This 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.
The Action Plan builds on the experience gained in 2014-2015 under the previous Italian Cybersecurity Action Plan (2013) and its review.

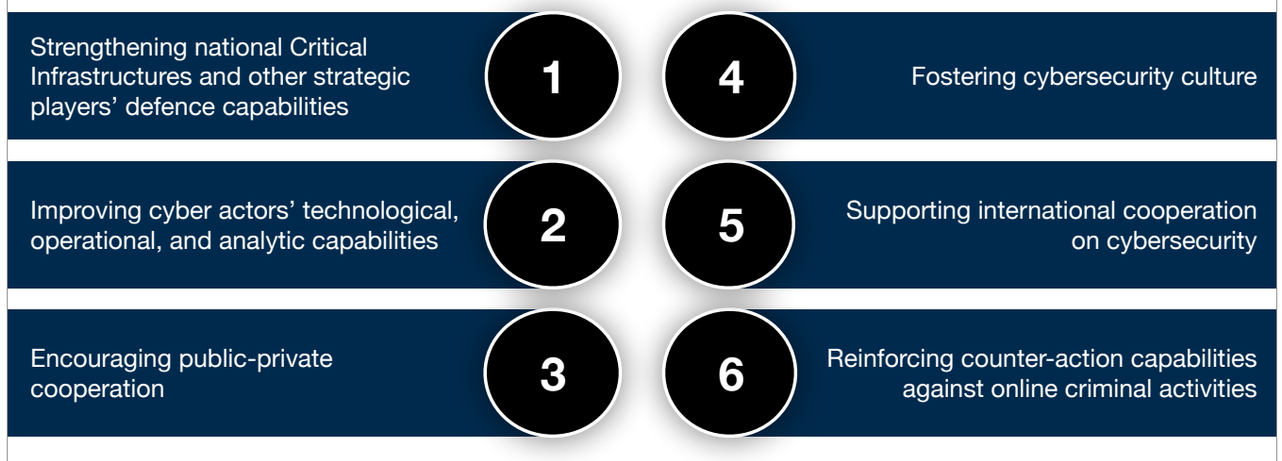
The review - jointly conducted by the Administrations that are part of the National cybersecurity framework - benefited from both the lessons learned from the first steps undertaken to build a national cybersecurity system and the experiences and choices adopted by relevant partners and Allies.

The outcome allowed to identify the changes needed to overcome some difficulties and to envisage a system for public and private stakeholders to contribute to the implementation of the new Action Plan.


Introduction
National Strategic Framework for Cyberspace Security - Strategic guidelines
Italian Action Plan - Action items
Core Tasks

Introduction

National Strategic Framework for Cyberspace Security - Strategic guidelines



The Action Plan is intended to outline the actions required to meet the guidelines set by the NSF for Cyberspace Security.

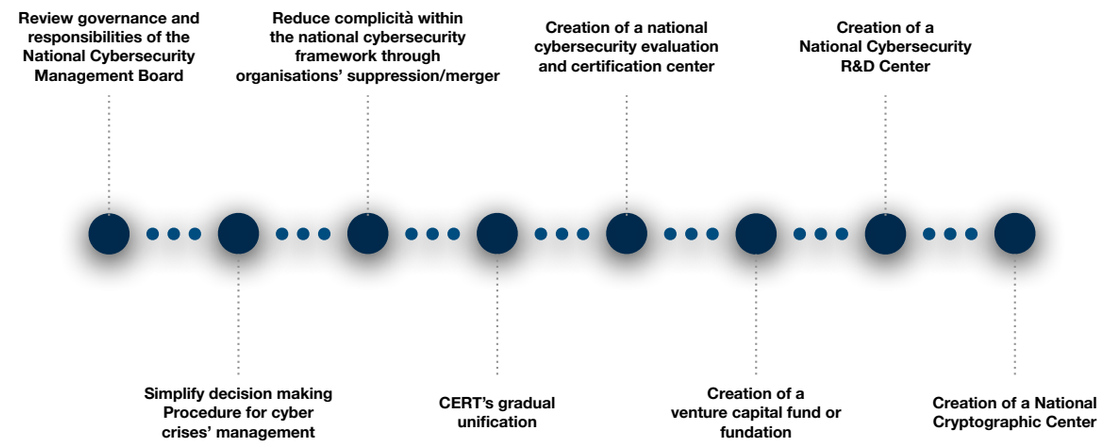
Introduction

Italian Action Plan - Action items

The plan outlines 11 action items, together with their associated objectives and implementing lines of effort.
The plan provides priority measures for the correct deployment of the NSF 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, Defence, Justice, Economy and Finance, Economic Development) as well as cyber delegates from the National Cybersecurity Management Board.
The review focused in particular on the following:

- AI 5 which includes provisions to strengthen the existing CERTs, to creare 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 cosec framework's stakeholders (CERT, CSIRT, intelligence, law enforcement, defence, …)
- AI 1 which, once updated according to the experience gained during the 2014-2015, aims at boosting national cysec response capability.

