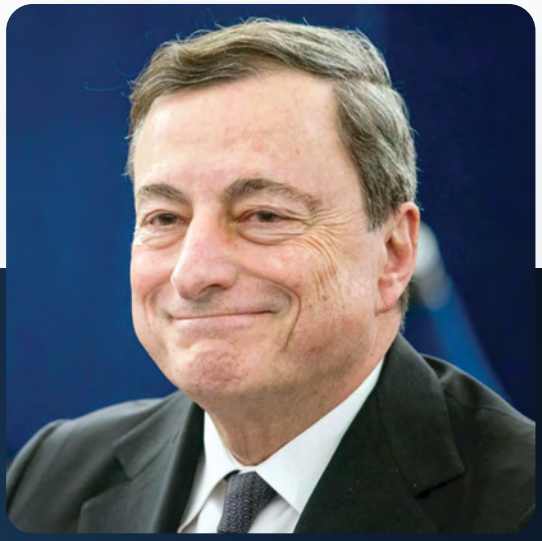
NATIONAL CYBERSECURITY

STRATEGY

2022 – 2026

Contents

Foreword



The new forms of strategic competition that characterize the geopolitical scenario, require Italy to continue and, where possible, increase cybersecurity initiatives. This, in compliance with the commitments undertaken within international organizations which Italy is a member Party of, also considering the high standards and massive investments made in this field by main international allies and partners. This highlighted the need for a total review of the concept and strategic vision of the national cybersecurity ecosystem.

The Italian cybersecurity strategy combines security and development, in compliance with the values of our Constitutional Charter. It takes into consideration the provisions of the European Union cybersecurity strategy of December 2020, the EU Strategic Compass for Security and Defence of March 2022 and the recent NATO strategic guidelines.

To achieve this new vision, Italy conceived a cybersecurity ecosystem based on the collaboration between public and private sectors. In such system, the active contribution of the Institutions is complemented by that of economic operators – primarily those entrusted with the management of infrastructures on which depend the provision of essential services by the State – the world of universities and research, and civil society as well. Everyone is called to take an active part in protecting its own IT assets, in compliance with internationally recognized rules.

A leading role is played by the producers and suppliers of ICT goods and services, who are required to place on the market products and technological solutions that meet adequate cybersecurity requirements. This will allow to increase the resilience of ICT devices and equipment, starting from 5G and the cloud, also to increase consumer confidence.

It is our firm intention to intensify technological development projects aimed at achieving an adequate level of strategic autonomy in the sector and thus guarantee our digital sovereignty. To do this, it will be crucial to allocate adequate funds, on a continuous basis.

Introduction

Connection speed, number of interactions among users, and online accessibility of data and information are not sufficient parameters to define the digital development that characterizes the contemporary age, nor are they able to describe, in its entirety, the complexity of cyberspace.

In this domain countless interconnected and communicating services meet the daily needs of our communities and carry out their economic activities: energy infrastructures, financial markets, drinking water supplies, mass transit and, last but not least, the essential functions of the State, including its defence and integrity. Systems complexity and interdependence has grown to the point of blurring the duality between the digital dimension and the real world, often making it difficult to identify borders and their respective characteristics.

If, on one hand, the relentless evolution of modern technologies makes digital "migration" more convenient, on the other hand, only the resilience and security of networks and systems on which these services are based on can guarantee, in the short term, the security for our community and, in the future, the economic development and welfare of the State.

Scientific research and industrial development determine the spread and progressive use of the so-called emerging and disruptive technologies (EDT), which include latest generation communication networks and protocols (5G/6G), blockchain, Artificial Intelligence (AI), quantum computing, High Performance Computing (HPC), Internet of Things (IoT), robotics, advanced cryptographic tools and other disruptive innovations.

The risks implied by such complexity – and the potential many economic, social and political implications – range from technological dependence and loss of strategic autonomy of the State to anthropogenic threats, in which human error is added to the initiatives of hostile actors, characterized by different degrees of sophistication and driven by different, but equally harmful, intentions. They are aimed at obtaining illicit profits (cyber-crime), gaining an information advantage for the purposes of geopolitical competition (cyber-espionage), spreading divisive and polariz-

ing narratives in adherence to specific ideologies or political motivations. No organization, even if technologically equipped and procedurally prepared, can come to completely eradicate the threats emanating from cyberspace.

This reality must be addressed by acting according to an approach that includes the adoption of risk prevention and mitigation measures aimed at enhancing the resilience of digital infrastructures. The latter not only include networks, systems and data, but also, and above all, users – be they institutional actors, private companies or citizens – whose awareness must be raised through a widespread cybersecurity culture. If today, in fact, there is a widespread perception of the risks related to physical security, for which every individual carries out, in their daily lives, actions aimed at protecting themselves and their assets, the same cannot be said for the digital dimension, which risks are not yet fully understood.

This aspect, combined with the increasingly wide availability – at relatively low costs – of offensive tools, the increased level of cyber-attacks complexity, the technical difficulty of attributing them to a certain actor, as well as the possibility of cybersecurity vulnerabilities in IT products and solutions, has registered an overall number of hostile actions in constant increase.

The recent attack trends provide evidence of economic and reputational damages to businesses, blocking of energy infrastructure operations, malfunctions of information systems used by hospitals and healthcare companies, dissemination of personal data aimed at discrediting public figures, journalists and political activists, to the point of sometimes endangering their safety.

Four essential considerations arise from this scenario:

1. one of the duties of the State is the **definition of adequate cybersecurity strategies** aimed at planning, coordinating and implementing measures meant to make the Country safe and resilient even in the digital domain, while ensuring citizens' trust in the possibility of exploiting its competitive advantages, in full protection of fundamental rights and freedoms;
2. cybersecurity, which has become a matter of strategic importance, must be the foundation of the Country's digitalization process, as an essential element of digital transformation, also with a view to **achieving strategic national autonomy** in the sector;
3. cybersecurity must then be perceived not as a cost, but as an investment and an **enabling factor for the development of the national economy and industry,** to increase the competitiveness of the Country at a global level;
4. cultural advance at every level of society, towards a **"security-oriented" approach,** must go in parallel with ensuring the security of infrastructures, systems and information from a technical point of view, as an indispensable element in protecting our value and democratic system.

