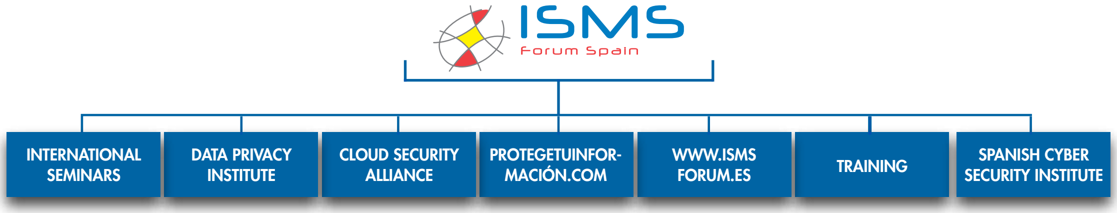
Section 14 lists a set of actions that will allow the objectives described in Section 13 to be achieved.

Finally, Section 15 sets out the main conclusions of the study.

2. All about the SCSI

2. All about the SCSI

In November 2011, within the scope of the **ISMS Forum Spain,** the **Spanish Cyber Security Institute** was conceived, hereinafter SCSI.



INTERNATIONAL SEMINARS

DATA PRIVACY INSTITUTE

CLOUD SECURITY ALLIANCE

PROTEGETUINFORMACIÓN.COM

WWW.ISMSFORUM.ES

TRAINING

SPANISH CYBER SECURITY INSTITUTE

2.1. Mission of the SCSI

The mission of SCSI is to conduct and publish studies, as well as to encourage debates and the exchange of ideas and knowledge, regarding the dependence that the socio-economic development of Spain has on Information and Communications Technology (ICT), and thus create a state of awareness of the need for cyber security in order to control and manage the risk status that this dependency generates.

2.2. Vision of the SCSI

The SCSI aims to become a meeting point of bodies, both private and public, and for professionals related to the practices and technologies associated with cyber security, as well as becoming the national reference for their publication for the whole of Spanish society.

2.3. Main activities of the SCSI

SCSI's main activities are:

1. Studies and publications on cyber security.
2. Dialogue with national and international authorities and regulators.
3. Cyber programmes - education/cyber awareness.
4. Holding events in relation to cyber security.

3. Evolving towards a Comprehensive Security Model

3. Evolving towards a Comprehensive Security Model

Security, in all its dimensions and spheres, is the first responsibility of any government. Traditionally security has been primarily handled by the defence sector, since the main risks to the survival and integrity of nations have been of a military nature. However the emergence of new players and risks of a heterogeneous nature have caused many states within our geopolitical environment to carry out an extensive review and transformation of their security and defence policies.

This review and transformation is due to a change in the guiding framework for security, driven mainly by the following:

1. **The security of states is no longer restricted to the defence of their borders and sovereignty;** it also extends to ensuring the welfare of their societies against new risks.
2. **Globalization benefits trans-border risks and threats** such as terrorism, proliferation of weapons of mass destruction and cyber crime, among others.
3. **The emergence of players from different locations and who have different motives,** as well as the desire to challenge the rule of law and international order, with the capacity to act within any security dimension, makes it more difficult to attribute responsibility for the assault, and therefore reduces the capacity of the State to respond to aggression.

Moreover, this new security model requires that the risks be identified beforehand. In other words, it is necessary to evolve from the current **reactive culture** to one of **prevention and resilience.**

The phenomenon of **globalization,** mentioned above, brings with it the freedom of movement of people, goods, services and capital, fostering an evolution towards **"linear security"** where the separation between domestic and overseas security, defence and domestic policy, and between the public and private, is no longer applicable.

Therefore, **national security** is no longer identified as a type of security or defence, it is not the responsibility of one particular ministry, nor is it separated into a domestic or overseas context, or a reactive or preventive approach, rather it fully includes all of the above.

The emergence of cyber space and the need to secure it has meant that the evolution in the security model has accelerated.

4. Cyber space and its security

4. Cyber space and its security

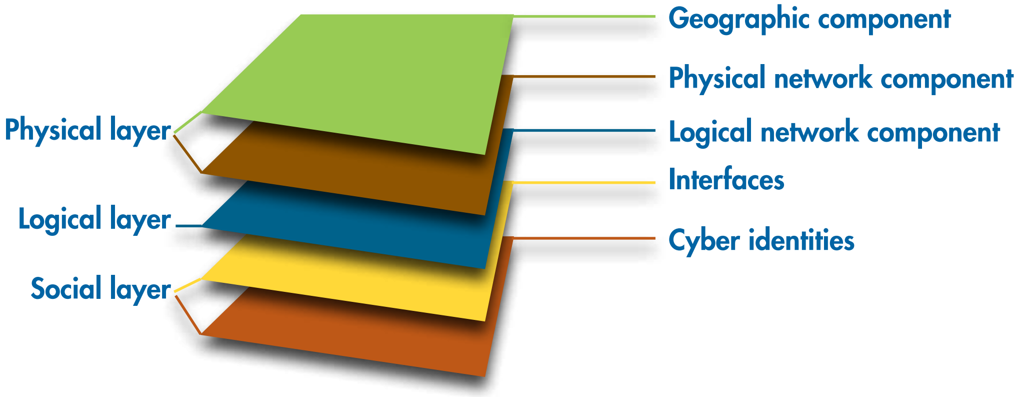
Cyber space is now an essential part of our societies and economies, and may even become a determining factor in the evolution of cultures and maybe their convergence.

4.1. An approach to the concept of cyber space

Cyber space is the set of means and procedures based on Information and Communications Technology (TIC) which is configured for the provision of services. Cyber space consists of hardware, software, the Internet, information services and systems of control that ensure the provision of services that are essential for the socio-economic activity of any nation, especially those that are connected to its critical infrastructure.

Cyber space is structured on three overlapping layers: **a physical layer, a logical layer** and **a social layer,** which are in turn comprised of 5 components (see diagram): geographic component, physical network component, logical network components, people and cyber identities.

Cyber space: Layers and Components



The **physical layer** encompasses the geographic component and the physical networks component. The geographical component refers to the physical location of the elements of the physical networks component. The physical network component is made up of hardware and infrastructure that support the networks and their physical connectors (cabling, encoders, routers, servers, computers, etc...).

The **logical layer** is formed of the logical networks component, these are logical connections that exist between the nodes of the networks, a node being any device that is connected to the communications and IT systems network.

The **social layer** is made up of components of people and cyber identity. The people component is formed of the people who interact with cyber space. The relationship between people and cyber identities may be from 1 to n or from n to 1, meaning that a person may have one or more cyber identities and a cyber identity may be used by one or more persons. These cyber identities may be real or spoofed, which allows the user to enjoy certain anonymity and makes it difficult to prosecute criminal conduct that takes place in cyber space. cyber identities are formed by, among other things, email accounts, network user accounts and social media profiles.

4.2. Cyber security

Previously cyber security followed an ***information security*** approach which only protected information against unauthorised access, use, disclosure, disruption, modification and destruction.

Currently this approach is evolving towards cyber space risk management ***(Information assurance)*** where cyber security consists of the application of an analysis and management process for risks associated with use, processing, storage and transmission of information and data, as well as risks associated with the systems and processes used, based on internationally accepted standards.

One of the reasons for the adoption of this new approach is the characterisation of the cyber space of a certain entity as an ICT system which provides services in a way that allows system security to be achieved when it is in a state of known and controlled risk. Actually, both approaches, information security and information assurance, are different but complementary, and are very often wrongly used without distinction.

Moreover, the cyber security of a nation requires that at least two dimensions be proposed:

1. The protection of goods, assets, services, rights and freedoms, within state jurisdiction;
2. And the responsibility regarding cyber security which is shared with other states, bilaterally or by means of supranational bodies.

The challenge is to ensure that the aggregation of partial solutions implemented by States, even if done in a coordinated manner, solves global problems created by technologies that break down borders. Cyber space is continually growing and rapidly evolving, reaching a capillarity which enables social, economic and cultural relationships and dependencies, which are fundamental to the development and growth of our country, to be sustained.

In summary, cyber security should be formulated proactively as an on-going process of analysis and management of risks associated with cyber space.

5. Cyber space: The new dimension of the operating environment

5. Cyber space: The new dimension of the operating environment

Some of our key partners have already formally identified cyber space as a new dimension of the operating environment. Therefore they are equipping their Armed Forces with the cyber capabilities necessary for the undertaking of their tasks.

The Armed Forces do not only depend on ICT and IT systems for communicating, directing and controlling operations, coordinating conflicts, obtaining and distributing information in relation to intelligence, carrying out surveillance and reconnaissance, among other military activities; rather they are also using these systems for transforming the way that these actions are planned and executed. At the same time adversaries of any kind (nations, criminal groups or terrorists, etc.) have access to and may use the same technologies in a completely singular and innovative way.