Introduction
Core Tasks

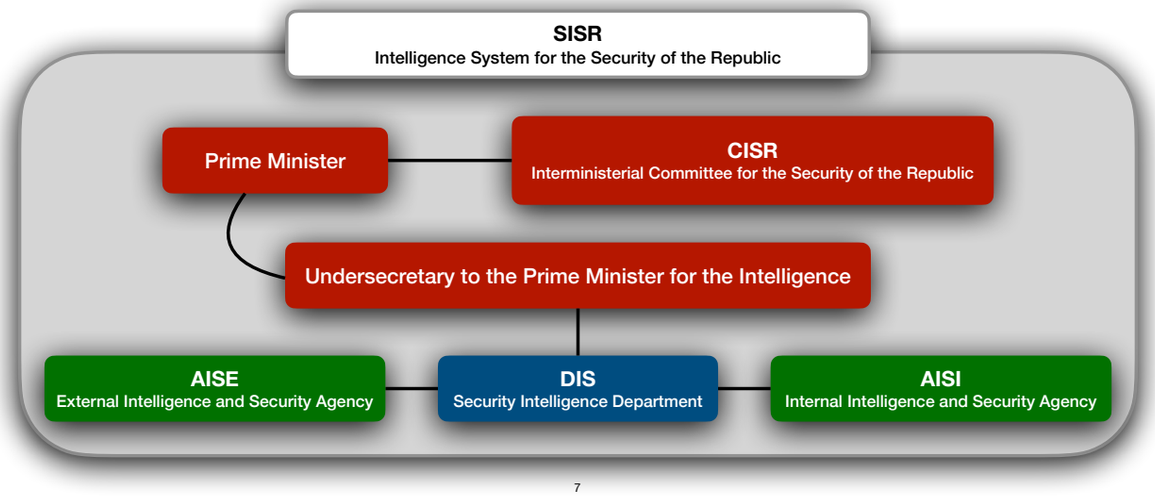


In order to ease a quick improvement of the national cosec framework, a series of core tasks to be pursued with priority was identified.
Tasks were chosen according with the review of the previous strategy and taking into account developments occurred both at national and international level.

To better understand the action plan, I will briefly explain which are the main actors and what roles they have

Intelligence System for the Security of the Republic

Organization



Italy's Intelligence System for the Security of the Republic is the collective name given to the authorities and organizations responsible for intelligence policies, coordination and operations. The Security Intelligence System includes:
Prime Minister
Undersecretary to the Prime Minister for the Intelligence (if appointed)
CISR – Interministerial Committee for the Security of the Republic
DIS – Security Intelligence Department
AISE – External Intelligence and Security Agency
AISI – Internal Intelligence and Security Agency

The overall political responsibility for intelligence is vested in the President of the Council of Ministers.
The President of the Council of Ministers has exclusive power:
to apply and confirm the invocation of State-secret status and protect State secrets
to appoint and dismiss the Director General of the DIS, the Directors of the AISE and the AISI
to determine the annual amount of financial resources to be allocated to DIS, AISE and AISI
The President of the Council of Ministers shall also:
authorize AISE and AISI agents, under specific circumstances, to carry out operations in violation of the law

The President of the Council of Ministers may delegate the duties which are not vested exclusively in him to a Delegated Authority (Undersecretary of State or a Minister without portfolio).

The CISR is an Interministerial Committee in charge of defining the goals of intelligence policies.
In particular, the CISR:
sets intelligence requirements
allocates the financial resources of DIS, AISE and AISI, and approves their budgets and final accounts
The CISR is chaired by the President of the Council of Minister and includes:
Delegated Authority
Minister of Foreign Affairs
Minister of the Interior
Minister of Defense
Minister of Justice
Minister of Economy and Finance
Minister for Economic Development

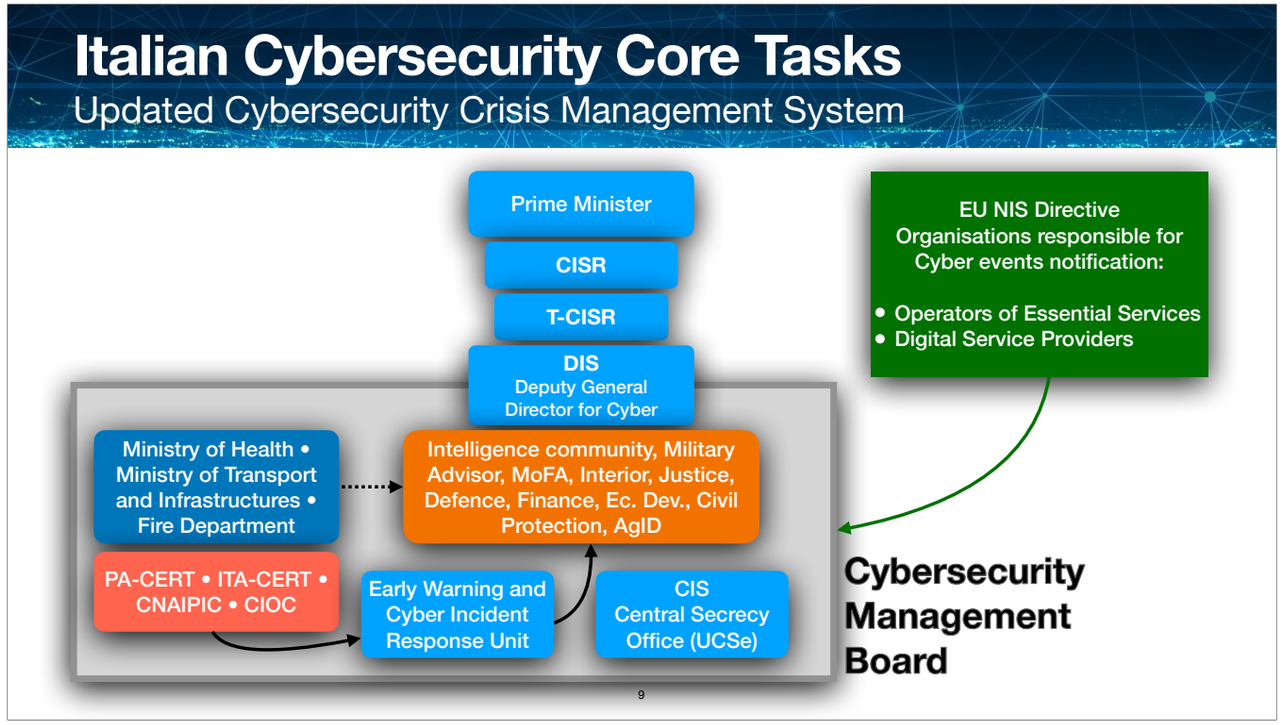
The Director General of the DIS acts as the Committee's secretary.