Being aware of what mentioned above and of the speed and breadth of technological change that require persevering in the work of regulatory and strategic adaptation, starting from 2013, a lot has been done by our Country in the field of cybersecurity. Over time, in fact, a series of measures have been adopted substantially aimed both at acquiring, developing and strengthening the necessary national cyber capabilities, and at

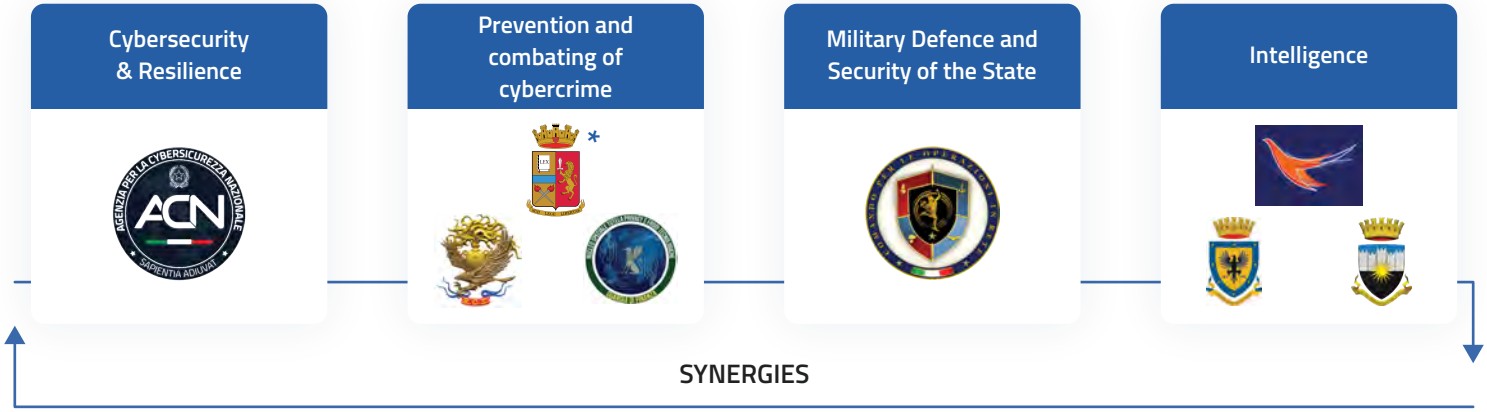
guaranteeing the institutional uniqueness of direction and action with respect to cybersecurity as an area of intervention extremely transversal and involving various stakeholders.

These goals are being pursued through the recent reform of the national cyber ecosystem, which was enacted by the adoption of the Law Decree of June 14, 2021, no. 82. The Decree established the National Cybersecurity Agency (ACN), with the aim of rationalizing and simplifying the fragmented system of skills, existing at national level – in compliance with the competences attributed to other Administrations by legislation in force – and further enhancing the cyber security and resilience, also for the purposes of protecting national security in the cyberspace.

As the National Cybersecurity Authority, the Agency has, among its tasks, that of developing the National Cybersecurity Strategy. Furthermore, pursuant to the aforementioned Law Decree, ACN is designated as the exclusive competent national authority and single point of contact (PoC) for the purposes referred to in the legislation on the security of networks and information systems (NIS), national cybersecurity certification authority, National Coordination Centre with reference to the European Cybersecurity Industrial, Technology and Research Competence Centre, and central element of the National Security Perimeter for Cyber (PSNC). These competences were previously attributed to a plurality of institutional actors.

The creation of ACN aimed at systematizing the experience gained in the previous five years of work, under the framework of the Prime Ministerial Decree of February 17, 2017 "Directive containing guidelines for national cyber protection and IT security", as well as that acquired by other countries, by recognizing cyber security and resilience as autonomous, placing them under the Prime Minister's responsibility and at the basis of the Country's digitization process, also through a broader role of coordination and close synergy with all competent Administrations. It was therefore defined a further pillar assigning it to a single government

THE TECHNICAL-OPERATIONAL PILLARS



The reorganization of the national cybersecurity architecture according to Law Decree No. 82/2021

* Postal and Communications Police Service - Central body of the Ministry of the Interior for telecommunication services' security and regularity.

entity which supplements those already existing on cybercrime prevention and countering (within the duties of National Police), military defence and security of the State in the cyber domain (pertaining to the Ministry of Defence) and intelligence (under the responsibility of the Intelligence community). This in order to ensure the coherence of initiatives, the efficiency of spending, the ability to provide a clear and updated situational awareness to the political Authority, as well as to identify a single interface in charge, in compliance with the competences attributed by the legislation in force to other Administrations, of the coordination between the public entities involved on cyber security and resilience matters, also to guarantee a common national posture consistent with cybersecurity and resilience policies defined by the Prime Minister in international fora.

To ensure cyber-resilience, the Agency aims to become a hotbed of skills, both to be employed internally as well as in other Public Administrations to raise our national cyber posture. In fact, to carry out its many institutional tasks ACN – as a structure of excellence and an asset for the Country – requires several and high-level professional skills. Starting from 2022, targeted campaigns will lead to the recruitment of experts who will reach the target of 800 units in 2027. This will also allow to stem the brain drain abroad and to return some of our talents to their homeland, envisaging a path of professional growth at the service of their Country's security.

The prevention and countering of cybercrime is provided by the Italian National Police through the Postal and Communications Police Service, within which operates the National Cybercrime Centre for Critical Infrastructure Protection (CNAIPIC) as a specialized unit for the protection of critical information infrastructures from cybercrime and as the national contact point for emergencies in the field of transnational cybercrime. Furthermore, the Central Directorate for scientific police and cybersecurity was recently established within the Department of Public Security which brings together the powers of central body of the Ministry of the Interior for the security and regularity of communications and those to fight against computer sexual exploitation crimes and prevent terrorism, previously ensured by the Postal and Communications Police Service. The Computer Emergency Response Team (CERT) of the Ministry of the Interior will operate at the Central Directorate for Cyber Security, established to ensure the security of the related networks and information systems, through the prevention and management of critical events.

Regarding the Carabinieri Corps, the Telematic Investigations Department of the Special Operational Group (ROS) is the specialized division of the Corps in the fight against cybercrime, in the study and experimentation of technologies for surfing the web and intercepting electronic flows. Within the Financial Police, such role is held by the Special Unit for the Protection of Privacy and Technological Fraud (NSTPFT) as a Special Department in charge of countering telematic and IT frauds, as well as protecting privacy.

In relation, then, to the defence and security of the State, the Ministry of Defence defines and coordinates military policy, governance and military capabilities in the cyber domain, as well as the development of cyber capabilities and the protection of its networks and systems both on the national territory and in operational theatres abroad. The Defence, through dedicated specialized divisions, conducts offensive and defensive military cyber operations in pre-defined cases.

The Ministry of Defence, therefore, ensures, even in case of cyber crises (both national and international), all the services and activities necessary, on the one hand, to guarantee the protection, resilience and efficiency of military networks and infrastructures. and, on the other hand, to develop their own peculiar abilities necessary for the implementation of support, defence, reaction and stabilization activities.

