CCDCOE

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Alexander Cendoya

National Cyber Security Organisation: SPAIN

Tallinn 2016

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Upcoming in 2016

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Poland

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of August 2016. We would like to thank all our reviewers for their helpful comments. Any errors or omissions remain our own.

About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and the coordination among them. In particular, it describes the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, Turkey, the United Kingdom and the USA as Sponsoring Nations, and Austria and Finland as Contributing Participants. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO command arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and/or technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

SPAIN

by Alexander Cendoya
Political Analyst

Table of Contents

1. Context and background: information society in Spain

1.1. Internet infrastructure availability and take-up

Spain's development in Information and Communication Technologies (ICT) and e-government is underpinned by the *Digital Agenda for Spain*, which was adopted on 15 February 2013 and conforms to the objectives of the Digital Agenda for Europe.[1] The Digital Agenda for Spain has time horizons for 2015 and 2020, and has 106 action items articulated in nine specific areas, including the rollout of ultrafast telecommunication networks, the incorporation of e-commerce into small and medium-sized enterprises (SME), and incentives to digital economy, digital contents and digital public services.

Spanish households have universal access to broadband services: 95% of all households live in areas covered by fixed broadband service and 100% in areas with 3G mobile broadband access. The actual take-up of broadband is 78% of households, which is near the European Union (EU) average.[2] Internet users in the last quarter of 2015 amounted to slightly more than the European average; 78.7% compared to 78% of the latter. This population of internet users currently amounts to 32.05 million, compared to 31.22 million in 2014.[3]

1.2. e-Government

Law 19/2013 of December 9 on Transparency, Access to Public Information and Good Governance, as well as the implementation of the Transparency Portal of the Government of Spain, have both contributed to Spain's position at the top of the European Union concerning e-Government. By 2013, 99% of services provided by central government authorities (General State Administration, GSA) were available electronically. In 2014, 76% of administrative interaction with the GSA was conducted over the internet, compared with only 23.8% done in person.

As of 2014, Spain was the fourth country in the EU to provide comprehensive public administration services to citizens and businesses through the Internet, amounting to 91.3% of all public administration services, including the GSA. This is 16.1 points higher than the European average, and a slight increase from 2013.[4] In response to citizen demand for e-government services, 49% of Spaniards aged between 16 and 74 made use of electronic administration services, which places Spain two percentage points above the European average.[5] The proportion of businesses using these services amounted to 91.1% in total, and varies depending on company size, from 66.2% in the case of micro-enterprises, to 99% in large corporations.[6]

The targets for electronic transactions between the citizens and public administration, set by the 2013 *Digital Agenda*, were met and exceeded. For example, the share of individuals who used the internet to deal with public authorities in 2015 was 49.37%, and the ratio of citizens submitting completed forms electronically was 30.01%. Both indicators represent a steady growth since 2014, and remain above the EU average.[7]

---

[1] 'Planes y Actuaciones de la Agenda Digital para España', Digital Agenda for Spain, <http://www.agendadigital.gob.es/planes-actuaciones/Paginas/planes-actuaciones.aspx>.
[2] 'Country ranking table, on a thematic group of indicators: Broadband take-up and coverage, Spain, 2015', European Commission, <https://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"broadband"",ref-area":"ES"",time-period":"2015"}>.
[3] 'Indicadores Destacados de la Sociedad de la Información en España, Diciembre 2015', ONTSI, <http://www.ontsi.red.es/ontsi/sites/default/files/indicadores_destacados_diciembre_2015.pdf>.
[4] Alberto Urueña (coord). 'La Sociedad en Red: Informe Anual 2014'. Spain's State Secretariat for Telecommunications and the Information Society, <http://www.ontsi.red.es/ontsi/sites/default/files/informe_anual_la_sociedad_en_red_2014_edicion_2015_0.pdf>.
[5] Ibid.
[6] Ibid.
[7] 'Indicadores Destacados de la Sociedad de la Información en España, Diciembre 2015', ONTSI, <http://www.ontsi.red.es/ontsi/sites/default/files/indicadores_destacados_diciembre_2015.pdf>.

This momentum made Spain worthy of the 2014 United Nations Award for Improving Public Services, and specifically for the Data Intermediation Platform of the Ministry of Finance and Public Administration, which is the second time the department had earned the prize.[8]

1.3. e-Commerce and e-Business

The **National Observatory for Telecommunications and the Information Society (***Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información,* ONTSI) relies on various indicators to monitor the gradual penetration of the Information Society into Spanish businesses, both for e-commerce and e-business. The primary index for e-commerce is the fraction of companies with broadband internet connections, either fixed or mobile, which amounts to 94.2% of all companies, slightly over the EU average. As of September 2015, there were 12.98 million fixed broadband lines for the entire user market – an increase of 4% within one year. The ratio of companies making online purchases amounted to 18.5%, below the European average of 22%, while the proportion of firms in Spain selling online exceeds the EU average, being 16% of all enterprises.[9]

An indicator that the ONTSI takes into account in terms of meeting the Digital Agenda is the number of individuals who use the internet to order goods and services, which in 2015 represented 42.33% of the total Spanish population. In 2014, this indicator was 37.33%, compared against the EU average of 48%.[10] In 2014, e-commerce activities generated €16.3 billion, representing an 11.3% increase from the previous year.[11]

It is worth contextualising these indicators of the Information Society in the landscape of the productive activities of the ICT sector. The latest available data (2014) indicates a recovery in the uptrend after a brief decrease in the ICT sector. The turnover of the industry reached €89.9 billion in 2014. Meanwhile, the number of ICT businesses amounted to 30,797, which represented an annual increase of 3.6%, and the number of employees increased by 3.6% to 427,348 people.[12]

Investment in the sector was €13.9 billion, representing a decrease of 3.1% from the preceding year, and the Gross Value Added (GVA) generated by the sector was €42.8 billion, representing a decrease of 2.0% from 2013. Even so, this GVA in the ICT industry was 4.4% of all the goods and services produced by the Spanish economy.[13]

1.4. Cyber threat landscape

As for cyber incidents, Spain was ranked the third country worldwide in 2015, behind only the United States and the United Kingdom.[14] In 2014 alone, 70,000 incidents were reported, including 80 attacks against critical infrastructures, where losses amounted to €14 billion. According to Spain's **National Cyber Security Institute** (*Instituto Nacional de Ciberseguridad*, INCIBE), by the end of October 2015, more than 42,000 cyber security incidents had been recorded, 63 of them involving critical infrastructure.[15]

[8] 'Líderes Mundiales en e-Government', Marca España, <http://marcaespana.es/talento-e-innovaci%C3%B3n/sectores-punteros/nuevas-tecnolog%C3%ADas/lideres-mundiales-en-e-government>.
[9] 'Planes y Actuaciones de la Agenda Digital para España', Digital Agenda for Spain, <http://www.agendadigital.gob.es/planes-actuaciones/Paginas/planes-actuaciones.aspx>.
[10] Ibid.
[11] 'Informe Anual del Sector TIC y de los Contenidos en España, 2015'. ONTSI, <http://www.ontsi.red.es/ontsi/sites/default/files/destacados_informe_sector_ticc_edicion_2015.pdf>.
[12] Ibid.
[13] Ibid.
[14] 'Moragues: «España es el Tercer País del Mundo que Registró más Ataques Cibernéticos el Año Pasado, cerca de 70.000 Ciberincidentes»', Spain's State Secretariat for Public Administration, 2015, <http://www.seap.minhap.gob.es/web/delegaciones_gobierno/delegaciones/comunidad_valenciana/actualidad/notas_de_prensa/notas/2015/10/15-10-19.html>.
[15] Antonio M. Martín, 'El Sistema GMV para Infraestructuras Críticas bajo Ciberataque', El Mundo, November 2, 2015, <http://www.elmundo.es/economia/2015/11/02/5637323722601dde688b459b.html>.