The President of the Council of Ministers and the Delegated Authority exercise their functions through the DIS.
In order to ensure a fully unified approach to intelligence operations, the DIS:
coordinates all intelligence activities, including national cybersecurity, and review results
submits relevant information collected by the Agencies to the President of the Council of Ministers and provide strategic analysis and assessments to policy-makers
ensures the exchange of information between AISE/AISI and police forces
Moreover, the DIS:
oversees, through the Central Inspection Office, the activities carried out by AISE and AISI
ensures the application of the directives issued by the President of the Council of Ministers regarding the administrative protection of State secrets and classified documents
sees to the management of the personnel and logistics for DIS, AISE and AISI
sees to institutional communication and the promotion of the culture of security

The AISE [External Intelligence and Security Agency] is responsible for safeguarding national security against threats originating abroad, protecting Italy's political, military, economic, scientific and industrial interests.
In particular, the AISE:
counters espionage and other hostile activities abroad
counters WMD (Weapon of Mass Destruction) proliferation

The AISI[Internal Intelligence and Security Agency] is responsible for safeguarding national security from threats originating within Italy's borders, and for protecting Italy's political, military, economic, scientific and industrial interests.
The AISI:
counters espionage and other hostile activities within national borders
counters subversion, criminal and terrorist activity in Italy


Italian Cybersecurity Core Tasks
Updated Cybersecurity Crisis Management System
National Cyber Security Framework



The action plan details the initiatives needed to achieve a step change in increasing national information system and network security levels.
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 an approach to national cybersecurity that provides for the implementation of minimum security requirements for Country-critical systems.
The core tasks were selected for their systemic relevance due to the fact that they:

- Leverage the competences and responsibilities of all relevant stakeholders
- Refer to the most relevant activities aimed at consolidating the national cyber defence system including: assets' common protection; SW/HW certification, identification of critical functions, info-sharing requirements in case of relevant cyber events, ecc.

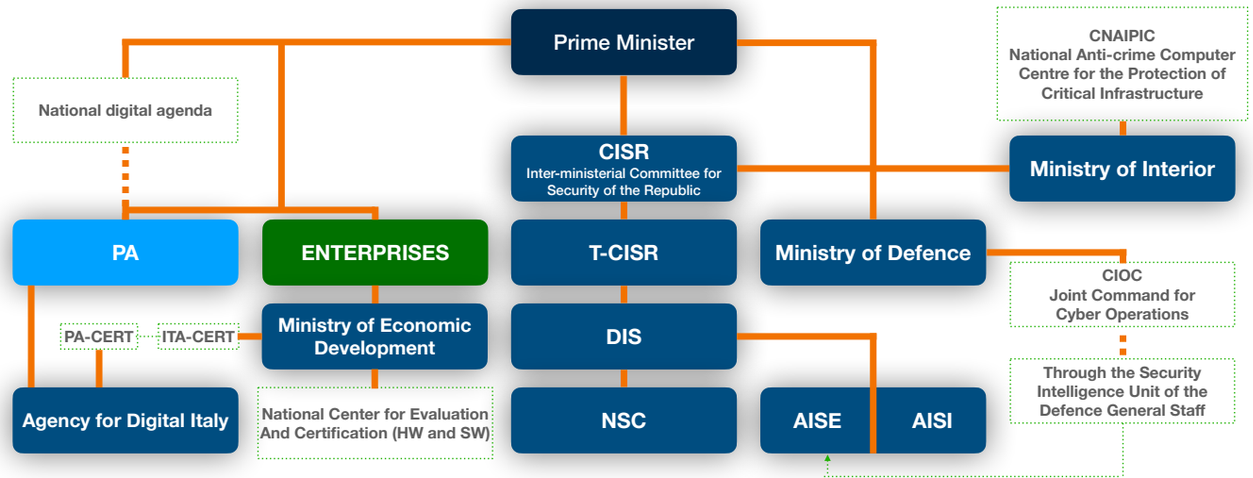
Of particular relevance are the measures intended to:

- Assign to the Director General of the Security Intelligence Department a central role among the entities composing the National cysec ecosystem.
- Relocate the National Cybersecurity Management Board within the Security Intelligence Department. The board is responsible for cysec crises' management and is supervised by a Security Intelligence Department Deputy Director.
- Promote close interaction between the National CERT and the PA CERT in order to facilitate their operational coordination.
- 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.
- 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 penalties.