The intelligence collection and analysis, aimed at protecting Italy's political, military, economic, scientific and industrial interests, is entrusted to the Intelligence Community, which for these purposes also provides, even through the conduct of cyber operations, for the activities aimed at the detection and systematic monitoring, prevention and contrasting of the most insidious cyber threats perpetrated in or through the digital environment.

An important role, transversal to the four pillars, is also constituted by cyber diplomacy as the use of diplomatic tools and initiatives to achieve national interests in the cyberspace and as part of the broader foreign policy activities considering the impact of technology on international relations. This activity is headed by the Cyberspace Policies and Security Unit of the Ministry for Foreign Affairs and International Cooperation (MAECI).

Beyond the competent institutional actors – which do not end with those mentioned above[1] – this strategy is inspired by a "whole-of-society" approach, which also involves private operators, the academic and research world, as well as civil society as a whole and citizenship. In this strategic vision, in fact, the latter is conceived not only as an indirect beneficiary of the measures envisaged in the Implementation Plan but also as an active part. Indeed, the ultimate goal of national cybersecurity can only be achieved with the contribution of all components of the social fabric, none excluded.

[1] A description of the national cybersecurity ecosystem can be found in the section "National Governance" of the Strategy's Implementation Plan.

#1

New challenges to face

#1

New challenges to face

The ongoing evolution of technology that has shaped our current society keeps raising new risks as it continues to develop, along with most sophisticated attack techniques. However, such a scenario doesn't always match with the society's cybersecurity awareness level.

Among those risks, the systemic ones are related to:

- cyber-attacks due to cybercriminals, hacktivists or coordinated state campaigns which exploit software errors, misconfigurations or protocols and/or human weaknesses to steal data or damage IT systems. This is the case of ransomware campaigns directly affecting the provision of services of a country (including the essential ones) and, as cascading effects, its GDP and its reputation;

- technology developed and produced by large companies, sometimes controlled or in any case influenced by the host-country governments in which they are based. This can lead to an interference in the supply chain, both in terms of availability on the market of the related components and of their own reliability;

- disinformation campaigns, fake news, deepfake and spreading misinformation through the cyber domain to manipulate and polarize the public opinion which finds itself overwhelmed by fast-moving and horizontal information coming from a massive number of sources, altering our sense of reality.

Given those risks, this strategy aims to target the strengthening of our resilience in the digital transition, by fostering the safe use of technologies essentials for our present and future economic prosperity, the achievement of cybersecurity strategic autonomy, the cyber crises management in complex geopolitical scenarios, as well as anticipating the evolution of cyber threats and tackling the spread of online disinformation, while respecting human rights, our values and principles.

NEW CHALLENGES TO FACE

Ensure cyber resilience in the public sector and industry's digital transition

There can be no digital transition without an adequate resilience to cyber-attacks and incidents. Cybersecurity of digital assets and services is, indeed, an essential condition for their usability by citizens, who will thus not only be encouraged to use them but will do it trustfully knowing that their data are protected. It goes without saying that resilience shouldn't be considered just as a technical circumstance but also as part of a broader vision which includes the cybersecurity culture and the availability of qualified workforce. Without the latter, indeed, there would not be any chance to achieve a real digital sovereignty. Moreover, another challenge adds to this one, the gender issue, as there is a low number of women who choose computer studies or STEM disciplines (Science, Technology, Engineering and Mathematics) and even fewer who specialize in cybersecurity.

National and European digital strategic autonomy

At EU level, excessive fragmentation and competition among Member States has been a major barrier to the development of "made in EU" technology and the establishment of large digital service providers across the Union. As a consequence, the EU and Italy found themselves in a position of technological dependency on other countries leaders in the production of software and so-called emerging disruptive technologies (EDTs) such as Artificial Intelligence and quantum computing. This also has inevitable consequences on the possibility of having direct control over the data stored, processed and transmitted through these technologies. Therefore, achieving an effective technological autonomy will allow the implementation of adequate information sovereignty policies.

Anticipating the evolution of cyber threats

Bearing in mind the experience acquired in the implementation of the "National Strategic Framework for Cyberspace Security" (2013) and the "Italian Cybersecurity Action Plan" (updated in 2017), as the first national cybersecurity strategies, it became clear the need to focus on active defence tactics – in addition to the best practices on cyber-resilience and due diligence – aimed at increasing the costs of cyber-attacks to make them disadvantageous. That implies a radical change of approach. While it's true that chasing the threat is not a winning strategy, it is also true that keeping up with it is no longer enough. It's necessary, as far as possible, to anticipate, predict and prevent it and to mitigate its impacts as much as possible.

Cyber crises management

The latest international tensions have highlighted the primary importance of having an effective cyber crises management mechanism supported by the contribution of all the entities involved and by which activities can be graded basing on pre-set cyber threat scenarios – ranging from alerts in view of possible large-scale cyber events to their actual occurrence – which trigger the prompt application of common tools, procedures and language norms. The speed at which cyber events can occur and follow one another, especially in complex geopolitical scenarios, asks for a continuous coordination among all the public and private stakeholders involved, as well as readiness in the deployment of a pre-set of measures.

Tackling online disinformation also in relation to hybrid threats

The digitalization of any aspect of social life, pivotal force behind the economic and social growth of the Western democratic systems, is more and more exploited to influence and interfere (or attempt to do it) in the exercise of fundamental freedoms, especially just up against crucial events for these democratic systems, such as elections, decision-making processes on issues of strategic importance or international crises. The increasingly massive use of online disinformation, especially when highly organized, demands for synergical and coordinated preventive and countering measures carried out at both national and international level to hinder any attempt to undermine the value system on which our Country is based.

THE TOOLS FOR THE IMPLEMENTATION OF THE STRATEGY

To implement this strategy and face the aforementioned challenges, a solid investments program and financial leverages are envisaged.

Beyond the financial tools already allocated to the Administrations in charge of cybersecurity, specific funds may also be made available annually as part of the national budget, to support the implementation of specific actions. To that end, a percentage of annual gross investments will be reserved on an annual basis. These leverages may also include tax breaks for businesses or the provision of more beneficial tax treatments for the creation, for example, of a "National Cybersecurity Campus" and the related national "hubs".

National funding
Percentage (1,2%) of annual gross investments

These funds will be dedicated to specific projects aimed at achieving digital technological autonomy, as well as further strengthening the cybersecurity of national information systems.