Spain has three major specialised CERTs[16] that operate at a national level, and employs more than 42,500 professionals in the field of network security, with steady growth expected in this area.[17] Nevertheless, at the moment, Spain is more a consumer than a producer of cyber security.

Spain has made cyber security a subject of national concern, and this awareness has launched a course of action that has brought about significant legislative changes over a short period to address the challenges posed by cyberspace. The *Law 36/2015 of September 28 on National Security* includes indeed cyber security as an area of special interest of National Security[18]. Nevertheless, cyber security has not been established yet as an entirely independent domain within national security.

2. Strategic national cyber security objectives

2.1. National Cyber Security Foundation

Spain was lagging behind the rest of Europe in developing a comprehensive and coordinated defence initiative to cyber risks and threats, although this area was dealt with in a minor way in the *National Security Strategy* (*Estrategia de Seguridad Nacional*, ESN) of 2011. That strategy, for the first time, listed cyber threats and cyber attacks as among the main risks to national security. Since then, a significant amount of work has been done to put this issue at the forefront of the Government's agenda. The formation in July 2012 of the **National Security Department** (*Departamento de Seguridad Nacional*, DSN) under the Prime Minister's Office represented a significant boost to the development of national security through a detailed revision of the ESN 2011.[19]

2.1.1. The National Security Strategy of 2013

As a consequence of the review of the ESN 2011, an improved ESN was passed in 2013. This upgraded strategy helped to define new strategic scenarios and to involve the civil society more actively in national security. In its fourth chapter, which is dedicated to key action lines, the ESN identifies cyber security as one of the twelve priority work areas. The cyber security challenge is equated with traditional threats, such as the fight against terrorism.[20,21]

The document calls for ensuring the safe use of communication networks and information systems through capacity building, to prevent, detect and respond to cyber attacks. To this end, the text traces the following lines of action:

- Increase capabilities for the prevention, detection, investigation and response to cyber threats supported by an efficient and functioning legal framework.
- Guarantee the security of information systems, communication networks and communication infrastructures common to all public administrations, reinforcing the safety of information systems that support critical infrastructures.
- Improve the safety and resilience of ICT in the private sector by deploying state capabilities, while pushing actions directed towards strengthening the public-private partnership and the security of ICT

[16] Computer Emergency Response Team.
[17] 'Estado de la Ciberseguridad 2015', U-tad University Centre, 2015, <https://www.u-tad.com/pdfs/resumen-ejecutivo-ciberseguridad-2015-u_tad.pdf>.
[18] 'Ley 36/2015, de 28 de septiembre, de Seguridad Nacional', Spain's Official State Gazette (BOE). <https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf>.
[19] Mar López Gil, 'Estrategia de Ciberseguridad Nacional', ASTIC, Boletic No 73, May 2015, <http://www.astic.es/sites/default/files/articulosboletic/monografico2marialopezgil.pdf>.
[20] *"Estrategia de Seguridad Nacional 2013: Un Proyecto Compartido",* Prime Minister's Office, <http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf>.
[21] Mario Laborie Iglesias, *"La Estrategia de Seguridad Nacional (Mayo 2013)"* – Spanish Institute for Strategic Studies (IEEE) – Documento de Análisis No 34/2013, <http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA34-2013_EstrategiaSeguridadNacional-2013_MLI.pdf>.

systems employed by the industrial sector.

- Promote professional training in cyber security and boost the Spanish industry through a programme for research, development and innovation (RDI).
- Develop a strong culture of cyber security, raising the awareness of citizens, professionals and companies of the importance of ICT security and the responsible use of new services in the knowledge society.
- Enhance international cooperation for the creation of a safe and reliable cyberspace in collaboration with international initiatives, while safeguarding national interests at all times.

2.1.2. The National Cyber Security Strategy

The *National Cyber Security Strategy* (*Estrategia Nacional de Ciberseguridad,* ENCS) was adopted in December 2013 and is the fundamental document for cyber security in Spain. As a result of the concern articulated in the ESN 2013, the ENCS developed a policy framework, as well as an executive structure, to propel cyber security to the top priorities of national security. The ENCS was adopted by the **National Security Council** (*Consejo de Seguridad Nacional,* CSN) to generate guidelines to ensure the security of cyberspace through the cooperation of all public administrations in Spain, as well as the private sector and the population. These guidelines follow the principles enshrined in the Spanish Constitution of 1978, fundamental rights treaties and international treaty obligations, and are consistent with the ESN and the initiatives developed within the European framework.[22,23]

The ENCS reflects the important raise of awareness of the Spanish authorities on cyber security issues in a very short period, although it leaves room for further definition of risks and threats, and keeps the central authority of the CSN in cyber security without establishing a national specialised agency with real executive capacity.

2.1.3. National Cyber Security Plan

In October 2014, the National Cyber Security Council adopted the *National Cyber Security Plan*, after identifying the challenges faced by Spain, by defining the action guidelines for the next two years to achieve optimal implementation of the objectives outlined in the ENCS. This action plan, which marked the first step in the development of the ENCS, allocates responsibilities within the group of agencies represented on the Council for the effective application of the ENCS. Its mission is implemented through a series of Derivative Action Plans that have established seven working groups whose activities were completed during the first half of 2015. These derivative plans include action items for:

- Strengthening and improving capabilities, and ensuring cooperation on cyber security and cyber defence;
- Guaranteeing the security of the ICT systems of the Administration;
- Protection and resilience of the ICT systems that support critical infrastructure;
- Activation of the resources available to fight cyber crime and cyber terrorism;
- Protection and resilience of the ICT systems of the private sector;
- Boosting industrial development and professional training, and increasing RDI;
- Fostering the culture of cyber security;
- International cooperation with countries in the EU and elsewhere; and
- Exchange of information on threats.

[22] 'Estrategia de Ciberseguridad Nacional 2013', Prime Minister's Office, <http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf>.
[23] María José Caro Bejarano, 'Estrategia de Ciberseguridad Nacional', Spanish Institute for Strategic Studies (IEEE) – Documento de Análisis No 65/2013, <http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf>.

