GOVERNO DE
PORTUGAL

Pedro Passos Coelho
Prime Minister

Society, the economy and the state depend on information and communications technology (ICT).

We have witnessed the accelerated development of an information society and the growing dependency on ICT in areas vital to the functioning of the nation.

The definition of a digital agenda allows the provision of economic and social benefits, stimulates job creation, sustainability and social inclusion, maximising the benefits new technologies have to offer and to improve the structure of the national framework.

These technologies are vulnerable, however, and create social and material risks. If on the one hand they bring clear benefits to society, on the other they significantly increase the risks resulting from dependency and the quantity of stored and circulating information that exposes the state, business and citizens.

Cyberspace transposes real life to a virtual world with unique characteristics that require new forms of interaction and relationships.

In terms of legal issues of a personal nature, there has been an exponential increase in sex crimes against minors facilitated by the Internet, with this phenomenon often involving a criminal transnational dimension and highly sophisticated methods, which demands firm, determined and effective intervention.

This “networked world” engenders new and unique criminal activities, such as cybercrime, in particular organised cybercrime associated with bank fraud and identity theft linked to the former, the many forms of political hacktivism (such as the leaking of sensitive or classified information and information sabotage), as well as an increase of state and industrial espionage.

There is evidence of the ability of political and religious activists with criminal and terrorist motivations to engage nationally and internationally in activities that have an impact on the

security of vital information infrastructures. These pose serious threats to the survival of the rule of law and to a space for freedom, security and justice.

The need to protect those areas embodying national sovereignty, ensuring the nation's political and strategic autonomy, as well as the growing number of malicious incidents and attacks, mean the security of cyberspace should be considered a national priority.

Therefore, it is important that the state has a National Cyberspace Security Strategy that establishes goals and lines of action that seek to ensure effective crisis management, the coordination of operational responses to cyber-attacks, the development of national synergies and improved national, European and international cooperation in this area.

Efforts to reduce weaknesses in the security of information networks and to increase the resilience of their critical infrastructures are also essential, both within the framework of the Cybersecurity Strategy of the European Union (EU) and the North Atlantic Treaty Organisation's (NATO) cyber defence policies. It is essential to invest in strengthening this cooperation, which will result in an exponentially improved effectiveness in protecting the above.

In this context, it is important to outline a vision and a strategic, logical and coherent framework.

28 May 2015,

Prime Minister *Pedro Passos Coelho*

PRESIDENCY OF THE COUNCIL OF MINISTERS

Resolution of the Council of Ministers 36/2015

In accordance to with articles 199 (d)(f)(g) and 200 (1a) of the Portuguese Constitution, the Council of Ministers resolves to:

1 - Approve the National Cyberspace Security Strategy, which is appended to and forms part of this current resolution.

2 - Establish that the current resolution takes effect on the date of its approval.

NATIONAL CYBERSPACE SECURITY STRATEGY

1. The National Cyberspace Security Strategy, henceforth "the Strategy", is based on a commitment to improve the security of networks and of information, in order to protect and defend critical infrastructures and vital information services and to promote the free, secure and effective use of cyberspace for all citizens, businesses and public and private bodies.

2. The Strategy is based on the general principles of state sovereignty, the general ideas contained in the Cybersecurity Strategy of the EU and on the strict observance of the European Convention on Human Rights, the EU Charter of Fundamental Rights, the protection of the fundamental rights, freedom of expression, personal data and privacy, and rests on the following five pillars:

   a) **Subsidiarity:**

   The security of cyberspace is an integral part of national security and is essential for the functioning of the nation, for economic development and innovation, as well as for citizen confidence in the digital marketplace and in cyberspace.

   The state confirms its strong commitment to defending cyberspace. Nevertheless, a large part of the technological infrastructures that make up cyberspace are owned by private operators, who are principally responsible for their protection. This responsibility begins with the individual and their responsible use of cyberspace and ends with the state as guarantor of sovereignty and of constitutional principles.

   b) **Complementarity:**

   Responsibility for the security of cyberspace is shared among different actors, whether public or private, military or civilian, or collective or individuals.

A broader and more integrated approach to cyberspace security brings together a number of actors with different responsibilities and abilities, for the benefit of all.

c) **Cooperation**:
In our highly interconnected and interdependent world, a secure cyberspace requires close cooperation and collaboration between national and international allies and partners, based on the development of mutual trust.

d) **Proportionality**:
The risks inherent to cyberspace must be assessed and appropriately managed, ensuring proportionality of means and measures for their exercise.

e) **Awareness**:
Guaranteeing the security of technological infrastructures, information systems and networks relies on end users knowing what steps to take in order to minimise the risks to which they are exposed. Raising awareness is a key aspect for maintaining a secure cyberspace.

