2024 YEAR IN REVIEW

2024 YEAR IN REVIEW

TABLE OF CONTENTS

PREFACE

The 2024 Year in Review offers an opportunity to grasp the complexity of the daily efforts of the Italian National Cybersecurity Agency (ACN) to protect the Nation's cybersecurity.

Although public debate on cybersecurity tends to focus mainly on the numerous cyberattacks – most of which have no real consequences – the Review reveals how cybersecurity is a complex challenge. Its success – never definitive – depends on multiple factors and on actions operating across various levels: strengthening critical public and private digital infrastructures; raising awareness and providing training to reinforce the "human factor," the first and indispensable line of defense for networks and IT systems; and improving the capacity to respond to cyberattacks. Finally, it is crucial to enhance the ability to generate technological innovation through investments in research and development as well as partnerships with universities, research institutions and businesses.

The Government has supported the Agency's efforts throughout 2024 in all the dimensions in which the cyber threat unfolds.

First of all, it did so by updating the regulatory framework: Law no. 90/2024 – initiated by the Government and approved by Parliament with near-unanimous support, thanks to a constructive engagement with opposition parties – introduced significant innovations, such as the strengthening of cybersecurity requirements in public procurement, a smoother interaction between the ACN, the Police forces and the Judicial Authority in the event of cyber incidents and the extension of key cybersecurity obligations to public entities previously excluded from the relevant legislation, such as Regions, Metropolitan Cities, Municipalities and Local Health Authorities. Moreover, the entry into force of Legislative Decree no.138/2024, which transposed the European Directive 2022/2555 (known as NIS2 Directive), profoundly reshaped the European digital space.

Considerable efforts have been made to strengthen the relationship between the ACN and various actors in Italy's digital ecosystem, both public and private. This was achieved by signing cooperation agreements and by conducting outreach and awareness-raising initiatives across the national territory, targeting Regions, local Administrations, Local Health Authorities and small and medium-sized enterprises. The MoU signed in December with the Ministry of Education and Merit will enable the implementation of similar initiatives in schools.

The Government supported the ACN's initiatives to stimulate investments in cybersecurity and technological innovation, with a particular focus in the artificial intelligence field. Europe and Italy are striving to assert, on a global scale, a vision of ethical, human-centered AI that respects fundamental rights; however, this commitment risks remaining aspirational if it is not supported by the technological capacity to effectively contribute to the development of this new technology. One emblematic example of such effort is the €400 mn investment (co-financed by the Italian Government and the European Commission), for the "IT4LIA AI Factory" project, which aims to create an AI-optimized supercomputer at the Tecnopolo of Bologna.

Global challenges require global responses. For this reason, the Government worked to strengthen cybersecurity at the international level as well. This started with the G7, in which Italy held the Presidency in 2024 and by promoting the establishment of a new Working Group on Cybersecurity, receiving broad support from our partners – as evidenced by the inclusion of a specific paragraph dedicated to cybersecurity in the G7 Leaders' statement. This represents a significant step forward towards deeper cooperation among Western democracies.

Despite the increasing complexity and turbulence of the global landscape – in which the cyber dimension is becoming one of the main outlets for geopolitical tensions – the ACN must be credited for having carried out a sensitive and critical task. Such work is continuing with determination into 2025, with the goal of further strengthening the cyber resilience of the Italian system.

Alfredo Mantovano

INTRODUCTION

In a context marked by a rapidly changing geopolitical landscape and an increasingly pervasive and intensive use of emerging technologies, 2024 confirmed itself as a year of challenges, in which malicious actors continued to exploit the cyber domain to pursue their goals. Within this scenario, the National Cybersecurity Agency continued its work on multiple fronts to strengthen the systemic resilience of the country, both by enhancing protection capabilities for the national digital surface and by promoting technological development.

This was not merely a response to the effects of a growing threat, but rather a broader and more structured commitment that encompasses the various elements contributing, in different ways, to the resilience of the national digital ecosystem.

In this complex task, the ACN operated within a now well-established institutional architecture, composed of multiple actors with distinct roles and responsibilities. This structure foresees a central role for the Agency, due to its legally assigned functions of coordination and liaison, and especially because of its responsibility in guiding and monitoring the implementation of the National Cybersecurity Strategy and its Implementation Plan.

The commitment demonstrated by the Agency, as outlined in this Review, has enabled it to engage and collaborate with Institutions, central and local Public Administrations, the academic community as well as private enterprises. In short, to address the entire national community.

Indeed, only with the contribution of all, we can face such a pervasive threat – one that is increasingly sophisticated and capable of affecting growing segments of the population, starting with the most vulnerable and exposed.

The development across various social sectors of a stronger awareness of digital risks is a prerequisite for laying more robust foundations for national resilience. Equally essential is the advancement of digital skills. Awareness and education are, in fact, integral components of a cybersecurity culture, as both recognize the human factor as a key domain of engagement, while employing different tools and approaches.

Strengthening and safeguarding cybersecurity is also crucial to digital democracy and for ensuring the effective protection of personal freedom and dignity of every citizen.

The global nature of the threat – where neither attacks nor solutions respect national boundaries – demands an equally global, coordinated and shared response at the international level.

During its Presidency of the G7, Italy was able to assert its significant international standing, also in the cyber domain.

The goal of advancing such an unprecedented strategy of global governance has now taken root. In fact, the G7 Working Group on cybersecurity will continue under the Canadian Presidency, offering new opportunities for joint reflection on issues crucial to cybersecurity; issues that today, more than ever, require close solidarity among the major Western democracies.

2024 was also a year marked by a comprehensive revision of the regulatory framework on cybersecurity, both at the national level and within the European Union. Two major developments in this regard were the adoption of Law no. 90/2024 and the national transposition of the NIS2 Directive.

The Agency committed fully to this process, in terms of organization – including the development of an IT platform for the registration of public and private NIS entities – through initiatives aimed at disseminating knowledge about the contents and by anticipating certain effects of the new European Directive. The Agency also played a leading role in coordination efforts, establishing the "Tavolo NIS"*, a specific working group which includes the participation from the 9 sectoral Authorities and representatives of the Regions. This complex coordination work aims, once again, to contribute to strengthening the national systemic resilience.*

In all of these ways, the Agency is supporting the country in elevating its cybersecurity posture, by leveraging both internal budget resources and funding from the National Recovery and Resilience Plan (PNRR).

To conclude, I wish to thank all the staff of the Agency for the intensity and quality of their work and to the Undersecretary of State and Delegated Authority for the Security of the Republic for the guidance, support and encouragement consistently provided.

Bruno Frattasi

1. 2024: A YEAR OF INTENSE UPDATES TO THE REGULATORY FRAMEWORK

In 2024, the National Cybersecurity Agency worked to keep cybersecurity regulations updated and consistent. In a world where technology evolves rapidly, it is essential for legislation to adapt accordingly. This ensures both the protection of the country and its citizens from increasing digital threats and the safe use of new technologies as tools for innovation and growth.

Throughout the year, numerous new measures were adopted – some specific, other more general – at both the national level and to align with European regulations. A relevant piece of legislation that was approved is Law no. 90/2024, which introduced provisions aimed at improving the cybersecurity of Public Administrations. This law also made it possible to anticipate some of the requirements of the European NIS2 Directive, which expands the protection of the European Union's digital infrastructure.

Law no. 90/2024 pursued multiple objectives: it strengthened the national cybersecurity system by introducing notification obligations and security measures aimed at protecting certain entities involved and preventing cyber attacks; it established coordination procedures among the various stakeholders, seeking a balance between resilience requirements, investigative activities and intelligence functions; it also updated the criminal law framework on cybercrime.

One of the central features of this piece of legislation is the obligation to report cyber incidents to CSIRT Italia, the operational unit of the ACN. Notification obligations as well as enhanced security measures are now required for certain categories, such as central Public Administrations, Regions, the Autonomous Provinces of Trento and Bolzano, municipalities with over 100,000 inhabitants, public transport companies with large user bases and Local Health Authorities. These new requirements are extended also to in-house companies that provide IT services, public transport and environmental services such as waste and wastewater management.