2.2. Objectives of the Cyber Security Strategy

The overall objective of the ENCS is to 'ensure that Spain makes practical use of ICT systems, reinforcing the capacities of prevention, defence, detection and response to cyber attacks, and building confidence in the use of ICT'.[24]

The National Cyber Security Policy is aligned with its counterparts in neighbouring countries and with the relevant European and international organisations, and in particular with the Cyber Security Strategy of the EU. Based on guiding principles, including leadership at Prime Ministerial level, shared responsibility, rational proportionality and international cooperation, the ENCS defines the following objectives for national cyber security:

1. Ensure that the ICT systems used by public administrations possess the appropriate level of cyber security and resilience, as much of the information they store amounts to a strategic national asset. This objective follows the second strategic action line of the ESN directly, referring to the security of public administrations.
2. Promote the security and resilience of the ICT systems used by the business sector in general, and the operators of critical infrastructure in particular, since private industry owns the vast majority of the communication networks and systems that provide essential services to society, including ICT resources. This purpose follows the third strategic action line of the ESN, which refers to the safety and resilience of the private sector, and is also linked to the fourth.
3. Improve the faculties for the prevention, detection, reaction, analysis, retrieval, response, research and coordination of activities against terrorism and crime in cyberspace. This objective reproduces the first strategic action line of the ESN almost entirely.
4. Raise awareness among citizens, companies and public administrations of the risks associated with cyberspace. This statement reproduces the fifth strategic action line of the ESN almost directly.
5. Achieve and maintain the knowledge base, skills, experience and technological capabilities that Spain needs to support its goals of cyber security. This goal also follows the fifth strategic action line and is linked to the fourth.
6. Contribute to the state-of-the-art in cyber defence in the international arena. This aim follows the sixth strategic action line of the ESN, which refers to international cooperation in cyber security.

To carry out these objectives, the ENCS prescribes more concrete lines of action, such as enhancing the detection capabilities and protection of classified government systems, and promoting regulation of critical infrastructure protection and the necessary strength for the protection of essential services, and ensures the implementation of the *National Security Scheme* (*Esquema Nacional de Seguridad*, ENS) for public administration.

3. National organisational structure for cyber security and cyber defence

3.1. National political and strategic level management framework

The ESN 2013 set up a new National Security System in which the **Prime Minister** holds responsibility for the management, leadership and promotion of the national security policy. The core of this system is the **National Security Council** (CSN) which is a collegiate organ comprised of the Deputy Prime Minister, the relevant State Secretaries, the Director of the Prime Minister's Office, and other members of the government. The CSN holds regular meetings which are chaired by the Prime Minister unless the King is present. The CSN is appointed as a Government Delegate Commission for National Security, and has an all-inclusive and flexible composition that

[24] 'Estrategia de Ciberseguridad Nacional 2013', Prime Minister's Office, <http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf>.

depends on the requirements of each situation. It is tasked with assisting the Prime Minister with the management and coordination of the National Security Policy.

On the initiative of the CSN, specialised committees have been established to support the Council in specific areas of ESN 2013. These committees are to be activated in particular situations that require the coordination of various agencies of the Public Administration, and are thus composed of the appropriate public authorities in the corresponding subject as well as private agents when required. The specialised committees are supported by the Situation Centre of the National Security Department (DSN) as a Technical Secretariat and permanent working body of the CSN to ensure their interconnection with the centres involved, and to develop an optimal response to the crisis. The Situation Centre can also be reinforced by specialists coming from relevant bodies, thus forming a coordination cell that is unique to the situation. In this sense, the powers of the specialised committees are defined in the provisions applicable to the given situation.

Within the field of cyber crises and cyber-related issues, two specific specialised committees assist the CSN with the operation of the ENCS: the Specialised Cyber Security Council and the Specialised Situation Committee.

3.1.1. The National Cyber Security Council

The **National Cyber Security Council** (CNC) is a collegiate body that supports the CSN in assisting the Prime Minister on cyber security issues, both nationally and internationally, through analyses, studies and initiatives. It assumes the coordination, collaboration and cooperation of the relevant public administrations on cyber security, and works to strengthen relations between the public and private sectors. The CNC is the specialised cyber security council ordered by the ENCS, and is chaired by a relevant State Secretary, with the DSN filling the positions of Vice Chairman and Secretary.

3.1.2. The Specialised Situation Committee

The **Specialised Situation Committee (***Comité Especializado de Situación*)[25] is tasked with assisting the CSN in crisis situations on cyber security matters that have not been channelled through conventional response mechanisms due to their extent or nature. The Situation Committee supports the CSN in the latter's mandate to manage a specific and effective response through a single governing body. The duties of the Situation Committee include giving political-strategic guidelines for the management of crisis situations; encouraging the optimum use of the resources available; promoting international cooperation; analysing possible crisis scenarios; and convening an extraordinary session of the CSN in an event of crisis.

3.2. National cyber incident response

The main official organ tasked with information security is the **National Cryptologic Centre** (*Centro Criptológico Nacional,* CCN). The CCN was established in 2004 under the Spanish intelligence service, the National Intelligence Centre (*Centro Nacional de Inteligencia*, CNI), which is currently part of the Ministry of the Presidency. The management of the CCN is assigned to the Head of the CNI by *Law 11/2002 of May 6*, which entrusts it with the security of information technology and the protection of classified information.

There is no specific legislation for the CCN, so it is regulated by the law applicable to the CNI. The CNI is governed by *Royal Decree 421/2004 of March 12*, a disposition that was later reinforced by *Royal Decree 3/2010 of January 8*, which outlines the National Security Scheme (ENS), an action plan determining the security policy to be applied to the use of electronic media of public administrations, and which established the basic principles and minimum requirements for the proper protection of information.[26] The measures launched by the ENS include the

[25] 'Comité Especializado de Situación', Spain's National Security Department, <http://www.dsn.gob.es/sistema-seguridad-nacional/comit%C3%A9s-especializados/comit%C3%A9-especializado-situaci%C3%B3n>.
[26] 'Esquema Nacional de Seguridad', Spanish Portal of Electronic Administration, <https://administracionelectronica.gob.es/ctt/ens#.VmhWutLhDs3>.

establishment of security policies, as well as the introduction of common elements to guide the actions of the Government on information security.[27,28] The ENS guides the actions of the CCN.

The responsibilities of the CCN include the security of systems belonging to the Government that process, store or convey information in electronic form, as well as the security of systems with classified information. According to the rules, these systems require protection and encryption to manage that confidential information, which may have originated and be used nationally, in addition to information related to NATO, the EU, and various international treaties.[29]

The CCN carries out functions on a technical level, which include the development and dissemination of rules, instructions, guidelines and recommendations to ensure the security of the ICT systems of the Public Administration, and the coordination of the promotion, development, procurement, commissioning and operation of security technologies. It also assesses and certifies the capabilities of encryption products and ICT systems to manage information securely though a certification body.[30] It also coordinates joint responses to security incidents at national and international level.

