Resolution of the Council of Ministers No. 92/2019

The Resolution of the Council of Ministers No. 36/2015, of 12 June, approved the first National Strategy for Cyberspace Security, aimed at deepening the security of network and information systems and potentiate a free, safe and efficient use of cyberspace by all citizens and by public and private entities. Given the rapid intrinsic development of cyberspace and consequently, the increasing evolution of threats, vulnerabilities, processes and infrastructures, as well as the economic, social and cultural models based on their use, it was defined that this strategy would be revised in a term limit of three years.

By the Resolution of the Council of Ministers No. 115/2017, of 24 of August, a project group was created, designated National Cybersecurity Council, having as one of its objectives to propose the revision and elaborate the new National Strategy for Cyberspace Security (NSCS). As part of this project group, a draft was prepared which formed the basis of the new NSCS that is now approved.

For its part, Law 46/2018 of 13 August established the legal framework for cybersecurity, transposing Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July concerning measures for a high common level of security of network and information systems across the Union. Through this law, the Superior Council for Cyberspace Security was created as the specific entity for consultation of the Prime Minister on cyberspace security issues.

The Superior Council for Cyberspace Security has as competences, namely, to verify the implementation of the NSCS, through the monitoring and evaluation of its execution, and, having to be consulted, under the terms of paragraph 2 of article 4 of Law No. 46/2018, of 13 August, in the frame of the NSCS approval process.

The NSCS 2019-2023 had a favourable opinion from the Superior Council for Cyberspace Security, pursuant to Article 6 (1) (c) of Law 46/2018 of 13 August.

Thus, considering the digital evolution since the approval of the NSCS 2015, the conditions for approving the NSCS 2019-2023 are met, as a structuring instrument for national capacity-building in this area, defining the framework, the objectives, and the lines of action of the State on the security of cyberspace, in accordance with the national interest.

NSCS 2019-2023 is based on three strategic objectives: maximizing resilience, promoting innovation and generating and securing resources. The implications and needs associated with each of the strategic objectives allow us to define a general and specific orientation, translated into six intervention axes, which form concrete lines of action aimed to reinforcing the national strategic potential in cyberspace.

The success of NSCS 2019-2023 will allow Portugal to become a safer and more prosperous country through innovative, inclusive and resilient action that preserves the fundamental values of the democratic rule of law and ensures the regular functioning of institutions corresponding to the digital evolution of society.

It´s also determined that the NSCS 2019-2023 Action Plan, which is an essential instrument for monitoring and evaluating its execution, will be prepared in the term limit of 120 days and should be articulated with the National Strategy for Counter-Terrorism , and include, namely, measures to protect against those threats to cyberspace security, with the ICT 2020 Strategy — the Public Administration Strategy for Digital Transformation , as well as the Strategy for Technological and Business Innovation for Portugal 2018-2030.

Therefore:

Pursuant to Article 4 (2) of Law No. 46/2018 of 13 August and pursuant to Article 199 (d), (f) and (g) and 200 (1) (a) of the Constitution, the Council of Ministers decides to:

1 — Approve the National Strategy for Cyberspace Security 2019-2023, which is annexed to this resolution and of which it forms an integral part.

2 — Determine the preparation of an Action Plan for the National Strategy for Cyberspace Security 2019-2023, to be approved in the term limit of 120 days after the entry into force of this resolution.

3 — Instruct the National Cybersecurity Centre, as the National Cybersecurity Authority, to coordinate the elaboration, monitoring of the execution and revision of the Action Plan referred to in the previous paragraph, in articulation and close cooperation with all entities responsible for the security of cyberspace.

4 — Determine that the coordinator of the National Cybersecurity Centre consults with the Superior Council for Cyberspace Security on the Action Plan for the National Strategy for Cyberspace Security 2019-2023 before its approval by the Government member responsible for cybersecurity.

5 — Determine that the commitment on the execution of the National Strategy for Cyberspace Security 2019-2023 depends on the existence of funds available from the competent public entities.

6 — Determine the annual revision, or any time as necessary, of the Action Plan for the National Strategy for Cyberspace Security 2019-2023.

7 — Revoke the Resolution of the Council of Ministers No. 36/2015, of 12 June.

8 — Determine that this resolution shall enter into force on the day following its publication.

Presidency of the Council of Ministers, 23 May 2019. — The Prime Minister, *António Luís Santos da Costa*.