3. The Strategy will develop the following strategic objectives:

   a) To promote awareness, free, safe and efficient use of cyberspace;

   b) To protect fundamental rights, freedom of expression, personal data and the privacy of citizens;

   c) To strengthen and guarantee the security of cyberspace, of critical infrastructures and of vital national services;

   d) To affirm cyberspace as a place for economic growth and innovation.

4. The implications and requirements associated with each of these strategic objectives sets out general and specific guidelines, which translate into six axes of intervention with actual measures and lines of action to enhance the strategic national potential in cyberspace:

   Axis 1 – Structure of cyberspace security

   Axis 2 – Tackling Cybercrime

   Axis 3 – Protecting cyberspace and national infrastructures

   Axis 4 – Education, awareness and prevention

Axis 5 – Research and development

Axis 6 – Cooperation

Axis 1 – Structure of cyberspace security

The complexity and extent of the challenges to cyberspace security require a strong and multidisciplinary leadership and governance; agile, responsive and effective operational coordination; the ability to respond to and protect the national interest and, above all, access to resources, knowledge and skills. Consequently, the following measures must be adopted:

1) Establish politico-strategic coordination for the security and defence of cyberspace:

   Responsibility for the security of national cyberspace is currently distributed across different actors with different missions and goals. There is no common thread and no consistency in the policies and initiatives each of them develops.

   As a result, developing a multidisciplinary approach that incorporates the sensitivities of the various sectors of society is a necessary priority.

   To this end, a coordinated politico-strategic plan for the security of cyberspace must be defined, under the leadership of the Prime Minister, with representatives of all interested parties.

   The politico-strategic coordination must assume responsibility for controlling and reviewing the current Strategy and the measures contained within it. Carrying out these measures is the responsibility of each party, which must provide periodic reports of their implementation;

2) Consolidate the operational coordination and national authority role of the National Centre for Cybersecurity (Centro Nacional de Cibersegurança – CNCS) in matters of the cybersecurity of public bodies and critical infrastructures:

   a) Confirm the CNCS's right to operate as the competent national authority in matters of the cybersecurity of public bodies and national critical infrastructures;

   b) Operational coordination is an essential factor in the successful implementation of the measures outlined in this Strategy. The CNCS will oversee the coordination between the various responsible parties;

c) Cyberspace security presupposes an understanding of existing threats and vulnerabilities. This knowledge is essential for carrying out a risk analysis designed to improve the use of available means and resources for dealing with the risks and identifying gaps that need to be filled;

d) The CNCS, as operational coordinator, must develop and implement measures that ensure the human and technological capacities of public and critical infrastructures, with a view to preventing and responding to cybersecurity incidents;

e) In order to achieve operational effectiveness and improved situational assessment, cybersecurity incident report mechanisms must be developed for public bodies and critical infrastructure operators. The desired situational assessment results from the establishment of conditions for the identification of a national alert level in matters of cyberspace security, which is then shared with all of the bodies involved;

f) In association with the competent authorities and the national cyberspace security community, CNCS will compile a knowledge base containing information about known threats and vulnerabilities, that will be made available to public bodies and critical infrastructure operators;

g) The CNCS must produce and submit a complete up-to-date picture of all incidents, threats and vulnerabilities to national cyberspace.

3) Develop the capacity for cyber defence:

a) Implement the Cyber Defence Policy Guidance, approved by Dispatch 13692/2013, dated 11 October, and published in the Diário da República, no. 208, 2nd series, 28 October, which created the national cyber defence structure;

b) Establish and consolidate a national cyber defence command and control structure, with the strategic-military aspects of cyber defence being the responsibility of the Council of the Chiefs of Staff (Conselho de Chefes de Estado-Maior) and the planning and immediate effective responses to cyberspace crises to the Cyber Defence Centre (Centro de Ciberdefesa – CCD) and the various branches of the armed forces;

c) To implement, develop and consolidate cyber defence capabilities ensuring military operations in cyberspace, defending the nation's freedom of action in cyberspace and, whenever required, the proactive use of cyberspace to impede or hinder hostile acts against the national interest;

d) Make cyber defence an area where it is necessary to promote synergies and encourage the dual use of its capabilities, under the scope of military operations

and national cybersecurity, developing and consolidating an information sharing system at various levels of decision-making.

