Presidency of the Council of Ministers

NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY

December 2013

Presidency of the Council of Ministers

NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY

December 2013

INDEX

FOREWORD

The advent of the Internet marks our time. Cyberspace has increasingly become the domain through which the citizen's fundamental liberties of information, expression and association are fulfilled, the transparency of public policies is pursued and the efficiency of public administrations is stimulated, growth and innovation are attained. In this global virtual arena, billions of connections are set everyday across geographical borders, knowledge is shared, and the world as we know it is redesigned at an unprecedented speed.

The security and the prosperity of any Country increasingly depend on the protection of the ICT networks that host this ever growing wealth of knowledge and connections, and it is therefore more and more compelling to ensure in cyberspace the respect of the rights and duties already preserved in the civil society, in the economic fabric of the society, and in the International Community. The digital arena is not a space outside of the law, and it is our duty to guarantee that also in this domain the democratic principles and values in which we believe are uphold and the norms preserving individual liberties, equality and freedom are safeguarded. Likewise, it is only in an environment of trust and mutual respect that it will be possible to fully reap the opportunities of growth offered by digital platforms, and to secure the development of an open, safe and reliable cyberspace for the benefit of our financial system, our companies and our consumers.

The ever-increasing reliance of modern societies on cyberspace implies that the harm occurring in case of a disruption of the ICT infrastructure or in the event of attacks carried out throughout the ICT networks could be dreadful at the least. Threats can stem from any point of the world wide web, and they often hit the weakest links, such as the most vulnerable individuals and the least protected computer systems and ICT networks. Appalling crimes are carried out through the world wide web, such as the exchange of child pornography, and online thefts and frauds can severely damage individual wealth and valuables, hampering the necessary level of trust within the digital community. Cybercrime is a plague that can cause the bankruptcy of firms and the theft of their intellectual property, crippling the wealth of an entire nation. We assist with growing concern to an increasingly insidious threat that exploits ICT vulnerabilities to stealthily steal the results of our research and development efforts in the field of new technologies and products. For a country like Italy, which places innovation at the cornerstone of its growth and competitiveness, *the potential harm is incalculable. Given the growing degree of sophistication of cyber attacks and the ever-increasing dependency of our infrastructures on ICT networks, our very national stability and security are at risk. It is therefore essential to ensure the finest possible protection of our critical ICT assets from attacks that can potentially have devastating effects, as it would be the case in the event of cyber attacks impeding or subverting the correct functioning of the national transport system, or of energy grids, or even of our military Command and Control centers. It is therefore necessary to develop and uphold an innovative defence posture, one that is able to engage the private sector and leverage its skills in the protection of the critical ICT that the latter owns and operates, and that factors the cyber dimension of future conflicts in its strategic doctrine and in the capability planning process.*

Networks interdependence, the intrinsic asymmetry of the cyber threat, and the pervasiveness of cyberspace in all aspects of everyday life are all features that call for a holistic approach and the synergic efforts of all involved stakeholders if we are to ensure an adequate level of security in cyberspace. The ultimate objectives must be to strengthen our collective ability to preempt an attack, to detect it while it happens, to react to it, to mitigate its effects, to attribute its origin, and to rapidly restore the original functionality, while at the same time retaining the lessons learned from the case.

At the international level, Italy is fully engaged in multilateral institutions, first of all within the EU and NATO, as well as with all our bilateral partners, to promote the endorsement and respect of a set of rules of behavior in the digital arena that is consistent with our values, and to facilitate the emergence of a shared approach to cyberspace governance, so that the International Community as a whole can effectively cope with the challenges laying ahead. At the domestic level, it is of outmost importance the promotion of a well-coordinated and multi-dimensional approach in order to provide for the convergence of all Public Administrations efforts toward the achievement of objectives that are mutually reinforcing with those of the private sector and the academia.

In the current financial and economic tightening, we cannot allow for any duplication of efforts and we must therefore seek any possible synergy, keeping in mind that the budget allocation that will be necessary constitute not only a net saving if compared with the possible damage cyber *attacks can entail, but also an extraordinary opportunity of cultural, social and economic growth.*

In line with what is set forth in the Prime Minister's Decree of the 24th January 2013, the present National Cybersecurity Strategic Framework highlights the nature and the evolving trends of the cyber threat as well as of the vulnerabilities to the national ICT networks, it outlines roles and tasks of public and private stakeholders involved in cybersecurity, and identifies tools and procedures to enhance the country's preparedness to confront head-on the new challenges posed by cyberspace. The attached National Plan identifies a limited set of priorities, and provides specific objectives and guidelines in order to give concrete implementation to the Strategic Framework.

With these two documents Italy sets out a strategy around which to coordinate all efforts, so that we can face with confidence the security threats and challenges stemming from cyberspace, and pursue our national interest where the wealth of nations will more and more prosper.

EXECUTIVE SUMMARY

Following the adoption of the Prime Minister's "Decree Containing Strategic Guidelines for the National Cyber Protection and ICT Security" of the 24th January 2013, the Cybersecurity Working Group was established on the 3rd of April 2013 under the auspices of the Committee for the Security of the Republic, chaired by the Department for Intelligence and Security (DIS), and developed this National Cybersecurity Strategic Framework.

The Cybersecurity Working Group saw the active participation of all the Administrations already represented in the Committee for the Security of the Republic (Ministries of Foreign Affairs, Interior, Defence, Justice, Economy and Finance, Economic Development), and included the Agency in charge for the Italian Digital Agenda as well as the Cybersecurity Unit within the Prime Minister's Office.

The point of departure of this National Cybersecurity Strategic Framework is an assessment of today's cyber threat. The growing importance of services provided through cyberspace in everyday life – from simple online payments to the management of strategic and critical national infrastructures – implies that also the cyber threat is becoming more and more pervasive and subtle, and yet it is still widely unnoticed and underestimated. In the first chapter, "The Nature and the Evolving Trends of the Cyber Threat and of the Vulnerabilities of the National ICT Infrastructures", the major cyber threats and their actors will be acknowledged – from cybercrime to cyber espionage and cyber terrorism, from hacktivism to cyber sabotage, concluding with cyber warfare – and a brief taxonomy of the cyber organizational, procedural and technical vulnerabilities will be proposed.

Cyberspace is a man-made domain essentially composed of ICT nodes and networks, hosting and processing an ever-increasing wealth of data of strategic importance for States, firms, and citizens alike, and for all political, social and economic decision-makers. The second chapter, "Tools and Procedures to Strengthen the National Cyber Defence Capabilities", identifies six strategic guidelines around which to converge,

with a holistic, coherent and synergic approach, all national efforts, so as to enhance the country's preparedness, resilience and reaction capabilities. These guidelines include: the enhancement of the technical, operational and analytic expertise of all institutions concerned with cybersecurity; the strengthening of the cyber protection of ICT networks and computer systems supporting our critical and strategic infrastructure; the facilitation of public-private partnerships; the promotion of a Culture of Security and of cyber hygiene; the improvement of our skills to effectively contrast online criminal activities; the full support to international cooperation initiatives in the field of cybersecurity.