Furthermore, the National Cybersecurity Agency will manage European funds to implement specific actions as National Coordination Centre, pursuant to the Law Decree of June 14, 2021, no. 82, as well as article 6 of Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021, establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, which will manage the cybersecurity-related financial support from **Horizon Europe** and the **Digital Europe Programmes.**

Horizon Europe
2021-2027 budget:
EUR 95,51 billion

Leading EU funding programme to facilitate collaboration and to bolster the effects of research and innovation in the development, support and implementation of EU policies, while addressing global challenges. It supports the creation and better dissemination of top-level know-how and technologies.
It also aims to create new jobs, fully engage the EU talent pool, stimulate economic growth, promote industrial competitiveness and maximize the impact of investments within a strengthened European research domain.

Digital Europe
2021-2027 budget:
EUR 7,59 billion

First European funding programme to expand the digital skills of citizens and businesses and to speed up the economic and social recovery.
The programme, which aims to bridge the gap between research on digital technologies and market uptake, supports projects in five key capacity areas:

- supercomputing
- artificial intelligence
- cybersecurity
- advanced digital skills
- ensuring a wide use of digital technologies across the economy and society.

These investments support the efforts to make EU greener and more digital, while strengthening its resilience and digital sovereignty.

THE NATIONAL RECOVERY AND RESILIENCE PLAN: INVESTMENT 1.5 “CYBERSECURITY”

Another strategic tool to address the aforementioned challenges is the **National Recovery and Resilience Plan (NRRP).** As part of Mission 1 "Digitalization, Innovation, Competitiveness, Culture and Tourism", activities aimed at achieving the digitalization of the Public Administration are included, such as the implementation of a National Cloud and the digitalization of processes and services for citizens. The fulfilment of such actions will lead to an enhanced national digital infrastructures and services’ resilience capabilities. In addition, the Investment 1.5 "Cybersecurity" – with EUR 623 million budget – assigned to the National Cybersecurity Agency as implementing entity, is intended to implement specific actions for the creation and development of cutting-edge cyber risk management services, in close cooperation at national and international level with all the main partners of Public Administrations, businesses and technology suppliers. That to achieve a national technological autonomy by placing cybersecurity and resilience at the foundation of the digitalization of the Public Administration.

NRRP (digital transition)
2021-2026 budget: EUR 122,6 billion

With NextGenerationEU (NGEU), the EU envisages investments and reforms to boost ecological and digital transitions, improve the professional development of female and male workers and achieve a better gender equality. Italy is the first beneficiary of the two main NGEU instruments: the Recovery and Resilience Facility (RRF) and the Recovery Assistance for Cohesion and the Territories of Europe (REACT-EU). To access the funds under the RRF Member States are asked to prepare their National Recovery and Resilience Plans (NRRP). Our NRRP is divided into six Missions and 16 Components.
The six Missions are: digitalization, innovation, competitiveness, culture and tourism; green deal and ecological transition; infrastructures for a sustainable mobility; education and research; inclusion and cohesion; health.

The implementation plan, in agreement with the Department for Digital Transformation (DTD) as the investment owner, is organized into three main areas of intervention and will involve all the main public and private cybersecurity national stakeholder, in accordance with the NRRP technical-organizational rules:

01 **174 M€**

NATIONAL CYBERSECURITY SERVICES

By contributing to ACN activation and full operation, the networks and services that will be implemented will enhance national prevention, monitoring, response and cyber-threats mitigation capabilities;

02 **301.7 M€**

ACTIONS TO ENHANCE PUBLIC ADMINISTRATION'S CYBER-RESILIENCE

Ensuring adequate cybersecurity capabilities for Public Administration represents the foundation of a safe national digital transition, ensuring appropriate levels of security for citizens' data and services;

03 **147.3 M€**

CYBERSECURITY SCREENING AND TECHNOLOGICAL CERTIFICATION LABORATORIES

the achievement of a national technological autonomy necessarily involves the strengthening of national technological screening and certification capacities, in close collaboration with industry and academia.

