



IMPLEMENTATION PLAN

NATIONAL CYBERSECURITY STRATEGY

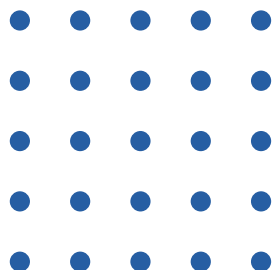
2022 – 2026

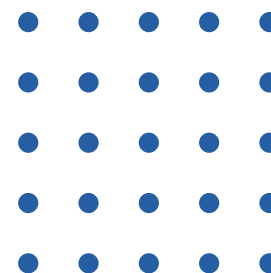




Summary

	Preface	2
01	Implementation plan	3
02	National governance	23
03	Glossary	34
	Acronyms	49





Preface

The effectiveness of a strategy is strictly correlated to the possibility of progressively measuring the results, also to be able to take appropriate corrections and updates during its implementation, whenever needed. That is why the legislator has assigned the Prime Minister the power to adopt specific guidelines for this purpose, after consulting the Interministerial Committee for Cybersecurity (CIC).

To this end, the public entities responsible for carrying out the following implementing measures communicate the outcomes of their actions to ACN by December 31st of each year, which then reports to the CIC the state of implementation of the strategy in consideration of its high surveillance duty upon its realization.

Moreover, the Intelligence Community provides ACN with an information and evaluation picture useful for guiding the further strengthening of the measures, which will ensure the effective implementation of this plan, also reporting on those for which it is responsible according to the procedures defined by Law no. 124/2007.

An update on achieved results is provided to the Parliament and citizens by April 30th of each year through the Prime Minister's Report on the tasks carried out by ACN in the previous year.





#1

Implementation plan

Implementation plan

The following implementation plan – which does not affect the powers attributed to the Administrations by the legislation in force – indicates for each goal defined in the National Cybersecurity Strategy – namely *protection, response, and development* – the measures to be put in place for its achievement, organized into thematic areas. A list of the entities responsible for their implementation, as well as other interested parties – for which reference has been made to the following paragraph on the national governance – is provided for every measure, without considering those who, directly or indirectly, benefit from the resulting effects. The above entities are therefore responsible to carry out all the necessary actions to implement their own measures, using the financial resources available and provided by the legislation in force, included NRRP funds, needed to the scope.

 PROTECTION	Technological screening
<p>Measure #1</p> <p>Strengthen the national technological screening system to support the security of the supply chain of specific categories of assets falling within the Perimeter and for the adoption of European cybersecurity certification schemes, also through the accreditation of public/private test laboratories.</p>	<p> Responsible entities ACN</p> <p> Other interested parties Min. Interior, Min. Defence, Industry</p>
<p>Measure #2</p> <p>Develop the capacities of the Assessment Centres of the Ministry of Interior and the Ministry of Defence accredited by the ACN, as conformity assessment bodies, for their own respective systems.</p>	<p> Responsible entities Min. Interior, Min. Defence</p> <p> Other interested parties ACN</p>
<p>Measure #3</p> <p>Activation of a central inspection team at the Agency to support the inspection activities in relation to the obligations arising from the cyber regulations in force.</p>	<p> Responsible entities ACN</p>

Measure #4

Activation of homologous inspection units at the Ministries of Interior and Defence, to support the inspection activities in relation to the obligations arising from the cyber regulations in force.



Responsible entities

Min. Interior,
Min. Defence



Other interested parties

ACN



Definition and maintenance of an updated and coherent national legal cybersecurity framework

Measure #5

Support the development of cybersecurity certification schemes, assessing their adequacy in terms of national security, and, in collaboration with the private sector, promoting their adoption and use by Italian service providers and companies, favouring the development of the specialized national entrepreneurial fabric to achieve a competitive advantage on the market.



Responsible entities

ACN, MITD



Other interested parties

MiSE,
Trade Associations

Measure #6

Introduce legal rules that enhance the inclusion of cyber security elements in Public Administration's ICT procurement activities, providing indications also to market operators to ensure that the IT goods and services purchased by public entities through tenders or specific framework agreements, respect adequate cybersecurity levels. This, compatibly with the rapid definition of the related award procedures.



Responsible entities

MITD, ACN



Other interested parties

MEF, Min. Justice, MPA,
other NCS Administrations

Measure #7

Promote the creation of a system of public tenders, at national and European level, based on criteria that guarantee quality solutions in terms of cybersecurity.



Responsible entities

MITD, MEF, ACN



Other interested parties

MPA, other
NCS Administrations

Measure #8

Introduce legal rules aimed at protecting the supply chain relating to ICT infrastructures relevant from the point of view of national security.



Responsible entities

PCM, ACN



Other interested parties

NCS Administrations



Measure #9

Define a national policy on coordinated vulnerability disclosure.



Responsible entities

ACN, Min. Interior,
Min. Justice

Measure #10

Publish cybersecurity guidelines for Public Administrations, with different degrees of cogency (with regard, for example, to MFA, registration and storage of logs, etc.), also with reference to the migration to the cloud and favouring a continuous and automated management of cyber risk, according to a "zero trust" approach.



Responsible entities

ACN



Other interested parties

NCS Administrations

Measure #11

Implement awareness-raising initiatives to encourage the application of the "National Framework for Cybersecurity and Data Protection" and "Essential cybersecurity controls", appropriately updated in line with the threat landscape, by the PA, businesses and SMEs.



Responsible entities

ACN



Other interested parties

MITD, Trade Associations



In-depth knowledge of the cyber threat scenario

Measure #12

Continue to increase national defence, resilience, fight against crime, and cyber intelligence capabilities, further strengthening situational awareness through continuous monitoring and analysis of threats, vulnerabilities, and attacks, according to specific areas of expertise.



Responsible entities

ACN, Min. Interior,
Min. Defence,
DIS, AISE, AISI

Measure #13

Create a national cyber risk monitoring service for organizations and the general public, to communicate the current level of the threat, as well as to adequately inform decision-making processes.



Responsible entities

ACN



Other interested parties

NCS Administrations,
Industry, University,
Research



Enhancement of Public Administration's cyber capabilities

Measure #14

Coordinate interventions to enhance the capabilities of identification, monitoring and control of cyber risk in the Public Administration for the safety of citizens' data and services.



Responsible entities

ACN



Other interested parties

MITD, MPA

Measure #15

Provide for the qualification of cloud services for the Public Administration, in implementation of the Italian Cloud Strategy, to ensure adequate levels of security for the services and data of the PA.



Responsible entities

ACN



Other interested parties

MITD

Measure #16

Facilitate the secure migration of Public Administration services and data to the cloud, namely PSN or Public Cloud, in line with the data and service classification activities as per the Italian Cloud Strategy.



Responsible entities

MITD, ACN



Development of protection capacities for national infrastructures

Measure #17

Promote the development of procedures, processes, and systems for monitoring and control of national BGP configurations, in cooperation with national IXP operators.



Responsible entities

ACN



Other interested parties

Industry

Measure #18

Promote the implementation of a national DNS resolution infrastructure at the service of public and private operators, supporting the application of security controls on navigation and protection against malicious activities also conducted through the DNS.



Responsible entities

ACN



Other interested parties

Regions and autonomous Provinces, CNR, Industry

Measure #19

Implementing monitoring services for vulnerabilities and erroneous configurations of digital services exposed on the Internet of interest to the Public Administration, implementing early warning policies.



Responsible entities
ACN

Measure #20

Promote the use of best practices in the management of Public Administration's e-mail domains, implementing a monitoring and protection service against phishing or abuse campaigns.



Responsible entities
ACN, Min. Interior



Other interested parties
Regions and autonomous Provinces

Measure #21

Promote the development and implementation of a national service for managing "cold" backup copies, to offer to Public Administrations and private operators an infrastructure with high levels of resilience to support a prompt reactivation of systems and services after breakdowns or incidents.



Responsible entities
ACN



Other interested parties
MITD, Industry



Promotion of the use of cryptography

Measure #22

Promote the use of cryptography in a non-classified environment, as a default setting and in any case from the design stage of networks, applications, and services, in compliance with the principles of security and protection of privacy, in line with the principles established by national and European legislation.



Responsible entities
ACN



Other interested parties
DIS (UCSe), Min. Justice, Min. Defence, MiSE, MITD, Industry, University, Research

Measure #23

Development of national encryption technologies/systems in the unclassified framework. In support of this initiative, the creation of a national ecosystem for its maintenance and evolution is envisaged.



Responsible entities
ACN



Other interested parties
DIS (UCSe), Min. Defence, University, Research



Definition and Implementation of a national coordination action to counter online disinformation

Measure #24

Implement a national coordination action, consistent with the initiatives adopted at European level and in synergy with like-minded countries, to prevent and tackle – also through information campaigns – online disinformation, which, by exploiting the characteristics of the cyber domain, aims to condition/influence the country's political, economic, and social processes.