CHAPTER 1

THE NATURE AND THE EVOLVING TRENDS OF THE CYBER THREAT AND OF THE VULNERABILITIES OF THE NATIONAL ICT INFRASTRUCTURES

Introduction

Definition

With the term cyberspace we refer to the complex of all interconnected ICT hardware and software infrastructure, to all data stored in and transferred through the networks and all connected users, as well as to all logical connections however established among them. It therefore encompasses the Internet and all communication cables, networks and connections that support information and data processing, including all mobile Internet devices.

A complex challenge

The very same nature of cyberspace and the related transformation of contemporary societies brought about by the digital ecosystem are accountable for the emergence of unprecedented cultural, social and political issues, which require a set of coherent, effective and in many cases original solutions. As the International Community is still very much divided with regard to the principles and values that apply to the cyber domain, seeking these solutions, even in the most advanced countries, is not an easy task, and it requires a broad involvement of the private sector. The private sector, in fact, has a key role to play in coming up with possible solutions to cope with the new challenges and threats stemming from the cyberspace which for the most part it owns and operates. The private sector therefore has the interest and the duty to agree with the public sector on mutual expectations and responsibilities in ensuring the protection of cyberspace. Cyberspace has become a domain of strategic importance for the economic, social and cultural development of nations, and it is hence critical to balance the right mix of pubic and private engagement in its governance and management, taking into account at the same time the requirements of national security and public order as well as the fulfillment of all the individual and economic liberties involved.

Balancing these often diverging objectives is a complex endeavor, if one considers for instance how monitoring the technical functionality of networks is essential to allow the fulfillment of the right to privacy and the integrity of one's communication appliances, or also how it can be difficult to find the right balance between the right to privacy and the fight against criminal activities such as child pornography, drugs smuggling, hate incitement or terrorism planning - crimes that not only hurt individual and social liberties, but also undermine the very existence of an open, democratic and free Internet.

Objectives

The present National Cybersecurity Strategic Framework and the related National Plan, both foreseen by the Prime Minister's "Decree Containing Strategic Guidelines for the National Cyber Protection and ICT Security" of the 24th January 2013, aim at enhancing the national preparedness to respond to present and future challenges affecting cyberspace, and are devoted to directing all national efforts toward common and agreed solutions, knowing that cybersecurity is a process rather than an end to itself, that technical innovations will always introduce new vulnerabilities in the strategic and operational horizon, and that the intrinsic nature of the cyber threats makes our defence, at least for the time being, mostly – although not exclusively–reactive.

The cyber threat and its actors

Definition

We define the cyber threat as the complex of malicious conducts that can be exercised in and throughout cyberspace, or against cyberspace and its fundamental elements. The threat is carried out by means of cyber attacks, by which we mean more or less automated actions of individuals and organizations, both governmental and non-governmental, aiming at disrupting, damaging or impeding the regular functioning of computer systems, ICT networks or supervisory control and data acquisition systems and data processing, or at compromising the authenticity, the integrity, the availability or the confidentiality of data residing in those systems or transiting through the networks.

The most sophisticated cyber attacks can be carried out through so called cyber-weapons, that is a malicious software (i.e. malware) designed to damage or alter an IT system with the aim of causing its malfunction, or even physical damage.

An insidious threat

A fundamental characteristic of the cyber threat is its asymmetric nature. The attacker:

- May strike from anywhere in the world, as long as he is connected to the Internet;
- Exploits one single vulnerability to hack into very sophisticated and otherwise well protected computer systems;
- Attacks instantaneously, allowing no time to mount an appropriate reaction;
- Can hardly be traced or even detected, making it extremely complex for the defender to put in place a response.

The intrinsic nature of the cyber threat, therefore, limits the scope of deterrence, favors the attack over defence, and requires that all major stakeholders, both public and private, implement a continuous process of analysis so as to be able to update their security standards and procedures to the evolving operational and technical circumstances.

Classification of the threat

Depending on the actors involved and the goals pursued, it is possible to distinguish four kinds of threats:

- Cybercrime: all malicious activities with a criminal intent carried out in cyberspace, such as swindles or internet fraud, identity theft, stealing of data or of intellectual property;
- Cyber espionage: improper acquisition of confidential or classified data, not necessarily of economic or commercial value;
- Cyber terrorism: ideologically motivated exploitations of systems' vulnerabilities with the intent of influencing a state or an international organization;
- Cyber warfare: activities and operations carried out in the cyber domain with the purpose of achieving an operational advantage of military significance.

The economic impact of cybercrime

The ever-increasing volume of companies' data and personal assets information stored in cyberspace, recently encouraged by the growing resort to cloud computing, makes cyber attack potentially very lucrative while being relatively risk-free for the attacker. It is therefore no surprise that the economic impact of cybercrime is quite worrisome. This is especially true for countries like Italy, for which the theft of the original scientific, technological and companies' know-how is a direct damage to their existing comparative advantage, undermining their competitiveness in the global markets.

Computer crime is a growing concern also because its illicit profits are often re-invested in the search of new system's vulnerabilities and in the development of more sophisticated, efficient and easy-to-use offensive capabilities, making cybercrime a threat of primary importance for the stability, the prosperity and the security of the country.

The computer crime market

The computer crime market represents therefore a very palatable and profitable sector for autonomous hackers and for criminal organizations alike. They both bolster a black market in which it is possible to trade illegal contents (such as drugs, child pornography or copyrighted material) and to sell ready-to-use toolkits for conducting all kind of attacks and exploitations to the computer systems of choice, either independently or with the technical support of criminal organizations. This, in turn, multiplies the opportunities for felonies against assets (such as swindles, blackmail, extortions, thefts, etc.), misappropriation of confidential information and identity

data (with the aim, for example, to demand ransoms or commit other kinds of violations), recycling of illicit capitals, gambling and illegal bets. By the same token, it is more and more evident the involvement of criminal organizations in cyber espionage activities, often on behalf of legitimate companies, with the objective of stealing industrial patent, company strategies, market researches, analysis and description of productive processes, etc.

The role of the State

Even though the digital arena is a reality that transcends, from many points of view, national borders, states are certainly among the main stakeholders of cyberspace, because they have the ultimate responsibility for the protection of ICT infrastructures on their own territory, even if they are owned and operated mostly by the private sector.

States have the human and financial resources as well as the capability to organize and manage, overtime, complex organizations. As such, they are in a unique position to mount a robust cyber operational capability.

Protecting the military command and control networks and ensuring their full operational capability and their resilience has always been a top priority for any State. The advent of cyberspace, and its key role in ensuring the functioning of virtually every national sensitive infrastructure, industrial process and public services, has extended the mandate of the State to the protection of all ICT critical networks. In fact, the most sophisticated cyber attacks may not only impair and paralyze the State's most vital communication nodes and the provision of essential public services, but may also have potentially destructive effects if directed against critical infrastructures such as, for instance, the aviation traffic management control system or dams and energy installation's supervisory control and management systems, resulting in great physical damages and the eventual loss of human life. The strategic advantage implicit in the possibility of inflicting a great loss to the enemy's critical infrastructures by striking at great distance makes it very likely that future military confrontation will entail the full use of cyberspace. It is therefore no surprise that nowadays virtually every nation considers it relevant in its force planning to foresee the requirements of a cyber defence capability that is adequate to protect national critical ICT infrastructures.