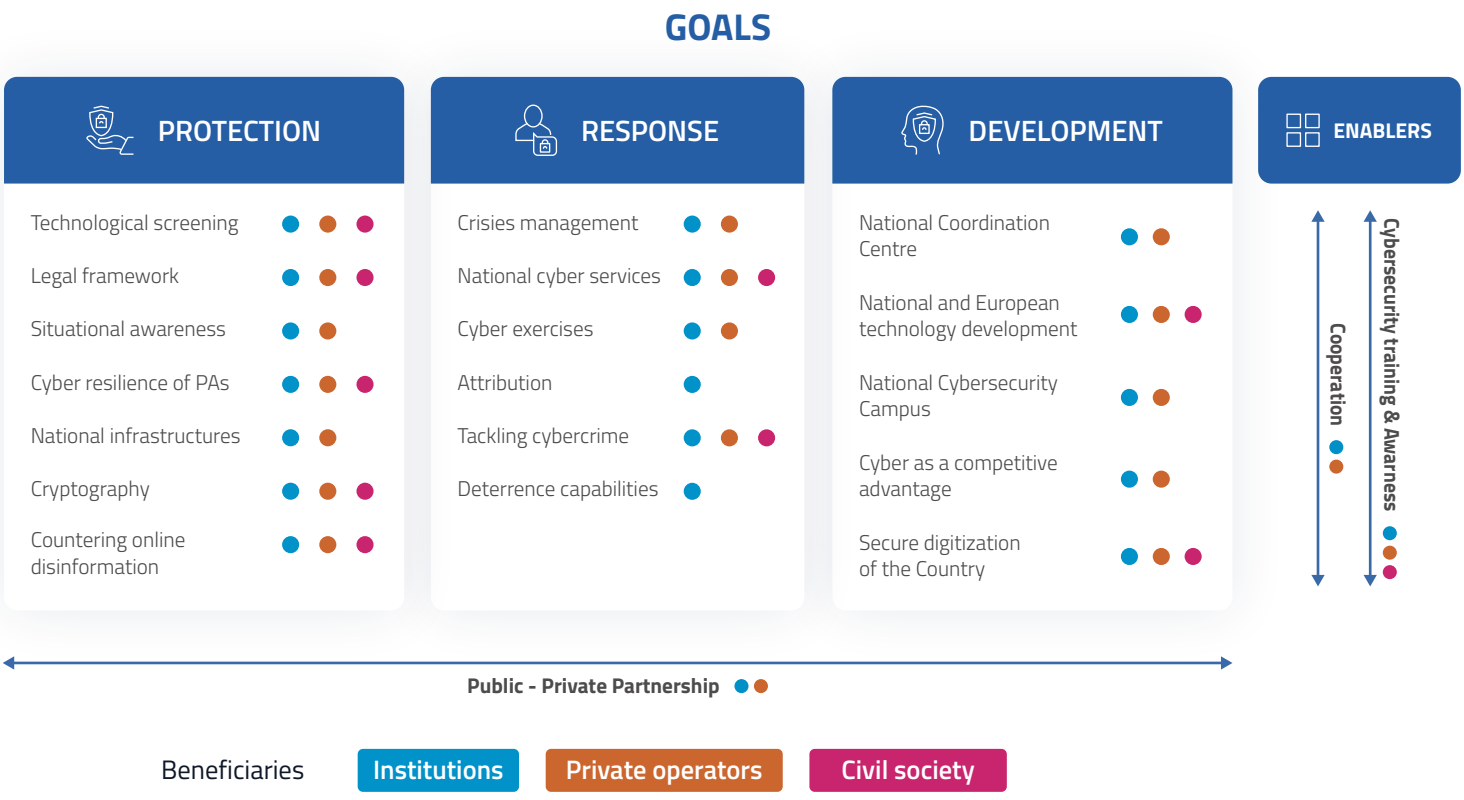
#2

Our vision: the goals to reach

#2

Our vision: the goals to reach

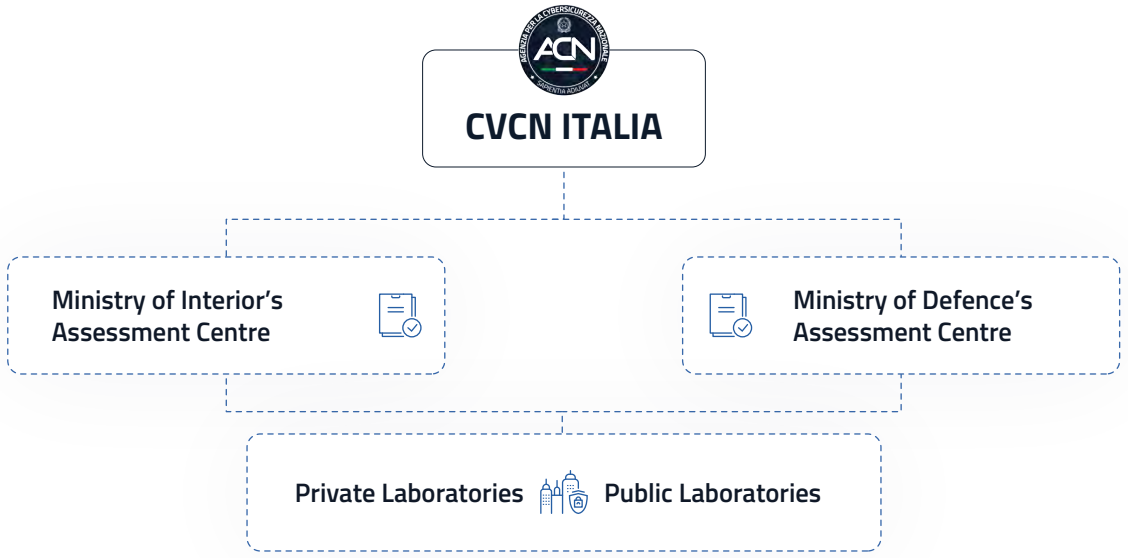
To better face the above challenges for the Country, three fundamental goals have been identified - protection, response and development – together with the related measures to ensure the concrete implementation of the strategy, grouped by thematic areas as regards organizational, policy and operational aspects. For each measure, associated with the most characterizing goal, the actors responsible for the implementation and all the other subjects involved are indicated, excluding the direct beneficiaries of the measures.



Referring to the Implementation Plan for a more detailed description of the measures, we intend to provide below a comprehensive overview of the salient aspects and related strategic vision underlying it.

1. PROTECTION GOAL

The **protection** of national strategic assets, through a systemic approach aimed at managing and mitigating risk, consisting in both a regulatory framework and measures, tools and controls that can enable a resilient digital transition in the Country. Relevant importance has the development of strategies and initiatives for verifying and assessing the security of ICT infrastructures, including procurement and supply-chain aspects with a national impact.



To ensure an effective and lasting level of protection it is, in-fact, essential:

A. the **strengthening of ACN National Assessment and Certification Centre's capacities (CVCN)** and of the Ministry of Interior and Defence's **Assessment Centres (CV)** for their respective areas of competence, as well as the integration with a network of Accredited Test Laboratories, which will allow the development of national vulnerability assessment capabilities for advanced technologies to serve the Country's most critical assets.

B. the **definition and maintenance of an updated and coherent national legal cybersecurity framework**, which considers the orientations and developments at the European and international level. This system does not only include the regulatory level but also a set of guidelines, certification schemes and sectorial policies addressed to public entities and private operators. In this context it is of primary importance:

- the *support to the development of European and international cybersecurity certification schemes and standards;*
- the *promotion of the use of European cybersecurity certification schemes* by specialized Italian companies to achieve a competitive advantage on the market;

- the *adoption of guidelines for Public Administrations* based on a "zero trust" approach as a new model for cyber risk management, so that their networks, systems and services can meet high cybersecurity standards;
- the *promotion of the inclusion of cybersecurity requisites in ICT procurement activities* of Public Administrations;
- the *definition of a national policy on coordinated vulnerability disclosure* to keep our Country up with its counterparts and the international community.

C. the **in-depth knowledge of the cyber threat scenario** along with adequate technical tools, specialized skills and operational capabilities of the different entities involved. The *further strengthening of situational awareness* through the *continuous cyber events monitoring* and the timely sharing of related findings, according to the specific areas of competence, constitutes a necessary condition for increasing our national defence, resilience, counter-cybercrime and cyber intelligence capabilities. To this end, the continuous public-private and public-public information sharing is essential, also through secure communication channels and an integrated cyber risk management system to identify and analyse vulnerabilities, threats and risks in a forecasting and programmatic way.

D. the **enhancement of Public Administration cyber capabilities' maturity level**, ensuring a secure and resilient digital transformation. To this end, the Public Administration's migration to the Cloud, both towards Public Cloud technologies and the creation of a National Strategic Hub (PSN) represents a fundamental element for ensuring appropriate warranties to the Country's technological autonomy. The reinforcement of Public Administrations' computational infrastructures also allows them to reduce the need for cybersecurity and IT governance experts. The *migration to Cloud technologies,* whether the PSN or the Public Cloud, will be guided and controlled by a risk management methodology whose main element is the classification of Public Administration's data and services (i.e. ordinary, critical and strategic). In this regard, *interventions to enhance cyber risk identification, monitoring and control for the Public Administration will also be coordinated.*

E. the ***development of protection capacities for national infrastructures***, also through ad hoc implementing programs with industry, including:

- Border Gateway Protocol (BGP) configurations monitoring through the development of procedures, processes and tools in cooperation with national Internet Exchange Points (IXPs) to increase the resilience of national BGP infrastructures;
- a national DNS resolution infrastructure with web browsing protection services for a safer use of the Internet by the Public Administrations;

- the monitoring of vulnerabilities and misconfigurations of Public Administration's digital services, both at DNS application and configuration level to proactively reduce potential attack surfaces;
- the monitoring of Public Administration's e-mail domains configurations supporting and facilitating the application of the best security configurations against phishing or related abuses.

