Area: Seguridad y Defensa
ARI 102/2010 (Translated from Spanish)
Date: 29/7/2010

Cyber Security in Spain: A Proposal for its Management (ARI)

Enrique Fojón Chamorro and Ángel F. Sanz Villalba[*]

Theme: Social, economic and cultural relations are increasingly dependent on information and communication technologies and infrastructures (cyberspace), making it necessary to devise a national security system (cyber security) that can manage the risks that threaten their adequate operation.

Summary: Information and Communication Technologies (ICTs) have contributed to the wellbeing and progress of societies to such an extent that countless public and private dealings depend on these technologies. Through the years, the advances in ICTs have given rise to threats that make it necessary to manage the security of these technologies. Early on, cyber security was conceived as a reactive system to protect information (Information Security); however, it later evolved to assume a proactive position that identifies and manages the threats to cyberspace (Information Assurance). This ARI explores the concepts of cyberspace and cyber security, the known risks and threats, their current management in Spain and the need to develop a national cyber security system that fosters the integration of all of the public and private agents and resources, to take advantage of the opportunities offered by the new technologies and to face the challenges that they present.

Analysis:

Introduction to the Concepts of Cyberspace and Cyber Security

The terms cyberspace and cyber security have now become widely used by broad sectors of society. Nevertheless, before analysing the state of affairs of cyber security in Spain and proposing an approach to its management, it is essential to define the concept of cyberspace in such a manner that everyone affected by it is aware of its social, economic and cultural implications. Once the concept of cyberspace has been defined, the concept and the need for cyber security will be more easily understood.

Cyberspace is a concept that is used within the ICT community to refer to the whole of the physical and logical media that comprise the information and communication system infrastructures. To attain a definition of cyberspace that enables an understanding of the implications mentioned above, it is helpful to consider the concept of service, which is conceived as something that a user or consumer receives from a provider.

Provider-consumer relations can emerge not only between companies and domestic users, but also between and among companies, public administrations and citizens, and of course individuals. These relations existed long before the advent of ICTs, in the mid-

[*] *Enrique Fojón Chamorro, Computer Systems Engineer*
Ángel F. Sanz Villalba, Telecommunications Engineer.

19th century, with the invention of the telegraph, and naturally, before its revolution with the discovery and application of the properties of semi-conductive materials that would enable the birth of the 'digital era'. However, it was precisely from that moment that ICTs became the catalysers of the traditional services that companies provided to their customers, spurring both their extension and their economic efficiency, while at the same time enabling the emergence of new services.

Therefore, cyberspace can be defined as the whole of ICT-based media and procedures that are configured for the provision of services. This definition immediately explains why cyberspace is now an essential part of our societies and economies and how it could even become a determining factor of the evolution, or perhaps the convergence, of cultures. Hence the importance of protecting cyberspace. In the past, cyber security focused on information security, as it solely set out to protect information from unauthorised access, use, disclosure, interruptions, modifications or destruction. Today this approach is evolving into a model of cyberspace risk management (known as 'information assurance'). Thus, cyber security now also entails the application of a risk analysis and management process regarding the use, processing, storage and transmission of information or data and the systems and processes used, based on internationally accepted standards.

One of the reasons behind this new approach to security is that cyberspace is characterised by a given unit such as a service-providing ITC, in such a manner that the security of the system is attained when the threats to that system are known and controlled. In fact, these two approaches, information security and information assurance, are different yet complementary, and they are often erroneously used interchangeably. In a word, cyber security must be formulated proactively as a continuous analysis and management process vis-à-vis the risks associated with cyberspace.

State of Risk of Cyberspace

The fear of the catastrophic consequences of a hypothetical 'cyber-Katrina' or a 'cyber-9-11' has led countries such as the US, France, the UK, Israel and South Korea, as well as international organisations including the UN and NATO, among others, to become aware of the importance and the need for a secure cyberspace. For this reason, they have developed or are developing regulatory frameworks and specific plans and strategies for the protection of cyberspace. In a word, they have taken the decision to systematically manage the security of the cyberspace for which they are responsible.

On the other hand, China, Iran, North Korea, Russia and Pakistan have acknowledged their strategic interest in cyberspace as a vehicle to attain positions of economic and political leadership in their geographical scopes of influence. As a result, they are defining policies and making great economic investments that target ICT resources and human resource training, in order to establish 'a belligerent defence' of their cyberspace. These countries, or at least their territories, have been identified as the sources of most of the aggressive actions that have taken place in cyberspace in recent years. The constant and accelerated evolution of ICTs has made for increasingly sophisticated attacks, giving rise to an ever more hostile cyberspace, thus forcing cyber security managers to develop state-of-the-art technical and human resources to confront the threats and their possible impacts.