Expanding the notification obligation to a wider range of entities aims to improve the ability to prevent and respond to incidents by reducing reaction times and overall impact. The same aim was also pursued by introducing the requirement for the Agency to issue targeted alerts to potentially vulnerable entities, whose recipients must promptly implement the recommended measures and inform it of the outcomes of the actions carried out.

Another key aspect is the strengthening of resilience across Public Administrations. The law required each Administration to establish an internal unit dedicated to cybersecurity and to appoint a cybersecurity officer and contact point (Referente per la cybersicurezza). The person in charge is responsible for ensuring that operational activities align with the Agency's directives, including those outlined in the guidelines issued by the ACN.

Law no. 90/2024 also recognizes the importance of cryptography as a key tool for cybersecurity and establishes the creation of a National Cryptography Center within the ACN. In this context, the law entrusts the Agency with the task of developing and disseminating standards, guidelines and recommendations to strengthen the security of IT systems as well as as-

sessing the reliability of the cryptographic systems in use. In order to achieve the desired results, the law calls the Agency to foster collaborative initiatives with universities and research centers to support the development of cryptographic algorithms, promote research and enhance national cryptographic capabilities.

The Agency is actively involved in matters relating to cryptography. In 2024, it continued its efforts to promote the proper use of cryptography by publishing a series of documents dedicated to "Cryptographic Functions Guidelines". The two most recent issues of the series were published in July.

In 2024, European regulatory activity in cybersecurity reached a key milestone with the 17 October deadline for the national transposition of the NIS2 Directive which aims to ensure a high and uniform level of cybersecurity across the European Union. Compared to the previous NIS framework, NIS2 strengthens and updates the existing system with the goal of improving cybersecurity and resilience, thereby contributing to the proper functioning of the European single market and the coordinated protection of Member States. Amongst other innovations, the NIS2 Directive significantly expands the number of sectors subject to its provisions (Figure 1).

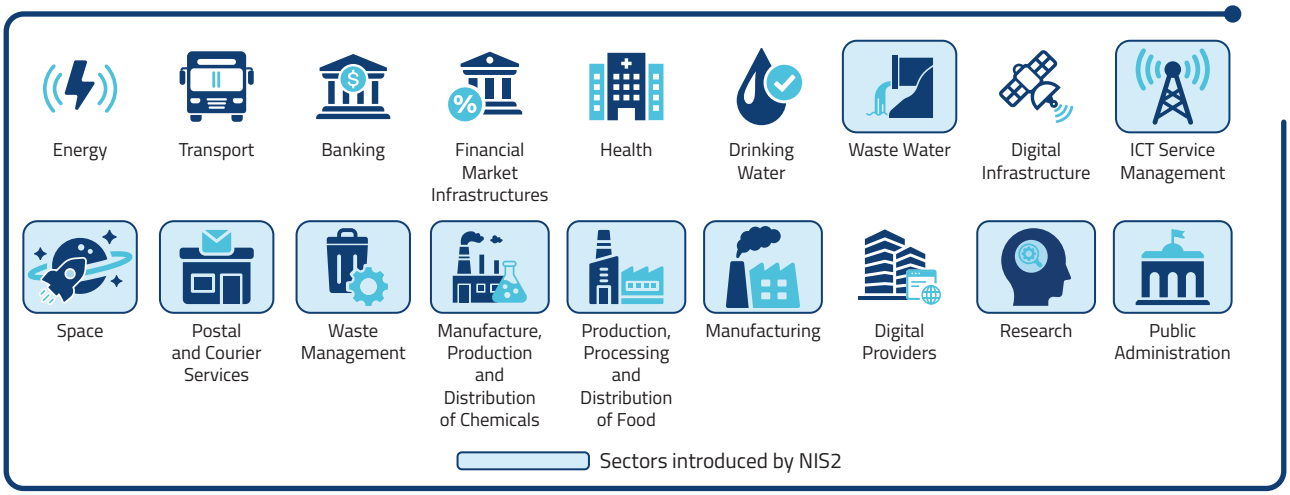


Figure 1 – NIS sectors: a comparison between NIS1 and NIS2

With the entry into force of Legislative Decree No. 138/2024, on 16 October 2024, Italy was among the first EU countries to complete the transposition of the NIS2 Directive within the established timeframe. The legislative process was carried out in a coordinated manner, involving both the relevant public Administrations and a selected group of private entities affected by the new rules. The decree introduces several national specificities compared to the text of the European Directive, aiming to ensure its effective implementation.

The decree confirms the central role of the ACN, which serves as the national competent Authority, NIS single point of contact and national CSIRT. The decree recognizes that the ACN and the Ministry of Defense are both involved in the management of large-scale cyber crises, with a special responsibility of the latter for issues related to national defense while the ACN is responsible in terms of civil resilience and is endowed with an overall coordinating function.

The decree also recognizes sectoral and territorial specificities, establishing 9 NIS sectoral authorities. These authorities, together with the representatives from Regions and Autonomous Provinces, are part of the so-called "Tavolo NIS" – the coordinating working group responsible for overseeing the implementation of the legislation.

The NIS2 decree introduces the principle of gradual implementation, which complements the proportionality principle already established by the European Directive. NIS subjects are required to initially adopt basic cybersecurity requirements. These will then be progressively strengthened through tailored risk analyses, allowing for the introduction of increasingly advanced obligations. The aim is to establish a gradual and collaborative path toward enhancing the overall security posture of all involved entities, both public and private. The implementation of the new framework is structured in three steps, in line with the timeline set for adopting regulatory measures and the entry into force of obligations for the concerned entities (Figure 2).

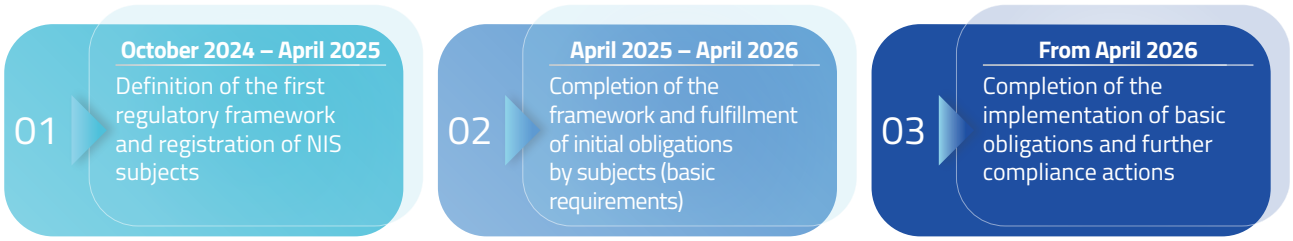


Figure 2 – NIS2 Implementation steps

At the European Union level, the year in review saw a major push toward regulation with significant implications for cybersecurity, marked by the conclusion of negotiations on several key legislative acts, to which Italy and the ACN actively contributed:

- Cybersecurity Act (CSA), introducing new provisions on managed security services;
- Cyber Solidarity Act (CSoA), which sets out measures to strengthen the EU's capacity to detect and respond to cyber threats and incidents;
- Cyber Resilience Act (CRA), establishing cybersecurity requirements for products with digital elements;
- eIDAS2 Regulation, enabling the introduction of the European Digital Identity Wallet; and
- Artificial Intelligence Act (AI Act), which defines harmonized rules on the use of artificial intelligence.

