Presidency of the Council of Ministers

THE ITALIAN CYBERSECURITY ACTION PLAN

March 2017

THE ITALIAN CYBERSECURITY ACTION PLAN

March 2017

TABLE OF CONTENTS

PREFACE

The 2017 Italian Cybersecurity Action Plan sets out the operational guidelines and the actions to be executed in order to implement the National Strategic Framework for Cyberspace Security, as approved by the Italian Prime Minister in his capacity as the political authority responsible for national cybersecurity. The 2017 Action Plan builds on the experience gained in 2014-2015 under the previous Italian Cybersecurity Action Plan (2013) and its review, which led to the adoption —on February 17th 2017— of a new Prime Minister Decree currently regulating the Italian cybersecurity architecture.

The Plan is also in agreement with the principles behind the reviewing process of Prime Minister Decree January 24th 2013. The process led to the mended National cybersecurity framework as regulated by Prime Minister Decree February 17th 2017.

The above mentioned review —jointly conducted by the Administrations that are part of the National cybersecurity framework— greatly benefited from both the lessons learned from the first steps undertaken to build a national cybersecurity system and the experiences and choices adopted by relevant partners and Allies. The outcome of such exercise allowed to identify the changes needed to overcome some difficulties of the past and to envisage a system intended to make it easier for public and private stakeholders to contribute to the implementation of the new Action Plan.

INTRODUCTION

The 2017 Italian Cybersecurity Action Plan is intended to outline the actions required to meet the guidelines set forth by the National Strategic Framework for Cyberspace Security.

While updating the 2013 Action Plan, the current document aims at realizing a major step toward the full implementation of the Italian cybersecurity system.

The Plan outlines eleven action items, together with their associated objectives and implementing lines of effort, as required by article 3.1c of Prime Minister Decree February 17th 2017 on "guidelines for cyberspace protection and IT national security".

The Plan provides priority measures for the correct deployment of the National Strategic Framework for Cyberspace Security, involving all cybersecurity relevant stakeholders on a proactive and iterative basis.

The Plan was reviewed by CISR Ministries (Foreign Affairs, Interior/ Homeland Security, Defense, Justice, Economy and Finance, Economic Development) as well as cyber delegates from the Agency for Digital Italy and from the National Cybersecurity Management Board (established within the Prime Minister's Military Advisor Office until February 2017).

NATIONAL STRATEGIC FRAMEWORK FOR CYBERSPACE SECURITY

Strategic guidelines

1. Strengthening national Critical Infrastructures and other strategic players' defense capabilities.
2. Improving cyber actors' technological, operational, and analytic capabilities.
3. Encouraging public-private cooperation.
4. Fostering cybersecurity culture.
5. Supporting international cooperation on cybersecurity.
6. Reinforcing counter-action capabilities against online criminal activities.

ITALIAN ACTION PLAN

AI 1. Reinforcing intelligence, law enforcement, and defence capabilities.
AI 2. Strengthening public-private cooperation.
AI 3. Fostering IT security culture. Education and training.
AI 4. International cooperation and cyber exercises.
AI 5. Incident prevention, response and remediation.
AI 6. Updating cybersecurity legislation and managing compliance at international level.
AI 7. Security protocols and standards compliance.
AI 8. Supporting industrial and technological development.
AI 9. Strategic and operational communication.
AI 10. Resources.
AI 11. Implementing national cyber risk management.

The review focused in particular on the following:

- AI 5 (Incident prevention, response and remediation) which includes provisions to strengthen the existing CERTs, to create the structures required by the NIS Directive (CSIRT, national single point of contact, National Authorities) and to establish efficient coordination procedures among all current and future cybersecurity framework's stakeholders (CERT, CSIRT, intelligence, law enforcement, defense, Agency for Digital Italy, etc.).
- AI 1 (Reinforcing intelligence, law enforcement, and defense capabilities) which, once updated according to the experience gained during the previous two years, aims at boosting national cybersecurity response capability.

In order to ease a quick improvement of the national cybersecurity framework, a series of core tasks to be pursued with priority was identified (see box below). Tasks were chosen according with the review of the previous strategy and taking into account developments occurred both at national and international level.

CORE TASKS

- Review governance and responsibilities of the National Cybersecurity Management Board.
- Simplify decision making procedure for cyber crises' management.
- Reduce complexity within the national cybersecurity framework through organizations' suppression/merger.
- CERTs' gradual unification.
- Creation of a national cybersecurity evaluation and certification center.
- Creation of a venture capital fund or foundation.
- Creation of a National Cybersecurity R&D Center.
- Creation of a National Cryptographic Center.