Espionage, sabotage, warfare and supply chain cyber threat

The defence of cyber networks requires the development of an effective and uninterrupted capability of monitoring and analyzing all ongoing malicious activities. States are striving to ensure themselves with this expertise, either directly or through proxies, and considering in many cases also the potential advantages of developing aggressive tools. It is a well-know fact that some States already possess the capability to penetrate public and private networks of other States, and use this capability for espionage and in order to map ICT systems that could be potential targets in case of future attacks. In such a situation, is also highly plausible that certain States may consider mobilizing their national industry to install through the ICT supply chain components that could allow for future stealthy cyber exploitation of the end-user computer systems and ICT infrastructure.

Hacktivism

Some cyber attacks are ideologically motivated and have primarily a demonstrative intent, like damaging the image of the target and/or causing a temporary malfunctioning of the attacked ICT systems. Examples of this type of cyber attack are the Distributed Denial of Service (DDoS) attacks, that, through coordinated attacks originating from a number of unaware and remotely controlled computer (botnets), cause the intentional overload of servers that host specific services. Another example is the so-called Web Defacement, that alters the data of a chosen Internet website with the specific goal to cause disinformation, defamation or simply mockery. In other cases, hacktivists make use of malware quite similar to the ones used by hackers and computer criminals to surreptitiously seize data that are owned by the government, or that belong to companies or individuals, in order to publically expose them, or just to demonstrate the computer skills that they have.

The use of the Internet for illegal activities

The digital arena is an extraordinary means to establish connections at the global level. There is unfortunately also the risk that this communication platform and the high level of anonymity it allows are used by some to spread racial hate, exchange illegal material (such as, for example, child pornography) or plan crimes, civil unrest or terrorist attacks. Even if we cannot call these phenomena cyber attacks in the literal sense of the word, inasmuch as cyberspace in this case is only used as a means of communication, there is no doubt that the inherent lack of attribution allowed by cyberspace makes the threat particularly insidious. We cannot hesitate to clearly assert that the same norms and rules of behavior that already exist in the civil society fully apply to the cyber domain. The challenge before us is therefore to preserve the greatest possible degree of freedom of expression while making sure that the Internet is not used to perpetrate activities that would be illegal in other conventional domains.

Terrorism

It is possible that in the next future terrorist groups or individual “lone wolves” might make use of cyber offence capabilities to hit military and civil targets. These cyber weapons might either be ready available to terrorists through criminals operating within the computer crime market, or might be developed independently by the terrorists through a process of reverse engineering of already existing cyber weapons. Fortunately, this is for the time being only a hypothetical threat, but it is essential to make sure that potentially destructive cyber tools remain out of the reach of dangerous users.

Unexpected event, incident

The full account of threats that stem from cyberspace is virtually impossible because this domain is characterized by continuous technological innovations; therefore unexpected developments might confront us with new technological and governance challenges demanding a collective and systemic effort. Cyberspace is a man-made domain, and as such it is potentially flawed. It is therefore necessary to develop the necessary skills to anticipate and prevent rare and unexpected events, focusing on the resilience and the business continuity of the services that are essential for the security and the stability of the country.

Cyber vulnerabilities

Cyber attacks undermine users' trust in ICT technologies and impair business continuity by exploiting organizational, procedural and technical vulnerabilities – often in various combinations. Organizational and procedural vulnerabilities depend both on the deficient implementation of protection against malware – such as inappropriate network design, update of anti-viruses and anti-spam software – and on the lack of appropriate physical protection intended to ensure continuity of the service and to minimize the impact of natural events on physical infrastructure.

Technical vulnerabilities are instead due to the vulnerabilities of hardware and software, and to faults in communication protocols. The latter are particularly worrisome when they affect the Domain Name System (DNS), because they impact both ends of the systems, that is to say the final electronic communication users as well as the supervisory control and data acquisition systems of critical infrastructures connected to the Internet.

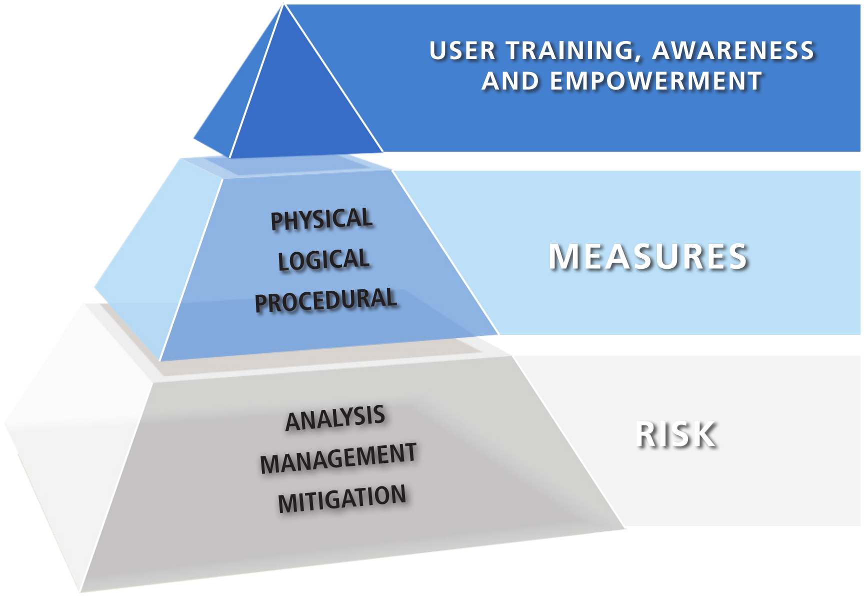
Such vulnerabilities can cause service unavailability, or they can compromise the integrity of the information stored and provided by the DNS. In both cases, the exploitation of such vulnerabilities has extremely serious consequences, possibly resulting in a grave malfunctioning of fundamental control nodes of the infrastructure.

In order to prevent these vulnerabilities from being exploited, we must first of all set up a risk assessment, mitigation and management plan, which must take into account physical, logic and procedural cybersecurity measures, and raise awareness among the personnel through training and education.

In principle, key requirements of the cyber security policy should extend to:

- Control of the access to physical installations: in order to minimize the risk of damage, tampering or theft of hardware assets, only traceable and authorized personnel should be granted access to the installations warehouse;
- Exclusive use of certified products in order to exclude from the supply chain foreign retailers considered "at risk"; use of up-to-date antivirus software; encryption of data and digital signature; identification and authentication of connected users; monitoring and logging of instances; updating of the access privileges of every user (logical measures);
- Norms and procedures instructing all phases and aspects of the security processes; definition of roles, tasks and responsibilities within the risk assessment, mitigation and management plan; adoption of specific measures that complete and reinforce the technological preparedness; recurring controls on the consistency and reliability of the ICT assets (procedural measures).

CYBER SECURITY



CHAPTER 2

TOOLS AND PROCEDURES TO STRENGTHEN NATIONAL CYBER DEFENCE CAPABILITY

Strategic guidelines

In order to allow the country to fully benefit from the social and economic advantages made possible by a safe cyberspace, and keeping in mind the overarching goal of enhancing the nation's cyber preparedness, resilience and reaction capabilities, this National Cybersecurity Strategic Framework sets out the strategic guidelines that must be pursued through a joint effort and a coordinated approach of all key stakeholders of the national cybersecurity architecture identified by the Prime Minister's Decree of the 24th January 2013, under the coordination and guidance of the Committee for the Security of the Republic.