Responsible entities

PCM-DIE ¹, DIS



Other interested parties

AISE, AISI, MAECI, Min. Interior, Min. Defence, ACN, AGCOM



RESPONSE

National and transnational cybersecurity crises management system

Measure #25

Develop a system of continuous coordination of all the Administrations that take part in the NCS, which guarantees a timely and synergistic management of the various possible cyber crisis scenarios, as well as an immediate implementation of response measures.



Responsible entities

ACN-NCS ²



Other interested parties

Other NCS Administrations

Measure #26

Contribute to the effective activation of European mechanisms for coordinated response to large-scale transnational cyber incidents and crises.



Responsible entities

ACN-NCS ²



Other interested parties

MAECI, other NCS Administrations

Measure #27

Ensuring and facilitating methods of uniform notification of cyber security incidents to the CSIRT to make the response and early warning capacity more effective.



Responsible entities

ACN



Other interested parties

Min. Interior

Measure #28

Further develop the capacities to ensure a prompt institutional communication activity in the event of significant cyber incidents or crises, as well as whenever it is necessary to carry out awareness-raising actions towards the civilian population.



Responsible entities

PCM, ACN-NCS ²



Other interested parties

Other NCS Administrations, Industry

¹ Department for Information and Publishing

² The CyberSecurity Cell is set up at the ACN, which carries out supporting activities



Measure #29

Ensure the periodic updating of the operating procedures relating to the response measures for the different cyber threat scenarios for the decisions of the Prime Minister, in accordance with the national legislation in force, and for the consequent correct implementation by the interested parties.



Responsible entities

ACN-NCS *



Other interested parties

Min. Interior, Min. Defence, DIS, AISE, AISI



National cybersecurity services

Measure #30

Create a HyperSOC collection and analysis system to aggregate, correlate and analyse security events of interest to early identify any complex attack "patterns", as well as to enable a preventive and integrated cyber risk management among multiple data sources, also by exploiting High Performance Computing infrastructures, Artificial Intelligence technologies, and machine learning.



Responsible entities

ACN



Other interested parties

Regions and autonomous Provinces, Industry, University, Research

Measure #31

Enter into agreements with Internet Service Providers (ISPs) to share events of interest, so as to support both the achievement of measure #30 and the early identification of any emerging threats, as well as the mitigation of attacks against our country.



Responsible entities

ACN



Other interested parties

DIS, ISP

Measure #32

Create a High Performance Computing infrastructure dedicated to national cybersecurity for the enhancement of the Agency's national cyber services, as well as the development of simulation tools, based on Artificial Intelligence and machine learning, to support the phases of prevention, discovery, response, and prediction of the impacts of systemic cyber-attacks.



Responsible entities

ACN



Other interested parties

NCS Administrations, University, Research, Industry

* The CyberSecurity Cell is set up at the ACN, which carries out supporting activities



Measure #33

Increase response and recovery capacities following cyber crises by implementing a network of sectorial CERTs integrated with the CSIRT Italia, as well as a national crisis management plan that defines procedures, processes, and tools to be used in coordination with public and private operators, with the aim of ensuring the business continuity of networks, information systems and IT services.



Responsible entities

ACN, NCS Administrations



Other interested parties

Industry

Measure #34

Create an ISAC at the ACN, with the task of coordinating the collation and analysis of operational and strategic added value information produced by the various national cyber services. The facility will be connected to the ISAC European network, contributing to the creation of the "European CyberShield", envisaged by the EU Cybersecurity Strategy.



Responsible entities

ACN



Other interested parties

NCS Administrations

Measure #35

Promote the creation of sectorial ISACs integrated with the ACN's ISAC, also through public-private initiatives, so as to encourage the enhancement of sharing information and best practices for the sake of Public Administrations and national industry.



Responsible entities

ACN



Other interested parties

Regions and autonomous Provinces, Industry

Measure #36

Create an incident response qualification program for SOCs/CERTs/CSIRTs of a group of selected companies, capable of providing support to the CSIRT Italia in case a multitude of systemic cyber incidents should occur.



Responsible entities

ACN



Other interested parties

Industry

Measure #37

Promote the creation of an integrated and continuous management of national cyber risk, facilitated by analysis of the security posture of the Public Administration, as well as by tools for controlling and monitoring the supply chain.



Responsible entities

ACN






Other interested parties


NCS Administrations


 **Cybersecurity exercises**

<p>Measure #38</p> <p>Provide for the organization of periodic interministerial exercises, also in the framework of the Perimeter, which concern technical and operational aspects of managing cybersecurity events or crises.</p>	<p> Responsible entities ACN</p> <p> Other interested parties NCS Administrations, Industry</p>
<p>Measure #39</p> <p>Promote and coordinate the participation in European and international exercises concerning the simulation of cyber events, to raise the resilience of the Country.</p>	<p> Responsible entities ACN-NCS *</p> <p> Other interested parties ACN, MAECI, Min. Interior, Min. Justice, Min. Defence, MEF</p>

 **Definition of a national posture and procedure for attribution**

<p>Measure #40</p> <p>Strengthen national mechanisms aimed at applying deterrence tools defined at European and international level for the response to cyber-attacks. In this context, there is a need for defining a document on the national positioning and procedure on attribution.</p>	<p> Responsible entities DIS, AISE, AISI, MAECI</p> <p> Other interested parties ACN, Min. Defence, Min. Interior, other CISR Administrations</p>
--	---

 **Countering cybercrime**

<p>Measure #41</p> <p>Further strengthen cybercrime prevention and countering actions from the National Police and the Postal and Communications Police Service, also through targeted training.</p>	<p> Responsible entities Min. Interior, Min. Justice, MEF</p>
---	---

* The CyberSecurity Cell is set up at the ACN, which carries out supporting activities

Measure #42

Enhance countering capabilities towards the spreading of online hateful, violent and discriminatory contents.



Responsible entities

Min. Interior,
Min. Justice, DIS



Other interested parties

Min. Education

Measure #43

Further reinforce international cooperation and information sharing on countering cybercrime with European and international counterparts and Member States.



Responsible entities

MAECI, Min. Interior,
Min. Justice



Other interested parties

ACN

Measure #44

Ensure an accurate statistical survey of data on cyber-crimes and cyber-assisted crimes acquired by the National Police and the Judicial Authority, to ease their analysis also for the purpose of legislative supplements.



Responsible entities

Min. Interior,
Min. Justice



Other interested parties

ACN



Deterrence capabilities in the cyber domain

Measure #45

Strengthen cyber deterrence capabilities according to the ongoing scenarios.



Responsible entities

DIS, AISE, AISI,
MAECI, Min. Defence



Other interested parties

ACN



DEVELOPMENT

National Coordination Centre

Measure #46

Implement and promote the participation of civil society, industry, as well as the academic and research communities in projects funded by relevant Union programmes, aimed at fostering the development of cybersecurity capabilities, technologies and infrastructures, while also seeking to establish synergies with relevant activities at national level.



Responsible entities

ACN (NCC)



Other interested parties

Central Administrations, Regions and autonomous Provinces, Industry, University, Research

Measure #47

Support national Digital Innovation Hubs and foster synergies between them and the National Coordination Centre, the highly specialized Competence Centres as well as the Technological Clusters, to promote technological transfer towards SMEs.



Responsible entities

MiSE, MITD, ACN



Other interested parties

Trade Associations, University, Research



Development of National and European technology

Measure #48

Develop national and European technology with particular regard to innovative and sensitive components (e.g. cloud and edge computing, blockchain based technologies, space, etc.) through the rollout of specific projects.



Responsible entities

ACN, Delegated Authority for Space and Aerospace Policies, Min. Defence (military research)



Other interested parties

MUR and other NCS Administrations, Industry, University, Research



Creation of a “National Cybersecurity Campus”

Measure #49

Create a “National Cybersecurity Campus” that provides the necessary infrastructures to perform research and development activities on cybersecurity and digital technologies and which is organized as a “widespread” structure with local branches throughout the Country.



Responsible entities

ACN, MITD, MEF, MiSE, Min.Defence (military research)



Other interested parties

Regions and autonomous Provinces, University, Research, Industry



Industrial, technology and research development

Measure #50

Foster the internationalization of Italian companies specialized in the supply of cybersecurity products and services by supporting investments, innovation, and exports.



Responsible entities

MAECI, MiSE, ACN

Measure #51

Implement a “National cybersecurity industry Plan” aimed at supporting companies and start-ups in the design and rollout of high-reliability products and services (included a national communication infrastructure), which comply with our national strategic interests and that can be sponsored in like-minded countries.



Responsible entities

MiSE, MITD, MAECI, ACN



Other interested parties

Regions and autonomous Provinces, Min. Defence (military research)

Measure #52

Encourage the establishment of Product Security Incident Response Teams (PSIRTs) by private operators to increase their ability to manage vulnerabilities of ICT products, and to contribute to the adoption and the implementation of national policies on coordinated vulnerability disclosure.