ITALIAN CYBERSECURITY CORE TASKS

The Action Plan details the initiatives needed to achieve a step change in increasing national information system and network security levels, as required by Prime Minister Decree February 17th 2017.

In spite of 2014-2015 efforts, the efficacy of measures adopted to protect networks and systems showed a patchy picture, with discrepancies persisting both horizontally —between public and private stakeholders— and vertically, within the same domain.

National security sensitive information is not just a government business. Private entities operating in strategic sectors must be considered as key assets and included into a holistic approach to national cybersecurity that provides for the implementation of minimum security requirements for Country-critical systems.

On these premises, the core tasks were selected for their systemic relevance due to the fact that they:

- Leverage the competences and responsibilities of all relevant stakeholders (public sector, private sector, research and academia).
- Refer to the most relevant activities aimed at consolidating the national cyber defense system including: assets' common protection (CERT); SW/HW certification; identification of critical functions; info-sharing requirements in case of relevant cyber events; etc.

Pending the transposition of the "EU Directive 2016/1148 concerning measures for a high common level of security of networks and information systems across the Union" into national legislation, the 2013 Italian cybersecurity framework has been revised and optimized through:

- The simplification of both ordinary and emergency management procedures (see AIs 1, 2, 5).
- The reorganization of the National cybersecurity framework (suppres-

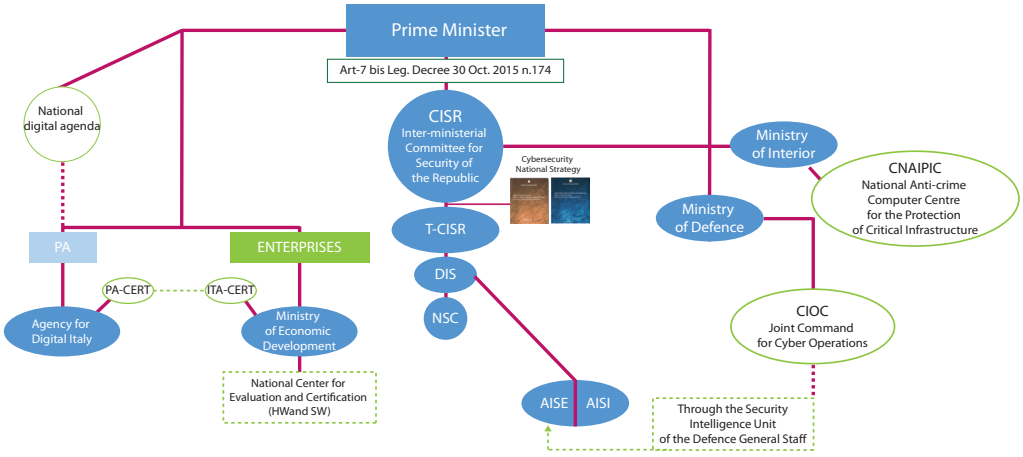
sion of the cyber NISP, new role for the National Cybersecurity Management Board/NSC, etc.) (see. AI 1).

- The simplification of the decision making for cyber crises', aimed at facilitating prompt and efficient response and remediation (see AI 5).

Of particular relevance are the measures intended to:

- Assign to the Director General of the Security Intelligence Department a central role among the entities composing the National cybersecurity ecosystem.
- Suppress the cyber NISP and relocate the National Cybersecurity Management Board within the Security Intelligence Department. The board will be responsible for cybersecurity crises' management and will be supervised by a Security Intelligence Department Deputy Director.
- Promote close interaction between the National CERT and the Public Administration CERT in order to facilitate their operational coordination and guarantee a single detection capacity, alert, and first cyber incidents' assessment (see AIs 5, 6, 7).
- Establish a national evaluation and certification center, within the Ministry of Economic Development, responsible for security and reliability check of ICT components for Critical Infrastructures (see AI 7).
- Enlarge and better define the number of actors operating in security relevant sectors (Operators of Essential Services and Digital Service Providers) required to notify serious cyber incidents or else to pay effective, proportionate, and dissuasive penalties (see AIs 2, 5, 6).