Given that the Armed Forces are increasingly dependent on electromagnetic resources and IT networks, which are in a continual process of convergence, a cyber battlefield is emerging. Since the technology that allows the communication and processing of information changes so quickly, the Armed Forces must constantly evaluate which aptitudes and capacities are necessary in order to achieve, conserve and take advantage of this emerging battlefield.

The way in which the cyber space technologies are integrated and are employed, in accordance with the operating circumstance of each scenario, will significantly affect the development and end result of military operations. While it is important to stay up-to-date with regard to the knowledge and the application of ICT, it is also important to establish a comprehensive approach to all aspects of cyber operations and to be able to gain an advantage by combining and adapting them to the operating conditions of any given moment. As with the other dimensions of the operating environment (land, sea, air, space), achieving mastery in cyber space implies simultaneously progressing in two aspects of operations: obtaining and maintaining superiority.

Although employing emerging technologies before one's adversary does so provides a great advantage, the vulnerabilities and dependencies generated from implementation in its own networks, systems and sensors should also be taken into account and mitigated. It will probably be even more important to disable, interrupt and cancel out the same capabilities when they are in the hands of our adversaries. To this end the Armed Forces must integrate their capacities from one principle, converting them into elements of one same dimension within modern operations. However, if said integration is not achieved, then at best the progress of operations will not be equal, and could also lead to operational failures.

The attendance and participation in this operating space by the security bodies and forces, together with civil initiatives by key organisations within a national security context, shall also have a specific weight on the modus operandi, and therefore mechanisms should be articulated that allow, not only the fluid exchange of information among the armed forces, but also in certain situations of close collaboration.

6. The risk status of cyber space

6. The risk status of cyber space

The rapid evolution of Information and Communications Technology (ICT) is increasing the speed, capacity, flexibility, efficiency and usefulness of the current networks and systems, both within the civil and military scope. These technologies are changing the way in which people interact between themselves and with their environment.

This continual and accelerated evolution of the ICT has led to attacks becoming more and more sophisticated and numerous, leading to a cyber space that is ever more hostile, forcing those responsible for National Cyber Security to adopt the most up-to-date technical and human means in order to address the threats and their possible impacts.

The main objectives of cyber attacks, the main cyber threats, and the authors of cyber attacks are described below.

6.1. Objectives

The objectives of cyber attacks are classified into three major groups:

- **Governments**
- **Private sector.** The private sector includes operators of Critical Infrastructures.
- **Citizens**

6.2. Threats

The main threats associated with cyber space can be classified into two major groups:

- **Threats against information**
- **Threats against ICT infrastructures**

The threats against information are those that cause the loss, miss-handling, disclosure or misuse of information. Among these threats are:

- Espionage. Within this category all varieties of espionage are included, from state espionage to industrial espionage.
- Theft and publication of classified or sensitive information.
- Theft and publication of personal data.
- Digital identity theft.
- Fraud.
- Advanced Persistent Threats (APT).

Threats against ICT infrastructure are those that cause the temporary, partial or total interruption of certain services or systems.

Among these threats are:

- Attacks against critical infrastructures.
- Attacks against networks and systems.
- Attacks against internet services.
- Attacks against industrial networks and control systems.
- Malware infection.
- Attacks against networks, systems or services through third parties.

6.3. Authorship

Cyber attacks may be classified, according to their authorship and impact, in accordance with the following categories:

- **State sponsored attacks.** Real world or physical conflict has extended to the virtual world of cyber space. In recent years cyber attacks have been detected against the critical infrastructures of countries and against very specific but equally strategic objectives. Some examples that are known to many sections of the public are the cyber attack of Estonia in 2007, which resulted in the temporary disabling of much of the Baltic country's critical infrastructures, the cyber attack by Russia against Georgia in 2008 as a prelude to the ground invasion, the Stuxnet cases with cyber attacks against SCADA systems, Duqu with cyber attacks against industrial organisations, the cyber attacks suffered by the classified networks of the United States Government at the hands of hackers based on Chinese territory, and the recent discovery of Flame. Likewise, in recent years it has been detected that some states have invested large amounts of economic, technical and human resources in the development of Advanced Persistent Threats (APT) which attack aggressively and choose very specific goals in order to maintain a constant presence within the networks of the victims. The APT attacks are very difficult to detect due to the fact that they use components and techniques that are especially designed to infiltrate their objectives and remain there without being detected.

- **Attacks sponsored by private organisations.** The objective of many private organisations is to obtain industrial secrets from other organisations or governments. This type of attack, on many occasions, is executed with government support making equal use of APTs.

- **Terrorism, political and ideological extremism.** Terrorists and extremist groups use cyber space to plan and publish their actions and acquire recruits to carry them out. These groups now recognise the strategic and tactical importance of cyber space for their interests. Social media and forums have become the main instrument used by terrorists.

- **Attacks by groups of organised crime.** Organised crime gangs (cyber gangs) have started to carry out their activities in cyber space, exploiting the possibility of anonymity that this sphere offers. The objective of these types of gangs is to obtain sensitive information for the subsequent fraudulent use thereof and for significant economic gains.

- **Hacktivism.** During 2011, hacktivism has become one of the major threats to governments and organisations. The principles of this movement are anonymity and the free distribution of information through cyber space, essentially through the Internet. The hacktivists are grouped in a decentralized manner using the under-ground to communicate and plan their actions. Among these groups are Anonymous and Luzsec, but these are not the only ones. Their mission is to 'attack' the cyber space that represents people, companies or organisations that violate any of their principles or interests. This implies that the cyber space of governments of the majority of countries around the world, banks, telecommunications companies, suppliers of critical infrastructure, internet service providers, and ultimately all of cyber space, are susceptible to denial of service attacks (DDoS) or to being hacked with the main objective of stealing sensitive information which will subsequently be distributed on the Internet for free access.

- **Low profile attacks.** These types of attacks are normally executed by people with certain ICT knowledge which allows them to carry out cyber attacks of a highly heterogeneous nature and for fundamentally personal reasons.

- **Personal privileged access attacks (insiders).** This group poses one of the greatest threats to the cyber space security of nations and companies as they are often an integral part of all the attacks outlined above. From a spy infiltrated by a State, or an employee working for gangs of terrorists or cyber criminals, to disgruntled employees; these can all be considered insiders.

Below, the following table sets out the players, objectives, authorship and types of cyber attacks.

Cyber space risk status summary

AUTHORSHIP	OBJECTIVES		
	Government	Private sector	Citizens
State sponsored attacks	Espionage, attacks against critical infrastructure, APT.	Espionage, attacks against critical infrastructure, APT.	
Attacks sponsored by the private sector	Espionage.	Espionage.	
Political and ideological terrorists, extremism	Attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems.	Attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems.	
Hacktivists	Theft and publication of classified or sensitive information, attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems.	Theft and publication of classified or sensitive information, attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems.	Theft and publication of personal data.
Organised crime	Espionage.	Digital identity theft and fraud.	Digital identity theft and fraud.
Low profile attacks	Attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems.	Attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems.	
Personal privileged access attacks (insiders)	Espionage, attacks against critical infrastructure, attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems, theft and publication of classified or sensitive information, malware infection, APT.	Espionage, attacks against critical infrastructure, attacks against networks and systems, attacks against internet services, malware infection, attacks against third-party services, networks and systems, theft and publication of classified or sensitive information, APT.	

	High
Impact	Medium
	Low

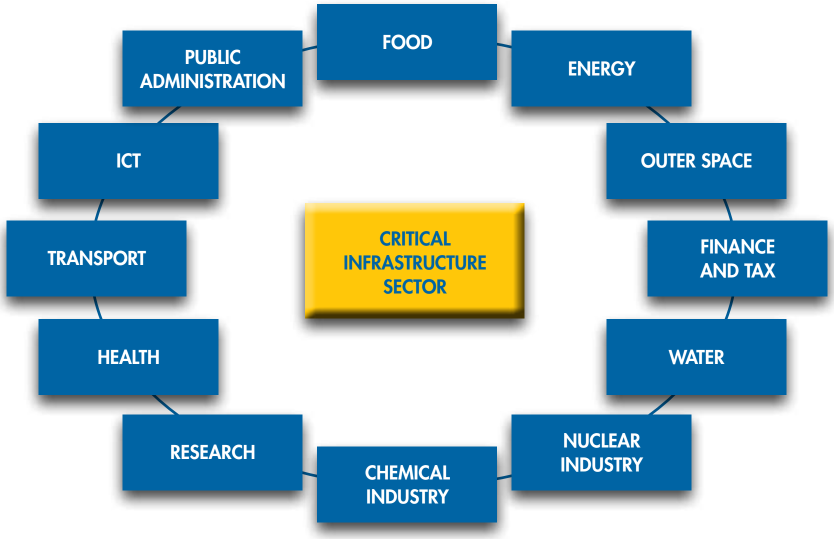
7. Cyber security in Spain: The current status

7. Cyber security in Spain: current status

Spain has 31 million Internet users, representing an Internet penetration rate of 65.5% in respect of the national population. This statistic places Spain at number 49 at international level with regard to the penetration rate of information society services (email, social media sites, e-business).