The response capacity of the CCN to incidents is embodied in the **CCN-CERT**, a centre established to become the core for national alerts and charged with helping all public bodies to respond quickly and efficiently to potential security incidents.[31] As with any CERT, it has the function of managing cyber incidents from initial notification to closure, thus completing the cycle defined in the incident management process. This process is subject to the implementation of mechanisms for both reactive and proactive protection based on the perceived threats, thus describing a constant and flexible relationship between threats and responses.[32]

The services offered by the CCN-CERT include:

- Incident management, which may be requested by any public body suffering a cyber attack.
- Alerting to threats and vulnerabilities through the publication and updating of various rules and procedures and a monthly report on security incidents. Among the publications of the CCN-CERT, the National Report on the State of Security (*Informe Nacional del Estado de Seguridad*, INES) aims to facilitate the work of the agencies with an additional report on the security situation of the public bodies, and the individual monitoring of each organ in the ENS.
- Audits of websites to ensure adequate management of potential vulnerabilities.
- An Early Warning System (EWS), which was created in 2008 for the quick and efficient detection of incidents within the public administration.
- Multi-antivirus or malware analysis systems, which allow the analysis of all kinds of code using multiple real-time antivirus engines, and consequently allow a public body with a potentially infected file be able to upload it to the CCN-CERT servers using a web interface to receive a report on that file via email.
- Web analysis system, which offers ICT managers a real-time security status of their websites for the monitoring of possible incidents. For this purpose, this system performs an analysis of the contents hosted on different websites of the public administration.

[27] 'Informe de Actividades 2008, 2009, 2010', National Cryptologic Centre, <https://www.ccn-cert.cni.es/publico/memoria/InformedeActividadesCCN2010.pdf>.
[28] An amendment to the ENS was passed in 2015 by revising *Royal Decree 3/2010 of January 8* to update and adapt the ENS in greater detail to the applicable European directives. This amendment was made in response to the goals of the ENCS. See 'Real Decreto 951/2015, de 23 octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema de Nacional de Seguridad en el ámbito de la Administración Electrónica', Spain's Official State Gazette (BOE) <https://boe.es/boe/dias/2015/11/04/pdfs/BOE-A-2015-11881.pdf> .
[29] 'Informe de Actividades 2008, 2009, 2010', National Cryptologic Centre, <https://www.ccn-cert.cni.es/publico/memoria/InformedeActividadesCCN2010.pdf>.
[30] Certification Body of the National Scheme for the Assessment and Certification of Information Technology Security.
[31] 'Informe Anual de Seguridad Nacional 2014', Spain's National Security Department, <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf>.
[32] 'Respuesta a Incidentes en Infraestructuras Críticas', INCIBE, <https://www.incibe.es/CERT/Infraestructuras_Criticas/>.

The EWS is a part of the SARA Network, which is a communication network created by the Spanish government to facilitate the exchange of information and access to services among the different public bodies in Spain, and between these boards and the European institutions. This EWS allows the proactive detection of anomalies and attacks on the various ministries and agencies of the GSA connected to this network. The EWS covers all administrative territorial units in Spain providing a real-time overview of the cyber security situation in the state infrastructures and classifying different threat levels.

Other analysis tools employed to improve preventive threat detection include LUCIA,[33] CARMEN[34,35] and PILAR.[36]

The CCN-CERT also employs an EWS to provide specific probes to particular individuals or firms, and has a web portal with a private area for more than 6,000 registered users. It offers a broad range of online courses for the dissemination of the cyber security culture and practical training on this subject.[37,38]

3.3. Military cyber defence

The **Joint Cyber Command** (*Mando Conjunto de Ciberdefensa,* MCCD), created by *Ministerial Order 10/2013 of February 19*, is the Spanish cyber command and the body in charge of cyber defence matters within the Ministry of Defence. As part of the Spanish Joint Chiefs of the Defence Staff, this institution commands and coordinates the activities of the Army Forces in this field, including the development, management and control of information security enforcement policies. Its mission is to plan and carry out military cyber defence actions in the telecommunication networks and information systems of the Armed Forces, or other networks that may be entrusted to it.

The MCCD contributes, at a tactical level, to the optimal response in cyberspace to risks or threats that may affect national defence. In this sense, it cooperates with national centres such as the INCIBE and the CNI in response to information security incidents, and takes responsibility for defining, managing and coordinating awareness and specialised training activities in the field of cyber defence.

In 2014, a **Centre for the Response to Cyber Security Incidents** (*Centro de Respuesta ante Incidentes de Ciberseguridad del Ministerio de Defensa,* ESPDEFCERT) was established by the Ministry of Defence at the offices of the MCCD. This centre operates at a technical level to facilitate the work of defence, exploitation and response, utilising forensic laboratories and other RDI facilities.[39]

3.4. Cyber aspects of crisis management

3.4.1. Cyber crisis prevention and coordination

In addition to the CCN-CERT, other institutions in Spain have a role in the prevention of and immediate response to cyber crises with regard to critical infrastructures. Critical infrastructures are defined by *Law 8/2011* as those 'whose operation is vital and do not allow alternative solutions, so its disruption or destruction would have a severe impact on essential services'.[40] The legislation over critical infrastructure (*Law 8/2011* and *Royal Decree*

[33] LUCIA: Unified List for the Coordination of Incidents and Threats (*Listado Unificado de Coordinación de Incidentes y Amenazas*).
[34] CARMEN: Centre for Record Analysis and Event Mining (*Centro de Análisis de Registros y Minería de Eventos*).
[35] 'Informe Anual de Seguridad Nacional 2014', Spain's National Security Department, <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf>.
[36] PILAR: Logic Computer Procedure for Risk Analysis (Procedimiento Informático Lógico para el Análisis de Riesgos).
[37] 'Informe de Actividades 2008, 2009, 2010', National Cryptologic Centre, <https://www.ccn-cert.cni.es/publico/memoria/InformedeActividadesCCN2010.pdf>.
[38] Ibid
[39] 'Informe Anual de Seguridad Nacional 2014', Spain's National Security Department, <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf>.
[40] 'Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas', Spain's Official State Gazette (BOE) <http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf>.

704/2011) recognises the need to ensure the best possible procurement of basic services through mechanisms that provide complete security at all levels of critical infrastructures.[41]

Under the State Secretariat for Security (*Secretaría de Estado de Seguridad,* SES) of the Home Ministry, the **National Centre for Critical Infrastructure Protection** (*Centro Nacional para la Protección de Infraestructuras Críticas,* CNPIC) is responsible for the protection of critical infrastructures. This agency, which operates at the tactical level, is charged with the promotion, coordination and supervision of all the activities concerning the protection of critical infrastructures for which the SES is competent at a national level.[42] In that sense, the CNPIC must refer to the SES in the event of a cyber emergency.

The annexe to the Royal Decree specifies twelve sectors of critical infrastructure: government, space, nuclear industry, research laboratories, chemical industry, water, energy, health, transport, food supply, the tax system, and ICT, without giving to the latter any particular importance over the remaining sectors.

Attached to the CNPIC is another agency – the **Office for Cyber Coordination** (*Oficina de Coordinación Cibernética*, OCC) – which was founded in 2014 to establish a secure and centralised channel within the competence framework of the Home Ministry for early warning and the permanent exchange of information regarding vulnerabilities, cyber threats and cyber attacks.[43,44]

A valuable public company dealing specifically with cyber incidents in critical infrastructure is INCIBE, the **National Cyber Security Institute** which works under the State Secretariat for Telecommunications and the Information Society (*Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información* SETSI), which belongs to the Ministry of Industry, Energy and Tourism, with the mission of strengthening cyber security and privacy, as well as trust in the services of the Information Society. INCIBE coordinates efforts with national and international agencies responsible for cyber security. In the event of a serious threat, the INCIBE will refer it to its corresponding State Secretariat.