ANNEX

(referred to in paragraph 1)

NATIONAL STRATEGY FOR CYBERSPACE SECURITY 2019-2023

1 — Values, definitions and principles

The, National Strategy for Cyberspace Security 2019-2023 hereafter referred to as the Strategy, is based on a commitment to deepen the security of network and information systems as a way to guarantee the protection and defence of the cyberspace of national interest and promoting its free, safe and efficient use for all citizens, companies and other public and private entities.

For an effective understanding of this Strategy, it is necessary to explain some of the most relevant concepts in this, allowing simultaneously the establishment of a conceptual basis that can be used by all.

Cyberspace is the complex environment of values and interests materialized in an area of collective responsibility that results from the interaction between people, networks and information systems.

Cybersecurity consists of a set of preventive, monitoring, detection, reaction, analysis and correction measures and actions aimed at maintaining the desired security level and guaranteeing the confidentiality, integrity, availability and non-repudiation of the information, networks and information systems in the cyberspace, and the people that interact in it.

Cyberdefence is the activity aimed at securing the national defence in or through cyberspace.

By cybercrime it´s understood the facts corresponding to crimes typified in the Cybercrime Law and to other criminal offenses committed using technological means, in which these means are essential to the execution of the crime in question.

Having presented the conceptual basis, should be mentioned that this Strategy builds on the existing law governing sovereign international relations, in particular the United Nations Charter and the International Humanitarian Law, as well as the international conventions governing the protection done by States of the fundamental rights and freedoms, in particular the Universal Declaration and the Covenant on Civil and Political Rights, and the corresponding European law, such as the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. It is also based on the general principles of State sovereignty, the protection of the freedom of expression, of the personal data and privacy, the outlines of the European Union Cyber Security Strategy, and the North Atlantic Treaty Organization's cyber defence policy; commitments done with the objectives of being resilient and having the capacity of quick and effective response to cyber-attacks. Thus, this Strategy is based on the following principles:

Subsidiarity principle:

Portugal states its strong commitment on the security of cyberspace. Considering that much of the technological infrastructure that makes up the cyberspace is owned by private sector entities, it is their primary responsibility to protect it. This responsibility begins in the individual himself, through the responsible way by which he uses cyberspace, and ends with the State, as the guardian of sovereignty and the constitutional principles.

Complementarity principle:

The security of cyberspace is a shared responsibility between the different actors, whether public or private, collective or individual. An inclusive, comprehensive and integrative approach to cybersecurity requires different responsibilities and capabilities to the benefit of the common interest.

The interdependence of technological infrastructures, and the consequent probability of the propagation of the impacts resulting from incidents, requires a complementary and reliable action, based on the awareness of the duty of reinforced cooperation between national structures and entities, considering such dependencies in order to maximize the digital protection and the digital resilience.

Proportionality principle:

Cyberspace security is also the result of a complex, verifiable and continuous exercise in assessing the risks associated with the digital ecosystem. Accordingly, the adequacy and allocation of resources should be proportional to the risks identified and to the execution of the action lines contained in this Strategy.

2 — Analysis of the context

When the first National Strategy for Cyberspace Security was approved in 2015, the technological emergence and its impact on our society was already evident.

The trend towards a growing increase of the dependence on information and communication technologies and the emergence of new phenomena with a direct impact on social development have also brought about, in connected societies like ours, significant opportunities for those wishing to compromise our network and information systems for potentially harmful purposes on the well-being of the Portuguese society.

In a strategic environment, in which the geopolitical landscape is in constant change, the threats on the cyberspace of national interest are originated from different agents and have different typologies and motivations.

The threats from state agents, which increase the risks of extending to armed conflict, stem from the political, military and economic motivation on which these actors, under the anonymity of cyberspace, seek to achieve their strategic objectives through cyber-espionage, interference and disinformation operations in a digital environment, including cyber sabotage actions aimed at reaching critical infrastructures and disrupting essential services to the proper functioning of society.

On the other hand, threats from non-state actors are often of criminal origin, with pecuniary motives, although there are also politically and ideologically motivated actions, as well as others aimed to denigrate institutional images and diminish the reputation of targets.

Through the massive exploitation of the use of malware (or «malicious code»), identity anonymization tools and the transnational character of cyberspace, organized cybercrime structures are increasingly present in the criminal landscape, not only directly but also placing their technical capabilities at the service of traditional criminal structures.