The new board, at the center of the framework, aims at facilitating governance simplification by cutting decision-making processes short and rationalising both ordinary and emergency procedures.

Italian Cybersecurity Core Tasks

National Cyber Security Framework



The Ministry of Interior (CNAIPIC) plays a key role in protecting IT Critical Infrastructures thanks to its investigative and forensic capabilities.
The Agency for Digital Italy is in charge of defining IT security guidelines and technical rules, setting standards, monitoring quality of public networks' security and PA's ICT programs.
The MoD developed specific cyber capabilities - to protect its network at both national and international level - which are also a significant asset for the board's improvement process.
Intelligence and MoD agreed on a specific protocol to align their strategies and tactics on cysec to facilitate the consolidation of the perspective Joint Command for Cyber Operations in compliance with NATO posture.
The Action Plan aims to secure national assets according to:

- Level 1: National security (Intelligence, MoD, MoI, MoFA, MoJ, MoEF, MoED)
- Level 2: National Critical Infrastructures (TLC, financial sector, transports) and other relevant PA (es. MoH)
- Level 3: National production system and population

2, 5, 6, 7

For the sake of time, I will only show 4 of the action items

Action item 1

Reinforcing intelligence, law enforcement, and defence capabilities

Threat and vulnerability analysis	Assess/Evaluate cyber threats and vulnerabilities
	Monitor technological innovations to anticipate potential vulnerabilities
	Share relevant analysis with OES and Critical Infrastructures
	Cooperate with universities and research centres
Cyber intelligence and cyber knowledge management	Improve capabilities on cyber threats
	Improve threat detection
	Implement early warning procedures
	Develop integrated intelligence capabilities

Countering cyber threats	Improve attribution capabilities
	Develop a consistent cyber situational awareness
	Facilitate info-sharing between public authorities and private sectors
	Improve incident and cybercrime integrated response capabilities
Cyberspace defines operational capabilities	Strengthen cyberspace defence structures
	Establish structures capable of cyberspace military operations planning/implementation
Cyber incident management	Create relevant tools for managing cyber incidents

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.
Assess and evaluate cyber threats and vulnerabilities on a regular basis.
Monitor tech innovations on ICT systems and platforms employed in strategic domains and Critical Infrastructures to anticipate potential vulnerabilities.
Share relevant analysis with OES and Critical Infrastructures through dedicated institutional platforms.
Cooperate with universities and research centres to develop new ways aimed at detecting vulnerabilities and threats.

2.
Improve collection, analysis, and dissemination capabilities on cyber threats.
Improve threat detection through the development of traffic monitoring and analysis capabilities.
Implement early warning procedures.
Develop integrated intelligence capabilities (interorganization and multi-sources).

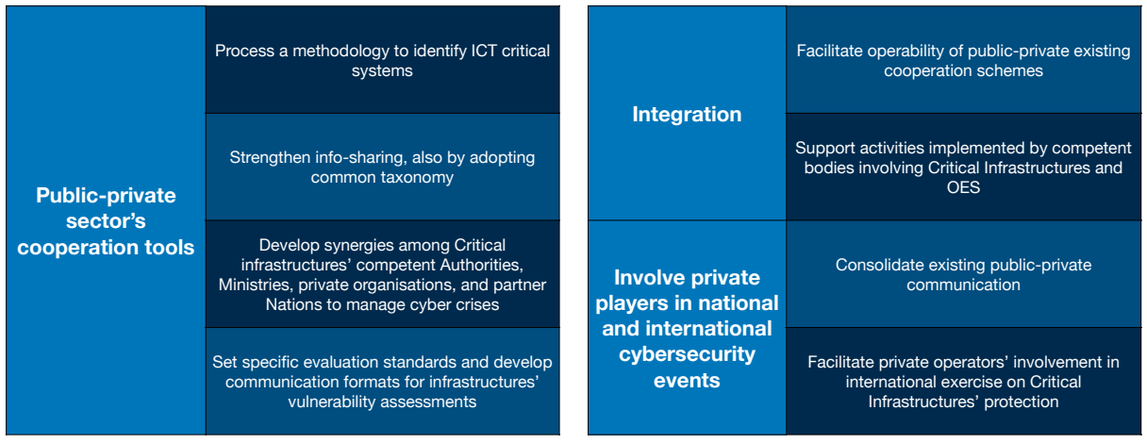
3.
Improve attribution capabilities.
Develop a consistent cyber situational awareness, through accurate assessments of cyber activities, in order to improve situational knowledge, threat prevention, and countermeasures.
Facilitate information sharing between public authorities and private sector.
Improve incident and cybercrime integrated response capabilities, accord- ing 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.