Responsible entities

ACN, MiSE



Other interested parties

Industry, Trade Associations



Driving technological innovation and digitalization

Measure #53

Promote initiatives aimed at strengthening the industrial and technological autonomy of our Country regarding strategic IT products and processes while safeguarding our national interests in that field, also promoting the development of proprietary algorithms, as well as the research and the achievement of new national cryptographic capabilities.



Responsible entities

ACN, MITD, MiSE, MUR, Min. Defence



Other interested parties

Regions and autonomous Provinces, University, Research

Measure #54

Support research and development especially on new technologies by encouraging the inclusion of cybersecurity principles while bolstering the rollout of cybersecurity projects from the private sector – even through dedicated funding, public and private investments or simplification mechanisms – with particular regard to start-ups and innovative SMEs, as well as from national competence and research centres.



Responsible entities

ACN, MITD, MEF, MiSE, MUR, Min. Defence



Other interested parties

Industry, University, Research

Measure #55

Foster the innovation and digitalization of the Public Administration while enhancing its security, also making use of NRRP fundings.



Responsible entities

MITD, ACN



Other interested parties

MPA, other Central Administrations, Regions and autonomous Provinces

Measure #56

Foster the innovation and digitalization of the national productive fabric also making use of NRRP fundings.



Responsible entities

MITD, MiSE, ACN



Other interested parties

Central Administrations, Regions and autonomous Provinces

Measure #57

Enhance the level of cybersecurity of national IXP to ensure an open, free and stable Internet.



Responsible entities

ACN



Other interested parties

IXP

Measure #58

Develop digital public services for central and local Public Administrations.



Responsible entities

MITD



Other interested parties

ACN



ENABLERS

Cybersecurity training

Measure #59

Intensify the development of cybersecurity training and educational programmes at different levels of specialization (primary and secondary school, post-diploma courses (ITS), university, post-graduate degrees, PhD and master’s degrees, Public Administrations’ Schools) – also investing on training and preparation for the professors – so that the educational offer can keep pace with the labour market needs and can support the creation of a solid national workforce.



Responsible entities

Min. Education, MUR, University, ACN, Min. Defence (higher education)



Other interested parties

PCM, Min. Defence, Min. Interior, Regions and autonomous Provinces

Measure #60

Activate Higher Technical Institutes (ITS) with specific education paths on cybersecurity, to support the specialization of local manufacturing. The courses and activities should be composed of academic training sessions by teachers from private companies (50%) and of an internship (at least 30% of the total time).



Responsible entities

Min. Education, MUR, University, ACN



Other interested parties

Regions and autonomous Provinces, Industry, Trade Associations, Accredited Training Organizations

Measure #61

Develop a national certification system for education and skills, both at school/university and at technical level. ACN approves and manages the training programmes’ list, at the end of which the degree and the pertaining certification is earned.



Responsible entities

ACN, Min. Education, MUR, University



Other interested parties

Industry, Regions and autonomous Provinces

Measure #62

Develop an online training and awareness tool for civil society, to self-test their level of cybersecurity competencies and awareness and to earn a certificate. This constitutes the first step to further rollout a dedicated “ACN e-Academy”.



Responsible entities

ACN

Measure #63

Distribute funds for public and private professional training, to facilitate the transition from education to the labour market and achieve a national digital skills sovereignty.



Responsible entities

MITD, MEF



Other interested parties

ACN, Min. Labour, Regions and autonomous Provinces, Industry

Measure #64

Provide incentive mechanisms for the development of cybersecurity start-ups and public-private partnerships with cybersecurity women-led companies.



Responsible entities

MEF, MiSE, MITD



Other interested parties

Min. Labour, Regions and autonomous Provinces

Measure #65

Foster the organization of national cybersecurity and innovation initiatives and challenges which, while considering the gender balance, aim at finding young talents and facilitating their entry in the labour market. This also to bridge the "confidence gap" of female students towards technical and scientific careers.



Responsible entities

PCM, Min. Education, MUR, University, CINI, ACN



Other interested parties

Min. Defence

Measure #66

Provide assisted mechanisms for the transition of cybersecurity students and graduates to the labour market through dedicated work-school programmes, as well as internships, apprenticeships and incentives to the employment of "junior" staff, while promoting the retraining and professional repositioning of those who find themselves outside the labour market.



Responsible entities

MiSE, MUR, Min. Education, MITD, MEF



Other interested parties

Min. Labour, Trade Associations, Industry, University

Measure #67

Establish European and international exchange programmes at academic and professional level which further support the participation of women.



Responsible entities

MUR, MITD, MAECI, CINI, Min. Defence



Other interested parties

ACN, Trade Associations, Industry, University

Measure #68

Promote specialized training for those who deal with the countering of cyber-crime in the judiciary and investigative field.



Responsible entities

Min. Interior, Min. Justice



Other interested parties

University, Min. Defence

Measure #69

Enhance the cyber diplomacy skills through targeted courses for the diplomatic staff.



Responsible entities

ACN, MAECI



Other interested parties

University

Measure #70

Foster specific refresher cybersecurity training courses and educational programmes for public and private employees, including the top managers, also with the aim to requalify the existing workforce.



Responsible entities

MiSE, MITD, ACN



Other interested parties

PCM, Min. Interior,
Min. Defence, Min. Labour,
MPA, other Administrations,
Trade Associations



Promotion of a cybersecurity culture

Measure #71

Launch awareness initiatives and campaigns to enhance users' capabilities and responsible behaviour in cyberspace, while avoiding negligence as well as increasing the awareness on the risks posed by the use of ICT and on how to protect privacy online, also considering the needs of specific categories such as elderly and disabled people other than some public employees (such as the judiciary). This, by the dissemination of clear and understandable information about security vulnerabilities of widely used ICT products and services.



Responsible entities

ACN, Min. Interior,
MUR, MITD, PCM



Other interested parties

MPA, Trade Associations,
Regions and
autonomous Provinces,
Min. Defence

Measure #72

Develop a widespread digital and cybersecurity education programme at all levels to promote the acquisition of technical and operational knowledge on secure ICT management, also through dedicated agreements with academia in order to optimize students' learning on that field.



Responsible entities

Min. Education, MUR,
University, ACN

Measure #73

Define and implement an autonomous national strategy and implementation plan on child online protection from cybercrimes, which includes the conduction of awareness campaigns targeting not only minors but also their parents, guardians and teachers.



Responsible entities

Min. Interior, PCM



Other interested parties

ACN, Min. Education,
Industry, University



Cooperation

Measure #74

Establish permanent operating working groups among the entities included in the Perimeter and divided by sector, which are in charge of incident prevention, alert, response, and recover duties.



Responsible entities

ACN



Other interested parties

Central Administrations,
Regions and
autonomous Provinces,
Trade Associations,
Industry

Measure #75

Further strengthen the role of Italy within international fora dealing with cybersecurity (such as EU, NATO, G7, OSCE and Council of Europe), as well as its European and global strategic positioning fostering synergies with like-minded countries.



Responsible entities

MAECI, ACN, Min. Interior,
Min. Justice,
Min. Defence, MiSE

Measure #76

Ensure the implementation of OSCE's Confidence Building Measures (CBMs) on cybersecurity.



Responsible entities

MAECI, ACN



Other interested parties

Min. Defence,
other NCS Administrations,
Industry



Measure #77

Increase cooperation with other countries to contribute to the stability and security in cyberspace.



Responsible entities
MAECI, ACN, Min. Defence

Measure #78

Define a national ecosystem aimed at implementing capacity building initiatives towards third countries.



Responsible entities
ACN, MAECI



Other interested parties
Other NCS Administrations

Measure #79

Stipulate bilateral and multilateral agreements with countries of interest also including the development of capacity building actions.



Responsible entities
MAECI, ACN, Min. Interior,
Min. Justice, Min. Defence



Other interested parties
Other NCS Administrations

Measure #80

Actively contribute, at EU level, to the definition of cybersecurity policies and regulations.



Responsible entities
ACN



Other interested parties
MAECI, MITD, MiSE

Measure #81

Actively contribute, at EU level, to the identification of research and development priorities, to reach the EU goal of achieving a digital technological autonomy.



Responsible entities
ACN, MITD, MiSE



Other interested parties
MAECI, Min. Defence
(military research)



Metrics and Key Performance Indicators

Measure #82

Develop, within 12 months from the adoption of this strategy, specific metrics and Key Performance Indicators (KPIs) to measure:

- the degree of implementation of the strategy
- the cybersecurity maturity level of OES/DSP
- the involvement of specific categories (e.g. women, young people, and unemployed or jobseekers) in cybersecurity awareness, education and training activities and their effectiveness
- the involvement of specific categories (e.g. women and young people) in the cybersecurity industry
- the initiatives and related investments on cybersecurity research and development, even from national companies
- the total amount of cybersecurity investments from public and private stakeholders
- the total amount of national companies insured from cybersecurity incidents

Responsible entities



ACN, other entities in charge of the implementation of the strategy

Other interested parties

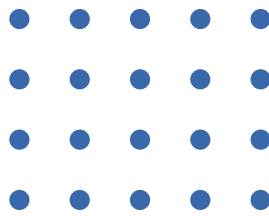


ISTAT, Trade Associations, Industry, University



#2

National governance



National governance

In light of the Implementation plan defined above, it is clear how the success of the national strategy can be guaranteed only through the synergic action of institutions, industry, university and civil society, whose contribution, with single actions in the respective fields, is essential for the achievement of the general goals.