It is necessary to identify which assets in Spain are dependent on cyber space, what regulation exists, which are the organisations with functions and responsibilities regarding this matter, and who are the participants. The defence of our cyber space covers all conceivable assets and players, but should focus primarily on the defence of critical infrastructure, business, and individual rights and freedoms. The critical infrastructure in Spain is grouped into the following 12 sectors:

Sectors of critical infrastructure



In any of these sectors, the degree of penetration of cyber space, both for internal management and for service provision, reached its critical level a long time ago. Any contingencies that might affect any of the key assets belonging to any of the 12 strategic sectors could compromise national security. With regard to the Spanish business community, the vast majority of **large companies** have an internal organisation which is mature enough to enable them to implement the activities and actions that are part of information security practices.

In the case of **small to medium size enterprises and self-employed entities** (more than 99% of the Spanish business community), the lack of awareness and e-education, as well as a lack of financial and human resources, impede the proper implementation of cyber security measures, limiting the focus to ICT activities.

Government players with responsibility for cyber security

Bodies	Administration	Ministry / Scope	Cyber security competencies
INTECO	Central	Ministry of Industry	Operation, analysis, incident response, international relations.
CCN	Central	Ministry of the Presidency	Operation, analysis, incident response, regulations, international relations.
CNPIC	Central	Ministry of the Interior	Operation, analysis, incident response, regulations, international relations.
REDIRIS	Central	Ministry of Industry	Operation, analysis, incident response.
Police Computer Crime Unit	Central	Ministry of the Interior	Operation, analysis, incident response.
Computer Crime Unit of the Guardia Civil	Central	Ministry of the Interior	Operation, analysis, incident response.
Spanish Data Protection Agency	Central	Ministry of Justice	Control authority and regulator (involves analysis of incidents and sanctions).
Ministry of Defence (various bodies and organisations)	Central	Ministry of Defence	Operation, analysis, incident response, regulation.
IT Crime Unit of the Police Force of Catalonia	Regional	Department of the Interior (Regional Government of Catalonia)	Operation, analysis, incident response.
IT Crime Unit of the Police Force of the Basque Country	Regional	Council of the Interior (Basque Country)	Operation, analysis, incident response.
CSIRT-CV (Community of Valencia)	Regional	Regional	Operation, analysis, incident response.
CESICAT (CERT - Catalonia)	Regional	Regional	Operation, analysis, incident response, advice and training.
CERT – Andalusia	Regional	Regional	Operation, analysis, incident response.
Community of Madrid Data Protection Agency	Regional	Regional	Control authority and regulator (involves analysis of incidents and sanctions).
Catalonian Data Protection Agency	Regional	Regional	Control authority and regulator (involves analysis of incidents and sanctions).
Basque Data Protection Agency	Regional	Regional	Control authority and regulator (involves analysis of incidents and sanctions).

The powers in relation to the management of cyber security are distributed among a set of organisations and institutions, which depend on different central government ministries as well as on regional governments. Among the most relevant are the following:

- The **National institute of Technology and Communication (INTECO),** dependent on the Ministry of Industry, Tourism and Commerce, is responsible for the management, via its CERT, of cyber space defence of Spanish SMEs and citizens in their domestic environment.

- The **National Cryptologic Centre (NCC),** under the National Intelligence Centre (CNI), which has among its missions the management of cyber space security, is dependent on any of the three levels of government: national, regional and local. The CCN-CERT (Response Capacity against Security Incidents) is a national alert centre which cooperates with all public authorities to respond quickly to security incidents that occur in their part of cyber space and, moreover, it is ultimately responsible for the national safety of classified information.

- The **National Centre for Critical Infrastructure Protection (CNPIC),** under the Ministry of the Interior, is responsible for promoting, coordinating and supervising all activities related to the protection of Spanish critical infrastructures. Its main objective is to promote and coordinate the necessary mechanisms to ensure the security of infrastructures that provide essential services to society, fostering the participation of each and every one of the agents of the system in their respective areas of power.

- **Computer Crime Unit of the *Guardia Civil* and the Unit Responsible for Research into Information Technology Crime of the National Police Force,** both of whom are dependent on the Ministry of the Interior, and are responsible for combating crime that occurs in cyber space.

- The **Spanish Data Protection Agency (AEPD),** an independent supervisory authority responsible for ensuring compliance with the regulations on personal data protection. In some autonomous communities (Madrid, Catalonia and the Basque Country) there are also data protection authorities with specific responsibilities regarding personal data files created or managed by the Autonomous Communities and Local Governments of their particular territory.

Similarly, within regional administrations there are state-level equivalent centres such as the CERTs of Valencia, Catalonia and Andalusia.

Moreover, the Spanish Armed Forces, within the specific scope of both the Army and Navy, and as a whole, led by the Chief of Staff of National Defence, develop different ICT programmes with the objective of providing secure networks and systems that incorporate the technologies required to provide the services and applications that support military commanders in the fulfilment of their missions.

8. Diagnosis of the current status of National Cyber Security

8. Diagnosis of the current status of National Cyber Security

Until the adoption, in May 2011, of the current National Security Strategy, cyber space had not been identified formally as a real threat to national security.

The belated recognition of the strategic importance of having a secure cyber space has led, among other things, to the Government of Spain not yet having created a complete National Cyber Security System, i.e., all the bodies, agencies, and procedures for the direction, control and management of the security of Spanish cyber space.

Set out below are the main reasons why National Cyber Security has not yet reached the required level to correspond to the actual risk from cyber space. These reasons can be divided into 4 groups: Organisational, Operational, Legal and Political.

Organisational reasons

a) **Absence of a cyber security management body.** The absence of a cyber security management body prevents the implementation of a common working methodology that would facilitate decision-making and the coordination and integration of all players under common procedures.

b) **Non-unified Management of the National Cyber Security due to a departmental approach.** The National Cyber Security management is shared, in a non-unified manner, by a set of organisations within the scope of multiple ministries (see diagram on Page 22 of this document).

c) **Insufficient human, technological and economic resources.** The existing management agencies lack the human, technical and financial resources to implement and manage the capabilities to achieve a level of cyber security that would match the known and controlled risk status.

Operational reasons

d) **Partial and insufficient knowledge of the national cyber situation.** Having a reliable and up-to-date cyber situation is essential for making decisions and for crisis management within cyber space. At present, the Government of Spain has a partial and insufficient knowledge of the cyber space of the State administration and, to a lesser extent, so does the private sector.

e) **Absence of a framework that would facilitate the sharing of information on cyber security.** The insufficient level of communication between public bodies in relation to National Cyber Security and between these public bodies and the private sector is due, principally, to the absence of a stable and open procedural framework that would allow the fluid and secure sharing of information.

f) Inadequate metrics regarding the degree of resilience of the ICT infrastructure of government networks and the major critical infrastructure of the country. The lack of metrics leads to significant uncertainty on the degree of resilience of ICT infrastructures on which the government networks and the critical infrastructures of Spain rely.

g) The minor role of private players regarding cyber security. At present National Cyber Security is a closed and exclusive system of government players. Currently more than 80% of Spanish critical infrastructure is the property of, and is directed and managed by, the private sector (national and international companies). Therefore, the private sector's contribution to the process of building National Cyber Security is essential.

Legal reasons

h) The absence of specific and comprehensive legislation on cyber security. There is legislation that is distributed across different regulatory areas or matters, but this has not been developed from a common political perspective covering the full national scope and establishing the strategic character of cyber security.

Political reasons

i) Absence of policies encouraging public and private sector collaboration on cyber security. Public and private sector collaboration is a cornerstone for achieving a level of security that would be appropriate for the known and controlled risk status. Spain does not currently have a framework for public and private sector collaboration in the field of cyber security.

j) Absence of a state policy on cyber awareness and cyber education. Many countries within our environment are developing ambitious cyber awareness and cyber security policies as a fundamental axis for creating a culture of cyber security.

These policies have been developed and supported, initially, by the private sector, and subsequently they have received strong government support. In this case, a dual role should be highlighted, on the one hand, fostering the awareness and education of all citizens regarding the risks of cyber space and, on the other hand, identifying future talent in the field of cyber security within the school and university community.

In Spain, INTECO and CCN have cyber awareness and cyber security programmes. In the private sector, organisations such as ISMS Forum Spain also have cyber awareness initiatives under the domain protegetuinformacion.com. So far, these initiatives have had insufficient impact on civil society.

k) Absence of specific policies for national R&D+innovation on cyber security. There are no policies, programmes or initiatives for R&D+innovation of a nationwide scope to promote and provide activities on cyber security, which is in sharp contrast with the leading role that the new Horizon 2020 framework (a continuation of the 7th Framework Programme) attaches to cyber security at an European level.