4.
Strengthen cyberspace defence structures and secure long term efficiency and effectiveness of their assets.
Establish Command and Control structures capable of effective cyberspace military operations planning and implementation.

5.
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.

1.
Process a methodology to identify ICT critical systems.
Strengthen info-sharing, also by adopting common taxonomy.
Develop synergies among Critical Infrastructures' competent Authorities, Ministries, private organizations, and partner Nations in order to effectively manage cyber crises.
Set specific evaluation standards and develop communication formats for infrastructures' vulnerability assessments.

2.
Facilitate operability of public-private existing cooperation schemes to detect threats, mitigate vulnerabilities, and coordinate response to cyber attacks.
Support activities implemented by competent bodies involving Critical Infrastructures and Operators of Essential Services' as well as others ICT strategic players.

3.
Consolidate existing public-private communication following a whole-of-society approach.
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.

1.
Participate in EU, NATO, and other international organizations' cybersecurity initiatives.
Raise awareness among decision makers on cybersecurity threats' latest developments.
Organize training exercises for cyber- security operators and managers as well as IT systems and networks officers.
Develop, test, and validate cyberspace operational activities through simulation tools, joint exercises and trainings on-the-job.
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.
Develop partnerships with universities and research centers to set up trainings and specific courses for Public Administration and private companies' personnel.
Map national cybersecurity excellence centers.

2.
Keep up with the latest international strategic posture. Develop cybersecurity doctrines based on best practices.

3.
Organize awareness initiatives for citizens, students, companies, and Public Administrations.

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.

1.
Promote and ease access to EU fund- ing initiatives among public and private operators.
Maximize access to EU funding.
Participate in EU funded projects.
Participate in NATO and other international organizations projects.

2.
Consolidate relations with EU and NATO members, and other partner nations.
Maximize integration and interoperability of cybersecurity operations' planning and implementation through joint activities at Defense, inter-Ministry, NATO, EU, and multinational level.
Participate in international fora to monitor latest evolutions and to keep up at national level.

3.
Organize recurring national cyber exercises (eg. Cyber Italy), involving Critical Infrastructures and Operators of Essential Services as well as others ICT strategic players.
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).

Action item 5

Incident prevention, response and remediation

Integrated capacity	Create a single point of contact and one or more CSIRT
	Establish one or more NIS National Authorities
	Fully implement legal framework for CSIRT/ CERT, SOC, and teams
	Align capacities of current national cybersecurity actors with NIS requirements
	Develop automated and standardised cyber incident management model
	Minimize the impact of IT cyber incidents
	Develop a proactive approach to IT security
	Develop a resilient approach

CERTs development	Develop CERTs functions according to the NIS Directive
	Increase CERTs' efficacy
	Find efficient approaches to support Local PA
	Support EU and international cooperation among CERTs
Procurement	Define PAs' purchasing mechanisms
	Identify procurement regulations and procedures for a cyber secure Public Administration supply chain

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.

1.
Create a single point of contact and one or more CSIRT with full incident response capabilities (according to NIS Directive).
Establish one or more NIS National Authorities.
Fully implement legal framework for CSIRT/CERT, SOC, and technical intervention teams (see also AI 1.3d).
Align capacities of current national cyber- security actors (N-CERT, PA-CERT, DoD- CERT, National Anti-Crime Computer Centre for the Protection of Critical Infra- structure, Intelligence) with NIS requirements. Identify cooperation mechanisms among them.
Develop automated and standardized cyber incident management model —with a specific focus on triage phases.
Minimize the impact of IT cyber incidents —in particular of those events that produced information loss and/or IT system disruption.
Develop a proactive approach to IT security and create integrated detection data- bases for incident & response and intrusion.
Develop a resilient approach to assure business continuity and disaster recovery.

2.
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.
Find efficient approaches to support Local Public Administrations.
Support EU and international cooperation among CERTs by actively taking part to the CSIRTs Network —NIS Directive— and other EU and international technological projects.

3.
Define Public Administrations' purchasing mechanisms in order to guarantee cybersecurity.
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

Legislation update	Share PAs' best practices and coordinate their legal cybersecurity capabilities
	Assess current legislation on cybersecurity
	Finalize critical infrastructures' national legislation bearing in mind sectors covered by the NIS Directive
	Harmonize national obligations for public and private operators
	Promote initiatives at EU level to harmonize legal obligations and to simplify processes
Attribution and sanctions	Create a legal framework for the attribution of security violations by network managers and users

National legal framework	Update legal framework on cybersecurity
	Introduce legal provisions for the deployment of tools aimed at detecting cyber threats
Directive concerning measures for s high common level of security of networks and information systems across the Union (2016/1148)	Promote dialogue with private operators facilitate the NIS Directive transposition process
	Assess impact of the NIS Directive over the National Cybersecurity Architecture to align national regulations
	Transpose the NIS Directive and unify new requirements with those concerning Critical Infrastructures

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

1.
Share Public Administrations' best practices and coordinate their legal cybersecurity capabilities.
Assess current legislation on cyber- security, follow-up on latest techno- logical developments and evaluate legislation updates taking account of international best practice.
Finalize critical infrastructures' nation- al legislation bearing in mind sectors covered by the NIS Directive.
Harmonize national obligations for public and private operators and simplify incident notification processes in order to maximize effectiveness of cybersecurity policies.
Promote initiatives at EU level to harmonize legal obligations and to simplify processes.