As such, an integral part of the strategic choice is the creation of a national cybersecurity ecosystem, in which the various interested subjects may operate in a coordinated way to allow the country as a whole to make the best use of the various opportunities offered by the technological innovation processes, contributing, in such way, to Italy's prosperity and socio-economic development.

This choice is at the basis of the recent reform of the national cyber architecture – enacted by Law Decree of 14 June 2021, n. 82 – by which the legislator has aimed at reorganising and rationalising the national competences regarding cybersecurity (previously fragmented and attributed to a variety of institutional actors), creating a central entity with competence on the subject, which could also represent the connecting point between the various interested subjects.

This also to allow the implementation of the strategic goals in a coordinated and harmonized system, in which the implementation of the directives defined by the political authority can be guaranteed through the coordinated action of the involved actors.



The evolution of the national cybersecurity legislation

To face the increased interconnection and interdependence between IT systems and their related threats, both the EU and Italy adopted some legislation in continuous evolution.

In a nutshell, during the last five years, Italy has adopted the following acts and regulations on cybersecurity:

- Prime Minister's Decree (DPCM) of 17 February 2017, which updated the national cybersecurity architecture established by DPCM of 23 January 2013;
- Legislative Decree of 18 May 2018, no. 65 (thereafter "NIS Decree"), which provides for an obligation upon Operators of Essential Services and Digital Services Providers to both notify cyber incidents having a relevant impact on service continuity and implement security measures based on risk assessment;
- Law Decree of 21 September 2019, no. 105 (thereafter "Perimeter Decree"), which established the National Security Perimeter for Cyber, with the aim of protecting digital assets the malfunctioning, interruption, also partial, or improper use of which may determine a prejudice for national security. It provides, compared to the NIS Decree, for stricter criteria on incident notification and higher security levels, also for the supply chain, as well as specific procedures for procurement of ICT intended to be used on such digital assets;
- Law Decree of 18 July 2020, no. 76, which moved forward digitalization of the Public Administration, providing that such digitalization shall happen in compliance with network and information security principles, including workforce's professional development and promotion of the awareness on the importance of network and information security;
- Law Decree of 14 June 2021, no. 82, providing for urgent provisions on cybersecurity, definition of the national cybersecurity architecture and establishment of the National Cybersecurity Agency;
- the Italian Cloud Strategy, adopted in the context of the triennial plan for ICT in the Public Administration for 2020–2022 and defined by the Department for digital transformation in collaboration with the National Cybersecurity Agency, with the aim of encouraging the use of solutions based on cloud computing by the Public Administration;
- Legislative Decree of 8 November 2021, no. 207, implementing the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. It provides, among others, for cybersecurity requirements for public electronic communication networks or for publicly accessible electronic communication services, the obligation to notify significant cyber incidents, as well as the adoption of cybersecurity measures, attributing the competence on the subject to the National Cybersecurity Agency;
- Law Decree of 21 March 2022, no. 21, which provides, among others, for the redefinition of the exercise of special powers on electronic communication services based on 5G, as well as on other services, goods, relations, activities and technologies which are relevant for cybersecurity, including those related to cloud technology. Specifically, it redefined the obligations and notification procedures by interested companies as well as the procedures for the exercise of the special powers, the monitoring and sanctioning by the Government, establishing the participation of the National Cybersecurity Agency, the possibility of using the National Assessment and Certification Centre (CVCN) and the carrying out of inspection and verification activities.



In this framework, the **Prime Minister**, as the head of the institutional architecture and the political-strategic body, carries out the high-level management and has the general responsibility for cybersecurity policies. The President may delegate to the **Undersecretary of State for the security of the Republic**, referred to under article 3 of the Law 3 August 2007, no. 124, the functions which are not exclusive.

Still at the political-strategic level, the **Interministerial Committee for Cybersecurity (CIC)** has primary importance. The CIC is established at the Presidency of the Council of Ministers and it has advisory, propositional and supervisory functions on cybersecurity policies. The CIC represents the political committee in which cybersecurity issues can be analysed and addressed, strategical goals and directives can be shared and the implementation of policies can be monitored. In this respect, the Committee is chaired by the Prime Minister and it is composed by the Undersecretary of State for the security of the Republic, if appointed, by the Minister of Foreign affairs and International Cooperation, the Minister of Interior, the Minister of Justice, the Minister of Defence, the Minister of Economy and Finance, the Minister of Economic Development, the Minister of Ecological Transition, the Minister of University and Research, the Minister in charge of Technological Innovation and Digital Transition and the Minister for Sustainable Infrastructures and Mobility.

Specifically, the CIC is consulted by the Prime Minister in relation to the adoption of the national cybersecurity strategy and it oversees its implementation. It also contributes to the definition of the strategy itself by proposing to the Prime Minister general directives to be pursued in the context of cybersecurity policies and by promoting the adoption of the necessary initiatives for the effective collaboration, at both national and international level, between institutional entities and private operators interested in cybersecurity, for the sharing of information, for the adoption of best practices and measures, as well as for the industrial, technological and scientific development on the subject.

Considering the cross-impacts of cyber policies, it was recognized the need to establish a specific authority connecting with the political-strategic level and coordinating the actors involved, as well as regulating, certifying, and supervising the cyber field. This in particular to ensure coherent initiatives, represent a clear and updated situational framework to the political authority and provide a single interlocutor at the national, European and international level, ensuring a uniform national posture.

Therefore, the **National Cybersecurity Agency (ACN)** was established which – as the national cybersecurity authority in charge of the protection of networks and information systems' security and resilience in the cyberspace, also with the aim of protecting national security and national interests – has a central role in the achievement of the three goals identified in the strategy.

As the National Cybersecurity Authority, ACN:

- ensures the coordination between the public entities involved in cybersecurity;
- promotes, also with the aim of strengthening public-private partnership, the realisation of a cybersecurity and resilience framework for the development of the digitalization of the Country, the productive

system and the Public Administration, as well as for achieving national and European autonomy with respect to ICT products and processes of strategic relevance, in protection of national interests in the sector.

The Agency's functions reveal a holistic approach to cybersecurity management, in which not only the interventions of a mainly technical nature aimed at guaranteeing the security and resilience of networks, information systems and ICT services, but also the projects for the development of new products and technologies, research and industrial competition, as well as the creation of a national workforce capable of addressing market's needs are relevant.

ACN ORGANIZATIONAL STRUCTURE

 Cabinet	Maintenance of an updated national cyber legal framework Interministerial cyber meetings/panels/committees (CIC, NCS, PSNC)
 Authority and Sanctions	Compliance with sectorial laws NIS, PSNC, and Telco Sanctions
 Certification and Supervision	National Assessment and Certification Centre (CVCN) National Authority for Cybersecurity Certification Inspections and verification of compliance with cybersecurity legal obligations
 Operations	Computer Security Incident Response Team (CSIRT) Italia Monitoring, prevention, response to cyber-attacks
 Industrial, Technological, Research and Educational Programs	Promotion of research programs National Coordination Centre (NCC) Promotion of cybersecurity education
 Human and Instrumental Resources	Recruitment and professional development Management of instrumental resources
 Strategies and Cooperation	Drafting of the national cybersecurity strategy Development of national policies and cyber awareness initiatives International relations and cooperation



Specifically, the Agency, in compliance with the competences attributed by the legislation in force to other Administrations:

- acts as a cybersecurity regulatory, certificating and supervisory entity defining, for example, the minimum levels of security measures for the different sectors (including energy, transportation, banking, financial markets infrastructures, health, supply and distribution of potable water, public administration), and being able to carry out inspections and impose sanctions;
- takes care of and promotes the definition and maintenance of an updated and coherent cybersecurity legal framework;
- contributes to reducing the risks deriving from technological supply by increasing security levels of the supply chain, with particular regard to solutions and products intended to be used on infrastructures and ICT systems relevant for national security;
- develops monitoring, detection, prevention, analysis, and response to cyber incidents capabilities;
- coordinates, in connection with the Ministry of Foreign Affairs and International Cooperation, international cooperation in the area of cybersecurity;
- supports the development of industrial, technological and scientific competences and capabilities and it promotes the education, technical-professional development and qualification of human resources;
- carries out cybersecurity communication activities and promotion of cyber awareness, contributing to the development of a national culture on the subject;
- is appointed as National Coordination Centre (NCC), according to article 6 of the Regulation (EU) 2021/887 of the European Parliament and of the Council of May 20th, 2021, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) and the Network of National Coordination Centres.