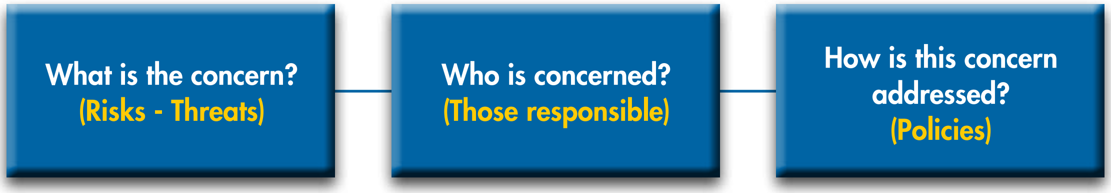
9. Why does Spain need a National Cyber Security Strategy?

9. Why does Spain need a National Cyber Security Strategy?

The National Strategy for Cyber Security should be an instrument to guide those responsible for the direction and management of National Cyber Security and its beneficiaries, but it will also serve as a deterrent to potential offenders.

The Government of Spain, through the Spanish strategy for cyber security, should explain the model that provides cyber security to the Spanish society, within the current context of global risk. The National Cyber Security Strategy must define the concept of cyber security based on the following three issues:

Concept of cyber security



What is the concern? (Risks - Threats)

Who is concerned? (Those responsible)

How is this concern addressed? (Policies)

9.1. What is the concern? (Risks-Threats)

The novelty, diversity and heterogeneity of the risks and threats related to cyber space require reliable and up-to-date knowledge of the cyber situation, providing, to those responsible for National Cyber Security, the know-how necessary for the administration, control and management thereof. Section 6 of the present document analyses the current risk status regarding cyber space.

9.2. Who cares? (Those responsible)

The security of cyber space is the responsibility of the government. **Presidency of the Government** should take the lead in national security. In doing so it should create an integrated **National Cyber Security System.**

Although the responsibility lies with the Government of Spain, participation should be encouraged, not only by traditional governmental players, but also by private players, the university community, associations, experts, and representatives of citizens.

9.3. How to respond to this concern? (Policies)

The Government of Spain should show **political determination** in order to confront cyber risks and threats, and therefore should **should establish objectives and priorities.**

Similarly, the creation of the National Cyber Security System will reduce the risk of each ministry and agency deciding its own course of action and it will also reduce the likelihood of a disproportionate coordination effort being deployed.

The main policies should aim to promote:

- Resilience of Spanish cyber space;
- Public and private sector collaboration;
- Education and awareness;
- R&D+innovation, and
- International collaboration.

10. Functions of National Cyber Security

10. Functions of National Cyber Security

National Cyber Security should make appointments for the following set of functions:

Functions of National Cyber Security

- Establishing the objectives and priorities of National Cyber Security.
- Integrating policies and players.
- Giving advice on National Security to those responsible for same.
- Promoting a culture of cyber security.
- Assessing the risk status of cyber space.
- Planning policies and managing cyber crises.
- Strengthening national capacities for risk prevention, response and recovery, as well as for cyber attacks.
- Deterring potential aggressors.

10.1. General functions

- **Establishing the objectives and priorities of National Cyber Security.** National Cyber Security should establish a set of objectives. These objectives must be achievable, measurable, and verifiable, and sustained over time, adapting to the needs that cyber space and its risk status require at any given moment.

- **Integrating policies and players.** It is necessary to avoid the current subdivided model of poor coordination, and to evolve into a model of comprehensive and unified management, with the capacity for planning and analysis in order to formulate joint proposals for adopting strategic decisions, monitoring their implementation and evaluating and monitoring their performance. To this end it will be necessary that all players participate: public sector, private sector, state, regional, municipal and even international.

- **Giving advice on National Security to those responsible for same.** The National Cyber Security System shall advise the President of the Government and all those involved in national security issues, liaising between these and other national and international players, as well as with public or private players.

- **Promoting a culture of cyber security.** The communication function is essential in the creation and promotion of the cyber security culture. This function is to direct the communication strategy on National Cyber Security issues and situations of crisis, promoting social and parliamentary participation in the review and approval of strategies, promoting public and private sector communication between departments, and disseminating warnings and recommendations to the public. The culture of cyber security will be achieved through the right combination and implementation of cyber security enablers described in Section 11 of this document.

10.2. Operational functions

- **Assessing the risk status of cyber space.** The Government of Spain is responsible for ensuring the capacity to manage National Cyber Security. As a first step to fulfilling its responsibility it must know what the status of our cyber security risk is quantifying the likelihood of threats materializing and estimating their potential impact.

- **Planning policies and managing cyber crises.** Planning policies and crisis management requires a change in the cyber security management model, from coordination to integration and unification in order to optimize the contributions of all players involved. Comprehensive management does not consist of copying the same tasks and capabilities, nor does it consist of coordinating independent initiatives, rather it focuses on the contributions of all players and policies involved from the very beginning.

- **Strengthening national capacities for prevention, response and recovery from cyber risks and attacks.** The Government of Spain must have the capability available for prevention, response and recovery from cyber risks and attacks. These capabilities should allow a reliable awareness of the status of the cyber situation. Moreover, the application introduces rationalization mechanisms of resources and capabilities, power economies of scale and multiplies synergies and performance by training initiatives, practical teaching, research, and common evaluation.

- **Deterring potential aggressors.** Having a resilient and safe cyber space available is a better dissuasive mechanism against state and non-state aggressors.

11. Enablers of National Cyber Security

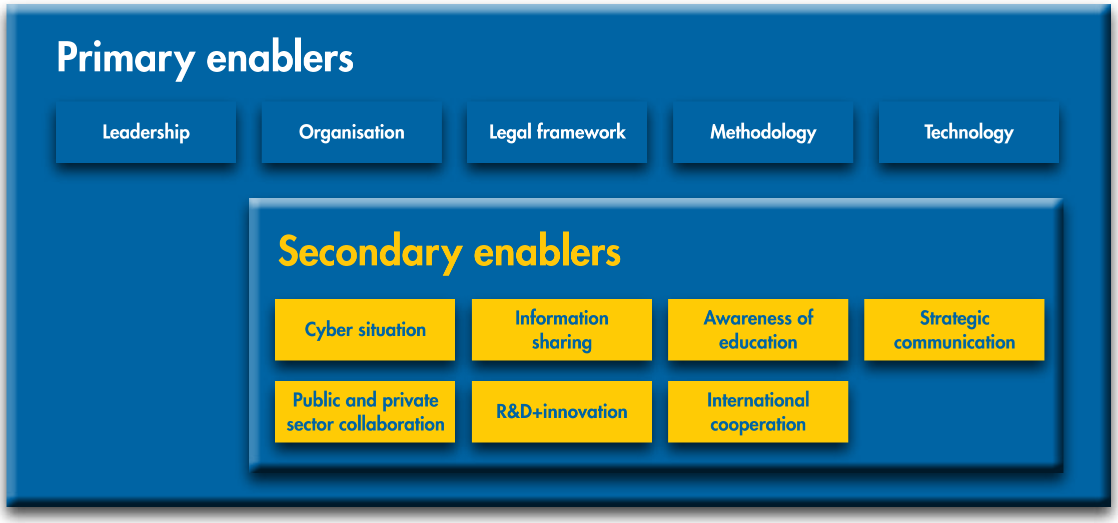
11. Enablers of National Cyber Security

The novelty of cyber space and its continuous evolution and transformation poses a challenge for National Cyber Security. It is therefore necessary to build National Cyber Space Security in a progressive manner, with the ability to evolve and adapt to a constantly changing environment.

The **National Cyber Security enablers** are those that allow the functions of National Cyber Security and are divided into two groups: primary and secondary:

- The **primary enablers** are those that enable the construction of National Cyber Security.
- The **secondary enablers** are those that enable the operation of National Cyber Security. The secondary enablers, independently, can carry out their specific function but would not reach their critical efficacy and efficiency.

Enablers of cyber security



11.1. Primary enablers

The primary enablers of National Cyber Security are:

- **State leadership**
  The State has an obligation to legislate and act in order to protect, or to enforce the protection of, the services provided in cyber space and to allow citizens, organizations and businesses to develop in social, cultural and economic spheres, among others. To comply with that obligation implies the exercise of leadership for the definition of policies, strategies and legal frameworks regarding cyber security, as well as creating the organizational tools that allow its application.

The Presidency of the Government must exercise this leadership together with the Government of Spain. Among its functions are approving, reviewing and communicating the strategies and policies of National Cyber Security, but also monitoring their development and implementation, as well as creating the necessary organisations and electing the persons responsible for them.

- **Organisational structure**
  The State should create an organizational structure that allows the direction and management of National Cyber Security and performs the *functions of National Cyber Security* described in Section 10, *Functions of National Cyber Security,* of this document. Similarly, Section 12, *Organizational Structure of National Cyber Security,* proposes a high-level organizational structure for National Cyber Security.

- **Legal framework**
  Although the essential legislation to regulate the management and operation of National Cyber Space already exists, it is scattered between different policy areas, and has been developed from a common policy that reflects national and strategic cyber security. It will therefore be necessary to develop a legislative framework to support National Cyber Security that is effective, and at the same, takes into account fundamental rights and public freedoms. The less dispersed the regulations that are part of the legislative framework, the higher the level of legal security.