NATIONAL CYBER SECURITY FRAMEWORK

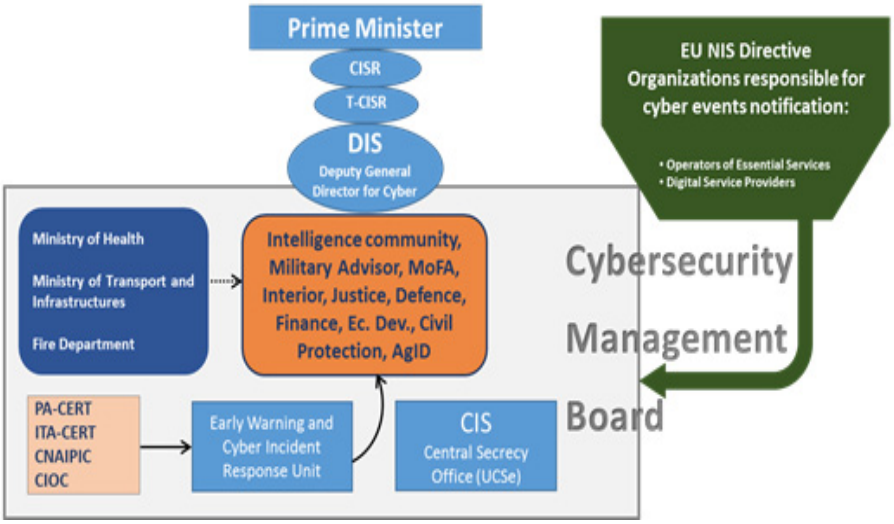


A real improvement of the Italian cybersecurity landscape cannot be achieved without full commitment of public and private stakeholders. For this reason, the Plan aims at engaging relevant private companies, academia and research centers (see AI 8).

As far as the research sector is concerned, specific initiatives —possibly backed by a legal entity (eg. foundation)— aim to (see AIs 2, 6, 7):

- Support start-ups or other relevant entrepreneurial activities (through venture capital funds).

UPDATED CYBERSECURITY CRISIS MANAGEMENT SYSTEM



- Create a National Cybersecurity R&D Center responsible —among other things— for developing malware analysis, security governance, Critical Infrastructures' protection, threat analysis, etc.
- Create a National Cryptographic Center responsible for codes/algorithms and blockchain development and security assessments.

Regarding the public sector, key institutions are called upon to take part in a systemic, coherent, and detailed intervention to improve national cybersecurity.

In particular, the new National Cybersecurity Management Board, at the center of the Italian cybersecurity framework, aims at facilitating governance simplification by cutting decision-making processes short and rationalizing both ordinary and emergency procedures.

The Ministry of Interior (in particular, the National Anti-crime Computer Centre for the Protection of Critical Infrastructure CNAIPIC) plays a key role in protecting IT Critical Infrastructures thanks to its investigative and forensic capabilities.

The Agency for Digital Italy's responsibilities are equally relevant. The Agency is in charge of defining IT security guidelines and technical rules, setting standards, monitoring quality of public networks' security and Public Administration's ICT programs.

The Ministry of Defense (MoD) developed specific cyber capabilities —to protect its networks at both national and international/operational level— which are also a significant asset for the National Cybersecurity Management Board's improvement process.

The Action Plan also aims at supporting the MoD on the following initiatives:

- Creation of a Joint Command for Cyber Operations in charge for MoD networks and systems protection, and cyber operations.
- Establishment of a virtual cyber range —to be located in Chiavari (Genova area) within the Armed Forces' TLC School facility.

Intelligence Community and MoD agreed on a specific protocol to align their strategies and tactics on cybersecurity in order to facilitate the consolidation of the perspective Joint Command for Cyber Operations in compliance with NATO recent posture.

The Action Plan aims to secure national assets according to the following priorities:

- Level 1 — National security [Intelligence Community, Ministry of Defense, Ministry of Interior, Ministry of Foreign Affairs, Ministry of Justice, Ministry of Economy and Finance, Ministry of Economic Development].
- Level 2 — National Critical Infrastructures [TLC, utilities, financial Sector, transports] and other relevant Public Administrations (eg. Ministry of Health).
- Level 3 — National production system and population.

ACTION ITEM 1

REINFORCING INTELLIGENCE, LAW ENFORCEMENT, AND DEFENSE CAPABILITIES

National cyber protection and ICT security require an in-depth knowledge of both technological and human vulnerabilities as well as of the threat that exploit them.