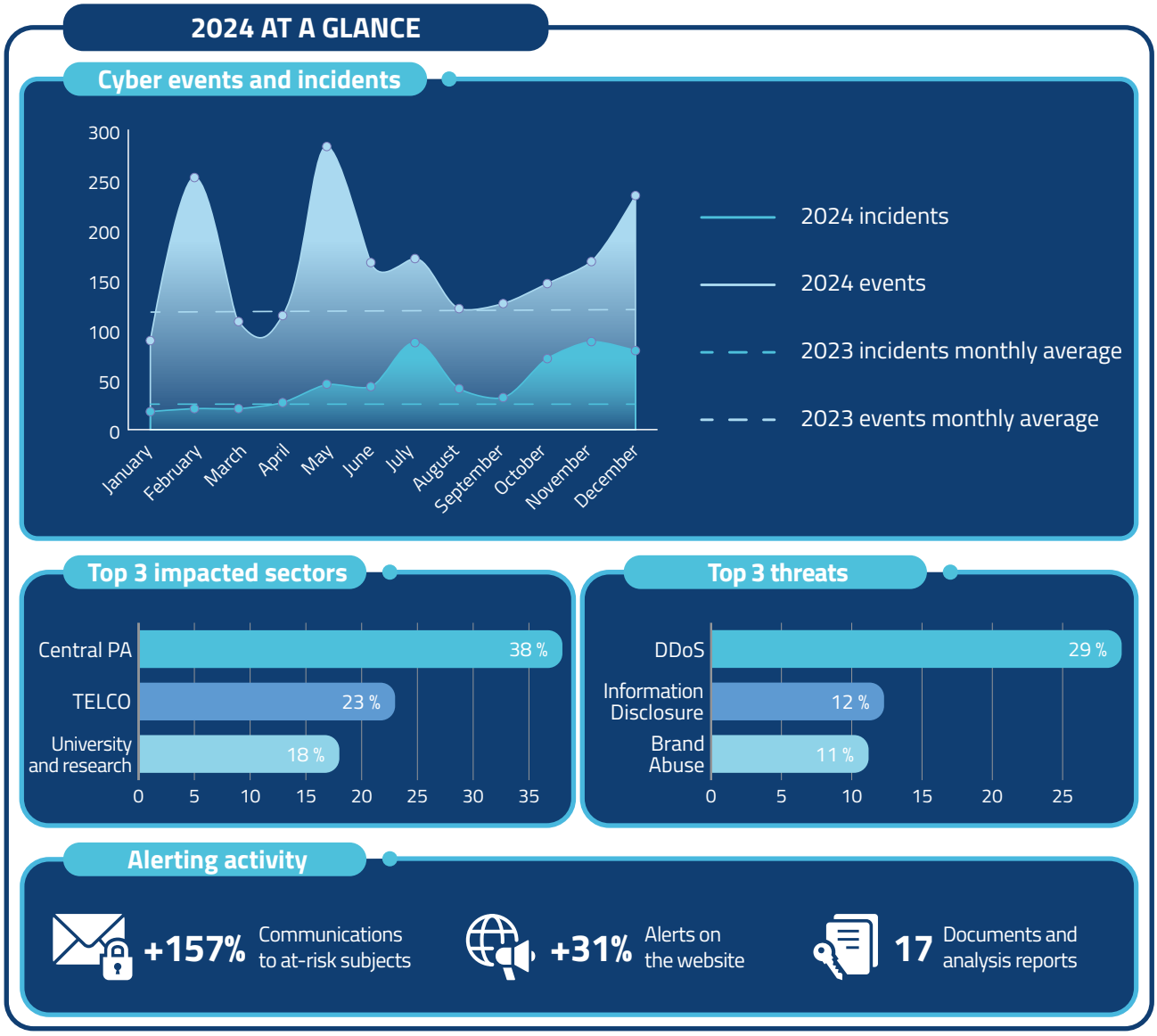
A further step aimed to strengthen the cybersecurity of the national system is the entry into force of the new Regulation for digital infrastructures and cloud services for Public Administration. Adopted by the ACN in agreement with the Department for Digital Transformation of the Presidency of the Council of Ministers, the new Regulation updates and rationalizes the process by which Public Administrations can move their data and services to the cloud, making sure that cybersecurity considerations are duly taken into account.

2. THE EVOLVING CYBER THREAT: PREVENTION AND MANAGEMENT OF CYBER EVENTS AND INCIDENTS

In 2024, the National Cybersecurity Agency faced a steadily growing cyber threat, both in terms of the number of attacks and their complexity. These attacks can have serious consequences not only for individual victims but also for the security and stability of the entire country. This year as well, Italy was targeted by DDoS (Distributed Denial of Service) attacks, ransomware and hostile activities carried out by APTs (Advanced Persistent Threat groups).

Such threats affected a wide range of entities – both public and private – operating in various sectors, including those that are most critical. The Agency was able to effectively monitor the situation through its operational unit, CSIRT Italia, which collects both mandatory and voluntary reports of cyber incidents as required by national legislation.

Thanks to the Agency's prevention and response activities, the impact of many harmful events was contained. In addition, timely alerts to potentially at-risk entities helped reduce the country's overall exposure to cyber threats.



In 2024, there was a significant increase in the indicators used to assess Italy's exposure to cyber threats. Notably, the number of notifications received by the Agency rose, partly due to the entry into force in July of Law no. 90/2024, expanding the number of operators under the Agency's oversight.

There was also a marked increase both in the number of cyber events (+40% compared to 2023) and in the number of incidents, which nearly doubled. From the analysis of the data, it emerges that this rise can be mainly attributed to the surge of DDoS attack campaigns targeting Italian entities, the increase in information disclosure incidents (i.e. the unauthorized release of sensitive data previously obtained through malicious activities) and the more frequent use of spearphishing campaigns.

During the year under review, CSIRT Italia identified 2,734 victims of cyber events. Some of these attacks targeted same entities. Nevertheless, the number of "unique victims" stands at 1,260, more than double compared to 2023. Moreover, CSIRT Italia handled a total of 1,979 cyber events, averaging around 165 per month, with a peak of 283 in May. Of these, 573 were classified as incidents, with a monthly average of around 48 cases (Figure 1).

The spikes recorded in February, May and December were caused by three DDoS attack campaigns claimed by the pro-Russian hacktivist group NoName057(16), which has been active since 2022 and targets various Western countries in the context of the Russia–Ukraine conflict. Another significant increase occurred in July, following a supply-chain attack that compromised an IT service provider and, in turn, numerous entities that relied on its services.

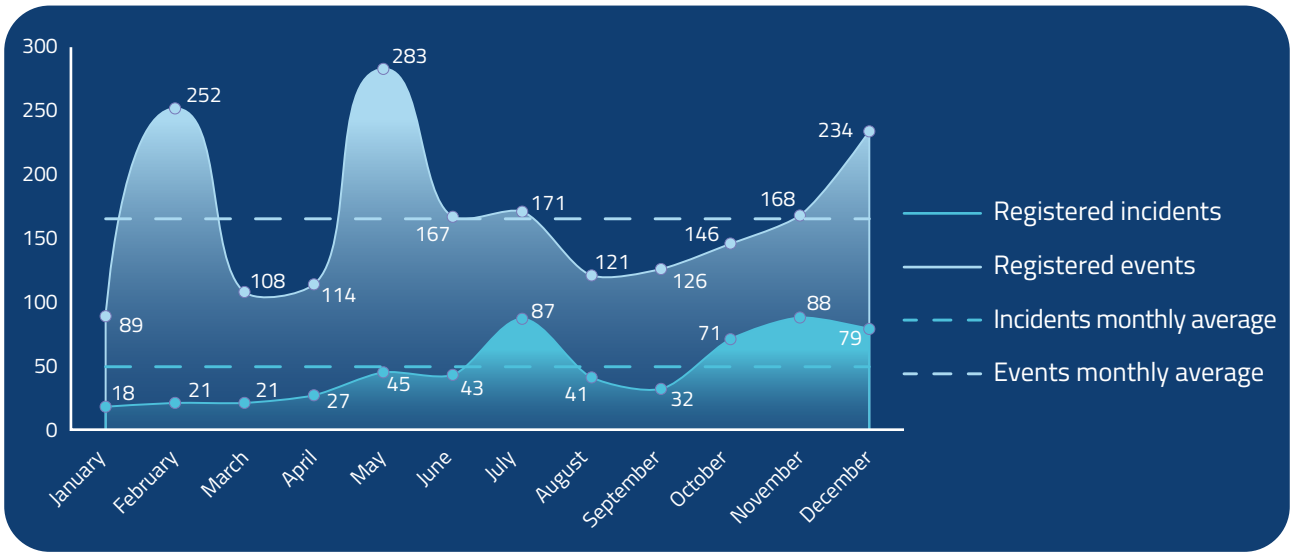


Figure 1 – Distribution of cyber events and incidents in 2024

The Agency's preventive activity also played a key role in helping to avoid or mitigate cyber incidents through the dissemination of timely information on threats and vulnerabilities. In particular, alerting activity grew significantly: over 53,000 direct communications were sent to potentially at-risk subjects, alongside public alerts published on the Agency's online platforms.