4) Develop a national incident response capability:

In a context of the distributed management of cyberspace, information sharing between interested parties is a critical success factor in ensuring improvements in detecting, preventing and responding to failures and breaches of cyberspace security.

a) The role of Computer Security Incident Response Team (CSIRT) communities must be strengthened as a platform of excellence for sharing good practices and information on cyber incidents, for operational response services to incidents in Portugal and abroad, in this case when they represent a threat to national sovereignty;

b) The various CSIRTs must use a common taxonomy and automatic mechanisms for sharing operational information among themselves and with the security forces and services.

5) Establish an office for managing cyberspace crises:

a) The response to high-impact cyber incidents requires specific and special procedures. It is important to establish a cyberspace crisis management office with an integrated approach for responding to threats and risks within an effective national crisis management system that includes important actors in this area;

b) National crisis management exercises in cyberspace must organised and held to enable the assessment of the level of preparation and maturity of the various bodies to cope with large-scale incidents, which should, whenever possible, leverage synergies resulting from the integration with other exercises in this field, organised and conducted at the national level.

6) Define and implement cyberspace governance and security processes:

Develop a proposal to address the various fields of action, containing legislative and regulatory changes as well as mechanisms for the self-regulation and governance of national cyberspace security.

Axis 2 – Tackling Cybercrime

Cyberspace has created new legal interests deserving of protection, new types of crimes and new ways to commit old crimes.

The challenges posed by cybercrime mean that laws need to be constantly updated in order to ensure their maximum effectiveness. Similarly, institutions concerned with the investigation of cybercrime must be fully equipped to carry out their mission while the judicial system in general must adapt to the new technologies. Consequently, the following measures must be adopted:

1) Review and update legislation:

   The competent authorities must adopt the measures necessary for the development and implementation of legislation designed to ensure the criminalisation of new types of crimes – whether against or taking advantage of cyberspace – and ensure improved judicial cooperation at a national and international level.

   Legislation supporting criminal investigations must be constantly updated to ensure their effective application in cyberspace.

2) Enhance the powers of the Portuguese Criminal Police (Polícia Judiciária):

   The Polícia Judiciária must improve its structures and technical and human skills for combating cybercrime, as it must strengthen its technical and forensic skills for cyberspace investigations.

Axis 3 – Protecting cyberspace and infrastructures

The threats to infrastructures and information systems are aimed at both public and private bodies and citizens. Public services are an example to society and must be capable of enhancing the protection of information systems and the information for which they are responsible.

The following measures must be taken to ensure the protection of cyberspace and its infrastructures:

1) Assess the maturity and ability of the public and private bodies that administer critical infrastructures and vital information services to ensure the security of cyberspace;

2) Promote the adaptation and continuous improvement of the security of the information systems of public bodies, critical infrastructures operators and vital information services, as a means of ensuring greater national resilience (survivability), adapting them to the new risks and threats from cyberspace;

3) Analyse the information environment in order to anticipate possible attacks and to take the necessary action by keeping up to date with the latest technological developments and by analysing and anticipating threats;

4) Develop the ability to detect attacks on information systems, especially those belonging to public bodies and critical national infrastructures, which will allow the competent authorities to be warned of and help them to understand the nature of the attack and develop the necessary countermeasures;

5) Promote the implementation, by public bodies, of the necessary measures to ensure the continuity of operations while responding to the main crises that are affecting or threatening the security of information systems or critical infrastructure operators;

6) Include cyberspace security measures in national critical infrastructures' protection plans, following a risk management based approach;

7) Include measures to address cyberspace threats to the security plans of national and European critical infrastructure operators;

8) Promote the use of information security norms for public body information and communications infrastructures. Adopt good cyberspace security practices that will operate simultaneously as mechanisms for ensuring harmonisation and interoperability and as a reference measuring instrument;

9) Promote an information security policy for public bodies and create instances that will guarantee information security in all these bodies with access to sensitive information, personal data or which provide critical online services, providing that the identification of the measures for applying the security policy follows a risk management based approach, in accordance with best international practice;

10) Improve the ability to prevent, detect and respond to cyberspace security incidents. Critical infrastructure operators must report any breach or attempted breach of the security of their cyberspace systems. Each of these operators must also establish the minimum set of technical and human resources required to ensure the security of

cyberspace. These resources must operate in a network within and outside their activity sector;

11) Assess and develop sectoral regulatory frameworks;

12) Adapt national legislation in order to respond to technological developments and new practices;

13) Guarantee and protect critical information infrastructures via a National Information Infrastructure Protection System (SPIIN).