1.1	Threat and vulnerability analysis	a. Assess and evaluate cyber threats and vulnerabilities on a regular basis. b. Monitor technological innovations on ICT systems and platforms employed in strategic domains and Critical Infrastructures in order to anticipate potential vulnerabilities. c. Share relevant analysis with Operators of Essential Services and Critical Infrastructures through dedicated institutional platforms. d. Cooperate with universities and research centers in order to develop new methodologies and technologies aimed at detecting/analyzing vulnerabilities and threats.
1.2	Cyber intelligence and cyber knowledge management	a. Improve collection, analysis, and dissemination capabilities on cyber threats. b. Improve threat detection through the development of traffic monitoring and analysis capabilities. c. Implement early warning procedures. d. Develop integrated intelligence capabilities (inter-organization and multi-sources).

1.3	Countering cyber threats	a. Improve attribution capabilities. b. Develop a consistent cyber situational awareness, through accurate assessments of cyber activities, in order to improve situational knowledge, threat prevention, and countermeasures. c. Facilitate information sharing between public authorities and private sector. d. Improve incident and cybercrime integrated response capabilities, according to preset protocols, and stimulate new legislative initiatives in order to create technical intervention teams to promptly support central Administrations, Operators of Essential Services and Critical Infrastructures in case of relevant cyber events (see also AI 5.1c).
1.4	Cyberspace defense operational capabilities	a. Strengthen cyberspace defense structures and secure long term efficiency and effectiveness of their assets. b. Establish Command and Control structures capable of effective cyberspace military operations planning and implementation.
1.5	Cyber incident management: lessons learned	a. Create relevant procedures and tools for processing lessons learned and managing cyber incidents (collection, analysis/evaluation, and sharing) on a need-to-know/need-to-share basis among public and private organizations.

ACTION ITEM 2

STRENGTHENING PUBLIC-PRIVATE COOPERATION

Cooperation among public stakeholders, as well as cooperation among public and private stakeholders, should be strengthened taking into account that Critical Infrastructures are managed and operated by private organizations. That is why interoperability among actors should be fortified at national and international level.

2.1 Integration	a. Facilitate operability of public-private existing cooperation schemes to detect threats, mitigate vulnerabilities, and coordinate response to cyber attacks. b. Support activities implemented by institutional fora, technical groups and competent bodies involving Critical Infrastructures and Operators of Essential Services' as well as others ICT strategic players.

2.2	Public-private sector's cooperation tools	a. Process a methodology to identify ICT critical systems. b. Strengthen info-sharing, also by adopting common taxonomy. c. Develop synergies among Critical Infrastructures' competent Authorities, Ministries, private organizations, and partner Nations in order to effectively manage cyber crises. d. Set specific evaluation standards and develop communication formats for infrastructures' vulnerability assessments.
2.3	Involve private players in national and international cybersecurity events	a. Consolidate existing public-private communication following a whole-of-society approach. b. Facilitate private operators' involvement in international exercises on Critical Infrastructures' protection.

ACTION ITEM 3

FOSTERING IT SECURITY CULTURE. EDUCATION AND TRAINING

Until now cybersecurity education and training have been directed only to experts and cyber operators. There is now a need to promote the culture of cyber security among citizens, businesses and public administrations.

3.1	Doctrine development	a. Keep up with the latest international strategic posture. Develop cybersecurity doctrines based on best practices.
3.2	Cybersecurity awareness	a. Organize awareness initiatives for citizens, students, companies, and Public Administrations.
3.3	Education, training, and exercises	a. Participate in EU, NATO, and other international organizations' cybersecurity initiatives. b. Raise awareness among decision makers on cybersecurity threats' latest developments. c. Organize training exercises for cybersecurity operators and managers as well as IT systems and networks officers.

d. Develop, test, and validate cyberspace operational activities through simulation tools, joint exercises and trainings on-the-job.
e. Concentrate cyber training capacities in education excellence hubs, consolidating existing centers and facilitating direct involvement of private organizations (from Italy and abroad), EU and NATO members, and other partner Nations.
f. Develop partnerships with universities and research centers to set up trainings and specific courses for Public Administration and private companies' personnel.
g. Map national cybersecurity excellence centers.

ACTION ITEM 4

INTERNATIONAL COOPERATION AND CYBER EXERCISES

Cyber threats are transnational by definition. A common level of competence and interoperability is needed in order to counter them.