F. the ***promotion of the use of cryptography*** as a cybersecurity tool fostering its commercial use throughout the entire ICT systems and services lifecycle in compliance with security and privacy protection principles and with those defined by national and European legislation. In this context and in specific sectors, ACN, together with the other Administrations, aims to realize national encryption technologies/systems, which will be based on the creation of a specific national ecosystem for their maintenance and development.

G. the ***implementation of a national coordination action*** consistent with similar European initiatives and in synergy with like-minded countries to prevent and counter ***online disinformation*** which, by exploiting the inherent features of the cyber domain, seeks to influence the political, economic and social processes of the Country.

2. RESPONSE GOAL

The **response** to national cyber threats, incidents and crises, through the deployment of enhanced national monitoring, detection, analysis and response capabilities and the activation of processes which involve all the stakeholders included in the national cybersecurity ecosystem. Indeed, a timely and resolved response must be based on:

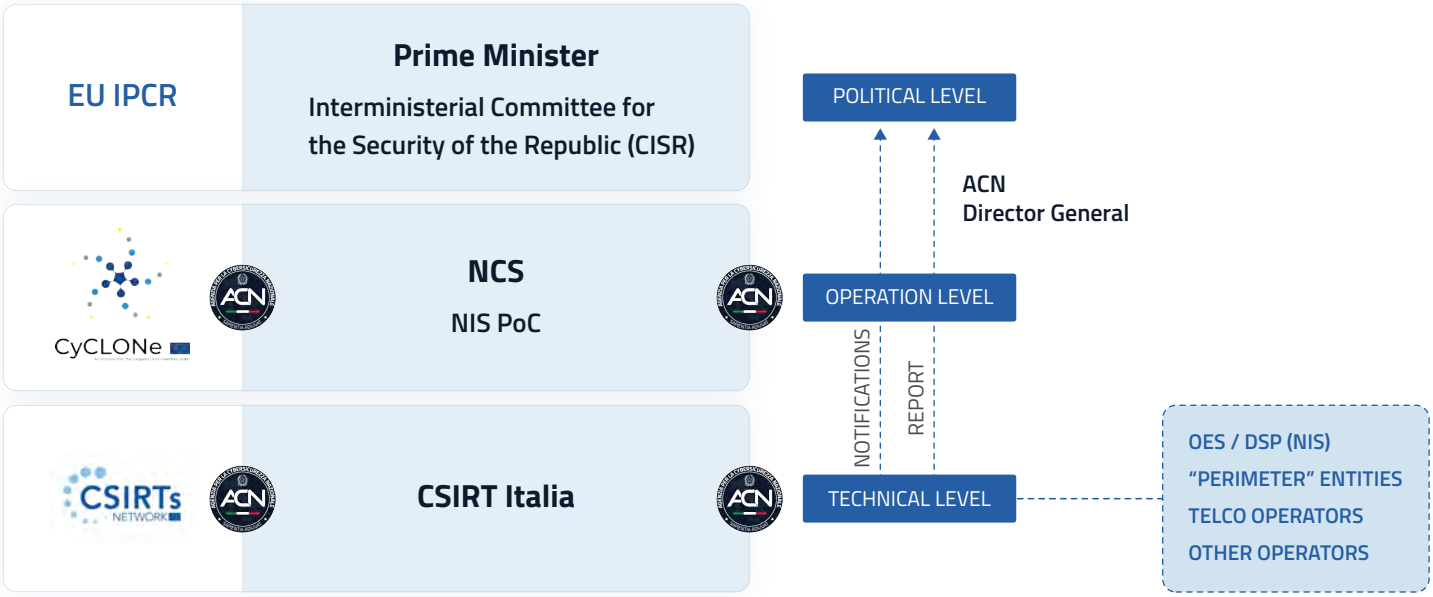
A. a ***cybersecurity crises management system*** at national level – guided by the National CyberSecurity Cell (NCS) – and transnational level, based on consolidated collaboration procedures between public and private entities supported by continuous sharing of information and knowledge, also through national and transnational networks and infrastructures. In that field, it should be ensured:

- the development of a *continuous coordination system* among all the NCS Administrations for the timely and synergic cyber crises management and response;
- the *regular update of operating procedures* on cyber-threat response measures for Prime Minister's resolutions in the event of cyber crises, according to the legislation in force, and for the effective implementation from all the actors involved;
- a *timely institutional communication* in the event of relevant cyber incidents or crises, as well as when awareness campaigns towards civil society are deemed necessary.

Focus box - The management of cybersecurity incidents and crises

The national cybersecurity incident and crises management architecture is fully compliant with the Recommendation (EU) 2017/1584 (so called Blueprint), with the:

- **political level**, represented by the Prime Minister, the Undersecretary of State for the security of the Republic, if appointed, and by the Interministerial Committee for the Security of the Republic (CISR);
- **operational level**, made up by the NCS, supported by ACN in connection with the competent units of NCS Administrations;
- **technical level**, carried out by the national CSIRT, in cooperation with the other technical units of NCS Administrations.



ACN, embedding the national CSIRT, the NIS PoC and the NCS, performs two of the three aforementioned levels necessary to achieve an adequate national prevention and response to potential cyber-attacks, by supporting the political level through ACN Director General, as cyber crises coordinator. This synergical architecture aggregates and correlates the information, alerts and notifications acquired by the operational and technical levels if a cyber event requires a NCS activation and its potential escalation in its alert state, up to cyber crisis status. Such a process is fully aligned with other European and international counterparts.

Moreover, this organization is integrated with the liaison role of ACN towards the European Union. At the EU level, indeed, ACN participates in the CSIRT Network and in the Cyber Crisis Liaison Organisation Network (CyCLONe). Specifically, CyCLONe aims at contributing to the implementation of the European Commission's Blueprint for rapid response to large-scale cross-border cyber incident or crisis, supporting Member States national authorities in charge of cyber crisis management and linking European political level – the Council of the EU, also through the Integrated Political Crisis Response mechanisms (IPCR) – with the technical one embodied by national CSIRTs and the EU CSIRT Network. CyCLONe's tasks, on voluntary basis, include crises management preparation, situational awareness and cooperation, as well as the support to national and EU political decision-making.