To enable the carrying out of the above-mentioned functions, the following structures operate within the Agency:

- the **Computer Security Incident Response Team (CSIRT) Italia**, the action of which is aimed at preventing, monitoring, detecting, analysing, and responding to cyber incidents;
- the **National Assessment and Certification Centre (CVCN)**, which will verify the security and the absence of known vulnerability in ICT goods, systems and services used in infrastructures which State's essential functions and services depend upon;
- the **National Coordination Centre (NCC)** on cybersecurity in the industrial, technology, and research field.

In order to reach high security levels in the cyber domain and to protect strategic assets, the overall framework of the institutional cybersecurity architecture necessarily includes the close synergic contribution of other Public Administrations, to which the legislation in force assigns exclusive prerogatives in relation to the respective institutional mandates.

Among these Public Administrations, in particular:

- the **Intelligence community**, competent for cyber-intelligence, carries out research and intelligence gathering aimed at the protection of Italy's political, military, economical, scientific and industrial interests and it elaborates analysis, assessments and predictions on cyber threats to preserve national security, also by carrying out cyber operations. In particular, according to the modalities and procedures established by the Law no. 124/2007, the Director General of the Security Intelligence Department (DIS), with the support of the Department's offices, coordinates intelligence gathering activities. The Agencies, each within their respective area of competence, carry out – according to the directives issued, after having consulted the CISR, by the Prime Minister, as well as the guidelines for the coordination of intelligence gathering activities established by the DIS Director General – research and intelligence gathering activities aimed at the national cyber protection and security;
- the **Ministry of the Interior**, as the national public security authority, protects public order and security, public aid and civil defence. In particular, the Department of public security ensures the prevention and fight against cybercrimes through the Postal and Communication Police, without prejudice to the competences, in the areas defined by the legislator, of the offices and commands of the Italian National Police, the Carabinieri Corps and the Financial Police. The National Cybercrime Centre for Critical Infrastructure Protection (CNAIPIC) of the Italian National Police acts to protect digitized critical infrastructures from cybercrimes, carrying out a continuous monitoring of the internet and the functions of national contact point for the emergencies related to transnational cybercrime.

Within the Department of Public Security, it has been established – by means of Decree of the President of the Republic 19 November 2021, no. 231, which modifies the DPCM 11 June 2019, no. 78 – and will soon be operational the Central Directorate for scientific police and cybersecurity. The Directorate will be competent for developing the cyber prevention and protection activities already attributed to the CNAIPIC, as well as those assigned to the Ministry of Interior by the Perimeter Decree, which is in charge, among others, of verifying the security conditions and the absence of known vulnerabilities in relation to ICT procurement intended to be used in its own ICT networks, systems and services that have been included in the Perimeter. The assessment is carried out through the Ministry's Assessment Centre which operates in close cooperation with the CVCN;

- The **Ministry of Defence**, in charge of the military defence and security of the State. In particular, the Ministry defines and coordinates military policy, governance and capabilities in the cyber domain, as well as the development of cyber capacities and the protection of their networks and systems both on national ground and in theatres of operations abroad. The Defence is also in charge of planning and conducting both offensive and defensive military cyber operations through the Joint Command for



Network Operations (COR) and with the specialized contribution of the Information and Security Division (RIS) of the Defence General Staff (SMD).

Therefore, the Ministry guarantees, even in the case of cyber crises (both at national and international level), all the necessary services and activities to ensure the protection, resilience and efficiency of military networks and infrastructures, as well as to develop its unique implementation capacities of support, defence, reaction, and stabilization actions.

At NATO level, the Ministry of Defence assures the participation of our Country in military actions following the recognition of cyberspace as a domain of operations. It also contributes to the definition of cybersecurity policies and to the strengthening and development of NATO's cyber capacities, in respect of the competences attributed to other Administrations by the legislation in force.

Like the Ministry of the Interior, the Defence assesses the security conditions and the absence of known vulnerabilities in relation to ICT procurement to be used in its own ICT networks, systems and services that have been included in the Perimeter. The assessment is carried out through the Ministry's Assessment Centre which operates in close cooperation with the CVCN.

In parallel, within the coordination operated by ACN, **each Ministry and authority with cross-cutting competences and interests in the cyber field** plays a role in the achievement of the aforementioned goals. Such role becomes relevant by both ensuring the safety of its own networks and digital infrastructures and participating in the inter-institutional bodies and initiatives promoted by ACN and aimed at increasing cybersecurity.

In particular, the **Ministry of Foreign Affairs and International Cooperation (MAECI)** develops cyber diplomacy initiatives, in accordance with the foreign policy national directives and promoting the protection of fundamental rights and freedom in the cyberspace. Moreover, the MAECI contributes to the definition of the Italian position in the highest international and European cyber fora.

The **Ministry of Economic Development (MiSE)** plays a strategic role in the development of the entrepreneurial system, through the promotion of research and innovation, spreading of digital technologies and new technologies, technology transfer, environmental sustainability. In such context, it supports the operability of the Digital Innovation Hubs that contribute to industry, with particular regard to the small-medium enterprises, and Public Administration's digital transition through the adoption of advanced digital technologies, artificial intelligence, high-performance computing, IT security.

The transfer to the National Cybersecurity Agency of the competences on cybersecurity – in application of Law Decree no. 82/2021 – still leaves the Ministry with relevant knowledge on cybersecurity, which will be essentially dedicated to the education activities carried out also through the Superior Telecommunications Specialisation and Research School in the area of innovative and digital technologies, also through collaborations with university and research entities, carried out in the context of the General Directorate for communication technologies and IT security – Communication and Information Technologies Superior Institute.



The Ministry of Economic Development is also a “Sector Authority” pursuant to the NIS Decree and it identifies the entities to be inserted in the National Security Perimeter for Cyber, according to Law Decree no. 105/2019, in relation to the sectors falling within its competence.

The **Ministry of Economy and Finance (MEF)** carries out, through the Financial Police – in particular the Special Unit for the Protection of Privacy and Technological Fraud (NSTPFT) – crime fighting activities against economic-financial crimes committed through ICT technologies.

The Bank of Italy, as the supervisory authority of the sector, issues regulations and guidelines for strengthening supervised operators’ cyber resilience. It also receives cyber incidents notifications from banks and financial intermediaries, pursuant to the principal sectorial legislation.

Moreover, the Bank of Italy chairs the CODISE, which is a structure with a coordinating role for the operational crisis of the Italian financial marketplace, which the Consob and the relevant sectorial businesses participate in. In case of cyber incidents on a large scale, the CODISE liaises with the Italian Financial CERT (CERTFin) to ensure a continuous situational analysis and the needed technical support. Bank of Italy’s CERT liaises with the principal interested national entities (first of all, the CSIRT Italia, the CNAIPIC and the CERTFin) and it is also responsible for the management of cyber incidents directed to the Bank, as well as for the organization of training and educational programs, info-sharing initiatives and cyber awareness campaigns.

The **Ministry of Education** and the **Ministry of University and Research (MUR)** promote – in close cooperation with ACN, the other Public Administrations and the private sector – a structured digital education and training plan which should allow to fill the gap of the professional profiles required by the market. Specifically, in relation to the competences related to scientific and technological research, the MUR ensures that any type of directive, programming and coordination aim at guaranteeing that new technologies are developed by taking into account cybersecurity aspects; it also promotes the scientific cooperation at the national, European and international level, also through specific relations between universities and research entities.

The **Department for Digital Transformation (DTD) of the Presidency of the Council of Ministers**, which supports the Prime Minister and the **Minister of technological innovation and digital transition**, promotes and coordinates Governmental actions directed to the definition of an uniform strategy on Public Administration’s digital transformation and Italy’s technological modernization, also in order to achieve the Italian Digital Agenda goals. Moreover, it carries out all the activities aimed at ensuring, in cooperation with the interested Administrations, the development and spreading of the competences needed for an adequate use of digital technologies in the educational, university, and research, central and local Public Administrations, justice, business, work and social activities sectors.

The **Agency for a Digital Italy (AgID)** promotes the digital innovation of the Country and the use of digital technologies in the Public Administration’s organization and in its relationship with citizens and companies. In particular: it drafts the Triennial plan for ICT in the Public Administration; it carries out functions in the context of procurement procedures of ICT goods and services, by issuing technical opinions on the central Public Administrations’ contracts’ schemes and framework agreements, beyond a specific threshold, concerning the acquisition of automatized ICT goods and services and on call for tenders issued by Consip and other con-

tracting authorities; it supervises on fiduciary services, certified e-mail operators, accredited digital documents registries, as well as on public and private entities that participate in the Public System of Digital Identity (SPID).

Fundamental and determining input is provided by the **Public Administrations which are members of the various interministerial fora**, among which the **National CyberSecurity Cell (NCS)** is particularly relevant.