4.1	Enhancing bilateral and multilateral cooperation	a. Consolidate relations with EU and NATO members, and other partner nations. b. Maximize integration and interoperability of cybersecurity operations' planning and implementation through joint activities at Defense, inter-Ministry, NATO, EU, and multinational level. c. Participate in international fora to monitor latest evolutions and to keep up at national level.
4.2	Cyber exercises	a. Organize recurring national cyber exercises (eg. Cyber Italy), involving Critical Infrastructures and Operators of Essential Services as well as others ICT strategic players.

		b. Coordinate public and private national players participating in exercises both at multilateral (EU and NATO) and bilateral level (eg. with the United States of America).
4.3	EU projects and other international organizations' initiatives	a. Promote and ease access to EU funding initiatives among public and private operators. b. Maximize access to EU funding. c. Participate in EU funded projects. d. Participate in NATO and other international organizations projects.

ACTION ITEM 5

INCIDENT PREVENTION, RESPONSE AND REMEDIATION

Computer Security Incident Response Team (CSIRT) —as defined by the NIS Directive— is responsible for actively support public and private operators in case of cyber attacks and disturbances. In the process of transposing the Directive, current public Computer Emergency Response Teams (National CERT and PA-CERT) will merge their tools and procedures in a coordinated cyber-incident management effort.

5.1 Integrated capacity	a. Create a single point of contact and one or more CSIRT with full incident response capabilities (according to NIS Directive). b. Establish one or more NIS National Authorities. c. Fully implement legal framework for CSIRT/CERT, SOC, and technical intervention teams (see also AI 1.3d). d. Align capacities of current national cybersecurity actors (N-CERT, PA-CERT, DoD-CERT, National Anti-Crime Computer Centre for the Protection of Critical Infrastructure, Intelligence) with NIS requirements. Identify cooperation mechanisms among them. e. Develop automated and standardized cyber incident management model —with a specific focus on triage phases.

		f. Minimize the impact of IT cyber incidents —in particular of those events that produced information loss and/or IT system disruption. g. Develop a proactive approach to IT security and create integrated detection databases for incident & response and intrusion. h. Develop a resilient approach to assure business continuity and disaster recovery.
5.2	CERTs development	a. Develop CERTs functions according to the NIS Directive transposition decree. b. Increase CERTs' efficacy and, in particular, of the National one towards corporate entities, including SMEs, and Public Administration CERT towards Public Administration. c. Find efficient approaches to support Local Public Administrations. d. Support EU and international cooperation among CERTs by actively taking part to the CSIRTs Network —NIS Directive— and other EU and international technological projects (see AI 4.3).
5.3	Procurement	a. Define Public Administrations' purchasing mechanisms in order to guarantee cybersecurity. b. Identify procurement regulations and procedures for a cyber secure Public Administration supply chain.

ACTION ITEM 6

UPDATING CYBERSECURITY LEGISLATION AND MANAGING COMPLIANCE AT INTERNATIONAL LEVEL

Uninterrupted growth and persistent progress of ICT solutions require continuous updates and high-paced legislation improvements in order to maximize national cybersecurity.

6.1	Legislation update	a. Share Public Administrations' best practices and coordinate their legal cybersecurity capabilities. b. Assess current legislation on cybersecurity, follow-up on latest technological developments and evaluate legislation updates taking account of international best practice. c. Finalize critical infrastructures' national legislation bearing in mind sectors covered by the NIS Directive. d. Harmonize national obligations for public and private operators and simplify incident notification processes in order to maximize effectiveness of cybersecurity policies. e. Promote initiatives at EU level to harmonize legal obligations and to simplify processes as mentioned in AI 6.1d.
6.2	National legal framework	a. Update legal framework on cybersecurity, including activities related to cyber operations, in compliance with the EU legislation and the international law. b. Introduce legal provisions for the deployment of tools aimed at detecting and tackling cyber threats.

6.3	Attribution and sanctions	a. Create a legal framework and methodology for the attribution of security violations (and related sanctions) by network managers and users.
6.4	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of networks and information systems across the Union	a. Promote dialogue with private operators in order to facilitate the NIS Directive transposition process. b. Assess impact of the NIS Directive over the National Cybersecurity Architecture in order to align national regulations. c. Transpose the NIS Directive and define implementation provisions to unify new requirements with those concerning Critical Infrastructures.