These guidelines include:

1. The enhancement of the technical, operational and analytic capabilities of all institutions concerned with cybersecurity, so as to leverage the national capability to analyze, prevent, mitigate and effectively react to the multi-dimensional cyber threat;

2. The strengthening of our capabilities to protect critical infrastructure and strategic assets from cyber attacks, with the aim also to ensure their business continuity and the full compliance with international requirements, security standards and protocols

3. The facilitation of all public-private partnerships designed to actively promote the protection of the national intellectual property and technological innovation;

4. The promotion of the Culture of Security among citizens and institutions, also leveraging the expertise of the academia, so as to raise awareness of the cyber threats among users;

5. The reinforcement of our capability to effectively contrast online criminal activities, in compliance with national and international norms;

6. The full support to international cooperation in the field of cybersecurity, with a special attention to initiatives underway in the International Organizations of which Italy is a member and with its Allies.

In accordance with these six strategic guidelines, eleven operational guidelines have been identified.

Operational Guidelines

1

Enhance the expertise of the intelligence community, the Armed Forces, the Police and of the Civil Protection Department to effectively prevent, identify, react to, manage, mitigate and neutralize malicious activities targeting national ICT networks in order to curb the negative impact that these activities may have on the systems that support the provision of services of public interest, and to restore their original functionality.

Increase monitoring and analytical capabilities in order to be able to foresee the potential risks that technological innovation can bring about.

Develop the capabilities of the Armed Forces to plan and conduct computer network operations.

2

Identify the Network and Information Security (NIS) Authority that will engage at the European level, both with individual member states and with the EU Commission, to share information and counter risks and incidents affecting ICT networks and systems.

Improve public-private partnerships in order to ensure a continuous, secure and trustworthy flow of information which would allow the private sector to share information on the attacks and incidents occurring in its networks, and to receive in turn risks and vulnerabilities assessment to strengthen its preparedness.

The public-private partnership will be facilitated by the following specific provisions:

- The creation of joint working groups, in which the objective of enhancing ICT cybersecurity prevails on any market competition consideration;
- Periodic national exercises involving, along with public sector stakeholders, relevant private sector operators;
- Compulsory reporting to competent authorities of computer incidents occurring in strategic sectors;
- The definition of information sharing procedures and templates.

Foresee a regular exchange of best practices and lessons learned between private and public stakeholders, with a view also to facilitate reciprocal understanding and to foster joint training of personnel.

3

Develop a widely shared cyber taxonomy and promote a common understanding of cybersecurity terms and concepts in order to enhance interoperability and ease of communication at the national and international level.

Promote the use of questionnaires to evaluate the level of situational awareness among stakeholders so as to identify those in need of further training and education efforts.

Sponsor training and education campaign, as well as courses designed to raise situational awareness among public and private sectors personnel, as well as among the general population, in order to spread the knowledge of the threats and the risks stemming from cyberspace, and to promote cyber hygiene and a responsible use of information and communication technologies.

Enhance and continuously evaluate education and on-the-job training programs, with a view to validating existing cybersecurity management and procedures. Aggregate as much as possible the training and education efforts around already existing Public Administration's learning centers (such as the ones of the Armed Forces), so as to avoid phenomena such as the "unaware insiders", and to mitigate vulnerabilities associated with new organizational models such as the "bring your own device" (BYOD).

Introduce cybersecurity curricula in schools of all levels, in order to promote cyber hygiene and the Culture of Security.

With the support of the academia, finalize measures to improve and disseminate security standards and requirements for ICT systems and networks.

4

Foster Italy's participation in international initiatives to enhance cybersecurity, both by joining endeavors underway in the International Organizations of which Italy is a member and by strengthening ties with friendly and allied nations. Participate actively in all relevant international forums and working groups aimed at:

- At the global level, defining a set of international norms of conduct and rules of behavior that clearly identify what is legitimate under international law;
- At the European level, reinforcing the protection of critical and strategic ICT communications supporting the single market; achieving a common cyber resilience capability; curbing cybercrime; developing a cyberdefence policy and the

related operational capabilities, in line with the goals and means of the Common Security and Defence Policy; stimulating a solid technological and industrial base for ICT and computer products, in line with the principles set out in the EU cybersecurity strategy and with the commitments made in the European Council and OSCE;

- At the Trans-Atlantic level, ensuring the efficiency and the interoperability of assets devoted to common defence, and supporting the full integration of the cyber domain in NATO defence planning process and in the military doctrine, so as to ensure the deployment of a robust capability against cyber attacks targeting the vital and strategic interests of both NATO and Italy;
- At the bilateral level, engage with countries of strategic importance, as well as with potential recipients of multilateral projects of technical assistance and capacity-building initiatives.

Participation in cybersecurity exercises organized by ENISA and NATO, with the aim of testing and improving national preparedness, also in dealing with cybersecurity events requiring international cooperation.

Italy's participation in the global debate about cybersecurity cannot ignore the interests of the national ICT and cybersecurity industrial base.

5

Attaining the full operational capability of the National Computer Emergency Response Team (CERT, as already identified by Article no. 16 of Legislative Decree no. 259/2003, and set within the purview of the Ministry of Economic Development), in order to enhance the national capability to survey and react to potential threats and actual attacks on the ICT domestic infrastructure through the creation of a secure and trustworthy exchange of information.

The national CERT (CERT-N), has the task to identify a shared communication framework with other CERTs as well as to designate roles, responsibilities and points-of-contact at the national level to effectively ensure crisis management capabilities and the consistency of a national cybersecurity community.

The national CERT works as a cooperative public-private partnership supporting citizens and firms through situational awareness and prevention campaigns, and acting as the coordination point in the response to large-scale cyber events.

Activation of all appropriate cooperation mechanisms at the national and international level, making the national CERT the main interface of other public and private CERTs operating both domestically and outside national borders, including the European CERT.

Development of a communication platform to facilitate, both at the technical and at the functional level, communications among all CERTs, so as to ensure timely and effective interaction between all stakeholders involved in preventing and countering malicious cyber activity.

Development and attainment of the full operational capability of the Public Administration's Computer Emergency Response Team (CERT-PA), which represents the evolution of the CERT developed with the Public System of Connectivity (SPC) established by the Presidential Decree of the 1st April 2008. The CERT-PA is the designated first point of contact for all Public Administrations, which will report to the national CERT in accordance with specific unitary models and procedures. The CERT-PA works in coordination with the other Public Administrations' CERTs at the European level through exchanges of information and agreed procedures.

The CERT of the Armed Forces follows the technical, functional and procedural developments and guidelines of the NATO Computer Incident Response Capability (NCIRC), and it will be fully integrated in the military operational planning.

6

Ensure effectiveness of cyber security countermeasures by means of organisational and regulatory proposals that adapt to the rapid progress of information technology.

7

Establishment of security standards and requirements for products and systems implementing security protocols. Introduction of processes to certify the compliance to these security standards and, where appropriate, implementation of new procedures for the procurement of ICT products on the national territory. These standards and procedures should always guarantee international interoperability, especially with NATO and UE countries.