As an inter-ministerial coordination forum, established within the National Cybersecurity Agency, which operates in support of the Prime Minister for the aspects related to the prevention and preparation to eventual crisis and for the activation of the alerting procedures, the NCS can facilitate, in particular, the achievement of goal no. 2. Indeed, the NCS ensures the alignment between ACN, the Military Advisor of the Prime Minister, the Intelligence, the Ministry of Foreign Affairs and International Cooperation, the Ministry of Interior, the Ministry of Justice, the Ministry of Defence, the Ministry of Economy and Finance, the Ministry of Economic Development, the Ministry of Ecological Transition, the Ministry of Sustainable Infrastructures and Mobility, the Ministry of University and Research, the Department for Digital Transformation. At the same time, the NCS, which has the function of proposing cybersecurity initiatives, is also a platform where to discuss the various initiatives with impacts on cybersecurity policies promoted by the Administrations and it can, as such, represent the principal forum where the coordinated development of initiatives related to goals no. 1 and 3 can be ensured. In this context, other interested subjects, including private entities, can be invited to participate.

Still in the context of inter-institutional coordination, besides the NCS, other fora where the strategic goals can be reached, in particular the protection one, are represented by the Interministerial Board for the implementation of the National Security Perimeter for Cyber as well as, once established, by the Technical Coordination Committee provided by the NIS Decree.

On the private side, the **business operators**, the **university** and **research** and, last but not least, **civil society**, represent essential elements for the resilience of the Country and are, therefore, an essential part of the national cybersecurity ecosystem. In this respect, also through the fundamental stimulus and contribution of ACN and based on its functions provided by the law, a continuous collaboration between the aforementioned Public Administrations, universities, research entities and private operators (also through trade associations) shall be searched and supported, through specific understandings and agreements. This in order to guarantee a fruitful interaction both with the entities who manage strategic ICT assets and the entire business sector, including SMEs and start-ups.

An example of a fruitful public-private collaboration is the National Framework for Cybersecurity and Data Protection, drafted by the CIS-Sapienza and by the National Interuniversity Consortium for Informatics. The Framework provides a cross-cutting and size-regardless applicable methodology, by public and private organizations, aimed at supporting cybersecurity and assets protection-oriented initiatives to reduce vulnerabilities and risks to which such organizations are exposed to. The document is periodically updated and integrated to ensure a full adherence to the most recent sectorial legislation, the General Data Protection Regulation (GDPR), the Cybersecurity Act and measures on supply chain's security.



Further initiatives aimed at increasing public-private partnerships as well as collaboration with the university and research, are those promoting and strengthening the awareness on the importance of cybersecurity. Among these, there are conferences and events organised on a national scale such as ITASEC, as well as those aimed at creating a strong national workforce of young talents highly specialised, such as the Cyber-Challenge.it, an educational program started by the CINI and which will continue benefitting also of ACN's collaboration.

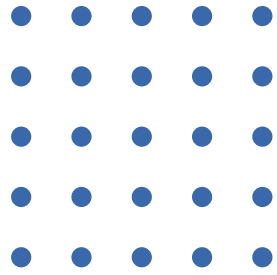
With respect to the development of cybersecurity research, the eight highly specialized Competence Centres created by the Ministry of Economic Development – in which the public-private partnership is intended to create training activities as well as support the creation of innovative projects in the Impresa 4.0 sector –, the Digital Innovation Hubs (DIH), and the twelves Technological Clusters established by MUR are relevant.

Similar cooperation initiatives will be continuously developed, in a synergic way, by interested entities, in the context of the coordination operated by ACN and in compliance with the directives issued by the Prime Minister, the Undersecretary of State for the security of the Republic, and the CIC, with the aim of contributing to the continuous increase in cybersecurity levels of the Country.



#3

Glossary



Glossary

A

Artificial Intelligence (AI)

Branch of knowledge that deals with the study of typical functions of human intelligence and their possible replication using IT methods and tools.

Assessment Centres (CV)

Evaluation Centres of the Ministry of the Interior and the Ministry of Defence, accredited by the CVCN pursuant to the Perimeter Decree.

B

Blockchain

Data structure in the form of a distributed register, made up of blocks in which the information necessary for the functioning of a given system are entered in chronological order and in an immutable and irreversible way. The distributed register is made up of several copies, each managed by a different entity. Since it is necessary to ensure consistency, the copies are updated independently, but must contain the same information in the same order. Blockchain technology is used for the development of the most disparate applications, such as cryptocurrencies.



Border Gateway Protocol (BGP)

Network standard that establishes the logical connection paths between autonomous systems (groups of network devices and networks under the control of a specific authority), through which data are transferred.

C

CERT (Computer Emergency Response Team)

Structure with prevention and cyber events response coordination tasks. Several CERTs also carry out training and information activities for their constituency.

CISR Administrations

Administrations that take part in the Interministerial Committee for the Security of the Republic, namely, Ministries of Foreign Affairs and International Cooperation, Interior, Justice, Defence, Economy and Finance, Economic Development, as well as of the Ecological Transition. The CISR is also composed of the Prime Minister, who chairs it, and the Undersecretary of State for the Security of the Republic where appointed. The Director General of the DIS acts as the Secretary of the Committee.

Cloud Computing

Usage paradigm and management of computational resources and IT services provided on request. Depending on the computational resources model offered, Cloud services can be divided into three service models:

1. infrastructure system services, so-called Infrastructure-as-a-Service (IaaS);
2. computational platform services, so-called Platform-as-a-Service (PaaS), for the provision of pre-configured and administered environments for the development of specific applications;
3. application services, so-called Software-as-a-Service (SaaS), for the delivery of an application to end users.

The services are provided by Cloud Service Provider (CSP) and the related distribution model can be organized in: Public Cloud, Private Cloud, Hybrid Cloud and Multi-Cloud.

Confidence Building Measures (CBMs)

Measures defined by the OSCE and aimed at reducing the risks associated with the possible emergence of politico-military tensions deriving from cyber-attacks and at strengthening cooperation between participating States.



Coordinated vulnerability disclosure

State-structured process, through which unknown cyber vulnerabilities, detected by researchers/ethical hackers, are reported to organizations to diagnose and eliminate them. Coordinated vulnerabilities disclosure also includes coordination between the persons reporting the vulnerabilities and the organization, regarding the timing for their removal and publication.

Cryptojacking

It is the malicious mining of cryptocurrencies, consisting in the unauthorized use of a device of a third party for the purpose of mining digital currencies.

CSIRT (Computer Security Incident Response Team)

Organizational unit responsible for coordinating the response to cyber incidents, mitigating their effects and preventing the occurrence of further events.

CSIRT Italia

Initially established at the DIS, following the changes introduced by the Law Decree no. 82/2021 (article 7, paragraph 3) the CSIRT was transferred to the ACN assuming the name of "CSIRT Italia". It has the following tasks: monitoring cyber incidents at national level; issuing early warnings, warnings, announcements, and sharing information to interested parties about cyber risks and incidents; intervening in the event of a cyber incident; carrying out dynamic analysis of cyber risks and incidents; enhancing situational awareness; participating in the EU CSIRTs network. To this end, the CSIRT establishes cooperative relationships with the private sector and promotes the adoption and use of common or standardized practices for cyber incidents and risks management processes, as well as for incidents, risks, and information classification systems.

CSIRT Network

Network of CSIRTs of the EU Member States in which the CERT-EU also participates. The European Commission participates in the network as an observer and ENISA acts as the secretariat of the network, with the task of actively supporting the cooperation between CSIRTs and, upon request, providing active support for the coordination of incidents. The CSIRT network provides a forum where members can cooperate and share information. Italy is represented by ACN's CSIRT Italia.

Cyber hygiene

Set of principles and rules for users of IT systems, aimed at minimizing the cyber risks which expose them to cyber-attacks.



Cybersecurity Act

Regulation (EU) 2019/881, that introduced a permanent mandate for ENISA, strengthening its tasks, and a European cybersecurity certification framework for ICT products, processes, and services according to a common and harmonized approach at EU level. This is to verify the compliance of ICT solutions based on specific security requirements aimed at protecting, throughout their life cycle, the availability, authenticity, integrity, and confidentiality of data, functions, and services. These requirements will be defined in specific certification schemes. The National Certification Authority within the European certification processes defined by the Cybersecurity Act is the National Cybersecurity Agency.

Cybersecurity essential controls

List of 15 cybersecurity essential controls that can be implemented easily and economically by medium, small or micro enterprises, to reduce the number of vulnerabilities present in their systems and increase the awareness of the staff. The controls, derived from the National Framework for Cybersecurity, were published by the Research Centre of Cyber Intelligence and Information Security (CIS) of La Sapienza University and by the National Cybersecurity Laboratory of the National Interuniversity Consortium for Informatics (CINI).

CyberShield

Project envisaged by the "EU Cybersecurity Strategy for the Digital Decade" of 16 December 2020, consisting in the creation of a network of European SOCs capable of sharing and correlating detected events more efficiently and to create high-quality analysis on threats, also recurring to artificial intelligence and machine learning techniques. The "EU Cyber Shield" is then completed with the role of ISACs and CSIRTs, which allow the timely reporting of cybersecurity incidents to the authorities and all the stakeholders involved in order to obtain a greater situational awareness.