- **Working methodology regarding cyber security**
  The novelty and complexity of the security of cyber space make it necessary to develop a methodology that provides a better understanding of the strategic importance of cyber space and its risk status. This methodology should provide the following:

  - A common language. This common language will range from technology to legal terms.

  - Homogenized theoretical fundamentals.

  - Procedures that describe how to act regarding cyber security.

- **Technology**
  Technology is the basis of cyber space. Understanding and adapting to continuous technological evolution is essential in order to improve the resilience and security of our cyber space.

11.2. Secondary enablers

The secondary enablers of cyber security are:

- **Knowledge of the cyber situation**

  Knowledge of the cyber situation should provide immediate awareness of one's own cyber space, that of other nations, that of the enemy and that of any other party of interest, as well as knowledge of the status and availability of operational capabilities that are necessary for planning, directing and managing the operations necessary to secure cyber space.

  Knowledge of the cyber situation not only occurs as a result of the combination of intelligence and operational activities in cyber space, but also in electromagnetic space and other dimensions of the operating environment (land, sea, air and outer space).

  The processes, procedures and capabilities of cyber situation awareness should be developed to contribute to the overall situational awareness of those responsible for the management of national security and the achievement of its objectives.

  Thus, knowledge of the cyber situation must:

  - Provide those responsible for National Cyber Security with the visibility, in real-time, of networks, systems, their own services and their dependencies.

  - Provide those responsible for National Cyber Security with the visibility, in real-time, of the enemy's actions on the networks, their own systems and services, as well as the possible impact on the achievement of operational objectives.

  - Provide those responsible for National Cyber Security with operational knowledge of the impact of their decisions on cyber operations, within their scope of action, contributing to the decision-making process.

  - Provide those responsible for national security with as much detail as possible, including intelligence information, essential to support the decision-making process regarding cyber space and cyber operations.

  - Coordinate and share efforts between different players (auxiliary bodies of the general administration of the State Security Forces and Bodies of the State, military, private sector, industry, social partners and any other public or private entities, whether national or international), obtain knowledge of the cyber situation to as great an extent as possible.

  - Identify threats in cyber space, including potential adversaries, in order to contribute to the understanding of the situation of those responsible for leading national security and intelligence and operational objectives.

- o Study the motivations, objectives and analyse the potential adversaries in their decisions to direct potential cyber attacks on national interests, so that a defence can be planned against them.

- **Information sharing**
  A set of mechanisms should be articulated to allow different players in National Cyber Security to share information efficiently. Moreover, the sharing of information:

  - o Will help to achieve reliable and up-to-date knowledge of the cyber situation;
  - o Will improve the availability and resilience of National Cyber Security assets;
  - o Will allow cyber crises to be managed efficiently;
  - o In another context, it will optimize economic investment in cyber security, rationalising the use of human and technical resources.

- **Studies and publications on cyber security**
  Spanish society must become aware of individual risks (privacy and intimacy) and collective risks (national security, economic, social and cultural prosperity) to which it would be exposed in the event of an irresponsible use of cyber space. The Government of Spain must lead an educational model and promote cyber security. The objectives of this model are:

1. Making Spanish society aware of cyber risks. A state of uniform opinion needs to be created on the need for secure cyber space in order to ensure the prosperity of our society and economy.

2. Training Spanish society in the responsible use of cyber space. It is necessary to address an ambitious education plan that allows training on cyber security awareness from an early age (primary education) right through to university. Similarly, it should promote training programmes for other sectors.

3. Identifying and training national “cyber talents.” Early education on cyber security will identify “national cyber talents.” These “cyber talents” should receive specialised guided training for future incorporation into the management and control bodies of National Cyber Security.

- **Strategic Communication**
  It is necessary to develop a strategic communication policy on matters of National Cyber Security and cyber crises, as well as boosting social and parliamentary debate on the review and approval of strategies, promoting public and private sector communication between administrations, and disseminating warnings and recommendations to the public.

- **R&D+innovation**

  The strong technological component of cyber space and cyber security makes it obligatory to promote competitiveness and R&D+innovation in the national public and private sectors. Therefore the Government of Spain should develop a set of policies, the objective of which is for national companies to commercialise their products and services, that the State maintains a technologically advanced status and, most importantly, that it has flexible "partners" in order to face the dynamic evolution of ICT.

- **Public and private sector Partnerships**

  The heterogeneity and the changing landscape of the risk status of cyber space is a continuous challenge for National Cyber Security. The Government of Spain does not have, on its own, the skills needed to ensure National Cyber Space Security and, therefore, it needs the private sector, among others, in order to reach a level of security appropriate to a known and controlled risk status.

  It is the responsibility of the Government of Spain to create and promote a framework of public and private sector collaboration.

  These public and private sector partnerships on cyber security should contribute to:

  - Improve knowledge of the cyber status. Private organisations are continuously and repeatedly victims of cyber attacks of various kinds. For this reason they have implemented their own capabilities to ensure the safety of their specific cyber space. These capabilities generate information and knowledge to be shared with the public bodies and agencies responsible for the direction and management of cyber security. It is necessary that this sharing be bi-directional.

  - Optimize the national cyber capabilities and resources by avoiding the duplication of efforts.

  - Improve the resilience of national cyber space.

  - Improve the competitiveness of domestic companies in the field of cyber security.

  - Improve R&D+innovation in cyber security.

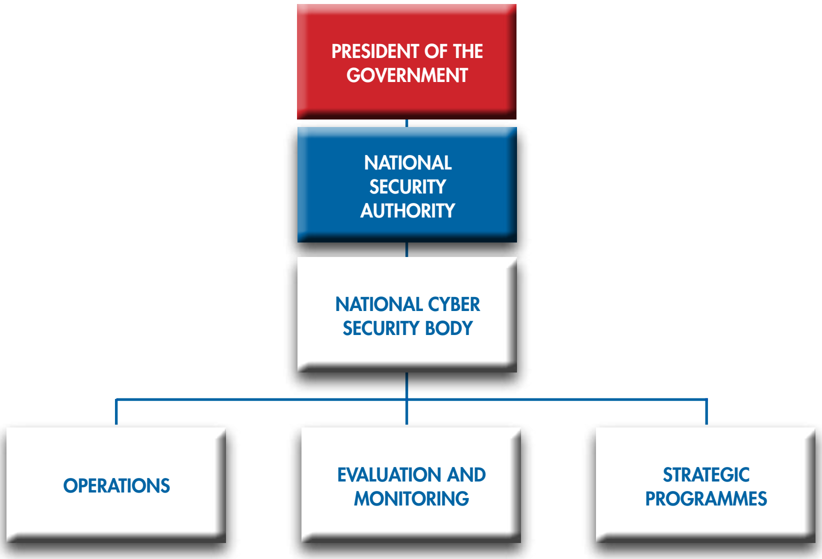
  - Promote awareness and education on cyber security.

12. Organisational structure of National Cyber Security

12. Organisational structure of National Cyber Security

A high level organisational structure is proposed below in order to direct, control and manage National Cyber Security.

Organisational structure of National Cyber Security


PRESIDENT OF THE GOVERNMENT
NATIONAL SECURITY AUTHORITY
NATIONAL CYBER SECURITY BODY
OPERATIONS
EVALUATION AND MONITORING
STRATEGIC PROGRAMMES

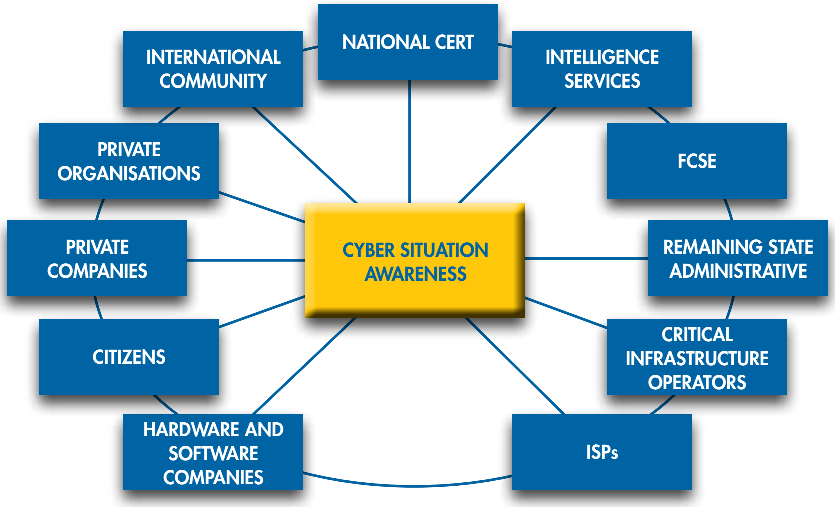
The National Cyber Security Body shall be responsible for directing National Cyber Security. This body will enable the implementation of the tasks entrusted to National Cyber Security. These functions have been described previously in this document.