Also, traditional cybercrime targets have been expanding with mass ransomware and payment methods that allow for seemingly anonymous financial transactions. Similarly, the growth of Internet-connected devices, known as the Internet-of-Things, could contribute to an increase in attack vectors available to organized cybercrime structures.

With regard to terrorism and its support activities, some of the most frequent and visible offensive uses of information and communication technologies by organizations and individuals associated with terrorism include, namely, actions aimed at the unauthorized alteration of the contents of national

Internet sites and the public exfiltration and disclosure of information or personal data without the consent of the respective subject for that purpose.

Finally, while active radicalization and mobilization phenomena are not restricted to the online aspect, it is worth mentioning the impact of services and social networks and instantaneous communication platforms on these phenomena, and in general, on the phenomenon of the distribution of propaganda or apologetic content of major terrorist organizations. Indeed, online communication services allow an almost permanent contact between radicalized individuals and the ones who do the radicalization, regardless of geography, as well as the dissemination and saturation of propagandistic and radicalizing content on such services and platforms.

Regarding cyberspace activism (hacktivism), a phenomenon with apparent political motivations or serving a cause, which in the generality of cases means the application of methods for the disruption of systems, exfiltration, and massive public disclosure of individual data, there is a dormant potential of threat agents with the specialized capabilities adequate to perform acts of major disruption of network and information systems.

The multiplication of available learning resources and user-friendly tools has increased the number of intentional attacks on network and information systems by various actors. Many of the aforementioned threat agents find in cyberspace a stage for action, facilitated by a set of vulnerabilities from which it suffers.

The identification of these vulnerabilities, coupled with the weak cybersecurity culture and awareness of individual responsibilities in this field, as well as the insufficient digital maturity to address the security needs in both the public and private sectors, are the main weaknesses that need to be solved.

Alongside this reality, the difficulty in training, maintaining and attracting human and financial resources to monitor the rapid technological evolution and the concomitant impact on life in society represents an additional national vulnerability, requires a strong investment to be tackled, innovative networking collaboration models and an increase in research, development and innovation.

There is also a need to strengthen the coordination and strategic and operational coordination of national entities involved in the security of cyberspace in order to safeguard the efficient and effective national crisis management.

3 — Vision

This Strategy sets the following vision for 2023:

Portugal to be a safe and prosperous country through innovative, inclusive and resilient action that preserves the fundamental values of the democratic rule of law and ensures the regular functioning of institutions corresponding to the digital evolution of society.

4 — Strategic Objectives

Strategic Objective 1 — Maximize Resilience:

Strengthen and guarantee the national digital resilience by enhancing inclusion and networking in order to safeguard the security of cyberspace of national interest against threats that may compromise or cause the disruption of the network and information systems essential to society.

Strategic Objective 2 — Promote Innovation:

Foster and enhance national innovation capacity by affirming the cyberspace as a domain for the economic, social and cultural development and prosperity.

Strategic Objective 3 — Generate and guarantee resources:

Contribute to obtain and guarantee the allocation of adequate resources for building and sustaining the national capacity on cyberspace security.

5 — Axes

The implications and needs associated with each of the strategic objectives make it possible to define a general and specific approach, translated into six intervention axes, which form concrete lines of action aimed at reinforcing the national strategic potential in cyberspace by increasing its security, namely:

Axis 1 — Cyberspace security structure;
Axis 2 — Prevention, education and awareness;
Axis 3 — Cyberspace and infrastructures protection;
Axis 4 — Response to threats and combating cyber-crime;
Axis 5 — Research, development and innovation;
Axis 6 — National and international cooperation.