Establishment and adoption of technical norms to guarantee the security of information (integrity, availability and privacy) by introducing of a methodology for ensuring the secure design of ICT products and systems.

Improvement of the support to ICT users, also through the introduction of suitable market incentive aimed at promoting the security of available products.

8

Cooperation with the industrial sector for the adoption of security protocols aimed at protecting ICT networks and products, as well as innovative technologies. Planning of public services of assistance and support, in particular to small and medium enterprises.

Definition and identification of best practices and procedures to mitigate supply chain risks and creation of audit mechanisms to verify the reliability of ICT products and vendors.

Development, within the Public Administration, of a flexible and swift process of procurement, evaluation, verification and certification of ICT products, which has to keep the pace with the rapid innovations that characterizes the sector.

Envisaging incentives to stimulate the national ICT industrial competitiveness: focusing the activities of R&D and of the national Centers of Excellence on sectors that are deemed strategic for the Armed Forces or have a potential operative impact, such as the development of resilient and secure ICT products and software.

9

Since the cyberspace is at the same time the means and the object of strategic communication, ensuring consistency between strategic communication and the activities carried out in the cyber domain may strengthen the effectiveness of the country's instruments of prevention and response to cyber attacks. An effective institutional communication of national dissuasion and deterrence capabilities in cyberspace may work as a disincentive to potential adversaries and criminals.

10

Allocation of adequate human, financial, technological and logistic resources to the strategic sectors of the Public Administration that are the most directly involved in the achievement of the short and medium term strategic objectives envisaged in this National Cybersecurity Strategic Framework.

11

Implementation of a national integrated system of information risk management which is able to:

- Establish an effective national structure for preventing and managing risk;
- Identify potential risks;
- Elaborate risk management policies and procedures.

The central Role of the Public-Private Partnership (PPP)

As envisaged in the Prime Minister's "Decree Containing Strategic Guidelines for the National Cyber Protection and ICT Security" of the 24th January 2013, public and private operators providing "public networks of communications or electronic communication services to the public, operating national and European critical infrastructures depending on ITC systems" are among the main stakeholders of the national architecture to guarantee cyber protection and national IT security.

According to the aforementioned Prime Minister's Decree, such subjects are obliged to:

- Communicate to the Cybersecurity Unit every significant security and integrity violation of their own computer systems;
- Adopt all the best practices and measures necessary to pursue cyber security;
- Share information with the agencies for intelligence and security and allow access to databases that are relevant to cyber security;
- Collaborate to the management of a cyber crisis by restoring the functionality of the networks and systems they operate.

The public-private partnerships therefore an essential component for ensuring the success of any cyber security strategy. In modern economic and institutional systems the majority of essential public services and national strategic infrastructures are managed by the private sector. The cooperation with these actors has been ensured through ad hoc agreements with the aim to substantiate even further the cooperation in this context. In light of further progress, to be pursued through an incremental process, the synergies with the private sector should be extended so as to include all entities that, independently of their size, are of strategic value for the scientific, technological, industrial and economic progress of the country.

ANNEX 1

PUBLIC STAKEHOLDERS' ROLES AND MANDATES

The Prime Minister's Decree of the 24th January 2013 outlined the institutional architecture devoted to cyber protection and ICT security, one in which the various stakeholders involved, both from the private and the public sectors, act in an integrated and consistent way so as to mitigate cyberspace vulnerabilities, identify threats, prevent risks and enhance the national capability to counter crisis situations.

At the top of such architecture is the Prime Minister, who adopts the present National Cybersecurity Strategic Framework and the National Plan, and who ensures its practical implementation through the adoption of specific directives. The Prime Minister is supported in this endeavor by the Committee for the Security of the Republic (CISR), which may propose the adoption of legislative initiatives, approves the guidelines to foster public-private partnerships, the policies for enhancing info-sharing arrangements and the endorsement of best practices, and approves other measures to strengthen cybersecurity. The Committee for the Security of the Republic at Working Level (the so called "Technical CISR") is in charge of the verification of the timely and correct implementation of the National Plan for cybersecurity, which complements the National Cybersecurity Strategic Framework.

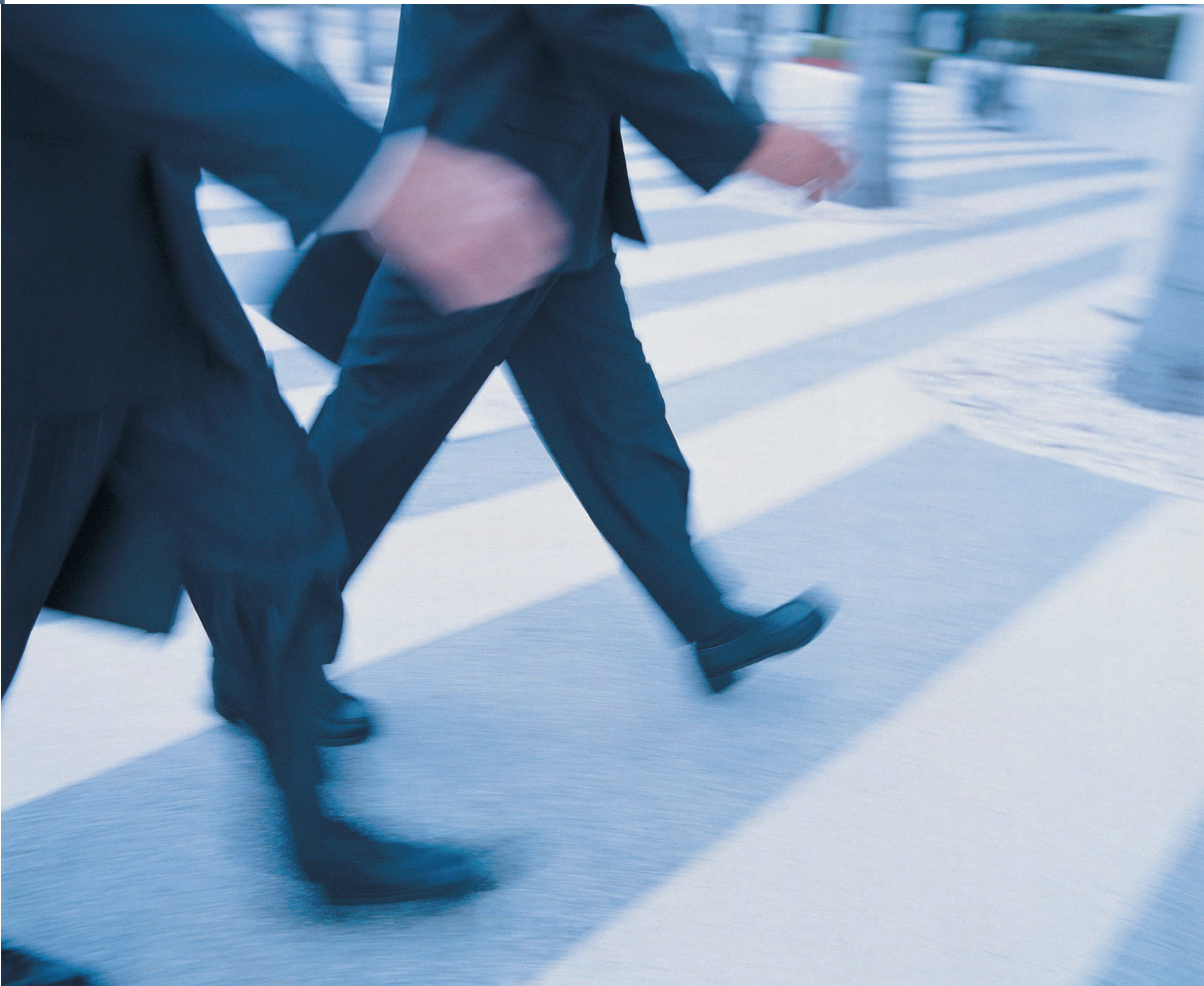
Supporting the political level is the national intelligence community, that gathers intelligence, produces all-source analysis, evaluations and forecasts about the cyber threat, contributes to the promotion of cybersecurity awareness and education, and provides relevant information and alerts to the Cybersecurity Unit and to other public and private stakeholders.