In the most complex situations, the Agency provides direct support to victims of cyber incidents through the CSIRT Italia teams specializing in Digital Forensics and Incident Response (DFIR). Such support includes on-site or remote assistance to address the impacts of the incidents and the underlying issues, identifying the necessary measures to contain the event and restore compromised services. Each intervention, which often lasts several days or even weeks, involves an initial assessment of vulnerabilities and critical issues, followed by the implementation of operational strategies for the acquisition and analysis of digital artifacts, planning recovery actions and verifying corrective measures. This intervention model integrates the resources already available in the affected infrastructures, reducing operational impact and improving incident management.

In terms of the sectors in which the victims of cyberattacks operate (Figure 2), Central Public Administration was the most affected, followed by the telecommunications sector. It is important to bear in mind that a single event may affect multiple victims across different sectors. Moreover, the higher incidence observed in the public and critical sectors is also linked to the fact that they are subject to stronger requirements in terms of incident notification obligations, thereby ensuring a deeper visibility for the Agency.

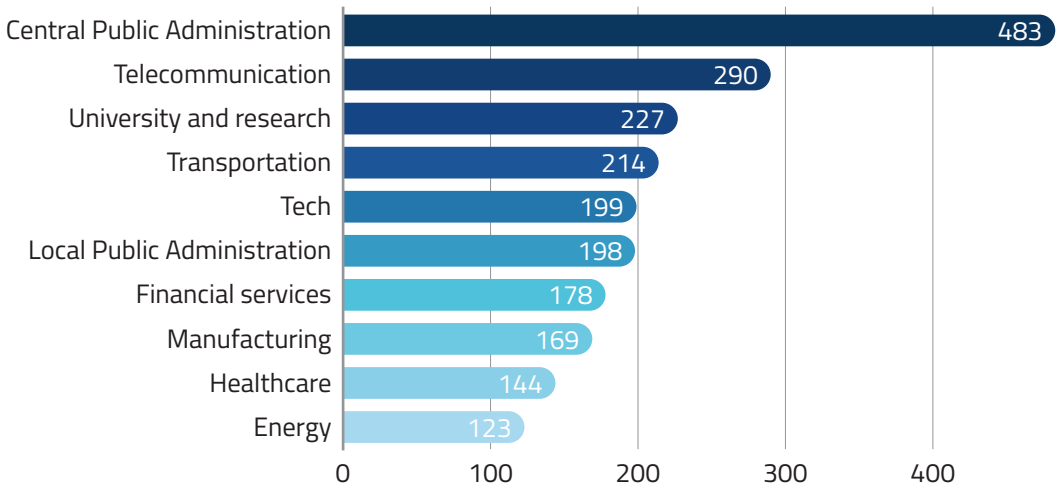


Figure 2 – Cyber events by victim's economic sector (top 10)

The analysis of the 1,979 detected cyber events enabled the classification of the main types of threats (Figure 3). Among these, DDoS attacks were the most frequent, followed by cases of information disclosure and brand abuse, which imply the unlawful use of logos and institutional imagery, often in phishing campaigns.

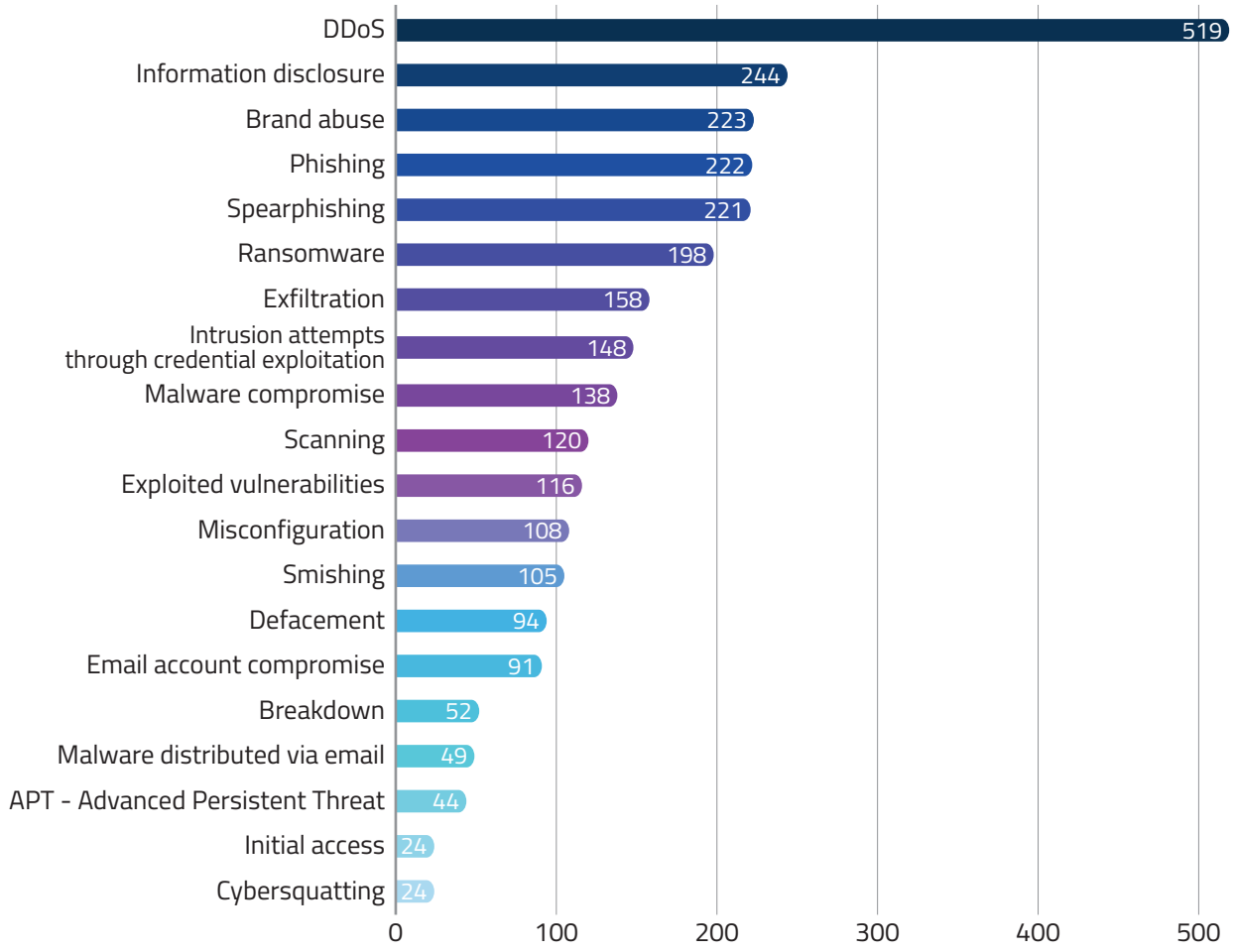


Figure 3 – Top 20 cyber events handled

In 2024, three major DDoS attack campaigns were recorded – in February, May and December – all claimed by pro-Russian hacktivist collectives. Of the 519 identified events, most resulted in no significant impact and only 15% caused measurable disruptions, which were always temporary: usually about an hour of unavailability of the targeted resources. By monitoring the communication channels used by hacktivist groups it was possible to conclude that Italy ranked 9th globally and 4th among European Union countries for the number of claimed DDoS attacks.

Although less frequent in numerical terms (198 cases), ransomware remains a particularly serious threat: in most instances, it results in prolonged data unavailability, with significant impacts on the operational continuity of public bodies and private companies.