In 2012, the **Information Security Incident Response Centre** (*Centro de Respuesta a Incidentes de Seguridad de la Información*, CERTSI) was launched in a joint operation of the Home Ministry and the Ministry of Industry through a Partnership Framework Agreement on Cyber Security between SES and SETSI, and it is currently governed by the Agreement of October 21 2015 signed by both ministries. Technically operated by the INCIBE, the CERTSI works under the coordination of the INCIBE and the CNPIC, giving technical support to the latter for the prevention and response to cyber incidents that could affect the networks and systems of critical infrastructure operators, either public or private. Additionally, the CERTSI must collaborate with the OCC and Spanish law enforcement bodies.[45] The CERTSI provides prevention, detection, early warning and incident response services to the relevant organisations under a three-way confidentiality agreement, and promotes the exchange of information among agencies. CERTSI also has responsibility for the management of cyber security incidents on the Iris Network, which is the academic and research network in Spain.[46]

For the prevention and detection of cyber crime in general, there is also an agency called the **Computer Crime Group** (*Grupo de Delitos Telemáticos,* GDT) within the Civil Guard, which is a Spanish military police body. Through its website, this agency offers the possibility of reporting cyber crimes. Hosted by the Home Ministry,

---

[41] 'Respuesta a Incidentes en Infraestructuras Críticas', INCIBE, <https://www.incibe.es/CERT/Infraestructuras_Criticas/>.
[42] 'INCIBE: Instituto Nacional de Ciberseguridad', INCIBE, <https://www.incibe.es/home/instituto_nacional_ciberseguridad/>.
[43] 'Instrucción Núm. 15/2014, de la Secretaría de Estado de Seguridad, por la que se Crea la Oficina de Coordinación Cibernética', Spain's State Secretariat for Security,
<http://www.academiauniform.es/mediapool/81/814638/data/2014/Instrucc._15_14_Oficina_coordinacion_cibernetica.pdf>.
[44] 'Informe Anual de Seguridad Nacional 2014', Spain's National Security Department,
<http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf>.
[45] Mar López Gil, 'Estrategia de Ciberseguridad Nacional', ASTIC, Boletic No 73, May 2015,
<http://www.astic.es/sites/default/files/articulosboletic/monografico2marialopezgil.pdf>.
[46] 'Informe Anual de Seguridad Nacional 2014', Spain's National Security Department,
<http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf>.

the GDT investigates all crimes committed via the internet. The GDT participates in cyber crime work groups within Interpol, in Europe and Latin America, the Group of Eight (G8), and Europol.

Last but not least, the **Technological Investigation Brigade of the National Police** (*Brigada de Investigación Tecnológica,* BIT), under the Home Ministry, also pursues cyber crime. Both the BIT and the GDT are part of Spain's law enforcement bodies.

3.4.2. Cyber crisis management

Cyber security is regarded as one of the areas of particular concern for national security, at the same level as economic, financial, health, and environmental protections. In the same way as these areas, cyber security is considered to require specific attention to preserving fundamental rights and freedoms and the well-being of citizens, and ensure the supply of essential resources and services. The public administrations with competencies in areas of particular concern have the task of establishing mechanisms for the coordination and exchange of information, in particular concerning surveillance and alerts to potential risks and threats, as well as providing essential resources.[47]

In this regard, *Law 36/2015 of September 28 on National Security* regulates basic principles, higher bodies, authorities, and key components of National Security. This Act encompasses the management of national crises, including decisions concerning cyber security, seeking a coordination framework for public administrations, and emphasising their participation.

Under the *Law on National Security*, crisis management will be developed through instruments of prevention, detection, response, return to normal, and evaluation. This development will be gradual and will involve the various organs that make up the structure of the National Security System, according to their competencies and the concrete crisis situations. Also, the authorities of the autonomous community affected will participate in the crisis management.

In Spain, crisis management is centralised in the **CSN** and, within that body, in the figure of the **Prime Minister**, even though the task of coordinating the various agencies involved corresponds to the DSN Situation Centre by creating coordination cells. Currently, there is no such thing as a central national authority dealing exclusively with cyber security in Spain. Because of this, the functions of the CSN in the management of cyber crises do not differ from crisis management of any kind. These duties include the following:

- Issue the necessary guidelines for planning and coordination of the national security policy;
- Lead and coordinate the activities of crisis management;
- Supervise and coordinate the National Security System;
- Verify the level of compliance with the ESN and promote and advance its reviews;
- Support and encourage the development of the necessary second-level strategies, and if appropriate, proceed with their approval and periodic evaluations;
- Organise the contribution of resources to National Security as provided in that Act;
- Approve the Annual Report of National Security before its presentation to Parliament;
- Agree on the creation and strengthening of support bodies that are necessary for the performance of its duties;
- Promote the appropriate legislative proposals to strengthen the National Security System; and
- Perform other functions assigned by the laws and regulations that may apply.

It is the Prime Minister's responsibility to declare a situation of interest to national security by Royal Decree and to define its essential aspects. The declaration of a situation of interest for the country's security will involve an obligation for the authorities to provide the necessary human and material resources that are under their control

[47] 'Ley 36/2015, de 28 de Septiembre, de Seguridad Nacional', Spain's Official State Gazette (BOE) <https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf>.

for the effective implementation of action mechanisms. Also, the Government will immediately inform Parliament about the measures adopted and the evolution of the situation of interest.

Another institution that plays a fundamental role in crisis management is the **DSN**. Created in 2012, this advisory body to the Prime Minister on National Security Affairs assumes the functions of both a technical secretariat and a permanent work group of the CSN. Its *raison d'être* resides in the need to strengthen the Prime Minister's Office to assist the Prime Minister in his or her responsibility to lead the national security policy of Spain. In a crisis, the DSN provides a comprehensive and transversal vision of the crisis to be managed and supports the activities of the Specialised Committee on the subject. The DSN shall perform the functions that are proper to this body and other functions under the applicable rules.[48]

In their capacity as head of the National Security System, the Prime Minister shall also be assisted by the CNC, the Situation Committee and the Cyber Security Coordination Cell.