- **Operations.** The National Cyber Security Body should seek capabilities of detection, prevention, containment and response to any cyber attacks or contingencies. These operational capabilities will be managed from a National Reference CERT and a Defence CERT.

- **Evaluation and monitoring.** The area of evaluation and monitoring will be assigned the following functions:

  - o **Knowledge of the cyber situation.** Knowledge of the national and global cyber situation is a fundamental aspect for the efficient administration and management of National Cyber Security. A reliable and up-to-date cyber situation is reached by means of integration and transformation of information from multiple sources: National CERT, intelligence services, State Forces and Security Bodies, the remaining State Administrative Bodies, critical infrastructure operators, internet service suppliers, hardware and software companies, citizens, private companies, private organisations and the international community.

Cyber situation awareness


NATIONAL CERT
INTERNATIONAL COMMUNITY
INTELLIGENCE SERVICES
PRIVATE ORGANISATIONS
FCSE
PRIVATE COMPANIES
CYBER SITUATION AWARENESS
REMAINING STATE ADMINISTRATIVE
CITIZENS
CRITICAL INFRASTRUCTURE OPERATORS
HARDWARE AND SOFTWARE COMPANIES
ISPs

- **Risk analysis.** Knowledge of the cyber situation will identify the causes of the threats and likely unwanted cyber events, as well as the damage and consequences they may have for national security. The innovative and rapid nature of cyber space requires a continuous risk analysis, in order to help determine the security measures warranted by the cyber space risk status.

- **Planning.** The plan will provide a long-term vision of procedures, activities and resources involved to help support the management of cyber security.

- **Managing cyber contingencies.** The on-going transformation of cyber space leads bodies and agencies that direct and manage National Cyber Security to face unknown events that may compromise the resilience and / or security of our cyber space.

- **Warnings.** It will be necessary to have a mechanism to inform all those involved in National Cyber Security about relevant issues.

- **Lessons learned.** Compiling the successes and failures in the direction and management of National Cyber Security is essential in order to improve weaknesses and enhance the strengths of our cyber space, as well as to make it more resilient and secure.

- **Doctrine.** Based on the knowledge of the cyber situation and all the lessons learned, it will be necessary to create a consistent set of teachings or instructions on cyber security.

  - **Development of policies and procedures.** As a result of the above, it will be necessary to develop policies and procedures that facilitate the control and management of National Cyber Security. These policies and procedures must take into account not only technological but also legal, operational and any other dimensions that could affect National Cyber Security.

- **Strategic Programmes.** Self-adaptation of National Cyber Space to a known and controlled risk status is a key aspect for National Cyber Security. Therefore it will be necessary to work continuously and to evolve a set of strategic programmes that facilitate gradual adjustment to a known and controlled cyber space risk status. Some of the strategic programmes are set out below:

  - Awareness and Training. Training and continuous awareness of all sectors of Spanish society is essential to the national security of cyber space.

  - Cyber exercises. In order to know the true state of maturity of National Cyber Security, cyber exercises will be required from time to time. These cyber exercises should take place not only in the sphere of national cyber space but also within major international organisations (NATO, EU, etc.)

  - Standards and best practices. It will be necessary to develop standards and best practices that improve the resilience and security of our cyber space. Many of these standards and best practices already exist, and have international acceptance and consensus.

13. Objectives of National Cyber Security 2012-2015

13. Objectives of National Cyber Security 2012-2015

The ultimate purpose of the National Cyber Security Strategy should be to achieve a set of goals. Here are the objectives that should be achieved regarding cyber security during the period 2012-2015.

Main objective		
Providing a secure cyber space in order to ensure the social, cultural and economic prosperity of Spain and the freedoms of its citizens through a culture of prevention and resilience involving, in an active and integrated way, all sectors of Spanish society.		
Objective 1	**Objective 2**	**Objective 3**
Having reliable and up-to-date knowledge of the cyber situation.	Improving national resilience in respect of cyber threats.	Creating and promoting a cyber security culture.

The main objective of National Cyber Security is to provide a secure cyber space in order to ensure the social, cultural and economic prosperity of Spain and the freedoms of citizens through a culture of prevention and resilience involving, in an active and integrated way, all sectors of Spanish society.

In order to achieve this objective it is first necessary to achieve the following sub-objectives:

- **Sub-objective 1. Having reliable and up-to-date knowledge of the cyber situation.** It is necessary to have immediate awareness of one’s own cyber space, as well as that of other nations, that of the enemy and that of any other parties involved, as well as knowledge of the status and availability of operational capabilities that are necessary for planning, directing and managing the operations necessary to secure cyber space.

- **Sub-objective 2. Improving national resilience in respect of cyber threats.** It is necessary to have the capacity available to allow to resist and recover from negative impacts resulting from activities that are known, unknown, predictable, unpredictable, uncertain and unexpected, and which occur in cyber space. This effort must be directed in particular to improving the resilience of the critical infrastructures of our country.

- **Sub-objective 3. Creating and promoting a cyber security culture.** The enablers of National Cyber Security, described in part 6 of this document, should foster the creation of a National Cyber Security culture. Reciprocally, the ‘essence’ of the National Cyber Security culture thus created should optimise the management of these enablers and, therefore, foster the consolidation of the cyber security culture.

14. Actions for attaining National Cyber Security objectives

14. Actions for attaining National Cyber Security objectives

To achieve the objectives described in Section 13 of this document it will be necessary to perform a set of actions in order to:

- Improve knowledge of the cyber situation.
- Improve the capacity of detection and analysis of cyber threats.
- Improve channels of communication between the different players involved in National Cyber Security.
- Improve resilience and national cyber space security.
- Strengthen the national and international legal framework regarding cyber crime.
- Improve public awareness, education, training and professional development in cyber security.
- Promote R&D+innovation programmes in cyber security.
- Support the competitiveness of the private sector in the field of cyber security.
- Promote international cooperation.

The following are the actions that should be implemented during the period 2012-2015, in order to improve the resilience and security of National Cyber Space:

Action 1. Approval of the National Cyber Security Strategy. In order to construct the National Cyber Security System allowing the administration, control and management of National Cyber Security, it is necessary to approve the National Cyber Security Strategy.

Organisational structure

Action 2. Design or create the national reference CERT. The national reference CERT should be created, in addition to those that may already exist. The mission of the national reference CERT shall be to collect operational information in relation to National Cyber Space status which is obtained by its own means and that of other national CERTs, as well as international CERTs with whom collaboration agreements have been signed.

Action 3. Create the Ministry of Defence CERT. It should provide the current Security Operations Centres of the Armed Forces with the human, economic and technical resources necessary to achieve the evolution towards becoming a CERT.

Action 4: Create the National Centre for Monitoring and Evolution of Cyber Security. This centre should develop the activities described in the Monitoring and Evaluation Centre described in Section 12 of this document.

Action 5: Create the National Centre for Strategic Programmes on Cyber Security. The unstoppable evolution and transformation of cyber space makes it necessary to develop strategic programmes in this area in order to allow the adaptation of the national security status to a known and controlled risk. Section 12 of this document defines the main strategic programmes on cyber security identified to date. These programmes should be directed and controlled by the National Strategic Programme on cyber security and management thereof must be distributed between agencies in the field of General Administration.

Operational actions

Action 6. Appointment of human resources necessary for the Administration, Control and Management of National Cyber Security. It will be necessary to provide all bodies with the professionals that they need. These profiles should cover all areas of knowledge within the scope of cyber security.

Action 7. Improve and extend the technological capacities which allow the detection, prevention, containment and response to cyber attacks.PIn order to improve the capacity of detection, prevention, containment and response to cyber attacks, it will be necessary to:

- Improve and expand the network of early warning sensors;
- Improve monitoring capabilities;
- Improve vulnerability scanning capabilities;
- Improve cyber incident solving capabilities.

Action 8. Create a framework for sharing information among different players of National Cyber Security. The National Cyber Security Body should articulate the mechanisms allowing the coordination and integration with the players involved in National Cyber Security in order to facilitate the fluid and efficient sharing of information. This framework should include legislative measures fostering an environment that respects fundamental rights and public freedoms, without compromising its effectiveness.

Action 9. Improvement of warning channels. It will be necessary to improve the channels of communication in order to allow, properly and in good time, the different sectors of Spanish society and players to be aware of cyber contingencies that pose a threat to national security.

Action 10. Develop a methodology for improving the resilience and security of the National Cyber Space.

Action 11. Encourage and promote the resilience and security of the ICT infrastructure of the private sector. It will be necessary to pursue policies that promote improved resilience and security of the ICT infrastructure.

International cooperation

Action 12. Bilateral or multilateral agreements with other nations regarding cyber security. The global nature of cyber space makes it necessary to enter into bilateral and multilateral agreements. These agreements should improve information channels, as well as the detection of and/or coordinated responses against cyber incidents. Special relevance should be given to agreements with the purpose of fighting cyber crime in any of its forms.

Action 13. Participation in multilateral and international forms on cyber security. Spain should actively participate in all multilateral and international forums in which cyber security is addressed (NATO, EU, UN, Interpol, Europol, OECD,…).