In terms of economic sectors (Figure 4), manufacturing continues to be the most exposed to cyberattacks. This vulnerability is largely due to the prevalence of small and medium-sized

enterprises, which often lack both specialized resources and dedicated cybersecurity structures. Special attention is also paid to the healthcare sector: while it did not register the highest number of events, it is among the most severely affected in terms of impact – due to both disruptions in service operations and the sensitivity of the personal data involved.

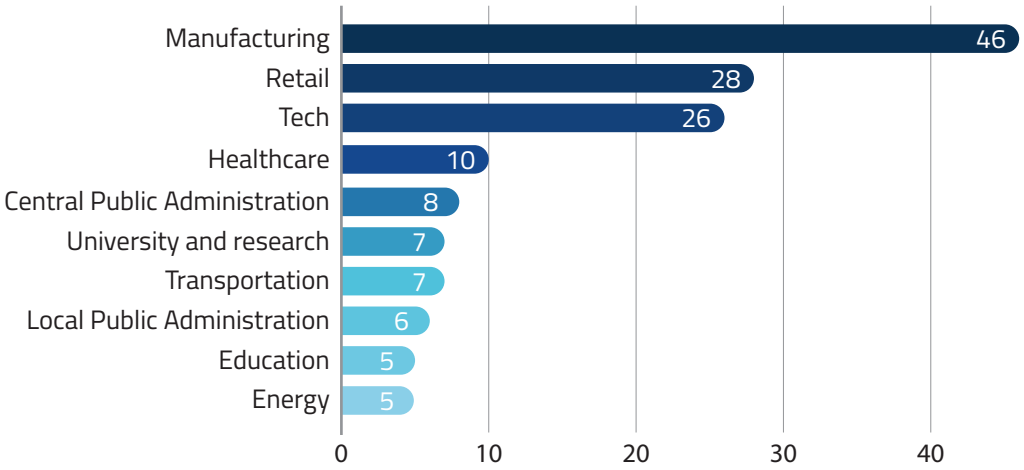


Figure 4 – Top 10 ransomware events by victim's economic sector

CSIRT Italia detected ransomware attacks conducted by at least 40 distinct criminal groups, a marked increase from the 20 recorded in 2023. This data highlights the ability of such organizations to reorganize and continue operating, despite periodic international countermeasures that lead to the dismantling of some of them. The new groups, often composed of members previously active in other gangs, demonstrate high operational flexibility and utilize models such as Ransomware as a Service (RaaS) to expand the scope of their activities.

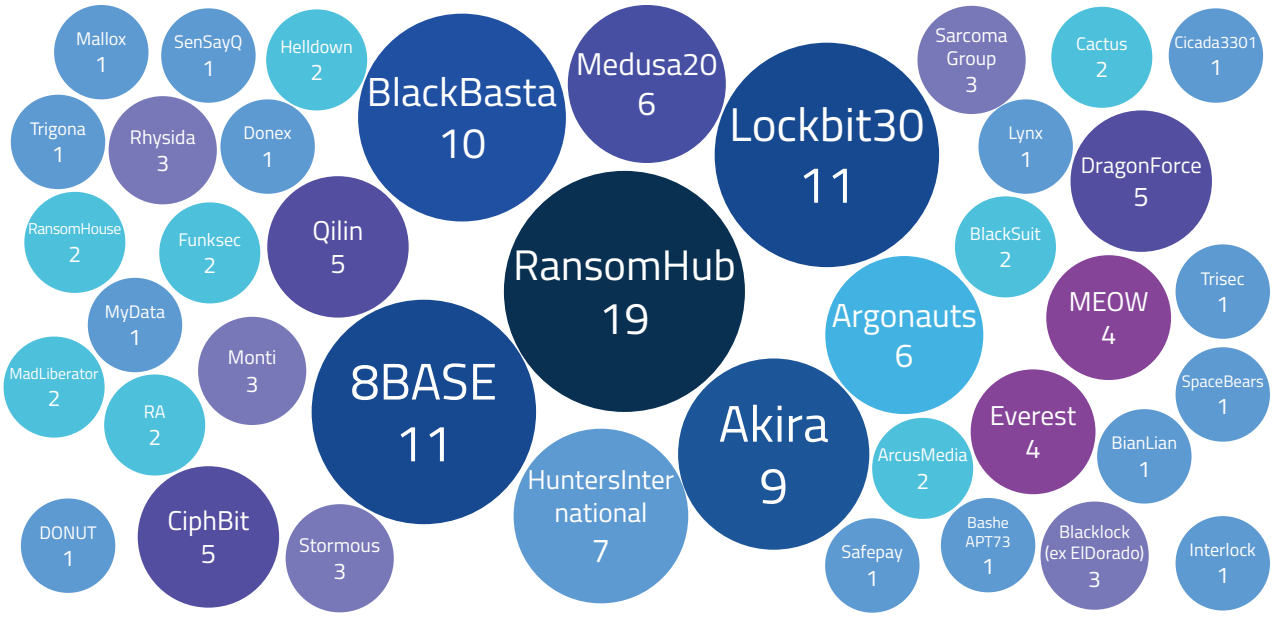


Figure 5 – Number of claims by ransomware groups

Particularly noteworthy is the distribution of targets between DDoS and ransomware attacks. Among DDoS victims, public entities were the most affected, with increased activity targeting secondary or peripheral non-critical services – often lacking anti-DDoS protection – rather than core services. By contrast, ransomware attacks primarily affected the private sector and small and medium enterprises (SMEs), which accounted for 75% of incidents targeting private entities. Such firms, in fact, tend to employ less sophisticated cyber defenses and sometimes avoid reporting incidents for fear of reputational impacts.

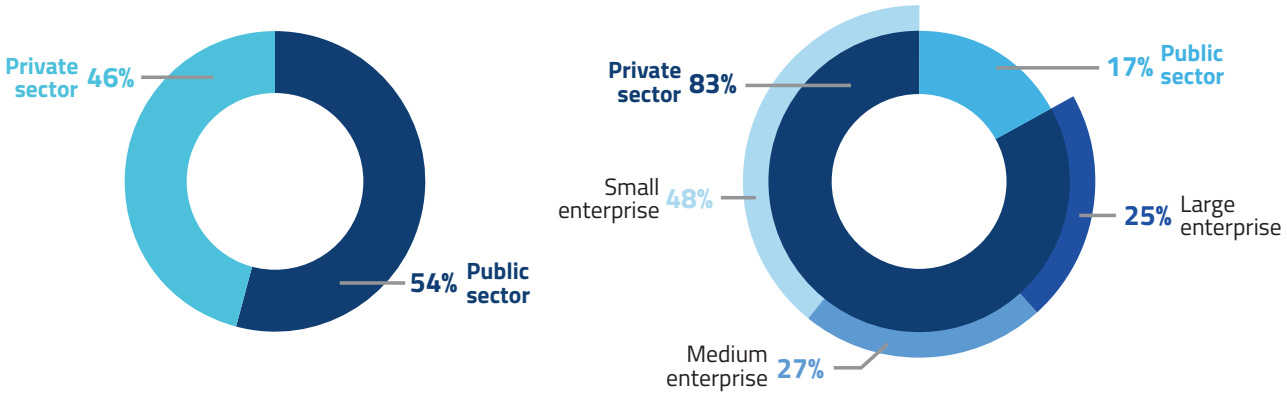


Figure 6 – Distribution of DDoS and ransomware victims: public vs. private

3. THE AGENCY IN THE INSTITUTIONAL LANDSCAPE: CONSOLIDATING CYBER COOPERATION

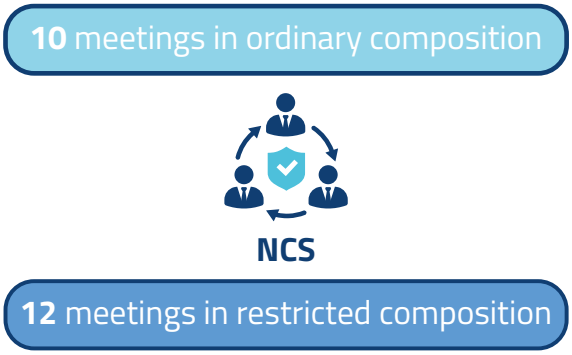
As part of the revised national cybersecurity framework, the Agency plays a central coordinating role among all stakeholders involved in the country's cyber protection. This responsibility is carried out through interministerial forums operating at both political–strategic and operational levels. In particular, the Agency actively participates in the Interministerial Committee for Cybersecurity (CIC) and leads the National Cybersecurity Cell (Nucleo per la cybersicurezza - NCS), the Perimeter Coordination Table and the NIS Table. In terms of institutional cooperation, dialogue with Parliament has also been paramount, both in terms of oversight and legislative activity, contributing significantly to the evolution of the legal framework on cybersecurity and digitalization.