2.
Create a legal framework and methodology for the attribution of security violations (and related sanctions) by network managers and users.

3.
Update legal framework on cybersecurity, including activities related to cyber operations, in compliance with the EU legislation and the international law.
Introduce legal provisions for the deployment of tools aimed at detecting and tackling cyber threats.

4.
Promote dialogue with private operators in order to facilitate the NIS Directive transposition process.
Assess impact of the NIS Directive over the National Cybersecurity Architecture in order to align national regulations.
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

ICT security certification	Manage the National Framework for ICT Certification of un-classified products/services through the CSCO
	Keep the national scheme for certification of information systems' processes up to date
	Enhance operational capability of the Evaluation Center
	Take part to the activities carried out by international organisations
	Increase evaluation competences of DIS-UCSe
Cyber defence measures for Essential Service Providers and Critical Infrastructures	Test protection systems on a regular basis
	Establish an independent control system

Standardization and compliance	Update the national framework to international standards
	Identify and update basic security measures for PA and Critical Infrastructures network and information systems
	Adopt standards, best practices, and minimum requirements to enhance security of networks and information systems
	Establish a validation and an audit system for organizations responsible for issuing digital and IT security certificates
Reference documents	Assess impact of the NIS Directive over the National Cybersecurity Architecture to align national regulations
Updating cybersecurity management programs	Transpose the NIS Directive and unify new requirements with those concerning Critical Infrastructures

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

1.
Manage the National Framework for ICT Certification of un-classified products and services through the Computer Security Certification Organization (Organismo di Certificazione Informatica OCSI).
Keep the national scheme for certification of information systems' processes up to date.
Enhance operational capability of the Evaluation Center (Centro Valutazione CE.VA), lab for technical assessment of ICT products and systems dealing with classified data.
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 un-classified information.

2.
Test protection systems on a regular basis through technical and procedural checks.
Establish an independent control system (eg. external audit).

3.
Update the national framework to international ratified standards and best practices.
Identify and update basic security measures for Public Administration and Critical Infrastructures network and information systems.
Adopt standards, best practices, and minimum requirements in order to enhance security of networks and information systems.
Establish a validation and an audit system for organizations responsible for issuing digital and IT security certificates.

4.
Publish guidelines, standards, best practices and taxonomies in order to facilitate information sharing.

5.
Carry out regular updates and reviews of cybersecurity frameworks (such as rules and procedures).

Action item 8

Supporting Industrial and Technological Development

Production, Innovation and Technological Cooperation	Stimulate the creation of a secure and resilient supply chain for ICT components
	Promote ICT innovation 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
	Enhance bilateral and multilateral cooperation programs to improve national R&D at both EU and international level
National laboratory for comparative analysis	Facilitate the creation of a government laboratory for comparative analysis of ICT systems to be adopted by PAs and Critical Infrastructures

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.

1.
Stimulate the creation of a secure and resilient supply chain for ICT components, supported by a flexible and efficient evaluation, validation and certification process.
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.
Enhance bilateral and multilateral cooperation programs in order to improve national Research & Development at both EU and international level.

2.
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

Strategic and operational communication

Develop coordination capacity on situational awareness to increase communication efficiency, to facilitate response and remediation activities and to identify appropriate communication channels

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.

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

Evaluation of cyber-events relevant costs	Identify relevant metrics for the evaluation of cyber-events' economic impact	**Financial planning**	Identify priorities and budget related to Critical Infrastructures' cybersecurity and cyberdefense
	Analyze Critical Infrastructures' interdependencies to improve the evaluation of cyber-events' economic impact in case of a "domino effect"	**Promoting efficient spending**	Implement efficient cyberdefence spending measures at national and international level
	Map incidents and potential scenarios from an economic point of view	**Human capital**	Facilitate inter-institutional coordinated recruitment activities of speicialized 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.

1.
Identify relevant metrics for the evaluation of cyber-events' economic impact (detection, remediation, reputational damage, loss of clients and competitiveness, etc.).
Analyze Critical Infrastructures' interdependencies in order to improve the evaluation of cyber-events' economic impact in case of a "domino effect".
Map incidents and potential scenarios from an economic point of view.

2.
Identify priorities and budget related to Critical Infrastructures' cybersecurity and cyberdefence as well as costs related to development of fundamental capacity both in terms of physical resources and human capital.

3.
Implement efficient cyberdefence spending measures at national (public, public-private) and international (through cooperation programs) level.

4.
Facilitate inter-institutional coordinated recruitment activities of specialized resources also by following international best practices.