Action 14. To work in a coordinated manner with allies in order to implement the Cyber Security Policies of NATO. The NATO Lisbon Summit in 2010 identified cyber space as the new threat to the organisation. Spain must work together with the rest of its allies in the protection of the Cyber Space of the Alliance.

Public and private sector collaboration

Action 15: Creation of the National Platform for the Coordination of Public and Private Sector Cooperation in respect of cyber security. A national platform for the coordination of public and private sector cooperation on cyber security should be created, where the principal players in Spanish society are represented: the public sector, the private sector (with representation of different types of organizations, large enterprises and SMEs), the academic community, technology and research centres, associations and organizations.

Action 16: Creation of sector working groups within the national platform for coordination of public and private sector cooperation in respect of cyber security. Following the creation of the national platform, sector working groups should be created in order to promote efficient and effective communication.

Education and awareness

Action 17: Develop a national education programme on cyber security. This programme will promote awareness, education, training and professional development in cyber security. This will require carrying out the actions set out below.

Action 18: Develop a National Cyber Awareness Campaign. A cyber awareness campaign should be developed in order for Spanish society to become aware of the individual (privacy and intimacy) and collective risks (national security, economic, social and cultural prosperity) posed by the improper use of cyber space. Similarly, specific campaigns should be carried out which are aimed at parents and teachers. www.protegetuinformacion.com of the ISMS Forum is proposed as the embryo campaign of Spain for the national cyber awareness campaign. In this campaign the role of the leading private companies in the country and the mainstream media (TV, radio, newspapers, Internet ...) is critical.

Action 19: Incorporation of materials related to the responsible use of new technologies and cyber security in primary, secondary, university and post-graduate curricula. It will be necessary to incorporate materials associated with cyber security. This education should begin at an early age (primary education) and be extended throughout secondary, university and post-graduate education. The purpose of starting this education at a young age is, on the one hand, to homogenize the awareness of the use of new technologies, such as its responsible use, and on the other hand, to identify national "cyber talents."

Action 20: Modify education programmes that are related to Science, Technology and Engineering, emphasising the important role of mathematics and computational thinking, not to mention the legal and regulatory aspects.

All initiatives regarding higher education, including the implementation of specific Education Programmes on cyber security, should be coordinated with the National Evaluation Agency for Quality and Accreditation (ANECA), as the state foundation whose object is to contribute to improving the quality of higher education through evaluation, certification and accreditation of teaching, teachers and institutions.

Action 21: Incorporation of materials related to new technologies and cyber security curricula at military academies. Officers and NCOs of the Spanish Armed Forces should receive a strong background in IT theory, electronics, radio wave propagation, among other things, as well as their application to tactical military operations and strategies.

Action 22: Incorporation of materials related to new technologies and cyber security in the curricula of business schools. Future managers of domestic firms should receive training in new technologies and cyber security. The support of senior management is crucial for organizations in order to implement them with a cyber security culture.

Action 23: Creation of a programme of academic centres of excellence in cyber security. The public - private partnership between the State administration, the private sector and the academic community should allow the appointment of a group of national universities and academic centres of excellence where education on cyber security will be provided as part of the Government's strategic programmes on this subject. These centres will provide specialised training and promote R&D+innovation in cyber security.

Action 24: Mandatory training and awareness plans, aimed at employees of public private or independent companies.

Action 25: Continual training plans for personnel responsible for the administration and management of Cyber Space and State Administrations, such as public and private organisations, which manage and administrate critical infrastructure in Spain. It will be necessary to develop a plan which includes training courses, degrees, masters and cyber security certification for personnel responsible for the administration and management of the Cyber Space of State Administrations, as well as bodies, public and private, that administrate and manage Spanish critical infrastructures.

R&D+innovation and Competitiveness

Action 26: Create a National Strategic R&D+innovation Plan concerning cyber security and its corresponding development in annual work programmes. Accompanying the National Cyber Security Strategy, with a similar timeframe as the defined action plan, a strategic plan for development of R&D + innovation on cyber security should be developed which is aligned both with the national needs voiced by the public and private sectors and with the strategic alignment marked by the new European Horizon 2020 framework. This strategic plan should be developed by using Annual Work Programmes that include specific themes and objectives towards positioning, improving and developing the cyber protection capabilities of different sectors, both public and private, as well as the citizens themselves, in addition to the promotion of the market for National Cyber Security products and services.

Action 27: Create a Technological Monitoring Observatory for International Cyber Security R&D+innovation. In order to maintain advanced awareness at the forefront of technology and cyber security, it shall be necessary to establish a process of technological monitoring concerning R&D+innovation into cyber security which guarantees awareness, valuation of partnerships and the promotion of joint projects, which ensure full integration, making full use of the opportunities, resources and international advances in national organisations in this area.

Action 28: Create a National ICT Product Certification Centre. The implementation of certain ICT products shall require prior approval by a national certification centre. This centre shall keep an up-to-date catalogue of certified products. This catalogue shall contain those products (hardware and software) that meet the security requirements in order to form part of the ICT infrastructure of the public sector and the main critical infrastructure of the country, for which compliance will be mandatory. Likewise, said catalogue shall be used as a guide for the rest of the private sector, providing advice on the use of its products.

Other actions

Action 29: Designate the first week of the month of November as 'Cyber Security Awareness Week'. With the purpose of promoting cyber security awareness, and in order to take advantage of the beginning of the school year, it is recommended to have a cyber security awareness week in all places of education in the country (primary, secondary, university and post-graduate levels).

Action 30: Hosting the cyber space conference 2014 or 2015. In 2011 the first international cyber space conference took place in London which was attended by the key players on the world stage. This conference will be held in Hungary in 2012 and South Korea in 2013.

Action 31: Promote and lead the first Ibero-American cyber exercise in 2013. Spain will promote and lead the first Ibero-American cyber exercise. This exercise will allow the level of maturity of our cyber space to be measured. Furthermore it will consolidate Spain's leadership in the field of Ibero-American cyber space, reaching agreements on cyber security with many countries.

15. Conclusions

15. Conclusions

Spain, despite the great efforts that have been made, still does not have a solid capacity allowing the efficient administration, control and management of its cyber security.

Security, in all its dimensions and spheres, is the first responsibility of any government. The Government of Spain should assume leadership regarding cyber security in order to make its citizens aware of the need for protecting our cyber space on which our basic services, critical infrastructure, economy and progress as a society depend.

ICT is not a problem, it is part of the solution and its resilience, protection and safe use are not only the responsibility of the Government, but also of independent and local administrations together with the private, business and domestic sectors. All of them share this responsibility; however it is up to the government to exercise leadership in the management of cyber security. These are responsibilities that cannot be delegated and which should result in providing the impetus, ideas and direction that Spain needs.

The changes in the guiding framework in recent years, including the emergence of new risks and threats (cross-border threats, globalization and the emergence of non-state players, etc.) make it necessary to move towards a comprehensive security concept and a culture of prevention and resilience.

This development is to consider cyber space as a key element in the overall risk management of national security and, therefore, grant the necessary importance to cyber security as a continuous process of analysing and managing the risks associated with it.

The risk situation has evolved and is evolving day by day. The increase in the amount and variety of threats against ICT infrastructure and information, the greater quantity and sophistication of cyber attacks and the varying nature of their objectives, even citizens, the private sector and governments, are experiencing certain changes that, together with the diversity of authors and interested parties, such as states, private organisations, terrorist organisations, organised crime or hacktivists, should be born in mind when developing an appropriate cyber security strategy.

Another key aspect to bear in mind for the future National Security Strategy is the identification of cyber space as the new dimension of the operating environment alongside more traditional forms (ground, sea, air and outer space). It will therefore be necessary to provide our Armed Forces with the cyber capabilities and human, technical and economic resources necessary for their exercise and functions.

In this sense, any contingencies that may affect any of the key assets of the twelve sectors grouped into our critical infrastructures could compromise national security.

It is therefore necessary to develop and approve the National Cyber Security Strategy. This strategy should be a tool to guide those responsible for the administration, control and management of National Cyber Security and its beneficiaries, but it will also serve as a deterrent to potential offenders. This strategy should be assigned a set of functions that can be achieved from the following set of primary enablers:

- The unquestionable leadership of State through Presidency of the Government;
- The creation of a National Cyber Security System integrated into the national security system;
- An appropriate method to provide a common language, theoretical homogenized fundamentals and procedures that describe how to proceed in respect of cyber security;
- All accompanied by the necessary technological developments to support them.

Moreover, these principle enablers should be fed by:

- An awareness of the cyber situation;
- Appropriate information sharing between different players;
- An awareness and education brought about by the momentum of an educational model on cyber security;
- A strategic communication policy on the issues of the National Cyber Security and Cyber Crisis Situations;
- The development and promotion of R&D+innovation in the national public and private sector;
- And a framework for public and private sector partnerships on cyber security.