Special attention was also devoted to strengthening cooperation with the wider cybersecurity ecosystem, in particular the private sector, which is essential for the practical implementation of security strategies. The Agency promoted, and took part, in numerous events, engaging with local communities, businesses, universities and associations.

The Interministerial Committee for Cybersecurity is chaired by the President of the Council of Ministers and includes the Ministers most heavily involved in cybersecurity issues (Foreign Affairs and International Cooperation, Interior, Justice, Defense, Economy and Finance, Enterprises and Made in Italy, Environment and Energy Security, University and Research and Infrastructures and Transport). The CIC is tasked with proposing strategic cybersecurity policy guidelines, overseeing the implementation of the National Cybersecurity Strategy and the financial management of the ACN as well as promoting initiatives to strengthen cybersecurity.

In 2024, the CIC met five times. During these meetings, the main cybersecurity dossiers were examined, including those related to the update of the regulatory framework. In particular, the CIC assessed changes to the list of entities included in the Cyber National Security Perimeter, aiming to adapt it to the new cybersecurity needs of the country. The proposals sent to the Prime Minister for final decisions took into account the recommendations made by the Perimeter Coordination Table, chaired by the Agency. The Table, which encompasses representatives from various Ministries, plays a key role in implementing the Perimeter's legal framework, being responsible for identifying the essential State functions and services as well as the entities that provide them.

As per the NCS, throughout the year, it continued to serve as the main interministerial coordination forum supporting the President of the Council of Ministers, tasked with promoting prevention and preparedness for potential cyber crises as well as activating alert procedures when necessary. In this context, the NCS, chaired by the Director General of the ACN is composed of the Military Advisor to the President of the Council of Ministers, a representative of the Security Intelligence Department, the External Intelligence and Security Agency, the Internal Intelligence and Security Agency and representatives from the Ministries that are members of the CIC as well as the departments of the Presidency of the Council of Ministers in charge of Civil Protection and Digital Transformation. The NCS facilitated the exchange of information among the involved Administrations and other relevant stakeholders, providing an updated situational awareness, which was useful for regularly informing political authorities and supporting Government decisions.



During 2024 the NCS took full advantage of the possibility to adjust its composition to the specific topics, so as to deepen the analysis of the challenges and threats faced and to enable the involvement of key stakeholders. An example is the first meeting of the NCS in the composition mandated by Law no. 90/2024, i.e. with the involvement of representatives from the Bank of Italy and of the Anti-mafia and Anti-terrorism National Directorate. Furthermore, representatives from key private firms from the telecommunication industry were invited to contribute to the NCS in its ordinary composition, giving rise to a regular engagement with private stakeholders. Throughout the year, the NCS met 10 times in its ordinary composition and 12 times in its restricted format.

In 2024, the Agency continued to place strong emphasis on cybersecurity exercises, which are considered essential for testing Italy's response capabilities in the event of a cyberattack, both at the national and international levels. In addition to the international exercises which saw the ACN's involvement (see Chapter 6), in 2024 the Agency launched a new program of recurring exercises. The first edition, "ACN-CyEX24", took place in December and involved around 50 representatives from the Administrations that are part of the National Cybersecurity Cell. The exercise – designed as a table-top simulation – provided a forum for participants to discuss and share technical and procedural best practices in response to a cyber incident, simulated as the result of a vulnerability detected through ACN's proactive services.

Regarding cooperation with Parliament, the Agency actively contributed to the work of Parliamentary Committees through six hearings by the Director General. These sessions provided Parliament with technical expertise to support the development of key cybersecurity regulations, particularly Law No. 90/2024. The Agency was also involved in the transposition process of the NIS2 Directive, in the yearly European Delegation Law and in discussions on the draft law on artificial intelligence, in addition to two fact-finding inquiries on cyber defense and on the digitalization of the Public Administration.

The ACN is also subject to oversight by the Parliamentary Committee for the Security of the Republic (COPASIR) for those activities related to safeguarding national security in cyberspace. To this end, the President of the Council of Ministers submits an annual report to the Committee on the Agency's work. The COPASIR may also request the ACN Director General for hearings, as it did once in 2024.

The ACN continued to establish agreements with public and private entities to strengthen cybersecurity and resilience, promote information sharing and enhance education and training. These agreements primarily focused on three areas: strengthening cooperation with other Public Administrations, expanding public-private collaboration and improving international relations with cyber agencies in other countries (see Chapter 6).

Regarding Public Administrations, one of the most significant agreements was signed with the Ministry of Education and Merit, aimed at promoting IT and cybersecurity education in Italian schools. Furthermore, following legislative changes in 2024, the agreement among the ACN, the National Anti-mafia and Anti-terrorism Directorate and the Department of Public Security ensured continuous and constant information alignment for the proper execution of the functions prescribed by law. Public-private cooperation was enhanced through agreements with organizations in the education sector and companies operating in areas relevant to the Agency's activities, aiming to strengthen collaboration with the productive sector.

Finally, the Agency was particularly dynamic in its involvement in events, actively participating in over 90 meetings with private operators and 66 events organized by associations, universities and companies. One particularly notable event was organized in collaboration with the Sapienza University, with the goal of raising awareness on the new NIS regulation and supporting the stakeholders involved in the implementation of it.

4. TECHNOLOGICAL SECURITY: A KEY ELEMENT TO PROTECT THE COUNTRY'S DIGITAL SURFACE

Assessing the compliance of certain technologies with an adequate level of cybersecurity is a crucial feature for ensuring the resilience of the national digital space. In this respect, the Agency is responsible for verifying that the technological tools in use in the country comply with adequate security standards by conducting numerous functions. Indeed, as the National Cybersecurity Certification Authority, the ACN issues certifications for digital products and services used in the country, and is also the entity in charge of verifying critical processes such as the transition to the cloud of Public Administrations and the technological screening mandated by the Cyber National Security Perimeter.

Such screening is an essential prerequisite for protecting the ICT components used by critical entities, since a cyber threat to them could have serious repercussions for the country system as a whole. The Cyber National Security Perimeter includes networks, information systems and IT services that are crucial for the country and whose compromise could constitute a threat to national security. In this context, the National Assessment and Certification Centre (Centro di valutazione e certificazione nazionale - CVCN) receives and evaluates the communications of entities included in the Perimeter regarding their intention to use certain ICT components. In 2024 the CVCN evaluated a significant number of such components, often also by conducting specific tests and making recommendations to the involved entities about their cyber-safe use (Figure 1).