Action item 11

Implementing National Cyber Risk Management

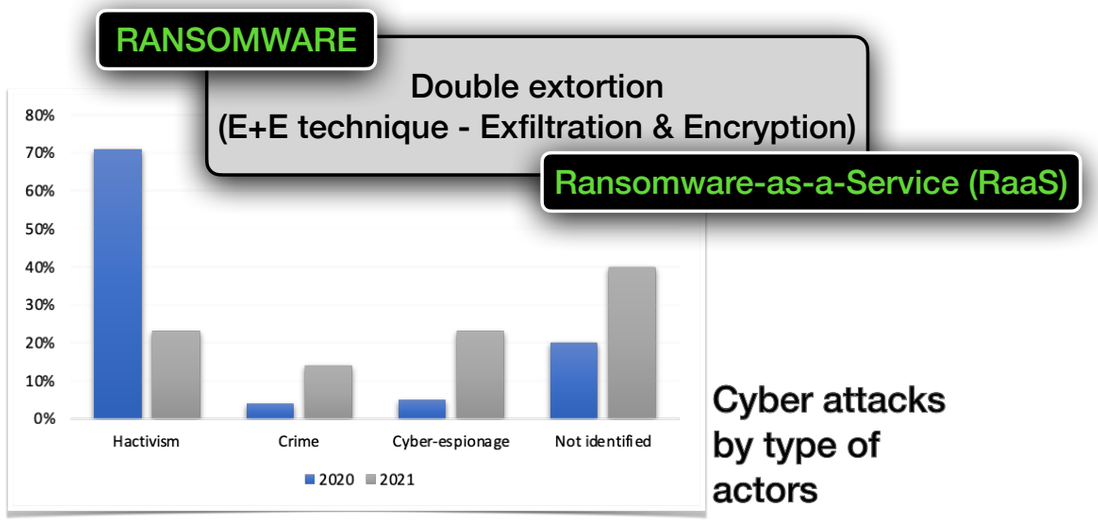
Protection of data authenticity, integrity, confidentiality, availability —main target of cyber attacks— is a key task of the Plan.

1.
Adopt risk evaluation measures at national level.
Identify a unique and agreed cyber-risk management methodology for essential services, Critical Infrastructures and other national strategic actors.
Engage research sector and Academia in developing performing risk management tools.

It is very interesting to understand the state and trend of the current cyber threat, considering the implementation of the action plan.
The data I will show are extrapolated - as indicated in the slide - from the current year report, which Italian intelligence provides to parliament every year.

The Cyber Threat

Status and trend of the Cyber Threat (Part 1)

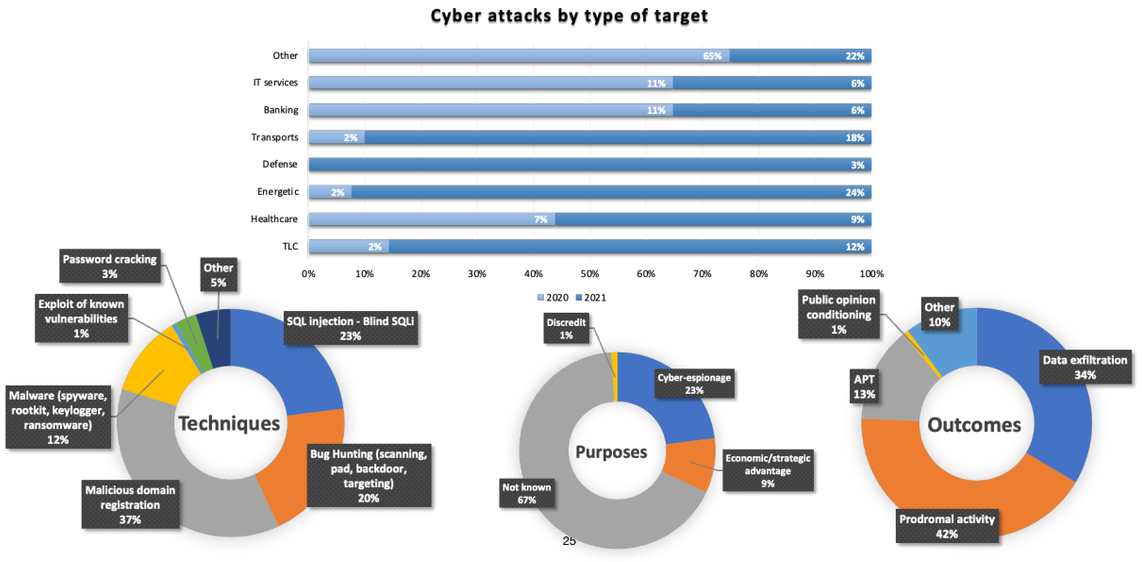


Cyber attacks by type of actors

The info-operational activity conducted by intelligence has made it possible to detect a significant growth in cyber actions of criminal origin (14% of attacks).
The prevailing attack model appears to have consolidated in the new configuration: the "Ransomware-as-a-Service (RaaS)", based on the interaction between two subjects; on the one hand, the developers of the digital weapon and, on the other hand, third parties who, after carrying out attacks on the target interest, transfer to the former a part of the illicit proceeds eventually obtained.
If previously the ransomware attack was solely attributable to the encryption of the data and therefore to the consequent unavailability of the same indefinitely, over the last year the dynamics concerning the disclosure of the data also on the dark web.
The info-operational monitoring then made it possible to detect the use by state actors (23%) of ransomware-type digital weapons, which were used, in this case, for purposes other than extortion, in order to block production activities or hide traces of previous espionage activities.
The same actors also resorted to cyber-criminal groups.
Cyber activism (23%) has suffered a substantial reduction in attacks on health structures and organizations, while most of the malicious actions have concerned the institutional portals of local authorities.
The actions of unidentifiable origin (40%) refer to actors of various kinds who make use of offensive tools freely available or distributed on parallel digital markets.