B. the integration of ***national cybersecurity services*** in the following fields:

- *threat detection* through the creation of an "Hyper SOC" that is a collection, correlation and analysis system of relevant events coming from Security Operation Centres (SOC) and *Internet Service Providers (ISP)* by specific agreements, to early detect potential complex attack patterns that could turn in significant emerging threats;
- *ensure and facilitate unitary cybersecurity incident notifications to the Computer Security Incident Response Team (CSIRT)* to make its response and timely warning capabilities more effective;
- *incident response* through the creation of a sectorial CSIRT/Computer Emergency Response Team (CERT) network, federated with the "CSIRT Italia" for sharing procedures, information and support in case of emerging threats and incidents response;
- *information sharing* through the creation of a central Information Sharing and Analysis Centre (ISAC) established at ACN and potentially integrated into a network of sectorial ISACs developed through public-private initiatives, which can bolster the dissemination and application of higher added-value information to enhance the Country's level of cyber resilience, such as sectorial best-practices, guidelines, security alerts and recommendations;
- *incident response companies' qualification* which can provide support to the CSIRT Italia in case of multiple and systemic cyber incidents.

These capabilities fully complement the "European Cyber Shield" initiative as part of the "EU's Cybersecurity Strategy for the Digital Decade" and will take advantage of the most recent artificial intelligence (AI) and machine learning technologies provided by an ad hoc "High Performance Computing" (HPC) centre and by integrated national cyber-risk monitoring and analysis systems. Italy will guide in Europe the process of development and integration of these new technological tools within Member States.

C. the organization of periodic ***cybersecurity exercises*** also within the scope of the National Security Perimeter for Cyber, as well as the *promotion and participation in the European and international ones.*

D. the ***definition of a national posture and procedure for the attribution*** of malicious cyber activities, which defines the different actors involved and their roles. Our Country, as a member of the EU and NATO, is, indeed, asked to bring its contribution to discuss the application of response measures to malicious cyber activities – including joint statements – among those defined by the EU Cyber Diplomacy Toolbox and the NATO Guide for Response Options to Malicious Cyber Activities. In any case it is important to highlight that, as already acknowledged in EU and NATO policy documents, attribution remains a national political decision of Member States.

E. the ***tackle of cybercrime***, which includes the prevention and countering of organized or terroristic criminal actions to the integrity of digitized critical infrastructures that supply essential public services; the tackle of financial cybercrimes and illicit actions against financial infrastructures; the investigative and informative activities, in close cooperation with the competent branches of the Italian National Police, applied to public order and counter-terrorism in the cyber domain; the safeguard of individuals, and above all the minors, from virtual or online attacks to individual and gender freedom, security and safety, privacy, honour and reputation.

F. the ***strengthening of cybersecurity deterrence capabilities.***

3. DEVELOPMENT GOAL

The conscious and safe **development** of digital technologies, research, and industrial competitiveness able to respond to the market needs. The entirety of centres of excellence and companies that together with academia compose the research and development fabric is, indeed, an essential asset for our Country with significant growth potential. Several tools and initiatives have been launched in recent years to support the development of national research ecosystem's capabilities as well as digital transformation and technological innovation, including those envisaged by the NRRP by the latest budget laws and by the National Plan Industry 4.0. To further increase this commitment, it is therefore essential:

A. the role of the **National Coordination Centre (NCC)** which contributes to the development and enhancement of a European and national technological, strategic and digital autonomy while supporting the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC) in fulfilling its mission and objectives. That, coordinating relevant activities on research and development and facilitating synergies between industry and the academic and research communities to projects and public-private partnerships in cybersecurity funded by relevant Union programmes. To that end, the involvement of national *Competence Centres and Digital Innovation Hub (DIH)* is crucial.

B. the **development of national and European technology** reducing the dependence on non-EU technologies through the implementation of specific projects to be carried out – thanks to dedicated national and European funds – within a "National Cybersecurity Campus" that will also include the *technological Clusters* operating on that field. This technology will foster the development of a competitive national and European industry also through the virtuous specialization of innovative start-ups and small and medium-sized enterprises (SMEs) able to provide highly secure enabling technologies and services mainly for digital critical infrastructures.

C. the ***establishment of a "National Cybersecurity Campus"*** which, by systematizing skills and resources from the Public Administration, industry and the academic and research community, provides all the necessary technological infrastructures for carrying out research and development activities in the field of cybersecurity and digital technologies such as artificial intelligence, quantum computing, cryptography and robotics. Its creation allows the gradual achievement of a greater national strategic autonomy on cyber technologies, supporting the development and production of national software and hardware to be used in strategic relevant networks and systems. The Campus is therefore conceived as an incubator of skills and technologies in which young talents and start-ups can interact with large companies and all the various national entities operating in the cybersecurity field. That is why the Campus must have a "widespread" structure in which, alongside a central "hub", there are local branches throughout the Country.

D. the introduction of new incentive mechanisms and solutions to keep supporting the **industrial, technological and research development** particularly regarding skills development and technology transfer (especially in advanced cybersecurity sectors).
This also with the aim to:

- continue *fostering the competitiveness of the Country's production system,* supporting companies in their digital and ecological transition, *facilitating their internationalization and attracting investments;*
- *develop highly reliable ICT products and services* also by encouraging the establishment of *Product Security Incident Response Teams (PSIRTs)* by private operators to increase their ability to manage vulnerabilities of ICT products.

E. the continuous ***drive towards technological innovation and digitalization*** *of the Country's Public Administration and productive fabric* ensuring steady compliance with cybersecurity principles and making use of *NRRP funds.* This goes hand in hand with the promotion of initiatives aimed at strengthening Italy's industrial and technological autonomy.

ENABLERS

To effectively achieve the aforementioned goals it is crucial to refer to three **enabling factors** – training, promotion of a cybersecurity culture and cooperation – which, given their wide scope, are necessarily related to the goals outlined above and are essential for their full implementation.

Firstly, **cybersecurity training** with a specific focus on new technologies. The development of new initiatives and the strengthening of the existing ones must be based on the increased need to foster the creation of a solid national workforce made up of experts and young talents with the necessary skills and knowledges on ICT and cybersecurity, for the benefit of Italian companies and administrations. This must be done through:

- incentive mechanisms that foster the progressive *familiarization of students with new information technologies*, with an educational and cultural approach, other than technical and practical. It is appropriate to introduce information technology as a discipline, in all levels of the educational system, from primary school to university and, from upper secondary school onwards, in all contexts, including generalist ones and those oriented towards non-technical professions;
- incentive mechanisms that foster the progressive *familiarization of students with new information technologies* supporting the attractiveness of technical and scientific careers (also to bridge the gender gap). Also in this case, specific levels of action are needed for: the technical and professional educational paths for secondary school; the *Higher Technical Institutes (ITS)*; the degree courses with professional orientation recently established by law; the degree courses, post-graduate and master's degrees and PhD. Specific attention also goes to the ITS and to the degree courses with profes-

sional orientation which, with the collaboration of industry, could facilitate the transition to the labour market and the modulation of the educational paths;

- the *continuous teaching update and the preparation of the professors* at all school and university levels *so that the educational offer can keep pace with the labour market needs* on the basis of the well-known bond between development and security;
- the *allocation of funds for specialized and professional training for the public and private sectors* to be carried out in a continuous and multilevel way to support the growth and qualification of human resources operating in the cybersecurity field, and to achieve a national digital skills sovereignty;
- the *creation of a national skills certification system* (both at school/university, and work) through ad-hoc training courses previously approved by ACN;
- *specific training courses for Public Administrations and private entities' employees, including SME*s, starting with top managers, to raise their awareness on the importance of conceiving cybersecurity as an investment rather than an expense;
- the *enhancement of cyber diplomacy skills* through targeted courses for the diplomatic staff working in the main international cybersecurity organizations, to keep up with other European and non-European counterparts.