CyCLONe

The Cyber Crisis Liaison Organization Network is a network envisaged by the European Commission Recommendation 2017/1584 (so-called Blueprint) and aimed at ensuring Union's preparation, situational awareness, and crisis management coordination, as well as supporting national and European cybersecurity policy makers. CyCLONe is tailored on the structure outlined in the Blueprint for the coordinated response to large-scale incidents and crises, creating a cross-border cooperation architecture based on three levels: political, represented by the Council of the EU, also through the Integrated Political Crisis Response mechanisms (IPCR); operational, embodied by CyCLONe; and technical, entrusted by the EU CSIRT Network. In this context, CyCLONe represents the cross-border infrastructure for ensuring effective coordination between the Chair of the NCS and his counterparts in other Member States. Italy is represented by the ACN.

D

Deepfake

Photos, videos, and audio created through artificial intelligence software which, starting from original contents (images and audio) can modify or recreate, in an extremely realistic way, the characteristics and movements of a face or body and to closely emulate a certain voice.

Digital Innovation Hub (DIH)

Connecting networks with the industry at a regional level, to facilitate the digital transformation process and the access of companies to the European market.

Digital Service Providers (DSP)

Legal entities providing an e-commerce, online search engine, and cloud computing services, pursuant to the NIS Decree.

E

Edge computing

Form of processing performed on-site or near a particular data source, minimizing the need to process data in a centralized data centre.

ENISA (European Union Agency for Cybersecurity)

Established by Regulation (EU) 2004/460 to help develop the Union's cyber capabilities and preparedness, promoting the exchange of best practices among Member States and operational cooperation between them and the European institutions, and acting as a point of reference for Union initiatives on cybersecurity. Its mandate has been made permanent and its tasks have been confirmed and extended, most recently, with Regulation (EU) 2019/881 (Cybersecurity Act).



European Cybersecurity Competence Centre (ECCC)

Established by the Regulation (EU) 887/2021, the ECCC has the overall objective of promoting research, innovation, and deployment in the area of cybersecurity to strengthen the Union's strategic autonomy, to support its technological capabilities and skills and to increase the global competitiveness of the Union's cybersecurity industry. This enhancing cybersecurity capacities, capabilities, knowledge, and infrastructure for the benefit of Member States, implementing actions under relevant Union funding programmes and promoting cybersecurity resilience and the uptake of cybersecurity best practices.

To fulfil its mission, the ECCC is responsible for the implementation of cybersecurity relevant parts of Horizon Europe and the Digital Europe programmes.

F

Fake news

False or distorted information content, artfully created, aimed at obtaining an illegal political or financial advantage.

H

High Performance Computing (HPC)

High-powered processing systems consisting of the combination of a large number of processing nodes.

Highly specialized competence centres

Public-private partnerships whose task is to carry out guidance and training activities for companies on Industry 4.0 issues, as well as support in the implementation of innovation, industrial research, and experimental development projects aimed at the creation, by those companies, in particular SMEs, of new products, processes or services (or their improvement) through advanced technologies in the Industry 4.0.



Hyper SOC

Centralized system to be set up at the ACN for the collection, correlation, and analysis of events of interest from the constituency.

I

Impresa 4.0 (National Plan Industry 4.0)

The National Plan Industry 4.0, developed by the MiSE, identifies a series of measures to encourage investments for innovation and competitiveness and to respond to the emerging needs of globalization and technological changes. The Plan involves all aspects of companies' life cycle, offering support in investments, in the digitization of production processes, in the enhancement of worker productivity, in adequate skills training and in the development of new products and processes.

Incident

Any event with a detrimental effect on the security of the network, information systems or IT services.

Information Sharing and Analysis Center (ISAC)

Organizations that provide a central resource for gathering information on cyber threats and enable two-way sharing of information between the private and public sectors on incidents and threats, as well as experiences, knowledge, and analyses.



Interministerial Board for the implementation of the National Security Perimeter for Cyber

Established with DPCM of July 30, 2020, no. 131, implementing the Perimeter Decree. With the Law Decree no. 82/2021, the Working Group is established within the National Cybersecurity Agency. It is chaired by the ACN Director General and is composed of two representatives of each CIC Administration, a representative of AISE and AISI, as well as two representatives of the other Ministries concerned, who are called to participate in the meetings, also on their request, in relation to the topics to be discussed. Specifically, the CIC makes use of the Board for the exercise of the preliminary functions relating to the listing of the entities included in the Perimeter and for the purpose of supporting any other activity attributed by the Perimeter decree to the same Board.

The Board meets periodically and at least once every 6 months. It can be convened on the initiative of the Chair or at the request of at least one designated member, in relation to the discussion of specific topics. Representatives of other Public Administrations, as well as public and private bodies and operators can be called upon to participate in the meetings.

Interministerial Committee for Cybersecurity (CIC)

Committee established at the Presidency of the Council of Ministers with advisory, proposal, and supervision functions on cybersecurity policies. Among its tasks, the CIC exercises high surveillance on the implementation of the national cybersecurity strategy and promotes the adoption of the necessary initiatives to foster effective collaboration, at national and international level, among Institutions and private operators interested in cybersecurity, as well as for the sharing of information and the adoption of cybersecurity best practices and measures, for the industrial, technology, and scientific development in the field of cybersecurity. It is chaired by the Prime Minister and is composed of the Undersecretary of State for the security of the Republic, where appointed, and of the Ministers of Foreign Affairs and International Cooperation, Interior, Justice, Defence, Economy and Finance, Economic Development, Ecological Transition, University and Research, Technological Innovation and Digital Transition, and Sustainable Infrastructures and Mobility. The functions of Secretary are carried out by ACN Director General.

Interministerial Committee for the Security of the Republic (CISR)

Collegial body of the Information System for the Security of the Republic with consulting, proposal, and deliberation tasks on the guidelines and general purposes of the intelligence and security policy. Among other things, the body is responsible for defining, on a yearly basis, the intelligence goals and to decide on the allocation of financial resources between the Security Intelligence Department and the Intelligence Agencies, as well as on the related financial statements. The CISR is chaired by the Prime Minister and is composed of the Undersecretary of State for the security of the Republic, where appointed, and of the Ministers of Foreign Affairs and International Cooperation, Interior, Justice, Defence, Economy and Finance, Economic Development, and Ecological Transition. The functions of Secretary are carried out by the DIS Director General.

Internet Exchange Point (IXP)

Network infrastructure that allows interconnection among more than two independent autonomous systems, mainly to facilitate the exchange of Internet traffic.



Internet-of-Things (IoT)

Neologism referred to the interconnection of objects and devices capable of transmitting and receiving data on a network, offering a new level of interaction and remote control of devices. The fields of use are many: from industrial applications (production processes) to logistics and info-mobility, from energy efficiency to remote assistance, from environmental protection to home automation.

Internet Service Provider (ISP)

Entity who carries out an entrepreneurial activity consisting in offering users the provision of Internet services, such as connectivity and e-mail.

L

Log

A log is the result of a sequential and chronological recording of the operations carried out by a computer system (a server, a client, an application or a program).

M

Machine learning

Machine learning is a sub-category of artificial intelligence, which efficiently automates the process of building analytical models and allows machines to adapt to new scenarios on their own.

Multi-Factor Authentication (MFA)

Multi-Factor Authentication is the technology that makes it possible to recognize, through more than two authentication methods, the person who logs into a system or an application.



N

National Assessment and Certification Centre (CVCN)

Initially established at the Ministry of Economic Development, following the changes introduced by the Law Decree no. 82/2021 (article 7, paragraph 4), the CVCN is transferred to the ACN. The CVCN has the task of: verifying – also making use of accredited laboratories – the conditions of security and absence of known vulnerabilities of ICT supplies, belonging to certain categories, to be used on the ICT assets included in the Perimeter; develop and adopt cyber certification schemes – taking into account the standards defined at international and European Union level – if, for national security reasons, those already existing are not deemed adequate for the protection needs of the Perimeter.

National Coordination Centre (NCC)

According to Article 6 of the Regulation (EU) 887/2021, among other things the NCC: acts as contact point at national level to support the ECCC in fulfilling its mission and objectives; implements specific actions for which grants have been awarded by the ECCC, including through the provision of financial support to third parties and the establishment of synergies with relevant activities at national level; encourages and facilitates the participation of civil society, industry, the academic and research community and other stakeholders at national level in cross-border projects and in cybersecurity actions funded by relevant Union programmes.

National Framework for Cybersecurity and Data Protection

Operational tool for the organization of processes and strategies aimed at protecting personal data and cybersecurity of public and private organizations, published by CIS Sapienza and by the CINI National Cybersecurity Laboratory.

National Interuniversity Consortium for Informatics (CINI)

The Consortium is made up of 49 public universities and more than 1,300 Professors. It promotes and coordinates scientific, research, and transfer activities, both basic and applied, in the field of information technology, in agreement with the relevant national scientific communities.