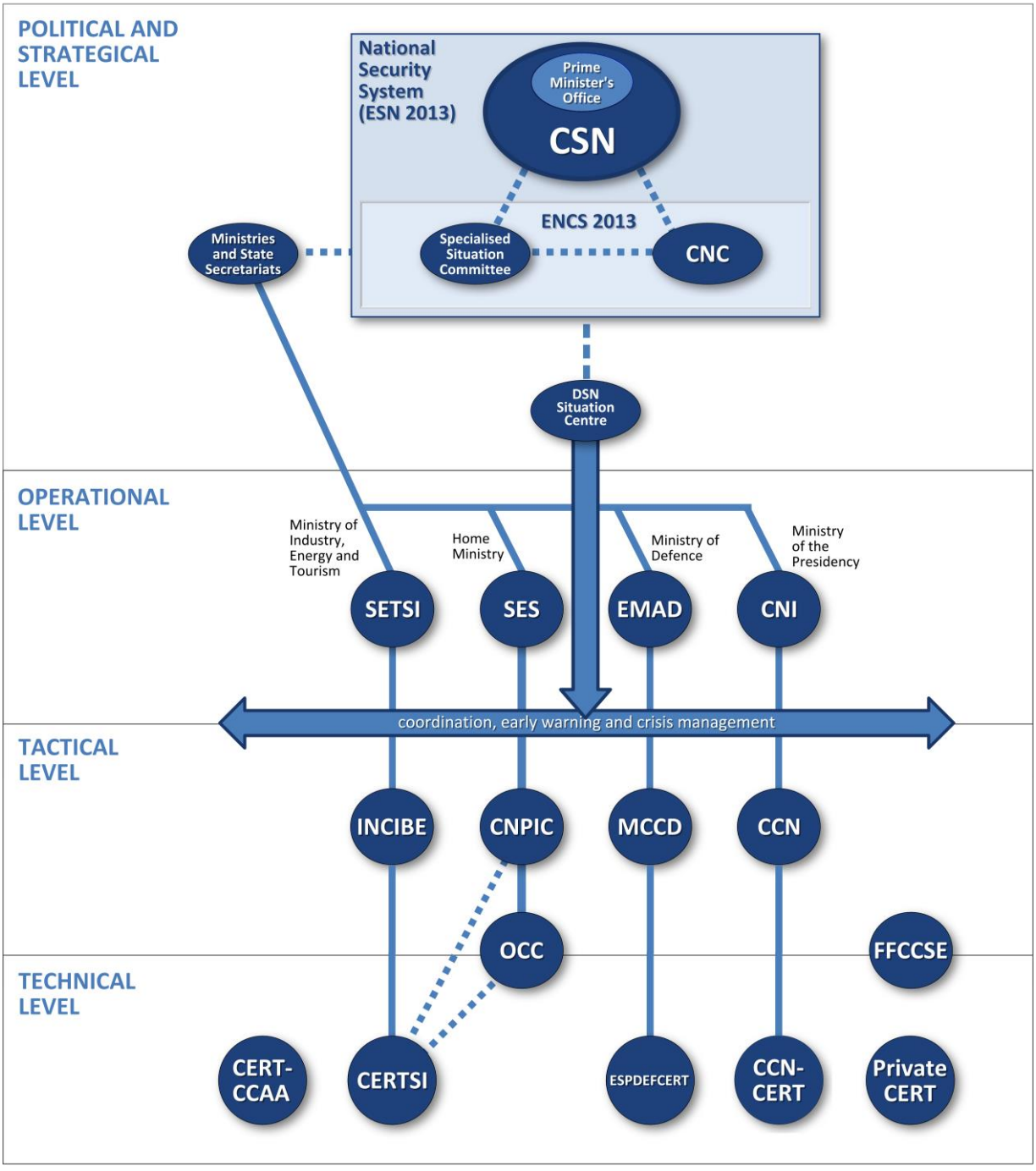
3.5. Private sector

The INCIBE fosters information and response services in the cyber security field that allow businesses and professionals to make an optimal use of ICTs and raise the level of digital trust, placing special emphasis on the protection of strategic operators. Specifically, the INCIBE works for the user's protection and privacy, creating mechanisms for the prevention and reaction to data security incidents, minimising their impact and promoting advances in the culture of data security through training and the raising of awareness. To that end, the INCIBE participates in various partnership networks with other public and private entities, either national or international, which allows its operations in the field of cyber security to be immediate, global and effective, and provides it a perspective based on experience and exchange of information.

In that sense, the INCIBE has organised an annual seminar of cyber exercises called CyberEx since 2012 in coordination with the CNPIC and several business associations. The objective of this event is to develop the responsiveness of the participating bodies, foster coordination and cooperation among institutions, and deepen awareness of the risks that exist in cyberspace. These exercises are carried out in a Capture the Flag (CTF) format and are based on a competition model of the deployment of security capacities, designed as training aimed at the growth of expertise in tracking intrusions and the development of skills against cyber attacks by reproducing incidents that may occur in reality.[49,50] In 2015, CyberEx obtained an international range, since it was held in the framework of the Organization of American States (OAS) with the name International CyberEx.

[48] 'Departamento de Seguridad Nacional', Spain's National Security Department, <http://www.dsn.gob.es/es/sistema-seguridad-nacional/departamento-seguridad-nacional>.
[49] 'Primera Edición del International CyberEx', INCIBE, <https://www.incibe.es/CERT/primera_edicion_international_cyberex>.
[50] 'Informe Anual de Seguridad Nacional 2014', Spain's National Security Department, <http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf>.

Annexe: Organisational Chart of Cyber Security in Spain



LEGEND:

relationship of dependence

operational relationship

Please, see acronyms in the next page.

List of Acronyms

BIT	*Brigada de Investigación Tecnológica* (Technological Investigation Brigade)
BOE	*Boletín Oficial del Estado* (Spain's Official State Gazette)
CARMEN	*Centro de Análisis de Registros y Minería de Eventos* (Centre for Record Analysis and Event Mining)
CCAA	*Comunidades Autónomas* (Autonomous Communities)
CCN	*Centro Criptológico Nacional* (National Cryptologic Centre)
CCN-CERT	Computer Emergency Response Team of the National Cryptologic Centre
CERT	Computer Emergency Response Team
CERT-CCAA	Computer Emergency Response Team belonging to an Autonomous Community
CERTSI	*Centro de Respuesta a Incidentes de Seguridad de la Información del Ministerio de Industria, Energía y Turismo y del Ministerio del Interior, i.e. CERT Seguridad e Industria* (Information Security Incident Response Centre of the Ministry of Industry, Energy and Tourism and the Home Ministry)
CNC	*Consejo Nacional de Ciberseguridad* (National Cyber Security Council)
CNI	*Centro Nacional de Inteligencia* (National Intelligence Centre)
CNPIC	*Centro Nacional para la Protección de Infraestructuras Críticas* (National Centre for Critical Infrastructure Protection)
CSN	*Consejo de Seguridad Nacional* (National Security Council)
CTF	Capture the Flag
DSN	*Departamento de Seguridad Nacional* (National Security Department)
EMAD	*Estado Mayor de la Defensa* (Chiefs of the Defence Staff)
ENCS	*Estrategia Nacional de Ciberseguridad* (National Cyber Security Strategy)
ENS	*Esquema Nacional de Seguridad* (National Security Scheme)
ESN	*Estrategia de Seguridad Nacional* (National Security Strategy)
ESPDEFCERT	*Centro de Respuesta ante Incidentes de Ciberseguridad del Ministerio de Defensa* (Centre for the Response to Cyber Security Incidents)
EU	European Union
EWS	Early Warning System
FFCCSE	*Fuerzas y Cuerpos de Seguridad del Estado* (all law enforcement bodies in Spain)
GDT	*Grupo de Delitos Telemáticos* (Computer Crime Group)
GSA	General State Administration
GVA	Gross Value Added