Once the assets to be protected have been identified and assessed, the next step is to detect the possible threats, which can be highly innovative and diverse. The threats to cyberspace are embodied by cyber attacks, which, depending on their origin and impact, can be classified in the following categories:

- State-sponsored attacks. The conflicts of the physical or real world spill over into the virtual world of cyberspace. In recent years, cyber attacks have been launched on the critical infrastructures of countries and on very specific, though equally strategic objectives. Some such examples, which are well known to the general public, include the attack on part of Estonia's cyberspace in 2007, which temporarily rendered much of the Baltic country's critical infrastructures useless, as well as the cyber attacks on the classified networks of the US government by hackers based in China.
- Terrorism and political and ideological extremism. Terrorist and extremist groups use cyberspace to plan their actions, to publicise them and to recruit followers to carry them out. These groups have already acknowledged the strategic and tactical importance of cyberspace for their interests.
- Attacks by organised crime. Organised crime groups (cyber gangs) have begun to move their action to cyberspace, exploiting the anonymity potential offered by this medium. These types of groups aim to obtain sensitive information for later fraudulent use and as a means to procure large economic profits. According to FBI data,[1] in 2009 the cybercrimes committed by organised crime groups generated losses of over US$560 million among US companies and individuals alike.
- Low-profile attacks. These types of attacks are usually perpetrated by people with enough ICT expertise to launch cyber attacks of very diverse natures, for essentially personal reasons.

A quick glance at the types of threats and impacts on cyberspace assets and dependent services shows that whilst ICTs make it possible for more and better services in many areas of our societies, they also increase the risk of attacks on such services. This is further aggravated by the extension and popularisation of ICTs, which weaken the lines of defence of the goods to be protected. It is just as easy for one person to access cyberspace to manage his/her bank accounts from home as it is for another person to access online information on how to break the security of that service and steal the private codes of that person, usurping his/her identity.

Cyber Security Management in Spain

Once the overall scope of cyberspace and its threats are defined, it is easy to understand the difficulty involved in ensuring its security in a given part of the whole. If we are to speak of cyber security in a given nation, we must consider at least two dimensions: the protection of the goods, assets, services, rights and freedoms that depend on State jurisdiction, and the shared responsibility for cyber security with other States, either bilaterally or through supra-national bodies.

In other words, the challenge resides in ensuring that the combination of partial solutions applied by States, albeit with a certain degree of coordination, will resolve the overall problems created by technologies that break down borders. Cyberspace is in constant growth and it is evolving so fast and reaching such a point of proliferation that it essentially sustains the social, economic and cultural relations and structures that are fundamental for a country's growth and development.

1 http://www.ic3.gov/media/annualreport/2009_ic3report.pdf

With reference to the first dimension of the problem, it is necessary identify the assets in Spain that depend on cyberspace, the existing regulations, the governing bodies responsible for this area and the specific participants. Though the protection of cyberspace encompasses every asset and agent imaginable, it must essentially focus on the protection of critical infrastructures, the business sector and individual rights and freedoms.

Spain's critical infrastructures are grouped into the following 12 sectors: administration, food, energy, space, the financial and tax system, water, the nuclear industry, the chemical industry, research facilities, health, transport and information and communication technologies. In all of these sectors, the degree of cyberspace penetration for both the internal management and the provision of services reached its critical level some time ago. Any contingencies that affect any of the assets belonging to any of the 12 strategic sectors could potentially jeopardise Spain'sa national security.

As regards the Spanish business sector, the vast majority of the large corporations have a sufficiently developed internal organisation that enables them to implement activities and measures that fall within information security and information assurance practices. In the case of the small- and medium-sized enterprises and self-employed workers (99% of the total),[2] the lack of economic and human resources is an obstacle for the implementation of cyber security, although their activities are fundamentally sustained by ICTs. The government is currently promoting access to the ICTs and good cyber-security practices among Spanish companies and self-employed workers through the funding lines of the Plan Avanza.[3]

As regards the country's citizens, the penetration index of the information society services (electronic mail, social networks and electronic commerce) is now high enough[4] for any of the types of threats described above to gravely affect individual rights and freedoms.