Axis 1 — Cyberspace Security Structure:

The complexity and scope of the cyberspace security challenges require a strong and transversal leadership and governance, an agile, quick and effective operational coordination, capacity to respond and safeguard the national interests and, above all, an involvement of resources, knowledge and competences. Thus, within this axis, the following lines of action shall be adopted:

Consolidate the national structure contained in Law No. 46/2018 of 13 August, reinforcing the Superior Council for Cyberspace Security as a specific consultative body for the Prime Minister to ensure the political-strategic coordination for cyberspace security, with representatives of all stakeholders to ensure a transversal and inclusive approach to policies and initiatives developed by the various entities with responsibilities on this area;

Strengthen the National Cybersecurity Centre as the National Cybersecurity Authority and, as a result, as the national single point of contact for international cybersecurity cooperation purposes, without prejudice to the legal attributions of other entities, namely the Public Prosecutor and the Criminal Police, concerning international cooperation in criminal matters, the Armed Forces in cyber defence, the Secretary-General of the Information System of the Portuguese Republic on the production of national and external security information and the Secretary-General of the Internal Security System regarding the Single Point of Contact on international police cooperation, alert situations and quick response to internal security threats;

Strengthen the national cyber defence capacity to maximize the resilience of the Armed Forces to deal with significant incidents or cyber-attacks that affect national interests and sovereignty; all means should be used to respond to cyber-attacks, including offensive cyberspace capabilities, proving to be essential a close liaison and coordination with the various relevant actors in case of incidents;

Strengthen the national cybersecurity capacity to maximize the resilience of the Security Forces and Services, to address significant incidents or cyber-attacks within their attributions, being fundamental a close connection and coordination with the various relevant actors in cases of incidents;

Deepen the dual use of cyber defence capabilities within military operations and national cybersecurity by developing and consolidating an information sharing system at various decision-making levels and thresholds;

Promote a greater articulation and coordination of the relevant entities in the areas of cyberspace security, notably through the creation of synergies with the entities that are in the Internal Security System, as well as with authorities and regulators on relevant sectors such as the electronic communications sector and the sectors of essential services;

Update the Public Prosecution structures through the establishment of specialized response structures for emerging requests arising from crimes in the digital environment to ensure evidence-based effectiveness and to be able to meet potential international cooperation requirements in criminal matters;

Strengthen the capacities of the Criminal Police by strengthening its structures and human and technical capacities for investigating and combating cyber-crime by fostering the human resources allocated to this area and its ability to carry out evidence-taking measures using technical means, and to respond to the requirements of the international cooperation of the police;

Strengthen the Security Intelligence Service, within its exclusive competence to produce information aimed at ensuring the internal security and necessary to prevent sabotage, terrorism, espionage and acts which, by their very nature, may alter or destroy the constitutionally established rule of law, as well as the Strategic Defence Intelligence Service, within its exclusive competence to produce information that contributes to safeguarding the national independence, national interests and external security of the Portuguese State, without prejudice to the intelligence activities carried out by the Armed Forces necessary to comply with their specific missions and to ensure military security, so that their human and technical research and analysis resources can have a clear picture of the capabilities and intentions of threat vectors that are being identified at all times, while strengthening international cooperation and consolidating proximity with national actors in this field.;

Apply the complementary legislation to the cybersecurity legal regime ensuring a clear legal framework for all, notably regarding the security requirements to comply with, the thresholds for determining the impact of an incident and the incident reporting requirements;

Enable «CERT.PT» as the national IT security incident response team to ensure the operational coordination of incident response, namely in connection with existing IT security incident response teams and all the other relevant national structures, considering that incident reporting improves the situational awareness of cyberspace of national interest and facilitates the sharing of information for the benefit of all;

Strengthen the role of the IT security incident response team communities as a platform of excellence for coordinated operational response and the sharing of best practices and incident information;

Increase the interoperability within the structures, in particular by developing and deepening existing taxonomy and procedures;

Develop, within the scope of the international action, cyber-diplomacy as the discipline of the State's external action aimed at promoting, inter alia, the application of the existing international law to cyberspace in order to ensure its stability, the transparent and shared governance of its universal use and the efficient creation of normative capacities, namely within the Portuguese-Speaking Countries Community.

Axis 2 — Prevention, education and awareness raising:

In the context of prevention, the key role of information sharing in early threat assessment should be safeguarded. The permanent uncertainty regarding the various diffuse threats, of undefined, ever-changing contours and developments that impose on the security of cyberspace of national interest requires a national capacity to detect and know in a timely manner indicators that may be associated with potential and ongoing threats. In this sense, it is crucial to develop the ability to obtain, in an automated, systematic and coherent way, knowledge on these indicators. A homogeneous and insightful knowledge of threat indicators will thus enable the entire national cyberspace security ecosystem to have an adequate prior knowledge to produce threat anticipation and security measures against unwanted impacts.