National NIS Working Group

Collegial body envisaged by the NIS Decree and established at the ACN, aimed at ensuring the collaboration of the sectorial authorities with the competent NIS authority, for the fulfilment of the obligations foreseen by the NIS Decree. The Working Group is chaired by the ACN, as the NIS competent authority, and is composed of the representatives of the State administrations identified as sectorial authorities and of representatives of the Regions and autonomous Provinces for a maximum of two members, designated by the Regions and autonomous Provinces in the Permanent Conference for relations between the State, the Regions and the autonomous Provinces of Trento and Bolzano.



National Recovery and Resilience Plan (NRRP)

Italy's plan part of the European Next Generation EU program, developed following the economic recession caused by the COVID-19 pandemic, to foresee investments and reforms to accelerate the ecological and digital transition, improve the training of workers, and achieve greater gender, territorial, and generational equality.

National Security Perimeter for Cyber

The National Security Perimeter for Cyber is aimed at protecting national security, through a high level of security of networks, information systems, and IT services for the exercise of an essential function or the provision of an essential service of the Country ("ICT assets"). It therefore applies to ICT assets that the entities included in the Perimeter have identified as necessary for performing such essential functions or services and that could be totally interrupted or impaired in the event of an incident, with irreversible effects in terms of the integrity or confidentiality of data and information.

The entities included in the Perimeter are Public Administrations, public or private bodies or operators, based in the national territory, which perform essential functions of the State or provide essential services for executing civil, social or economic activities deemed vital for the interests of the State. The exercise of such functions/services depend on networks, IT systems, and services.

National Strategic Hub (PSN)

In accordance with the Italian Cloud Strategy, the National Strategic Hub (PSN) will be an infrastructure, distributed throughout the national territory, managed by an economic operator selected through a Cloud-oriented public-private partnership, with adequate levels of business continuity and fault tolerance.

Scope of the PSN is to host the critical and strategic data and services of the central Administrations, the local health authorities (ASL) and the main local Administrations.

NCS Administrations

Administrations that compose the National CyberSecurity Cell: the Prime Minister's Military Counsellor, Security Intelligence Department (DIS), Agency for External Information and Security (AISE), Agency for Internal Information and Security (AISI), the Ministries of Foreign Affairs and International Cooperation, Internal Affairs, Justice, Defence, Economy and Finance, Economic Development, Ecological Transition, University and Research, Technological Innovation and Digital Transition, Sustainable Infrastructures and Mobility, as well as the Civil Protection Department.



NIS national competent Authority

Authority in charge of implementing the NIS Decree, supervising its application, and exercising the related inspection and sanctioning powers. Following the changes introduced to the NIS Decree by the Law Decree no. 82/2021 (Article 15, paragraph 1, letter g), the ACN is designated as the competent NIS National Authority for the sectors and subsectors referred to in Annex II and for the services referred to in Annex III of the NIS Decree.

NIS Point of Contact (PoC)

Following the changes introduced to the NIS Decree by the Law Decree no. 82/2021 (article 15, paragraph 1, letter g), the ACN is designated as the NIS single point of contact. The PoC performs a liaison function to ensure cross-border cooperation of the NIS competent national authority with the competent authorities of other Member States, as well as with the NIS Cooperation Group – established at the EU Commission – and the CSIRT Network.

NIS sectorial Authorities

Following the changes introduced to the NIS Decree by the Law Decree no. 82/2021 (Article 15, paragraph 1, letter g), the NIS sectorial authorities are:

- the Ministry of Economic Development, for the digital infrastructure sector; IXP, DNS, TLD subsectors, as well as for digital services;
- the Ministry of Sustainable Infrastructures and Mobility, for the transport sector; air, rail, water and road subsectors;
- the Ministry of Economy and Finance, for the banking sector and for the financial markets infrastructures sector, in collaboration with the sectorial supervisory authorities, the Bank of Italy and Consob, according to methods of collaboration and information-sharing established by Decree of the Minister of Economy and Finance;
- the Ministry of Health, for health care activities, provided by operators employed or appointed by the same Ministry or affiliated with it, and the Regions and autonomous Provinces of Trento and Bolzano, directly or through the healthcare Authorities territorially competent for health assistance activities provided by operators authorized and accredited by the Regions or autonomous Provinces in the territorial areas of their respective competence;
- the Ministry of Ecological Transition for the energy sector; electricity, gas, and oil subsectors;
- the Ministry of Ecological Transition and the Regions and autonomous Provinces of Trento and Bolzano, directly or through the territorially competent Authorities, regarding the supply and distribution of drinking water sector.



O

Operators of Essential Services (OES)

Pursuant to the NIS Decree, OES are public or private entities that provide essential services for society and the economy in the health, energy, transport, banking, financial market infrastructures, supply and distribution of drinking water, and digital infrastructures sectors.

P

Public Digital Identity System (SPID)

The Public Digital Identity System is the key to access digital services of local and central Administrations. A single credential (username and password) that represents the digital and personal identity of each citizen, who is thus recognized by the Public Administration to use digital services in a personalized and secure manner.

SPID also allows access to public services of EU member States and of companies or traders who have chosen it as an identification tool.

The private sector can also benefit from digital identity by improving the user experience and the management of their customers' personal data.

Q

Quantum computing

Calculation method, implemented by computers based on quantum mechanics, capable of simultaneously processing, through parallel computing, several solutions to the same problem.



S

Security Operation Centre (SOC)

The SOC is the centre providing main services for the operational management of an organization IT systems' cyber risks. Typically, in addition to the monitoring and management of security components, the SOC performs a first evaluation and management of cyber events.

T

Technological clusters

Networks of public and private entities that operate as resource catalysts to coordinate the research world and businesses in sectors such as industrial research, training, and technology transfer.



Acronyms



Acronyms

ACN	National Cybersecurity Agency
AGCOM	Communications Authority
AgID	Agency for Digital Italy
AI	Artificial Intelligence
AISE	Agency for External Information and Security
AISI	Agency for Internal Information and Security
BGP	Border Gateway Protocol
CBM	Confidence Building Measure
CERT	Computer Emergency Response Team
CERTFin	Italian Financial CERT
CIC	Interministerial Committee for Cybersecurity
CINI	National Interuniversity Consortium for Informatics
CIS Sapienza	Research Centre of Cyber Intelligence and Information Security
CISR	Inter-ministerial Committee for the Security of the Republic
CNAIPIC	National Cybercrime Centre for Critical Infrastructure Protection of the Italian National Police
CNR	National Research Council
CONSP	Public Information Services
COR	Joint Command for Network Operations
CSIRT	Computer Security Incident Response Team
CSP	Cloud Service Provider
CV	Assessment Centre
CVCN	National Assessment and Certification Centre
CyCLONe	Cyber Crisis Liaison Organisation Network

DIE	Department for Information and Publishing
DIH	Digital Innovation Hub
DIS	Security Intelligence Department
DNS	Domain Name System
DPCM	Prime Minister's Decree
DSP	Digital Service Providers
DTD	Department for Digital Transformation
ECCC	European Cybersecurity Competence Centre
ENISA	European Union Agency for Cybersecurity
EU	European Union
G7	Group of Seven
GDPR	General Data Protection Regulation
HPC	High Performance Computing
IaaS	Infrastructure-as-a-Service
ICT	Information and Communication Technologies
IoT	Internet of Things
IPCR	Integrated Political Crisis Response
ISAC	Information Sharing and Analysis Center
ISP	Internet Service Provider
ISTAT	Italian National Institute of Statistics
ITASEC	Italian Conference on Cybersecurity
ITS	Higher Technical Institutes
IXP	Internet Exchange Point
KPI	Key Performance Indicator
MAECI	Ministry of Foreign Affairs and International Cooperation

MEF	Ministry of Economy and Finance
MiSE	Ministry of Economic Development
MITD	Minister of Technological Innovation and Digital Transition
MFA	Multi-Factor Authentication
MPA	Minister for Public Administration
MUR	Ministry of University and Research
NATO	North Atlantic Treaty Organization
NCC	National Coordination Centre
NCS	National CyberSecurity Cell
NIS	Network and Information Security
NIS PoC	NIS Single Point of Contact
NRRP	National Recovery and Resilience Plan
NSTPFT	Special Unit for Privacy Protection and Technological Fraud
OES	Operators of Essential Services
OSCE	Organization for Security and Co-operation in Europe
PA	Public Administration
PaaS	Platform-as-a-Service
PCM	Presidency of the Council of Ministers
PSIRT	Product Security Incident Response Team
PSN	National Strategic Hub
PSNC	National Security Perimeter for Cyber
RIS	Information and Security Division
SaaS	Software-as-a-Service
SMD	Defence General Staff
SME	Small and Medium Enterprise



SOC	Security Operation Center
SPID	Public Digital Identity System
TLD	Top Level Domain
UCSe	Central Secrecy Office