These actions will be developed in close cooperation with universities, upper secondary schools, Regions – on the basis of specific agreements – as well as with Public Administrations and private entities.

Another enabling factor, along with training needs, is the **promotion of a cybersecurity culture** to increase the awareness of the public and private sector, and of civil society, on cyber risks and threats which include not just cyber-attacks but also the spread of fake contents and cyberbullying which, although not new, does not cease to create social alarm.

In this regard, it is therefore important that public entities, private operators, and civil society perceive their active and responsible role within the Country by implementing safe and virtuous behaviour in cyberspace. This must happen:

- through a *widespread digital education program* – to be developed also online – for the sake of the community and aimed at the adoption of good practices and the acquisition of the capabilities to check online contents and information as well as "fake news" indicators;
- *within public and private organizations* through a strong awareness campaign for the employees – starting from top levels to the entire line – not only to promote an internal "cyber hygiene" but to increase the perception of the organization's security needs and the threats to which it is exposed, as well as to implement the most effective preventive actions;
- promoting the responsible management of the so called "residual risk", also by providing for the adoption of self-assessment tools based on specific "cyber index", which allow organizations to independently manage the level of exposure.

Finally, there is **cooperation** to be increased:

- at the national-governmental level, in public-private and public-public interaction, as well as with the academic and research community. In this context, it is envisaged the creation of permanent operating working groups among the entities included in the Perimeter, divided by sector and depending on matters and needs, to increase the synergies between Public Administrations and industry;
- internationally, proactively participating in European and international initiatives and promoting bilateral collaborations.

At national level, each part of the cybersecurity ecosystem is not only responsible for security in the digital domain for its areas of competence but is the bearer of experiences and knowledge crucial to increase the capacity to prevent and tackle threats, to promote know-how, technologies and human resources' transfer, as well as to allow innovative companies to expand more easily on the market. At international level, Italy collaborates in promoting respect for human rights, fundamental freedoms and democratic values in the cyber domain to ensure that it remains a global, open, stable and secure space in which international law and shared principles are respected. To this end, our Country participates in the main cooperation, cyber diplomacy and *capacity building initiatives* towards partner countries which are experiencing a rapid digital development. This also through the *implementation of OSCE's confidence building measures (CBMs)* to avoid the emerging of political and military tensions stemming from the use of ICTs. In addition, Italy shares the methodologies and tools for cyber-attacks deterrence and response defined within the EU and NATO. In this context, the participation in international initiatives and the prosecution of dialogues and relations with like-minded countries are crucial elements *to further strengthen the positioning of our Country,* to foster the exchange of knowledge, and to promote the internationalization of national cybersecurity companies.

Transversal to the aforementioned goals of protection, response, and development, as well as to the enabling factors of training, promotion of the cybersecurity culture, and cooperation, is the **Public-Private Partnership (PPP)** that fully permeates this strategy based, as already said, on a "whole-of-society" approach in which the public sector acts synergically with the industry, civil society, academia and research, as well as the media, families, and individuals, to strengthen the cyber resilience of the Country and the society as a whole. Moreover, cyberspace is made up of ICT products and services mainly produced or provided by private entities. For this reason, this strategy cannot exclude the close cooperation and continuous public-private consultation which translates into a series of structured actions, such as cyberspace monitoring through the cooperation of SOCs, incidents mitigation through CSIRTs collaboration and qualified incident response, the network of test laboratories, as well as training and awareness dissemination.

METRICS AND KEY PERFORMANCE INDICATORS

Finally, the strategy cannot be considered complete without a set of ***metrics*** and ***Key Performance Indicators (KPIs)*** as tools to measure not only its concrete implementation but also all of the related actions, whose actual effectiveness and impact would otherwise remain unexplored.

Acronyms

Acronyms

ACN	National Cybersecurity Agency
AI	Artificial Intelligence
BGP	Border Gateway Protocol
CBM	Confidence Building Measure
CERT	Computer Emergency Response Team
CISR	Inter-ministerial Committee for the Security of the Republic
CNAIPIC	National Cybercrime Centre for Critical Infrastructure Protection of the Italian National Police
CSIRT	Computer Security Incident Response Team
CVCN	National Assessment and Certification Centre
CV	Assessment Centre
CyCLONe	Cyber Crisis Liaison Organisation Network
DIH	Digital Innovation Hub
DNS	Domain Name System
DSP	Digital Service Providers
DTD	Department for Digital Transformation
ECCC	European Cybersecurity Competence Centre
EDT	Emerging and Disruptive Technologies
EU	European Union
GDP	Gross Domestic Product
HPC	High Performance Computing
ICT	Information and Communication Technologies
IoT	Internet of Things
IPCR	Integrated Political Crisis Response
ISAC	Information Sharing and Analysis Centre

ISP	Internet Service Provider
ITS	Higher Technical Institutes
IXP	Internet Exchange Point
KPI	Key Performance Indicator
MAECI	Ministry of Foreign Affairs and International Cooperation
NATO	North Atlantic Treaty Organization
NCC	National Coordination Centre
NCS	National CyberSecurity Cell
NGEU	Next Generation EU
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
PPP	Public-Private Partnership
PSIRT	Product Security Incident Response Team
PSN	National Strategic Hub
PSNC	National Security Perimeter for Cyber
REACT-EU	Recovery Assistance for Cohesion and the Territories of Europe
RRF	Recovery and Resilience Facility
ROS	Special Operations Group of the Carabinieri Corps
SME	Small and Medium Enterprise
SOC	Security Operation Center
STEM	Science, Technology, Engineering and Mathematics


REPUBBLICA ITALIANA
AGENZIA PER LA CYBERSICUREZZA NAZIONALE
ACN
SAPIENTIA ADIUVAT