The Current Situation of Cyber Security in Spain

Unlike other countries around it, Spain has not yet defined a specific and complete legislation for cyber security. Whilst legislation does exist in different ministerial areas, it has not been developed on the basis of a common policy that reflects the national and strategic scope of cyber security.

Royal Decree 3/2010, of 8 January, which regulates the National Security Scheme in the area of Electronic Administration,[5] is a good place to start; however, as its very name suggests, this law solely covers the public administration sector, leaving out other important sectors for cyber security management, such as other critical infrastructures, companies and citizens. In addition to the Royal Decree mentioned above, there are national, European and international laws that address the issue of cyber security. These include the Organic Law on Data Protection, the General Telecommunications Law and the Information Society and Electronic Commerce Law.

Despite the existence of this regulatory framework, in some cases its degree of compliance is distressingly low, which implies an increase in threats to the cyberspace. The competences associated with cyber security management are distributed among a

2 http://estaticos.expansion.com/estaticas/documentos/2010/05/pymessocietarias.pdf.
3 http://www.planavanza.es/Paginas/Inicio.aspx.
4 http://www.mityc.es/dgdsi/esS/Servicios/Biblioteca%20Indicadores/METRICA_SI_06.pdf.
5 http://www.csi.map.es/csi/pg5e42.htm.

group of bodies and institutions that depend from different governmental ministries. Among others, these include:

- The National Cryptology Centre (*Centro Criptológico Nacional*, CCN), which depends from the National Intelligence Centre (*Centro Nacional de Inteligencia*, CNI). This centre aims to manage cyberspace security pertaining to any of the three levels of public administration: state, regional and local. The CCN-CERT (*Capacidad de Respuesta ante Incidentes de Seguridad*, Capacity to Respond to Information Security-Related Incidents) is a national alert centre that works with all of the public administrations to respond quickly to the security-related incidents in its area of cyberspace. Moreover, this agency is the highest body responsible for classified national information security.
- The National Institute of Communication Technologies (*Instituto Nacional de Tecnologías de la Comunicación*, INTECO), which answers to the Ministry of Industry, Tourism and Trade, handles cyberspace protection for Spain's small and medium-sized enterprises and domestic-use citizens, through its CERT (Computer Emergency Response Team).
- The National Centre for Critical Infrastructure Protection (*Centro Nacional para la Protección de las Infraestructuras Críticas*, CNPIC), which depends from the Spanish Ministry of the Interior, promotes cyber security relating to these infrastructures.
- The Civil Guard's Telematic Crime Group (*Grupo de Delitos Telemáticos de la Guardia Civil*) and the National Police Information Technologies Crime Investigation Unit (*Unidad de Investigación de la Delincuencia en Tecnologías de la Información de la Policía Nacional*), both of which depend from the Ministry of the Interior, work to combat crime in cyberspace.
- The Spanish Data Protection Agency (*Agencia Española de Protección de Datos*, AGPD), which depends from the Ministry of Justice, enforces compliance with personal data protection regulations.

Moreover, the regional autonomous governments have centres equivalent to those of the state. These include the Valencian Community's CSIRT-CV and the Data Protection Agencies of both the Community of Madrid and the Catalan Regional Government, which are similarly responsible for cyber security management within their respective autonomous regions. In a word, despite the existence of bodies with clearly defined responsibilities in different areas of the public administrations, Spain is lacking a single body at the highest tier of government that will assume the strategic value of cyber security and exercise the necessary leadership, so that all of the other bodies can operate in accordance with a single national policy.

Industry

Spanish industry in connection with cyber security is in the middle of a growth and development process. This is reflected in INTECO's most recent 'Catalogue of Companies and Security Solutions',[6] which calculates that there are currently in existence over 1,000 Spanish cyber security companies. In 2009, the main companies in the sector came together in the National Cyber-Security Advisory Council (*Consejo Nacional Consultor sobre Ciber-Seguridad*, CNCCS), which aims to foster the protection of cyberspace, making itself available to government agencies and private organisations to

6 http://www.inteco.es/Seguridad/Observatorio/Estudios_e_Informes/Estudios_e_Informes_1/estudio_lopd_pymes

offer guidance on cyber security issues and to strengthen the resultant technological innovation and economic growth.