At the same time, cyberspace security depends on promoting a culture of security, framed by the principles of ethics, which provides all with the knowledge, awareness and confidence needed to use information networks and systems, reducing exposure to the risks of cyberspace. In this context, it is essential to inform and raise awareness not only of public bodies, but also of companies and civil society. On the other hand, it is crucial for the country to equip itself with qualified human resources to deal with the complex cyberspace security challenges.

Ensuring the security of technology infrastructures, network and information systems depends on the ability of end users to take measures to prevent the risks to which they are exposed. Thus, permanent awareness is an essential factor in the prevention of cyberspace security.

Thus, in the context of prevention, education and awareness, the following lines of action shall be adopted:

Strengthen the means of information collection and processing and analysis capabilities;

Know the threat agents, their intentions and capabilities and assess the potential impacts generated by their activity;

Anticipate the emergence, evolution and mutation of threats, enabling the timely adoption of actions that add resilience;

Create a more resilient society by stimulating the development of digital skills in the citizens, without prejudice to other similar national programs, such as the «National Digital Skills Initiative e.2030 — INCoDe.2030»;

Create tools and strengthen civil society awareness-raising measures for the safe and responsible use of digital technologies, with particular emphasis on capacity building and knowledge gained by children, adolescents, seniors and other at-risk groups;

Promote robust and cross-cutting cyber security training programs for all organizations and the average citizen, enabling users to understand their responsibilities, using and adequately protecting the information and resources entrusted to them;

Strengthen cyberspace security skills and knowledge in education, including such themes in the syllabus of primary, secondary and tertiary education and in continuing teacher training;

Promote digital education and literacy as a prerequisite for the trust and use of new technology digital resources by new generations and especially vulnerable groups in a conscious, informed and responsible manner;

Encourage the identification of young people with high potential for cybersecurity and promote their timely integration into a professional context;

Promote the advanced technical training on cyberspace security in universities and polytechnics to meet the national needs of professionals in the sector;

Value the inclusion of a conscious and responsible behaviour regarding the use of technology as an integral and transversal part of the current academic and professional training;

Promote specialized training and sensitize decision makers, public managers and operators of critical infrastructures and entities that provide essential services to society, with a view to raising awareness and prevention of the need to safeguard the interests and critical national information;

Value professionals in the field of cyberspace security, increasing the number of specialists, qualifying professionals and involving the various actors from all society;

Ensure a high level of quality of cybersecurity training and requalification courses, obtained through the certification of this framework;

Create retention mechanisms in national human resources entities qualified in cyberspace security;

Organize and conduct exercises to assess the preparedness and maturity of the various entities to deal with incidents with relevant impact, enhancing synergies. Additionally, participate in exercises of international scope;

Take advantage of national and international military and police education and training structures, in particular by taking advantage of the opportunity in Portugal to build specific teaching structures of the North Atlantic Treaty Organization and the European Union and associated initiatives to deepen the knowledge related to cyberspace and contributing to the awareness and prevention of its use;

Promote specific awareness programs with public and private institutions that strengthen the behavioural aspect of security in the digital environment, based on the sharing of specialized knowledge about threat agents and their modes of action;

Sensitize national entities to their specific vulnerabilities that could be infiltrated, exploited or subverted in the digital field by various threat agents.

Axis 3 — Cyberspace Protection:

The security of cyberspace is an integral part of national security and is essential for the regular functioning of the state, the economic development and innovation, as well as for citizens' confidence in the digital market and cyberspace. Thus, for this axis, the following lines of action shall be adopted:

Identify and reinforce the knowledge on the critical information infrastructures, following the profound change and dynamics of the national and international cyberspace security legal framework;

Promote the continuous development of the capabilities and maturity of national entities for the prevention, detection, response and recovery from adverse cyberspace security scenarios that may impact their network and information systems and ecosystem that characterize them, building the mutual trust, the sharing of information and knowledge, and the quick and effective cooperation;

Promote national and sectoral cyberspace protection cooperation structures, including from the public sector at central, regional and local levels, and also from the private sector, including small and medium-sized enterprises, for information sharing and the promotion of mutual collaboration in the protection of common interests;

Ensure the application of mechanisms and incentives to enable the development of national and international cyberspace security management frameworks and their adoption by national authorities with responsibilities for critical infrastructures and essential services;

Maximize the security and defence of the Armed Forces and National Defence information networks and systems with a view to maintaining operational capability in cyberspace through the capability of defensive cyber defence.