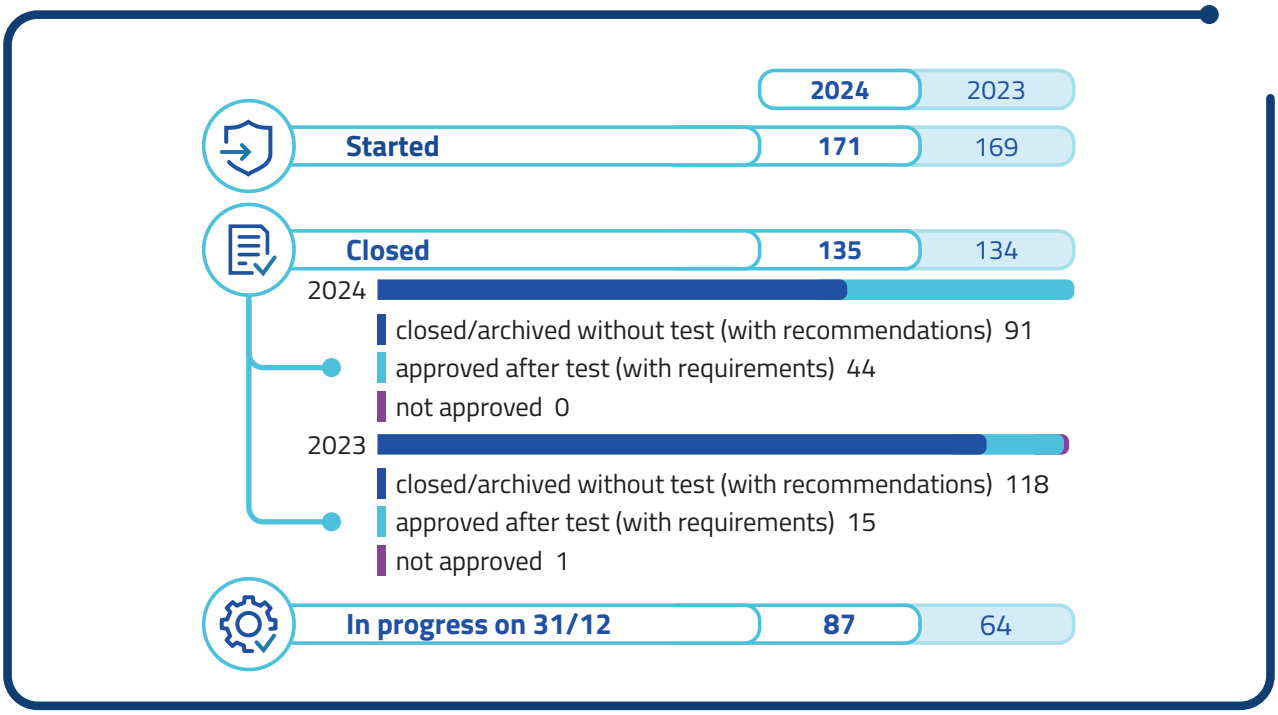


Figure 1 – Proceedings carried out by the CVCN

Through the technological screening activities, the CVCN has been able to identify several vulnerabilities, 40 of which had never been identified before, the so-called zero-day vulnerabilities. Following an assessment of their level of severity (Figure 2), the Agency notified them to the producers of the different ICT components within a process of responsible vulnerability disclosure. As such, most zero-day vulnerabilities identified by the CVCN have been or are being corrected by the producers (Figure 3).

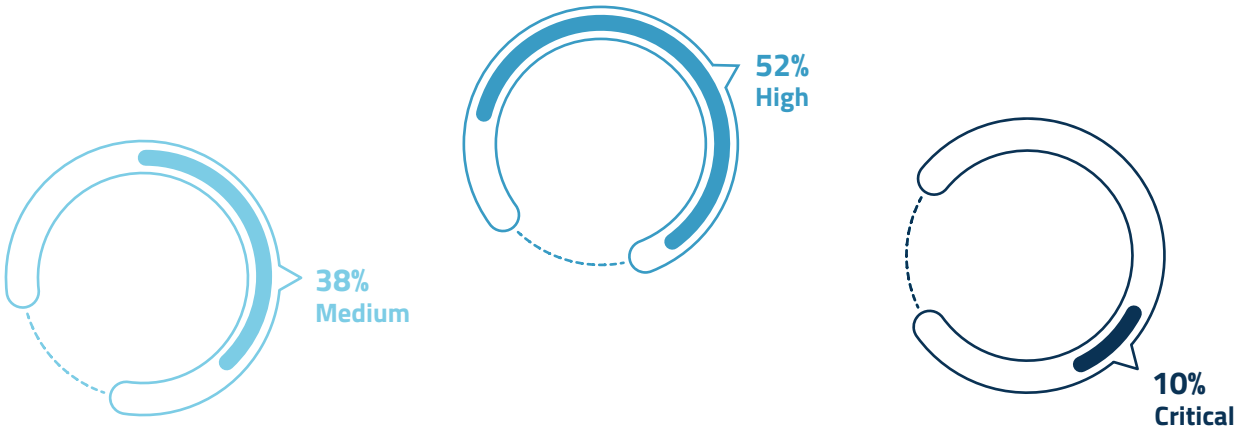


Figure 2 – Identified zero-day vulnerabilities by severity

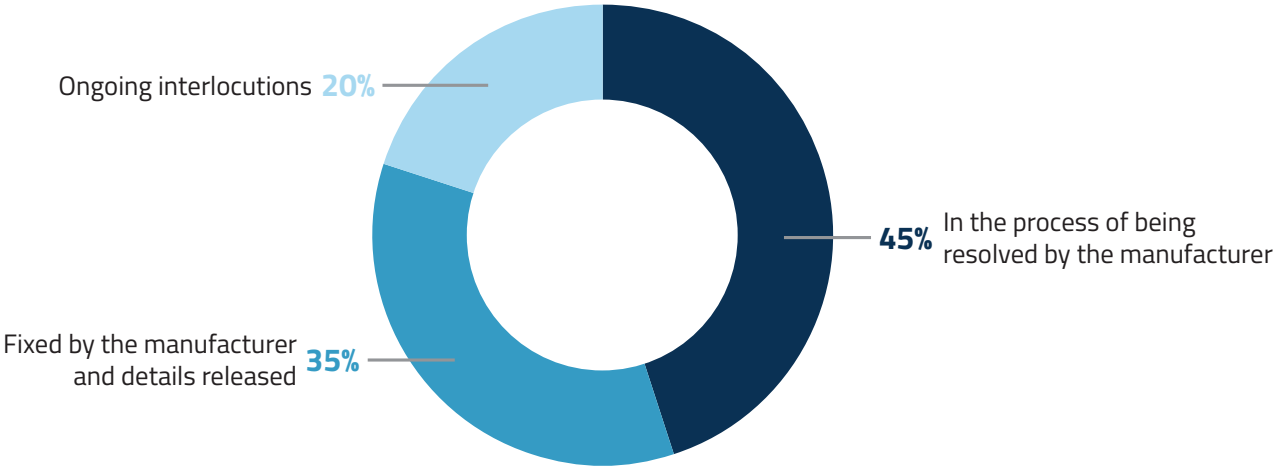


Figure 3 – Status of identified zero-day vulnerabilities

The Agency also plays a key role in evaluating the respondence of commonly used digital products and services to adequate cybersecurity standards, so as to ensure their resilience. As the National Cybersecurity Certification Authority, in 2024 the ACN issued 10 certifications based on the internationally recognized Common Criteria standard (23 assessments are still ongoing) and evaluated 4 Accredited laboratories that assist the activities of its Cybersecurity Certification Body (Organismo di certificazione della sicurezza informatica-OCSI). It also issued 7 conformity assessments for digital identity systems in the framework of the eIDAS Regulation.

The introduction, in 2024, of the first EU cybersecurity certification system based on the Common Criteria (EUCC) will soon replace the national schemes, allowing for harmonized certifications across the 27 Member States. Similar systems are also under development for cloud services (EUCS) and for 5G networks (EU5G).

The Agency has been involved in the complex process of evaluating the characteristics of cloud services and of their supporting digital infrastructures to make sure that the transition of Public Administrations' data and services to the cloud takes cybersecurity in consideration. 2024 has been a year of transition in this regard, with the entry into force of the new national Regulation (see Chapter 1). The infrastructures and services qualified by the ACN are listed in the Catalogue of Digital Infrastructures and Cloud Services, which contains technical data for each of them, detailing the type and the corresponding qualification level. In addition to the procedures regarding public entities or their direct providers, the Agency has managed numerous requests for qualification of cloud services (over 1,500) and conformity tests for digital infrastructures (over 140) by almost 600 private operators. Such requests resulted in assessments that span across four levels, with 4 being the most critical (Figure 4).