The companies soon acknowledged the strategic value of cyberspace, both their own and the globally conceived cyberspace, thus giving rise to security departments in their organisations and groups such as the CNCCS. Nevertheless, there are virtually no governmental initiatives that foster state-industry cooperation. This relationship ought to be a two-way system: companies need to create value around the cyber security business, and the State needs technology that will provide it with a reliable and state-of-the-art capacity for cyber security.

Citizen Participation
In 2009, Spain reached an Internet penetration rate of 71.8%,[7] which translates into over 30 million potential cyber users. If we subtract the population of preschoolers and senior citizens over age 75, which still takes in more than 70% of the population with access to cyberspace services, it can be surmised that practically the entire Spanish population accesses these services. The current Spanish legislation on cyber security places special emphasis on the need for education and public awareness in this area, as well as the responsible use of the cyberspace. All the same, these principles have scarcely been applied to date, due primarily to the generalised lack of knowledge of the legislation. The INTECO and the CCN, within the scope of their competence, run interesting awareness and educational campaigns on ICT security, although the impact of those initiatives has left much to be desired. The Spanish industry in the cyber security sector has similarly launched different private campaigns to raise awareness and educate certain sectors of the society, including schoolchildren, retirees and unemployed workers.

International Cooperation
Spain is a member of international organisations that promote the protection of cyberspace. A few such examples include the country's participation in NATO's Cooperative Cyber Defence Centre of Excellence and in bodies such as ENISA (European Network Information Security Agency),[8] the AWG (Anti-Phishing Working Group),[9] and the Article 29 Data Protection Working Party.[10] Spain's participation in and cooperation with international bodies not only enables the country to share experiences and knowledge of the risks and solutions, it also confirms the fact that no national cyberspace can be managed efficiently if the other portions of the global cyberspace do not share the same level of risk. One of the unwritten principles of ICT security asserts that the chain is always broken at the weakest link. It is of little or no use to a nation to implement a highly advanced cyber security plan if all or some of the other countries that take part in cyberspace do not enjoy a similar level of protection.

Conclusions

Proposals for Spain's Management of Cyber Security
Despite the efforts that have been made, Spain continues to lack a solid system that will enable it to effectively and efficiently direct and manage its cyber security. To define and develop such system, the following principles would need to be applied:

7 http://www.inteco.es/icdemoest/Seguridad/C_Demostrador.
8 http://www.enisa.europa.eu/.
9 http://www.apwg.org/.
10 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm.

(1) The Spanish government must identify the security of its cyberspace as a strategic objective of its National Security, as the materialisation of a threat to its cyberspace could have very grave effects on the country's social, economic and cultural development.

(2) A National Cyber Security Strategy needs to be developed as the foundation for a specific regulatory framework that governs cyberspace and its security. The recent publication of Royal Decree 3/2010, which governs the National Security Scheme in the area of Electronic Administration, is a good starting point. All the same, it will be necessary to adjust and enforce the current applicable legislation.

(3) The management of cyber security must be undertaken from a centralised perspective. As a corollary of the principle above, the State must create a body that aims to direct national cyber security, coordinating the public and private institutions involved.

(4) The government needs to foster and reinforce international cooperation in cyber security. Multinational and bilateral alliances for cyber security are crucial. In the case of Spain, there is the opportunity to assume a role as a responsible leader with Latin American countries. Moreover, it is advisable that it enters into agreements with those countries, which are not located within its immediate geopolitical sphere, though they are very important in the control of threats to its cyberspace.

(5) The State administrations ought to promote a culture of cyber responsibility, based on awareness and ongoing cyber security training. To do so, the study plans of the primary, secondary and university school systems should include subjects pertaining to responsible cyberspace use in their syllabi.

(6) The State needs to promote and invest in research, development and innovation (R & D & I) in the cyber security sector, to provide top-quality ICT solutions and qualified employment.

Thus, the government must assume a leadership role in cyber security to make the public aware of the need to protect the cyberspace upon which Spain's basic services, critical infrastructures, economy and progress as a society depend. ICTs are not the problem; rather, they form part of the solution. Moreover, their protection and secure use are not just the responsibility of the central government; they are also the responsibility of the other regional autonomous and local administrations, along with the private, business and domestic sectors. Everyone shares part of this joint responsibility, yet it is the central government that must assume the leadership and undertake the national management of cyber security. These responsibilities cannot be delegated, and they must translate into providing Spain with the momentum, the ideas and the direction that are needed.

Enrique Fojón Chamorro
Computer Systems Engineer

Ángel F. Sanz Villalba
Telecommunications Engineer