ACTION ITEM 7

SECURITY PROTOCOLS AND STANDARDS COMPLIANCE

High levels of network and information systems' security require compliance with national and international standards and protocols

7.1	Standardization and compliance	a. Update the national framework to international ratified standards and best practices. b. Identify and update basic security measures for Public Administration and Critical Infrastructures network and information systems. c. Adopt standards, best practices, and minimum requirements in order to enhance security of networks and information systems (including AI 7.1a and 7.1b). d. Establish a validation and an audit system for organizations responsible for issuing digital and IT security certificates.
7.2	Reference documents	a. Publish guidelines, standards, best practices and taxonomies in order to facilitate information sharing.
7.3	Updating cybersecurity management programs	a. Carry out regular updates and reviews of cybersecurity frameworks (such as rules and procedures).

7.4	ICT security certification	a. Manage the National Framework for ICT Certification of un-classified products and services through the Computer Security Certification Organization (Organismo di Certificazione Informatica OCSI). b. Keep the national scheme for certification of information systems' processes up to date. c. Enhance operational capability of the Evaluation Center (Centro Valutazione CE.VA), lab for technical assessment of ICT products and systems dealing with classified data. d. Take part to the activities carried out by international organizations managing mutual recognition of certification standards. e. Increase evaluation competences of DIS-UCSe (Security Intelligence Department-Central Office for Secrecy) when issuing security certificates and homologations for ICT systems managing classified data, including assessment procedures for classified and unclassified information.
7.5	Cyber defense measures for Essential Service Providers and Critical Infrastructures	a. Test protection systems on a regular basis through technical and procedural checks. b. Establish an independent control system (eg. external audit).

ACTION ITEM 8

SUPPORTING INDUSTRIAL AND TECHNOLOGICAL DEVELOPMENT

Security of hardware and software components, especially those adopted by Critical Infrastructures and national strategic operators, depends on security measures implemented on the entire value chain.

8.1	Production, Innovation and Technological Cooperation	a. Stimulate the creation of a secure and resilient supply chain for ICT components, supported by a flexible and efficient evaluation, validation and certification process. b. Promote ICT innovation, also through a potential stimulus package, in order to develop a competitive industrial base at national and international level and facilitate the creation of a vertical supply chain based on security-by-design. c. Enhance bilateral and multilateral cooperation programs in order to improve national Research & Development at both EU and international level.
8.2	National laboratory for comparative analysis	a. Facilitate the creation of a governmental laboratory for comparative analysis of ICT systems to be adopted by Public Administrations and Critical Infrastructures.

ACTION ITEM 9

STRATEGIC COMMUNICATION

Communication of an occurred cyber-event and about its consequences has a strategic value. Public and private stakeholder –when public awareness is needed– have to share precise, correct, and transparent information without generating unnecessary alarms nor increasing economic and social impacts.

9.1	Strategic and operational communication	a. Develop coordination capacity on situational awareness in order to increase communication efficiency, to facilitate response and remediation activities, to assess when dissemination to the public is needed, and to identify appropriate communication channels.

ACTION ITEM 10

RESOURCES

Analysis of costs related to cyber events is a useful baseline for financial planning and allocation of resources, since risk relevance is proportional to event probability and impact. Adequate costs' evaluation can also support intervention activities over specific vulnerabilities and redirect investments within both the public and the private sector.

10.1	Financial planning	a. Identify priorities and budget related to Critical Infrastructures' cybersecurity and cyberdefense as well as costs related to development of fundamental capacity both in terms of physical resources and human capital.
10.2	Evaluation of cyber-events relevant costs	a. Identify relevant metrics for the evaluation of cyber-events' economic impact (detection, remediation, reputational damage, loss of clients and competitiveness, etc.). b. Analyze Critical Infrastructures' interdependencies in order to improve the evaluation of cyber-events' economic impact in case of a "domino effect". c. Map incidents and potential scenarios from an economic point of view.
10.3	Promoting efficient spending	a. Implement efficient cyberdefence spending measures at national (public, public-private) and international (through cooperation programs) level.
10.4	Human capital	a. Facilitate inter-institutional coordinated recruitment activities of specialized resources also by following international best practices.

ACTION ITEM 11

IMPLEMENTING NATIONAL CYBER RISK MANAGEMENT

Protection of data authenticity, integrity, confidentiality, availability —main target of cyber attacks— is a key task of the Plan.

11	Methodology	a. Adopt risk evaluation measures at national level. b. Identify a unique and agreed cyber-risk management methodology for essential services, Critical Infrastructures and other national strategic actors. c. Engage research sector and Academia in developing performing risk management tools.