The main objective of National Cyber Security is to provide a secure cyber space in order to ensure the social, cultural and economic prosperity of Spain and the freedoms of citizens through a culture of prevention and resilience involving, in an active and integrated way, all sectors of Spanish society.

16. Main and auxiliary bibliography and websites consulted

16. Bibliography and websites consulted

Main bibliography

- **ARTEAGA, FÉLIX** "Propuesta para la implantación de una Estrategia de Seguridad Nacional en España" DT 19/2011. December 2011. Real Instituto Elcano.

- **BETZ, DAVID J. & STEVENS, TIM** "Cyberspace and the State. Toward a strategy for cyber-power". June 2011.IISS.

- **CLARKE, RICHARD & KNAKE, ROBERT "CYBERWAR".** February 2010. Ed HarperCollins.

- **COZ FERNÁNDEZ, JOSÉ RAMÓN & FOJÓN CHAMORRO, ENRIQUE** "La Geoestrategia del Conocimiento en Ciberseguridad". January 2012. Revista RED SEGURIDAD.

- **COZ FERNÁNDEZ, JOSÉ RAMÓN & FOJÓN CHAMORRO, ENRIQUE** "Un modelo educativo para una Estrategia Nacional de Ciberseguridad". October 2011. Congreso ENISE (Encuentro Internacional de la Seguridad de la Información).

- **FOJÓN CHAMORRO, ENRIQUE & SANZ VILLALBA, ÁNGEL FRANCISCO** "Ciberseguridad en España: Una propuesta para su gestión" ARI 102/2010. June 2010. Real Instituto Elcano.

- **FOJÓN CHAMORRO, ENRIQUE & COZ FERNÁNDEZ, JOSÉ RAMÓN** "Panorama Internacional en el establecimiento de Estrategias Nacionales de Ciberseguridad. June 2011. Revista SIC". Seguridad, Informática y Comunicaciones.

- **FOJÓN CHAMORRO, ENRIQUE & SANZ VILLALBA, ÁNGEL FRANCISCO** "El ciberespacio: La nueva dimensión del entorno operativo" perteneciente al documento de seguridad y defensa n° 44 "Adaptación de la fuerza conjunta a la guerra asimétrica". November 2011. Centro Superior de la Defensa Nacional (CESEDEN). http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/DSEGD_44.pdf

- **KNAPP, ERIC D.** "Industrial Network Security". September 2011. Ed. SYNGRESS.

- **LIBICKI, MARTIN** "Cyberdeterrence and Cyberwar". October 2009. RAND project Air Force.

- **LINARES, SAMUEL "LOS AMIGOS SE ESCOGEN, LA FAMILIA…NO".** June 2012. Revista RED SEGURIDAD.

- **MULLIGAN, DEIRDRE K. & SCHNEIDER, FRED B.** "Doctrine for Cybersecurity". September 2011. Universidad de Berkley.

- **SHOSTACK, ADAM & STEWART,ANDREW** "The new school of information security". April 2008. Ed Addison-Wesley.

- **STIENNON, RICHARD** "Surviving Cyberwar". January 2010.

Auxiliary bibliography

- **CIBERSEGURIDAD. RETOS Y AMENAZAS A LA SEGURIDAD NACIONAL EN EL CIBERESPACIO,** Cuaderno de Estrategia 149. Ministry of Defence http://bibliotecavirtualdefensa.es/BVMDefensa/i18n/catalogo_imagenes/grupo.cmd?path=17029

- **CYBER SECURITY STRATEGY OF THE UNITED KINGDOM.** June 2009. Cabinet Office, Government of the United Kingdom.
http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

- **CANADA'S CYBER SECURITY STRATEGY. FOR A STRONGER AND MORE PROSPEROUS CANADA**. 2010. Government of Canada.
http://www.capb.ca/uploads/files/documents/Cyber_Security_Strategy.pdf

- **CYBER SECURITY STRATEGY FOR GERMANY.** 2011. ENISA.
http://www.enisa.europa.eu/media/news-items/german-cyber-security-strategy-2011-1

- **CYBER SECURITY STRATEGY OF THE CZECH REPUBLIC FOR THE 2011 – 2015 PERIOD.**
http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

- **CYBER SECURITY STRATEGY OF THE UNITED KINGDOM**. June 2009. Cabinet Office. Government of the United Kingdom.
http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

- **DÉFENSE ET SÉCURITÉ DES SYSTÈMES D'INFORMATION STRATÉGIE DE LA FRANCE.** February 2011. National Agtency for the Security of Information Systems. Government of France.
http://www.enisa.europa.eu/media/news-items/french-cyber-security-strategy-2011

- **ENHANCING THE USABILITY AND AVAILABILITY OF INFORMATION INFRASTRUCTURE ESSENTIAL FOR SECURING THE VITAL FUNCTIONS OF SOCIETY".**
http://www.lvm.fi/c/document_library/get_file?folderId=1551284&name=DLFE-11788.pdf&title=Julkaisuja%203-2011

- **ESTONIA CYBER SECURITY STRATEGY.**
http://www.mod.gov.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf
Ministry of Defence Government of Estonia.

- **ESTRATEGIA ESPAÑOLA DE SEGURIDAD.** June 2011. Government of Spain.
http://www.lamoncloa.gob.es/NR/rdonlyres/D0D9A8EB-17D0-45A5-ADFF-46A8A-F4C2931/0/EstrategiaEspanolaDeSeguridad.pdf

- **INDIA CYBERSECURITY STRATEGY.** http://www.mit.gov.in/content/cyber-security-strategy
Government of India.

- **JAPAN: THE FIRST NATIONAL STRATEGY ON INFORMATION SECURITY.** February 2006. Information Security Policy Council. http://www.nisc.go.jp/eng/pdf/national_strategy_001_eng.pdf

- **JOHN H. DEXTER. THE CYBER SECURITY MANAGEMENT SYSTEM: A CONCEPTUAL MAPPING.** February 2002. The SANS Institute.

- **KOWTKO, M. SECURING OUR NATION AND PROTECTING PRIVACY. SYSTEMS, APPLICATIONS AND TECHNOLOGY CONFERENCE (LISAT),** 2011 IEEE Long Island Issue Date: 6-6 May 2011. On page(s): 1 – 6. ISBN: 978-1-4244-9878-9. May 2011. Network, IEEE.

- **LARGE OIL COMPANIES FALL VICTIM TO CYBER-ESPIONAGE POSSIBLE CONNECTION WITH OPERATION AURORA.** January 2010. Sofpedia. http://news.softpedia.com/news/Large-Oil-Companies-Fall-Victim-to-Cyber-Espionage-133317.shtml

- **NEW ZEALAND: THE DIGITAL 2.0 STRATEGY".** ISBN 978-0-478-31645-2. August 2008. Government of New Zealand. http://www.med.govt.nz/upload/11162/Digital%20Strategy%202.0%20FINAL.pdf

- **PROTECCIÓN DE INFRAESTRUCTURAS CRITICAS 2011. S2 GRUPO.** http://www.securityartwork.es/wp-content/uploads/2011/12/Informe_PIC2011_S2Grupo.pdf

- **RAIN OTTIS. ANALYSIS OF THE 2007 CYBER-ATTACKS AGAINST ESTONIA FROM THE INFORMATION WARFARE PERSPECTIVE. PROCEEDINGS OF THE 7TH EUROPEAN CONFERENCE ON INFORMATION WARFARE AND SECURITY.** June 2008. University of Plymouth, UK.

- **SINGAPORE'S STRATEGY IN SECURING CYBERSPACE.** October 2009. Government of Singapore. http://www.ida.gov.sg/News%20and%20Events/20050717164621.aspx?getPagetype=21

- **STEW MAGNUSON. CYBER EXPERTS HAVE PROOF THAT CHINA HAS HIJACKED U.S.-BASED Internet TRAFFIC: UPDATED.** December 2010. NDA's Business and Technology Magazine.

- **STOP. THINK. CONNECT. THE ANTI-PHISHING WORKING GROUP (APWG) AND NATIONAL CYBER SECURITY ALLIANCE (NCSA).** U.S. Department of Homeland Security. http://stopthinkconnect.org/

- **THE US NATIONAL COMPREHENSIVE NATIONAL CYBERSECURITY STRATEGY.** March 2010. National Security Council, EEUU. http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

- **T.M. CHEN. "STUXNET, THE REAL START OF CYBER WARFARE?"** November-December 2010. Network, IEEE.

- **THE NATIONAL CYBER SECURITY STRATEGY (NCSS).** June 2011. Ministry of Security and Justice. The Netherlands.

Websites consulted

- www.inteco.es
- www.ccn-cert.cni.es
- www.dhs.gov
- www.whitehouse.gov
- www.thehackernews.com
- www.ciberseguridad.es
- www.securityartwork.es
- www.rootedcon.es

SCSI
Spanish
Cyber Security
Institute

An iniciative of:

ISMS
Forum Spain

C/ Castello, 24, 5º Derecha, Escalera 1
28001 Madrid T.: 34 91 186 13 50

Further information: www.ismsforum.es