Axis 4 — Response to threats and combating cyber-crime:

In the area of post-incident response, according to the characteristics of cyber-attacks, in addition to the criminal authorities and the entities that make up the Internal Security System, other entities that, because of their attributions, detain information, including their own, or resulting from national and international cooperation relevant to the attribution of authorship or supporting the criminal investigation itself, shall intervene.

The national security of cyberspace is also based on its ability to build deterrent mechanisms. The achievement of such a goal involves training cyberspace security authorities in defensive and response mechanisms so that any unlawful action against cyberspace in the national interest will be the object of an appropriate action.

Thus, the indispensable existence of mechanisms for the threat identification, analysis, assessment and disruption make it imperative to reinforce the means of threat identification and appropriate response through the strengthening of national cyberspace security structures.

Also, cyberspace has led to the creation of new patterns of human behaviour and action for the benefit of society, as well as new threat typologies and crimes that need a timely, coherent, participatory and collaborative response, where it is important to protect legally established property and the rights of citizens. Furthermore, in addition to opening the way for the practice of new types of crime, it has also given rise to an enabling environment for old crimes to develop with new, far-reaching offensive methods and actions detrimental to the national interest.

It is also important to highlight that cyberspace threats are characterized by their transversality, rapid network propagation, anonymity and persistence. Considering this threat typology, only one network response will enhance and strengthen the effort and capacity of the entire community involved in risk mitigation, minimizing or preventing the respective impacts and ensuring a high common level of security in the cyberspace of national interest.

The challenges posed by the prevention and investigation of these phenomena imply a careful and permanent observation, which allows, to prepare for timely legal developments and, to adapt the capacity of public and private entities to respond to threats that undermine the operational continuity and the fight against cyber-crime. Likewise, these challenges require institutions to make a permanent effort to equip and to enable them to fully fulfil their missions. It is therefore important that the threat response systems, such as the police and the judiciary systems, in coordinated effort, adapt to the ways in which threats are responded to and investigated through the use of new technologies. Therefore, the following lines of action shall be adopted:

Develop and reinforce the cyber defence capacity to ensure the conduction of military operations in cyberspace, ensuring the country's freedom of action in the cyberspace and, where necessary and determined, the proactive exploitation of the cyberspace to prevent or hinder its hostile use against the national interest;

Adapt, for crisis management purposes, the capabilities of the Armed Forces, Security Forces and Services and other public and private entities, with the objective of boosting an integrated approach to the threats and risks of cyberspace security;

Carry out an assessment of the needs for revision and updating of legislation. Accordingly, the competent authorities should take the necessary measures to enable them to prepare such draft legislation as may be necessary, both in the area of substantive criminal law and in procedural and institutional, police and judicial cooperation, national and international instruments;

Assess in the context of cyber-crime the need to adjust criminal procedural rules to the global challenges it poses, and in particular as regards possible cross-border access to data (digital evidence), possible cooperation with foreign communications operators and speeding up online investigative actions, including those that may fall within the context of covert actions under the law;

Consider updating the existing legal framework for data retention and the legal framework for the seizure of e-mail and other similar communications;

Enhance threat response capacity by maximizing the synergies created by the cooperation and trust that exist between computer security incident response teams, enabling the creation of new teams of this nature in all public and private bodies, with responsibility for the security of network and information systems;

Promote, at the sectoral and business level, the creation of outside operational and technical information sharing *fora*, a coordinated response to security incidents and the production of specific safety references, ensuring their connection with their international counterparts, if any, and their alignment with the relevant references;

Consolidate and promote the national capacity to know cyberspace security threats, in a collaborative manner between national authorities with responsibility in this area and with the active participation of public and private bodies, thereby producing and sharing aggregate knowledge that enable anticipation of impacts, proactive action and better awareness of the threat for all concerned;

Encourage and boost the participation of computer security incident response teams in national and international cyberspace security *fora,* benefiting from knowledge sharing and peer confidence building.

Axis 5 — Research, development and innovation:

Building technological capabilities in the field of cybersecurity is key in this Strategy for a sustained development and the relevant observation of the future. As a result, it aims to strengthen, support and promote the national research, development and innovation potential of cutting-edge cybersecurity processes and technologies, based on the individual and collective capacities of the public and private sector, academia and industry.