The Cyber Threat

Status and trend of the Cyber Threat (Part 2)



In 2021, hostile cyber activities carried out against IT assets relevant to national security continued to affect mainly the public infrastructures of the PA (69%, down by 14 percentage points compared to 2020).
The actions mainly concerned Central State Administrations (56%, an increase of 18 percentage points compared to 2020) and IT infrastructures of local authorities and healthcare facilities.
Attacks on private individuals mainly affected the energy (24%), transports (18%, increased by 16 percentage points) and telecommunications (12%, up by 10 percentage points) sectors.

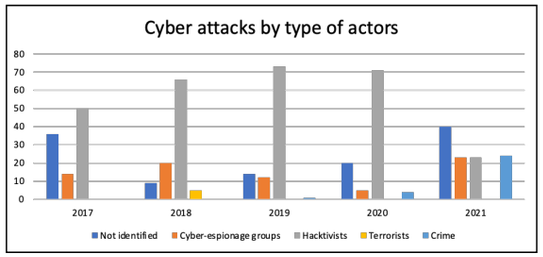
As for the types of attack:
37% concerns the registration of domains with names and characteristics similar to those of institutional and government sites to hijack unsuspecting users on malicious sites.
The search for technical vulnerabilities exposed by the selected targets has been increased to 20%, preparatory to attempts to breach networks, such as SQLi (23%).

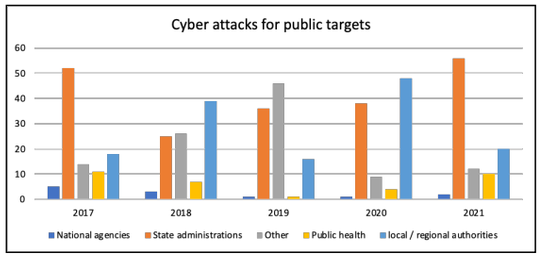
Outcomes of hostile actions:
prevalence of prodromal actions to potential subsequent attacks (42%) and those aimed at stealing information from compromised assets (34%).

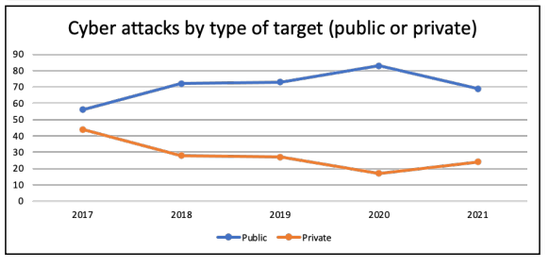
Purpose:
67% could not postpone a clear purpose, while 23% refer to spying campaigns conducted by structured groups and financially supported government apparatuses.

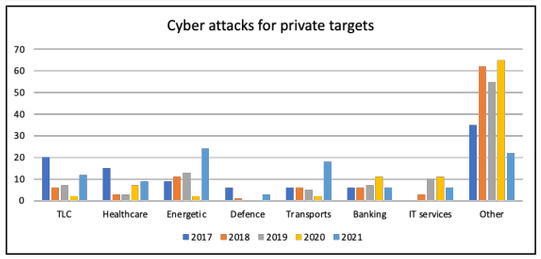
The Cyber Threat

Differences from 2017 to today









Even with the adoption of the national action plan and the definition of other laws or regulations related to cybersecurity, looking at these graphs and analyzing the reports of each year, relevant trends emerge.
Negative data is on the rise: number of compromises, vulnerabilities, new malware and the average cost of a recovery. Solutions are available everywhere, but to be effective they require competent personnel and appropriate contextualizations.
- Most attacks do not require special skills: computerized social engineering techniques to extract confidential information for later use.
- Over 50% of attacks are generated by incorrect behavior by end users.

The main problems are two:
- Despite refresher programs and certifications on the subject, there are still too many people in prestigious decision-making positions who ignore or underestimate the IT risk.
- The average employee is not adequately prepared on time and, his unpreparedness leads to neglect the basic security of his workstation (clear communications, outdated software, etc.).

In the scenario outlined, the ACN acts as a national authority to protect interests in the field of cybersecurity and, among other things, coordinates the public entities involved in the sector at a national level, promoting the implementation of common actions aimed at ensuring cyber security and resilience; prepare the national cybersecurity strategy; develop national capabilities for prevention, monitoring, detection, analysis and response, to prevent and manage IT security incidents and related attacks. In addition, the ACN acts as a competent national authority and single point of contact for the security of networks and information systems (for the purposes referred to in the NIS decree).

The organizational structure includes:

- CSIRT Italy: the technical structure for prevention, coordination and response to IT events and incidents with an actual or potential impact on the national territory.
- The CVCN: the technical structure that, together with a network of accredited laboratories, will be responsible for verifying the security and absence of known vulnerabilities in ICT goods, systems and services, with the aim of raising the level of cybersecurity and, resilience of the infrastructures on which the country's essential functions and services depend.
- The National Coordination Centers are public sector entities, or mostly state-owned, or which perform public administration functions. They have the capacity to support the European Cybersecurity Competence Center (ECCC) and the network in fulfilling their mission.

THANK YOU

for your precious time and attention