ICT	Information and Communication Technologies
INCIBE	*Instituto Nacional de Ciberseguridad de España* (Spain's National Cyber Security Institute)
INES	*Informe Nacional del Estado de Seguridad* (National Report on the State of Security)
LUCIA	*Listado Unificado de Coordinación de Incidentes y Amenazas* (Unified List for the Coordination of Incidents and Threats)
MCCD	*Mando Conjunto de Ciberdefensa de la Fuerzas Armadas* (Joint Command of Cyber Defence of the Armed Forces)
NATO	North Atlantic Treaty Organization
OAS	Organization of American States
OCC	*Oficina de Coordinación Cibernética* (Office for Cyber Coordination)
ONTSI	*Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información* (National Observatory for Telecommunications and the Information Society)
PILAR	*Procedimiento Informático Lógico para el Análisis de Riesgos* (Logic Computer Procedure for Risk Analysis)
R&D+i	Research, Development and Innovation
SARA	*Sistema de Aplicaciones y Redes para las Administraciones* (System of Application and Networks for Administrations)
SES	*Secretaría de Estado de Seguridad* (State Secretariat for Security)
SETSI	*Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información* (State Secretariat for Telecommunications and the Information Society)
SME	Small and Medium-sized Enterprise

References

Policy

Ciberseguridad GITS Informática. 2015. *"Ciberguerra, Ciberespionaje, Ciberterrorismo y Ciberdefensa".* Accessed December 2, 2015. http://www.gitsinformatica.com/ciberguerra.html

Digital Agenda for Spain. 2016. "Planes y Actuaciones de la Agenda Digital para España". Accessed January 5, 2016. http://www.agendadigital.gob.es/planes-actuaciones/Paginas/planes-actuaciones.aspx

Spain's National Security Department. 2015. *"Consejo Nacional de Ciberseguridad".* Accessed December 2, 2015. http://www.dsn.gob.es/es/sistema-seguridad-nacional/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad#collapseSix

Spain's National Security Department. 2015. *"Informe Anual de Seguridad Nacional 2014".* April. Accessed December 2, 2015. Madrid: Boletín Oficial del Estado: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2015/Informe_Anual_de_Seguridad_Nacional_2014.pdf

Spain's Prime Minister's Office. 2013. *"Estrategia de Seguridad Nacional 2013: Un Proyecto Compartido".* May. Accessed December 2, 2015. http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf

Spain's Prime Minister's Office. 2015. *"El Ministerio del Interior Activa el Plan Nacional de Protección de Infraestructuras Críticas para Proteger los Servicios Esenciales tras el Atentado en París".* January 8. Accessed December 2, 2015. http://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/mir/Paginas/2015/080115proteccioninfraestr.aspx

Spain's Prime Minister's Office. 2015. *"Estrategia de Ciberseguridad Nacional 2013".* Accessed December 2, 2015. http://www.lamoncloa.gob.es/documents/20131332estrategiadeciberseguridadx.pdf

Law

Spain's Official State Gazette (BOE). 2011. *"Ley 8/2011, de 28 de abril, por la que se Establecen Medidas para la Protección de las Infraestructuras Críticas".* April 28. Accessed December 2, 2015. http://www.boe.es/boe/dias/2011/04/29/pdfs/BOE-A-2011-7630.pdf

Spain's Official State Gazette (BOE). 2013. *"Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno".* December 9. Accessed January 5, 2016. https://www.boe.es/boe/dias/2013/12/10/pdfs/BOE-A-2013-12887.pdf

Spain's Official State Gazette (BOE). 2015. *"Ley 36/2015, de 28 de septiembre, de Seguridad Nacional".* September 29. Accessed January 5, 2016. https://www.boe.es/boe/dias/2015/09/29/pdfs/BOE-A-2015-10389.pdf

Spain's Official State Gazette (BOE). 2015. *"Real Decreto 951/2015, de 23 octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema de Nacional de Seguridad en el ámbito de la Administración Electrónica".* November 4. Accessed January 5, 2016. https://boe.es/boe/dias/2015/11/04/pdfs/BOE-A-2015-11881.pdf

Spain's State Secretariat for Security. 2014. *"Instrucción Núm. 15/2014, de la Secretaría de Estado de Seguridad, por la que se Crea la Oficina de Coordinación Cibernética".* November 19. Accessed December 2, 2015. http://www.academiauniform.es/mediapool/81/814638/data/2014/Instrucc._15_14_Oficina_coordinacion_cibernetica.pdf

Other

Arteaga, Félix and Enrique Fojón Chamorro. 2015. *"En Favor de una Política Nacional de Ciberseguridad en España".* Comentario 21/2015, March 23. Accessed December 2, 2015. http://www.realinstitutoelcano.org/wps/portal/web/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/defensa+y+seguridad/comentario-arteaga-fojon-en-favor-de-una-politica-nacional-de-ciberseguridad-en-espana

Caro Bejarano, María José. 2013. *"Estrategia de Ciberseguridad Nacional".* Spanish Institute for Strategic Studies (IEEE) – Documento de Análisis No 65/2013, December 9. Accessed December 2, 2015. http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA65-2013_EstrategiaCiberseguridadNacional_MJCB.pdf

Elcano Royal Institute and THIBER, the Cyber Security Think Tank. 2015. *"Informe Mensual de Ciberseguridad nº 8".* November. Accessed December 2, 2015. http://www.realinstitutoelcano.org/wps/wcm/connect/ffcecf804a6f8329b55dbf207baccc4c/Ciber_Elcano_Num8.pdf?MOD=AJPERES&CACHEID=1446483227266

European Commission. 2015. *"Country ranking table, on a thematic group of indicators: Broadband take-up and coverage, Spain, 2015".* Accessed December 2, 2015. https://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"broadband"“,ref-area":"ES"“,time-period":"2015"}

Fojón Chamorro, Enrique. 2013. *"La Estrategia de Ciberseguridad Nacional… aún queda mucho trabajo por hacer".* The Elcano Royal Institute's Blog, December 11. Accessed December 2, 2015. http://www.blog.rielcano.org/la-estrategia-de-ciberseguridad-nacionalaun-queda-mucho-trabajo-por-hacer/

Fojón Chamorro, Enrique. 2014. *"Año I de la Estrategia de Ciberseguridad Nacional".* The Elcano Royal Institute's Blog, December 11. Accessed December 2, 2015. http://www.blog.rielcano.org/ano-de-la-estrategia-de-ciberseguridad-nacional/

Kaska, Kadri and Lorena Trinberg. 2015. "Regulating Cross-Border Dependencies of Critical Information Infrastucture" Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE). Accessed December 14, 2015. https://ccdcoe.org/sites/default/files/multimedia/pdf/CII_dependencies_2015.pdf

Laborie Iglesias, Mario. 2014. *"La Estrategia de Seguridad Nacional (Mayo 2013)".* Spanish Institute for Strategic Studies (IEEE) – Documento de Análisis No 34/2013, June 3. Accessed December 2, 2015. http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA34-2013_EstrategiaSeguridadNacional-2013_MLI.pdf