The task of creating these technological capacities lies primarily with the National Scientific and Technological System, including companies, public and private institutions, within the framework of their national and international commitments, assumed in *fora*, organizations and partnership systems representing Portugal. Therefore, the following lines of action shall be adopted:

Promote scientific production, development and innovation in the various fields of cyberspace security with the aim of maintaining and affirming national independence in this field;

Stimulate and leverage through appropriate funding the country's scientific, technical and industrial capacities, with particular emphasis on critical domains and emerging technologies, giving priority to the development of cybersecurity technologies and meeting identified innovation needs;

Support the stakeholders participation in research, development and innovation in international projects;

Enhance the synergies arising from the national participation in the various international *fora* in this field and the presence in the national territory of international organizations dedicated to research, development and innovation in this area;

Enhance national synergies and address ongoing cooperative efforts in international organizations of which Portugal is an integral part, notably within the framework of the European Union (pooling & sharing), the North Atlantic Treaty

Organization (smart defence) and multinational initiatives to, in collaboration with universities, research centres and industry, to develop technological solutions of interest for dual civil and military use;

Promote the development of secure by design and secure by default products, systems and services;

Participate in the work of national and international technical committees to implement internationally accepted technical standards and specifications applicable to the security of network and information systems, without imposing or discriminating in favour of the use of a particular type of technology;

Promote innovation combined with the State's cybersecurity through the most effective information and communication technologies, in accordance with other relevant national strategies, notably the Strategy for Digital Transformation in Public Administration — ICT 2020 Strategy as well as the "Digital Development Strategy National Digital Skills Initiative e.2030 — INCoDe.2030";

Ensure the articulation of public and private entities, academia and business, namely, the entrepreneurial ecosystem and clusters, promoting the technological innovation in the country;

Promote foreign investment in cyberspace security.

Axis 6 — National and international cooperation:

In a highly interconnected and interdependent world, cyberspace security requires a strong cooperation and collaboration between national and international allies and partners, building on the development of mutual trust. This is a key factor in enhancing the resilience of the network in which all co-workers participate. As a result, this Strategy calls for an enhanced duty of cooperation between national structures and entities with responsibility in areas contributing to the security of cyberspace, whether public or private. At the same time, it promotes Portugal's international action, both bilaterally and multilaterally, in order to deepen the solid network of existing alliances, to exert influence by affirming its presence in the world and empowering others through strategic partnerships, namely between Portuguese speaking countries, thereby actively contributing to shaping the international ecosystem while safeguarding the national interest. Additionally, it is important to characterize the national participation in the various cyber defence activities in the international context in which Portugal operates, which allow the aggregation of knowledge and experience, also enabling the national affirmation in this field. Therefore, within this axis the following lines of action shall be adopted:

Contribute to the regulation and universalization of the cyberspace by promoting the respect for the applicable international law, the transparent sharing of its governance among all actors, their universal accessibility and the dissemination of good usage practices;

Deepen the national participation in the relevant bodies, organisations and agencies, in particular of the United Nations, the European Union and the North Atlantic Treaty Organization. It should also deepen national participation in the Organization for Security and Cooperation in Europe, in particular in the effort to reduce the risk of inter-state tensions within cyberspace security;

Participate in cybersecurity and cyber defence exercises by strengthening and increasing the level of maturity for cyberspace protection, where sharing information and knowledge is a key factor;

Integrate international cyber security and cyber defence organizations with a view to international cooperation and the affirmation of Portugal in this field;

Deepen the coordination and cooperation between the various national entities responsible for cyberspace security, with a view to better alerting and responding to threats;

Deepen the articulation between the National Cybersecurity Centre and ANACOM — National Communications Authority, as well as between the first and the entities that compose the State Electronic Certification System within the scope of their respective attributions;

Develop the international cyber-discipline framework in which Portugal should be inserted, identifying priority initiatives, namely the international or intergovernmental organizations for the exchange of good practices to which it should adhere.

6 — Strategy Evaluation and Review

This Strategy shall be subject to an annual review by the National Cybersecurity Council. Such an assessment shall include a verification of the strategic objectives and action plan and their adequacy to changing circumstances.

On the other hand, the rapid intrinsic evolution of cyberspace requires this Strategy to be regularly and periodically revised, considering that, without prejudice to extraordinary revising processes when required by the circumstances, it should take place within a maximum of five years.