The Cybersecurity Unit is established within the Prime Minister Military Advisor's Office with the mandate of coordinating the various institutions that compose the national cybersecurity architecture, preventing and preparing for situations of crisis, and for early warning. Notwithstanding the primary responsibility of each Administration for the ownership, custody, protection and data processing of their database and digital archives, the Cybersecurity Unit:

- Promotes, with the full participation of the relevant public and private stakeholders, contingency planning activities and the preparation of crisis management operations in response to crises affecting cyberspace; elaborates inter-ministerial coordinating procedures to manage crisis;
- Ensures a 24/7 Alert and Response Cell;
- Evaluates and promotes procedures for ensuring info-sharing and early warning alerts for crisis management;
- Receives notice - including from private operators providing public ICT networks or publicly accessible computer communication services, or that manage relevant national and European critical infrastructures -concerning significant cyber incidents regarding security violation or loss of integrity. Private operators cooperate actively in crisis management and contribute to the restoration of the functionality of systems and of networks they operate;
- Promotes and coordinates the execution of inter-ministerial drills and Italy's participation in international exercises;
- Is the national point-of-contact in cyber crisis situations involving the United Nations, the EU, NATO as well as other International Organizations and countries.

In order to activate the response and restoring procedures, the Cybersecurity

Unit receives warnings of cybersecurity incident and disseminates the relative alarms. In the event of an incident of a magnitude, intensity or nature such that it is considered of national security relevance, or it cannot be dealt with by the individual concerned Administrations and it therefore requires a coordinated inter-ministerial response, the Cybersecurity Unit declares the so-called "situation of national cyber crisis", and activates the Inter-ministerial Situation and Planning Unit in its "Inter-ministerial Cyber Crisis Unit" composition. This ensures that all stakeholders' response and stabilization activities are coordinated, and ensures the full support of the national Computer Emergency Response Team (CERT) set within the purview of the Ministry of Economic Development.



ROLES AND TASKS OF THE DIFFERENT PUBLIC ENTITIES

THE AGENCY FOR DIGITAL ITALY

In charge of attaining the goals set out in the Italian Digital Agenda through the monitoring of the ICT development plans of Public Administrations and the promotion of annual reviews, in line with the European Digital Agenda Program.

- Is in charge of planning and coordinating all strategic initiatives aimed at providing access to Public Administration's online services to citizens and firms in the most effective way;
- Identifies objectives, technical regulations, and guidelines regarding IT security and taxonomy, as well as procedures and standards (including open standards), so as to guarantee full interoperability and cooperation among the Public Administration computer systems and between these and the EU's (Decree Law no. 83/2012, Art. 20 (3) (b);
- Ensures the technical quality and the security of the Public Administration's computer systems and ICT connections, so as to safeguard the integrity, availability and privacy of its databases, of digital archives, and of the services provided to citizens, in a way that is consistent throughout the national territory and fully integrated at an European level. In particular, this activity focuses on database of national interest such as those identified as critical by Art. 2-bis of the Decree Law no. 179/2012 as amended by the conversion law no. 221/2012;
- Operates the CERT-SPC (Computer Emergency Response Team of the Public System of Connectivity), managing its transformation in the CERT-PA (Computer Emergency Response Team of the Public Administration), that ensures the cybersecurity and inter-connection of Public Administration's information systems, coordinating all different players involved in security management (ICT-ULS, SOC, CERTs), in respect of their respective competences. The CERT-PA cooperates with the national CERT and with the Armed Forces CERT for the achievement of national security objectives;

- Is the national hub in charge for fostering Italy's participation in European and national programs devoted to the development of the IT society;
- Follows the digitalization of administrative documents, oversees the quality of IT-related services and the spending efficiency in IT Public procurement, contributes to the diffusion and use of ICTs to foster innovation and economic growth, also promoting the diffusion of new generation's networks.
- Looks after the promotion and diffusion of computer literacy campaigns through innovative educational technologies for citizens and civil servants, concluding to that end appropriate agreements with the Higher Educational Institute for Public Administration (Scuola Superiore della Pubblica Amministrazione) and the Centre for Services, Assistance, Studies and Training for the Modernization of the Public Administration (Formez-PA).

PRESIDENCY OF THE COUNCIL OF MINISTERS

DIS, AISE, AISI

Intelligence collection finalized to strengthening national cyberspace protection and IT security.

- The Department for Intelligence and Security (DIS) and the two intelligence Agencies carry out their activities in the field of cybersecurity by making use of the tools, means and procedures set forward by Law no. 124/2007, as amended as by Law no. 133/2012. To that end, following the Prime Minister's directives for the strengthening of intelligence collection activities for the protection of physical and intangible ICT critical national infrastructure, and taking into account the general guidelines and objectives put forward by the Committee for the Security of the Republic (CISR), the General Director of DIS coordinates all intelligence collection activities to bolster national cyberspace protection and ICT security.
- The Department for Intelligence and Security, through its various offices:
  - Ensures the support to the Director General's coordinating role;
  - Provides analysis, assessment and previsions regarding the cyber threat, taking into account relevant information, analyses and reports originated by the two Agencies, the Police, the Armed Forces, all Public Administrations and public and private research Institutes, all-sources intelligence, and data gathered from Public Administrations and public utilities service providers;
  - In full compliance with the Prime Minister's Decree of the 24th January 2013, it provides for the transmission of relevant information and alerts regarding cybersecurity issues to the Cybersecurity Unit, to Public Administrations and to other subjects, including in the private sector, interested in the acquisition of such security information;
  - On the basis of what is foreseen in the Prime Minister's Decree of the 22nd July 2011, defines the cybersecurity requirements that need to be adopted for the protection of ICT systems and infrastructures that store and process classified or secreted information, issuing the required technical homologations and

evaluating eventual security violations or breaches of classified information following accidental or intentional events;

- Together with the two Agencies, acting in their respective competences, and in line with the guidelines defined by the Prime Minister and the specific research objectives set out by the General Director of DIS, carries out the information gathering activity and its elaboration for the national cyber protection and the ICT security.