López Gil, Mar. 2015. "Estrategia de Ciberseguridad Nacional", ASTIC, Boletic No 73, May. Accessed December 2, 2015. http://www.astic.es/sites/default/files/articulosboletic/monografico2marialopezgil.pdf

Marca España. 2015. *"Líderes Mundiales en e-Government",* Accessed December 14, 2015. http://marcaespana.es/talento-e-innovaci%C3%B3n/sectores-punteros/nuevas-tecnolog%C3%ADas/lideres-mundiales-en-e-government

Martín, Antonio M. 2015. *"El Sistema GMV para Infraestructuras Críticas bajo Ciberataque".* El Mundo, November 2. Accessed December 2, 2015. http://www.elmundo.es/economia/2015/11/02/5637323722601dde688b459b.html

Robles Carrillo, Margarita. 2015. *"El Ciberespacio y la Ciberseguridad: Consideraciones sobre la Necesidad de un Modelo Jurídico".* Spanish Institute for Strategic Studies (IEEE) – Documento de Opinión 124/2015, November 17. Accessed December 2, 2015.

http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO124-2015_Ciberespacio-CIberseguridad_Margarita-Robles.pdf

Spain's Centre for Higher Studies of National Defence (CESEDEN). 2013. *"Guerra Cibernética, Aspectos Organizativos".* Paper presented at the 33rd Course on National Defence by the Work Group No 3, Gen. Ramón Prieto Osés (pres). – School of High Studies of Defence (EALEDE) – Madrid, Spain. January, 14 - April, 25. Accessed December 2, 2015. http://www.defensa.gob.es/ceseden/Galerias/ealede/cursos/curDefNacional/ficheros/Ciberseguridad_nuevo_reto_del_siglo_XXI_Guerra_cibernetica_aspectos_organizativos.pdf

Spain's Chiefs of the Defence Staff. 2013. *"Ciberseguridad y Ciberdefensa Nacional".* Paper presented at the seminar "Network Security: Protecting Society from the Threats of the XXI Century" held at the Spanish Institute of Engineering (IIES) by Col. Francisco Zea Pasquín on September 10, Madrid, Spain. Accessed December 2, 2015. www.iies.es/attachment/439459/

Spain's National Security Department. 2016. *"Departamento de Seguridad Nacional".* Accessed January 5, 2016. http://www.dsn.gob.es/es/sistema-seguridad-nacional/departamento-seguridad-nacional

Spain's Ministry of Industry, Energy and Tourism. 2015. *"Informe Anual de la Agenda Digital en España, Julio 2015"* July. Accessed December 2, 2015. http://www.agendadigital.gob.es/Seguimiento/Informesanuales/Informes/informe-agenda-digital-espana.pdf

Spain's Ministry of Industry, Energy and Tourism. 2015. *"Presentaciones Sectoriales: Sector Electrónica y TIC, Abril 2015".* April. Accessed December 2, 2015. http://www.minetur.gob.es/es-ES/IndicadoresyEstadisticas/Presentaciones%20sectoriales/Electronica%20y%20TIC.pdf

Spain's National Cryptologic Centre. 2011. *"Informe de Actividades 2008, 2009, 2010".* Accessed December 2, 2015. https://www.ccn-cert.cni.es/publico/memoria/InformedeActividadesCCN2010.pdf

Spain's National Cryptologic Centre. 2013. *"Informe de Actividades 2011-2012".* Accessed December 2, 2015. https://www.ccn.cni.es/documentos/CCN-Informe-de-actividades-2011-2012.pdf

Spain's National Cryptologic Centre. 2015. *"Ciberamenazas 2014, Tendencias 2015: Resumen Ejecutivo"* ref. CCN-CERT IA-09/2015. Accessed December 2, 2015. https://www.ccn-cert.cni.es/publico/dmpublidocuments/IE-Ciberamenazas2014-Tendencias-2015.pdf

Spain's National Cyber Security Institute (INCIBE). 2015. *"INCIBE: Instituto Nacional de Ciberseguridad".* Accessed December 2, 2015. https://www.incibe.es/home/instituto_nacional_ciberseguridad/

Spain's National Cyber Security Institute (INCIBE). 2015. *"Primera Edición del International CyberEx".* Accessed December 2, 2015. https://www.incibe.es/CERT/primera_edicion_international_cyberex

Spain's National Cyber Security Institute (INCIBE). 2015. *"Respuesta a Incidentes en Infraestructuras Críticas".* Accessed December 2, 2015. https://www.incibe.es/CERT/Infraestructuras_Criticas/

Spain's National Institute of Statistics (INE). 2015. *"Indicadores del Sector de las Tecnologías de la Información y de las Comunicaciones, Año 2013".* July 22. Accessed December 2, 2015. http://www.ine.es/prensa/np922.pdf

Spain's National Observatory for Telecommunications and the Information Society (ONTSI). 2015. *"Indicadores Destacados de la Sociedad de la Información en España, Diciembre 2015".* December. Accessed December 10, 2015. http://www.ontsi.red.es/ontsi/sites/default/files/indicadores_destacados_diciembre_2015.pdf

Spain's National Observatory for Telecommunications and the Information Society (ONTSI). 2016. "Informe Anual del Sector TIC y de los Contenidos en España, 2015". Accessed January 5, 2016. http://www.ontsi.red.es/ontsi/sites/default/files/destacados_informe_sector_ticc_edicion_2015.pdf

Spain's State Secretariat for Public Administrations. 2015. *"Moragues: «España es el Tercer País del Mundo que Registró más Ataques Cibernéticos el Año Pasado, cerca de 70.000 Ciberincidentes»".* October 19. Accessed December 2, 2015. http://www.seap.minhap.gob.es/web/delegaciones_gobierno/delegaciones/comunidad_valenciana/actualidad/notas_de_prensa/notas/2015/10/15-10-19.html

Spain's National Security Department. 2015. *"Comité Especializado de Situación".* Accessed December 14, 2015. http://www.dsn.gob.es/sistema-seguridad-nacional/comit%C3%A9s-especializados/comit%C3%A9-especializado-situaci%C3%B3n

Spanish Portal of Electronic Administration. 2015. *"Esquema Nacional de Seguridad".* Accessed December 2, 2015. https://administracionelectronica.gob.es/ctt/ens#.VmhWutLhDs3

Tikk, Eneken, Kadri Kaska and Liis Vihul. 2010. *"International Cyber Incidents: Legal Considerations".* Tallinn: Cooperative Cyber Defence Centre of Excellence (CCD COE). Accessed December 2, 2015. https://ccdcoe.org/publications/books/legalconsiderations.pdf

Urueña, Alberto (coord). 2016. *"La Sociedad en Red: Informe Anual 2014".* Spain's State Secretariat for Telecommunications and the Information Society. Accessed January 5, 2016. http://www.ontsi.red.es/ontsi/sites/default/files/informe_anual_la_sociedad_en_red_2014_edicion_2015_0.pdf

U-tad University College. 2015. *"Estado de la Ciberseguridad 2015".* Accessed December 2, 2015. https://www.u-tad.com/pdfs/resumen-ejecutivo-ciberseguridad-2015-u_tad.pdf