Axis 4 – Education, awareness and prevention

The success of cyberspace security is the result of promoting a culture of security that supplies the necessary knowledge, awareness and trust to use information systems and reduces exposure to the risks of cyberspace. It is important to inform, educate and raise the awareness of public bodies and critical infrastructures as well as of businesses and Civil society in general. It is also important for the nation to provide qualified human resources capable of dealing with the complex challenges of cyberspace security. The following measures must be adopted in the field of education, awareness and training:

1) Promote information campaigns and alerts for all citizens and businesses;

2) Raise awareness among public and private operators of the critical nature of computer security;

3) Promote a culture of cyberspace security through campaigns and initiatives that are coordinated and developed with a common and positive approach. These will draw attention to the dangers and threats on the Internet and, at the same time, offer solutions and measures to mitigate them. Therefore, it is important to create resources and raise awareness in Civil society in order to promote the secure and responsible use of ICT;

4) Improve cyberspace security training. Improve and extend instruction and training in primary, secondary and higher education as a means of improving skills and knowledge on the safe use of ICT;

5) Promote the safe use of ICT and cyberspace, paying particular attention to the knowledge and skills obtained by adolescents, the elderly and other high-risk groups;

6) Promote specialist training in cyberspace security by creating or enhancing the provision of multidisciplinary courses, and by changes to the existing curriculum;

7) Promote specialist training of decision-makers and public body and critical infrastructure administrators from an awareness and prevention perspective for the need to safeguard critical national interests and information;

8) Establish special programmes for Small and Medium Enterprises (SME), socio-professional associations and, particularly, freelance professionals.

Axis 5 – Research and development

Taking the strategic importance of cyberspace security into account, it is important to support, develop and enhance technological capabilities in order to create certifiable national, secure and trustworthy solutions that will improve the protection of systems facing a number of threats. It is essential to develop and support all research and development activities and initiatives involving businesses and industry, research bodies and academe. Consequently, the following measures must be adopted:

1) Promote scientific research and development in various aspects of cyberspace security. Scientific and applied research and the development of innovative solutions are important factors in cyberspace security. Scientific output across various areas of knowledge and the development of applied solutions in the many domains must be promoted and encouraged;

2) Stimulate and enhance the nation's scientific, technical, industrial and human capabilities in order to confirm national independence in this domain;

3) Support national participation in international projects;

4) Maximise synergies resulting from national participation in international fora in this domain, and from the presence on national territory of international bodies dedicated to research and development in this area;

5) Exploit the experience gained in this field as a result of the involvement of the armed forces in overseas missions, so that, in collaboration with the universities, research centres and industry, technological solutions with dual military and civilian use can be developed;

6) Support the participation of academe and national businesses in international research and development projects.

Axis 6 – Cooperation

The security and defence of cyberspace require close cooperation and collaboration between national and international allies and partners. Responding to the challenges of cyberspace security and defence requires a networked approach, through which national and international cooperation in the various fields is of great importance. Consequently, the following measures must be adopted:

1) Develop cooperation initiatives. Develop cooperation initiatives in areas linked to the security of information systems, cybercrime, cyber defence and cyber terrorism, cyber espionage and cyber diplomacy, in such a way as to enhance the necessary knowledge to protect national information systems;

2) Multilateral cooperation and collaboration. Current national and international multilateral cooperation mechanisms must be strengthened, particularly within the framework of the Cybersecurity Strategy of the EU and the NATO cyber defence and cybersecurity partnership;

3) Participate in and cooperate with CSIRT forums. CSIRT forums are instruments for sharing information and creating the trust necessary to respond to cyberspace incidents. Promote participation in CSIRT's main forums;

4) Participate in exercises. Cyberspace security exercises enable the evaluation and development of doctrinal and operational capabilities. Promote participation in major cyberspace security and defence exercises, alongside national and international actors, particularly in the context of the EU and NATO.

Strategy Review:

A rapid evolution is intrinsic to cyberspace and, consequently, there is an increase of threats, vulnerabilities, processes and infrastructures, as well as an evolution of the economic, social and cultural models upon which their use is based. This demands that this Strategy be periodically reviewed. It is believed that, without prejudice to any extraordinary review procedures that can be carried out whenever circumstances demand, this document should be reviewed:

a) Within no more than three years;

b) Annual verification of the strategic objectives and lines of action and their adaptation to changing circumstances.