- Together with the two Agencies, it interacts with Public Administrations and public services providers, as well as with Universities and research institutes, instructing to that end appropriate agreements. The Public Administrations and the public services providers allow DIS and the two Agencies to access their digital databases and archives in line with the procedures defined in the Prime Minister's Decree no. 4/2009;

- Encourages every initiative aimed at promoting and spreading the knowledge and the awareness of the cyber threats and the measures to mitigate them, also following the recommendations of the Scientific Committee;

- Composes the national security document highlighting the activities for the defense of the critical, physical and intangible infrastructures, the national cyberspace protection and IT security, that is annexed to the Annual Report to the Parliament on national security strategy and policies.

MINISTRY OF FOREIGN AFFAIRS

The Ministry of Foreign Affairs is responsible for representing the Italian national position within uppermost multilateral and international political forums.

- Ensures a coherent promotion and safeguard of Italian national interests in cybersecurity issues in all international forums and at all levels;
- Coordinates Italian participation and efforts in the various multilateral forums of discussion on cybersecurity issues, also encompassing the contribution of the private sector and of the academia;
- Negotiates, involving other national relevant authorities, all international agreements and arrangements on the subject matter, verifying their coherence and their suitability with respect to the wider national strategic guidelines for the projection of national interest in its various international formulations (security policies, human rights and fundamental liberties' protection, countering of transnational threats, safeguard and development of the financial, economic and commercial exchanges, etc.);
- Cooperates for the swift introduction at the domestic level of international obligations undertaken by Italy and of the guidelines emerging in the subject matter in all international forums (i.e. soft law, CSBM);
- Coordinates and ensure the services and the activities - also with respect to the education and awareness raising of its employees - for enhancing the protection, the resiliency and the efficiency of ICT systems of the Ministry and the diplomatic and consular ICT network;
- Participates in the security communities of the Public Connectivity System (CERT-SPC, now CERT-PA) through the Ministry of External Affairs' CERT (the so called "Local Security Unit"), already officially accredited to the CERT-SPC.

MINISTRY OF INTERIOR

National Public Security Authority

Law enforcement and public order, public rescue and civil protection, contrast to threats that involve or stem from cyberspace and that affect the population, the institutions, the firms or business continuity of the Government.

- Ensures, through the Public Security Department, the prevention and the contrast of cybercrime;
- Guarantees, through the Postal and Communication Police, the integrity and the correct functioning of the ICT network, here included the protection of critical ICT infrastructures (through the National Anti-crime Computer Centre for the Protection of Critical Infrastructure - CNAIPIC), the prevention and the contrast of computer attacks to strategic assets of the country, the security and reliability of telecommunication services, the hindering of online child pornography and of crimes affecting means of payment and copyright whenever the exclusive or prominent means to execute those crimes has been the distorted use of the computer systems or of the ICT tools;
- Contributes to the prevention and hindering of terrorist activities and of support to terrorism executed by means of computer systems and ICT networks;
- Ensures preventive and hindering activities against the wider range of cybercrimes;
- Preempts cybercrime by promoting awareness-raising campaigns to inform citizens about cybersecurity threats.

MINISTRY OF DEFENCE

Defence of the State, peace-enforcing and peace-keeping operations, support in safeguarding the freedom of national institutions.

- Defines and coordinates the military policies and strategies, the cyber governance and the military capabilities in the cyber domain;

- Plans, executes and sustains Computer Network Operations (CNO) in the cyber domain in order to prevent, localize, defend (actively and in-depth), oppose and neutralize all threats and/or hostile actions in the cyber domain targeting ICT networks, computer systems and services on the national territory or in-theatre. In this context, the Ministry of Defence negotiates memoranda of understanding and international agreements concerning the norms and rules of engagement governing the subject matter, and coordinates its cyberdefence activities with NATO, the UE and the Defence Forces of allied and friendly countries;

- Contributes to the intelligence gathering in support of in-theatre cyber operations of the Armed Forces, as foreseen in Law no. 124/2007 and subsequent amendments;

- Supports the prevention and the contrast of terrorist activities and of support to terrorism executed by means of computer systems and ICT networks against the Armed Forceson the national territory and in-theatre, as foreseen in Law no. 124/2007 and subsequent amendments;

- Ensures all those services and activities necessary to guarantee the protection, resilience and efficiency of military assets and installations, and contributes to reaction and stabilization activities carried out in case of crisis situations affecting cyberspace, working as the link between the CERT of the Ministry of Defence, the National CERT and NATO's Computer Incident Response Capability (NCIRC);

- Contributes to the prevention and contrast of cyber attacks targeting ICT systems of national strategic relevance;

- Ensures the training and education of its personnel and makes available its own training centers to other Administrations.

MINISTRY OF ECONOMY AND FINANCE

Protects national savings in their wider sense (the regulation of financial markets to state-participated companies), manages the verification and collection of taxes through the Central Tax Records.

- MEF, as a whole and through its Departments, the Fiscal Agencies and the Italian Finance Police, is responsible for various National Critical Computer Infrastructures and is provided with a complex security organization;
- Actively participates in the security communities of the Public Connectivity System (SPC), by means of the so called "Local Security Units" - ULS MEF/Sogei and ULS DF/Sogei, officially accredited among the CERT-SPC - that takes care of the coordination of the activities of prevention and management of incidents within the SPC;
- Within the MEF, there are several divisions in charge of guaranteeing the security of cyber networks and systems through the prevention and repression of financial and economic fraud carried out through IT networks and the Internet (Italian Financial Police).

MINISTRY OF ECONOMIC DEVELOPMENT

Communication Department

Promotes, develops and regulates electronic communications.

- It is the national Authority in charge of the regulations in matters of security and integrity of electronic communication system – as set in Art. 16 bis of Legislative Decree no. 259/2003 – and cooperates with other national and international bodies in this subject;
- As set in the above mentioned law, the Ministry of Economic Development:
  - Identifies technical and organization measures for the security and integrity of the networks and verifies that the networks operators and the suppliers of ITC services comply with them;
  - Collects from the networks operators and the suppliers of ITC services notifications of severe cyber incidents and forward them to the EU Commission and ENISA;
  - Operates the national CERT (CERT-N);
  - Represents Italy at ENISA - through the Director of the Institute for Communications and Information Technologies (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione-ISCOM).
- ISCOM is:
  - Is the Certification Authority of IT Security (OCSI);
  - Participates in the activities promoted by ENISA for the protection of critical IT infrastructures;
  - Participates in the works of several international and European bodies involved in the issue of Internet Governance;
  - Is in the charge of the surveillance of country-code top-level domains in the context of the Italian Registry of ccTLD ".it";
  - Is involved in the European program "safer Internet";
  - Carries out research activities in cooperation with research centers and Universities in various fields regarding electronic

communications so as to highlight concrete actions for the implementation of the objectives pursued by the European Digital Agenda.

- The Permanent Observatory for Security and Protection of Networks and Communications – chaired by the Head of the Telecommunication Department – is in charge of the Culture of Security education, the reporting of the set of compulsory services that the Internet Service Providers (ISPs) must make available to the Law Enforcement Authorities; the promotion to the Internet access, etc.

ANNEX 2

GLOSSARY OF CYBERSECURITY

AGCOM – The Communications Regulatory Authority

The two main tasks assigned to this independent Authority by Law no. 249/1997 are to ensure equitable conditions for fair market competition and to protect fundamental rights of all citizens.

APT – Advanced Persistent Threat

A threat entailing a targeted attack, aimed at installing a number of malwares in the networks of the target in order to establish links necessary for remotely exfiltrating relevant information from the networks of the targeted entity.

BYOD – Bring Your Own Device

A policy allowing company employees to bring their own mobile devices (laptops, smart phones, tablets, etc.) to their workplace and using them in order to have access to information and corporate applications, i.e. emails.

ccTLD – Country Code Top Level Domain

The last part of the Internet domain name used by a State. It consists of two letters: ".it" for Italy.

CERT – Computer Emergency Response Team

Organization with the tasks of preventing cyber incidents and coordinating response to cyber events. Several CERTs also carry out training and information functions for ICT users.

CERT-PA – *Computer Emergency Response Team – Public Administration*

Evolution of the CERT-SPC (see next paragraph) with a competence extended to Public Administration's ICT and computer systems and to all its services, in addition to the interconnecting networks. It has the task of supporting and coordinating the Public Administration in preventing to, responding to, and recovering from cyber incidents.

CERT-SPC – Computer Emergency Response Team – System of Public Connectivity

The structure responsible, at the national level, for preventing, monitoring, ensuring information sharing and analysis of the security incidents within the Public Administration SPC. It has also the mandate of ensuring the implementation of a coherent and uniform methodology for managing ICT incidents. The CERT-SPC is primary point of contact for all Local Units of Security (ULS) established for each network domain connected with the SPC.

CNA – Computer Network Attack

Activities that are conducted in and through the cyberspace in order to manipulate, obstruct, deny, downgrade or destroy information stored in the ICT networks or in the computer systems, or the ICT networks or in the computer systems themselves.

CNAIPIC – National Anti-crime Computer Centre for the Protection of Critical Infrastructure

The CNAIPIC, established by Law no. 155/2005 and with a Decree of the Minister of the Interior of 9th February 2008, is set within the Service of Postal Police and Communications, which is responsible for the security and the integrity of IT communications of the Ministry of the Interior, National Authority of Public Security. The Centre, as provided for by law, is responsible for ensuring prevention and repression of cyber crimes against critical infrastructures or ICT assets of national relevance, even through partnership agreements with the structures concerned.

CND – Computer Network Defence

Actions taken by using computer networks for protecting, monitoring, analyzing, detecting, and hindering non-authorized activities carried out against computer networks and IT systems.

CNE – Computer Network Exploitation

Operations carried out in cyberspace in order to extract information from targeted ICT networks or computer systems. They are intelligence gathering activities, or actions preparing the execution of a cyber attack.

CNO – Computer Network Operation

This term generally encompasses Computer Network Attack (CNA), Computer Network Defence (CND) and Computer Network Exploitation (CNE).

CPS – Cyber Physical System

ICT networks and computer systems supporting, managing and supervising physical assets such as civil infrastructures, aerospace, transports, health care, energy and production processes.

CSBM – Confidence and Security Building Measures

Measures aimed at preventing or resolving hostilities among States, and at avoiding their worsening by developing mutual confidence. Such measures can have formal or informal, bilateral or multilateral, military or political nature.

DoS – Denial of Service

Attack aimed at making a computerized system or resource unavailable to legitimate users by saturating and overloading server's network connections.

DDoS – Distributed Denial of Service

A DoS attack launched by several compromised and infected systems (Botnets).

DF – Digital Forensics

A discipline – also called computer forensics– that deals with identifying, storing, analyzing, and reporting computer finds, in order to present valid digital evidence that can be submitted in civil or criminal proceedings.

DNS – Domain Name System

A classification system of domain consisting of a distributed database converting automatically a website address into a Internet Protocol numerical code (IP address), which identifies the server web hosting the site.

ENISA – European Network and Information Security Agency

An Agency of the European Union established to foster ICT security through technical counseling to national authorities and EU institutions, to facilitate the sharing of best practices as well as the emergence of a community of ICT security practitioners, and to promote the Culture of Security.

Exploit

A code using a bug or a vulnerability of a computerized system.

IC – Critical Infrastructures

Critical infrastructure is an asset or system within the EU which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption may have a significant negative impact for the security of the EU and the well-being of its citizens (Art. 2 lit. b) (Directive 2008/114/CE).

ICE – European Critical Infrastructures

Critical structure within the EU member States whose damage or destruction can have a significant impact on at least two member states. The relevance of such an impact is assessed comprehensively, that is to say in terms of the impacts on other sectors, including the impact on other sectors related to other infrastructures (Art. 2 lit. e) (Directive 2008/114/CE).

Social Engineering

Art of manipulating the psyche of people in order to force them to carry out specific actions or disclose confidential information, such as the login credentials to computerized systems.

IoE – Internet of Everything

A network where people, objects, data and processes are connected to one another through the Internet, and where information is transformed into actions in real time, thus creating new and as today unforeseen business opportunities.

IoT – Internet of Things

A buzz word referred to the extension of the Internet to the world of objects, which become remotely accessible through the Internet and are therefore able to communicate information about themselves connecting to other objects and users. The objective is to ensure that the Internet traces a map of the real world, giving an electronic identity to things and places in the physical environment. The potential applications of the IoT are multiple: from the industrial applications (productive processes), to logistics and info mobility, up to the energetic efficiency, remote assistance and environment protection.

ISP – Internet Service Provider

A company that provides commercial internet access and other services through a telephone line such as Dialup and ISDN or broadband connections like optical fibers or DSL.

Malware

Contraction of “Malicious software”. A program injected in a computer system, generally surreptitiously, with the intention of compromising privacy, integrity or the availability of data, of the applications or of the operative systems of the target. To this general category belong, for example: viruses, worm, trojans, backdoor, spyware, dialer, hijacker, rootkit, scareware, rabbit, keylogger, logic bombs, etc.

Phishing

A cyber attack having, generally, as objective the wheedling of sensitive information (user-id, password, credit card numbers, PIN) by sending false emails to a large number of addresses. The emails are designed to convince the receivers to open an attachment or to access a false website. The phisher uses the data it gets to acquire goods, transfer money or only as a “bridge” for further attacks.

Reverse engineering

An analysis designed to understand the functioning of hardware and software products in order to reengineer them, for example, to enhance their functions or in order to use them for different and further aims with respect to the original ones.

SCADA – Supervisory Control and Data Acquisition

Systems employed in the monitoring and control of plants and equipment in sectors such as traffic control (air, rail, automobile), the control of systems of fluid stransportation (aqueducts, pipelines, etc.), of the distribution of the electrical energy, managing production lines that realize industrial processes and remote environmental detection surveys.

SOC – Security Operations Center

A center that provides services aimed at the security of computer systems in firms (internal SOC) or external clients. A SOC can also supply incident response services: in this case it acts as a Computer Security Incident Response Team(CSIRT), even if this function often depends on a separate entity within the firm.

TCP/IP – Transmission Control Protocol/ Internet Protocol

A set of standard protocol developed in the second half of the' 70s by the Defence Advanced Research Project

Agency (DARPA), with the aim of allowing communication among different types of computers and computer networks. TCP/IP is, still today, used by the Internet.

UTM – Unified Threat Management

An integrated security product to protect from multiple threats, consisting of a firewall, an antivirus software, and systems to filter spam and its contents.

Web defacement

An attack carried out against a website and consisting in modifying the contents of the homepage or of other pages of the website.