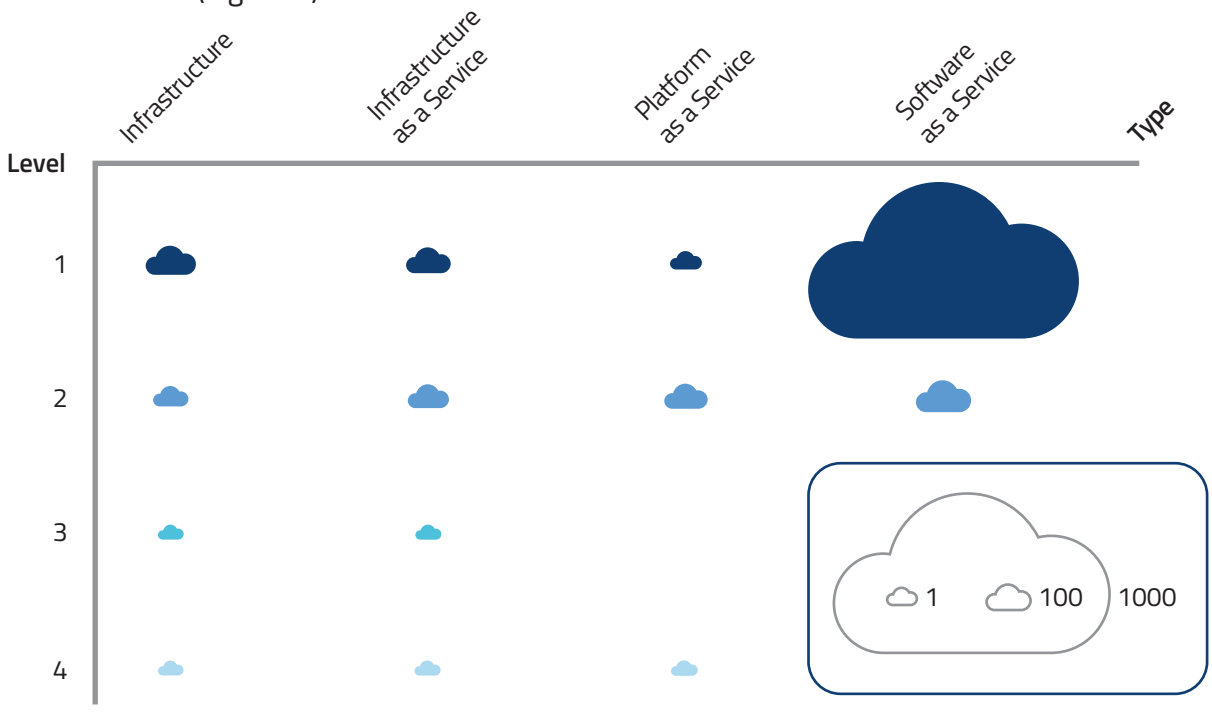


Figure 4 – 2024 qualified cloud services and conformity tests for digital infrastructures of private operators

Furthermore, the Agency gave its contribution to the national procedure for the exercise of the so-called Golden Power, regarding both 5G technologies and other assets falling within the scope of the relevant regulation. As such, the ACN conducted assessments and provided opinions conducive to the collegial evaluation of all of the 19 notifications for 5G technology and of 46% of the 641 notifications for other assets. The results of the latter, which never amounted to the imposition of a veto, are summarized in Figure 5.

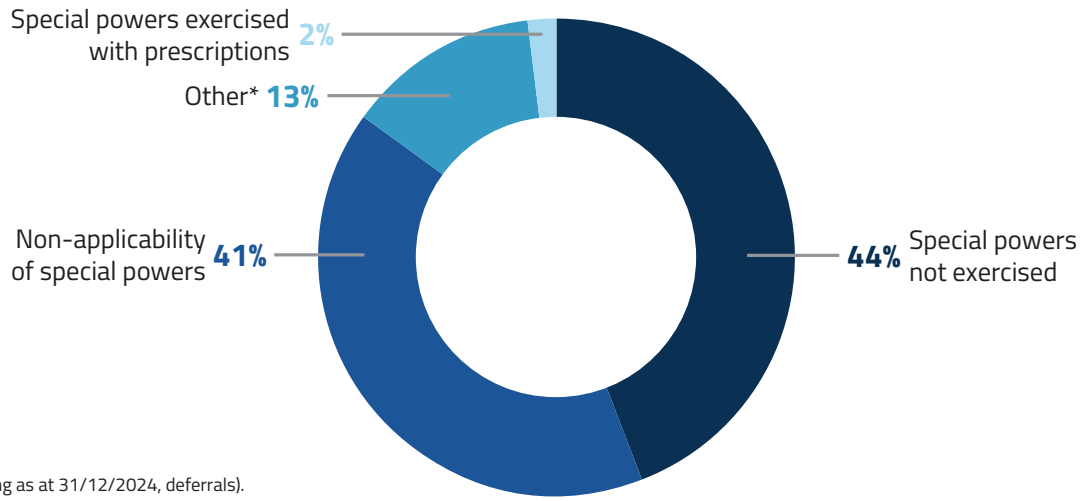


Figure 5 – Outcome of the Golden Power proceedings with ACN's involvement

5. CYBERSECURITY INVESTMENTS: CONCRETE SUPPORT FOR THE COUNTRY'S SYSTEMIC RESILIENCE

In order to achieve a consistent resilience of the whole digital surface, the ACN has been engaged in supporting the broader national cybersecurity ecosystem through various programs aimed at strengthening security and resilience while fostering innovation. The objective of making Italy more secure has found in the investment program of the PNRR the keystone to start the process of developing national cybersecurity. In addition to such resources, the ACN also deployed funding programs for the development of the productive system, both in support of innovative startups and dedicated to equipping the country with cutting-edge technological tools with which to ensure better protection from threats and guarantee the ability to positively exploit the technological developments of today and tomorrow. In this context, the need for a constant dialogue with the academic and research world remains primary, with a view to encouraging technology transfer and the creation of innovation in the most strategic sectors.

The Agency is responsible for the implementation of Investment 1.5 "Cybersecurity" of Mission 1, Component 1, Axis 1 of the PNRR, managed by the Department for Digital Transformation of the Presidency of the Council of Ministers, with a budget of €623 mn. The Agency was able to meet all the milestones and targets of the investment before the deadline of December 2024. It also allocated almost all of the resources available both through projects handled directly and developed by other actors, for a total of €621,26 mn (Figure 1).

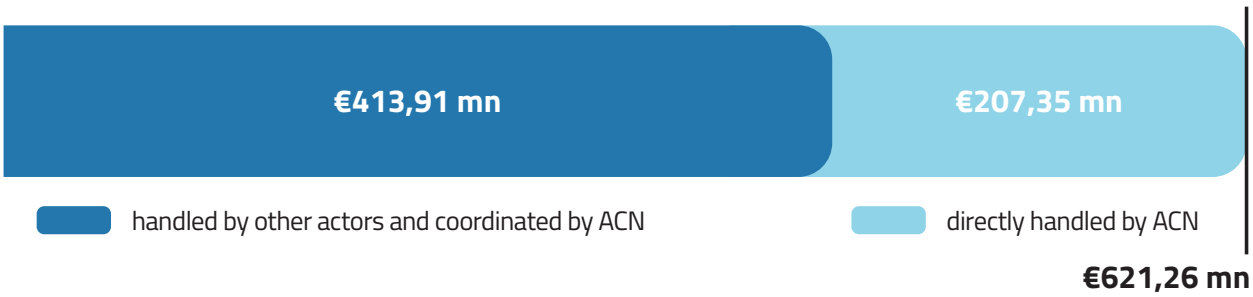


Figure 1 – Allocated resources for the implementation of the PNRR related to cybersecurity

Such funding allowed the strengthening of national cyber capabilities under three main directions:

- the cyber capabilities of a wide range of Public Administration, from Ministries to local bodies, by evaluating and elevating their respective cybersecurity posture;
- the cyber resilience capabilities across the State with better and more interconnected tools: a HyperSOC for enhanced monitoring and analysis of cyber threats, CSIRT Italia and the network of regional and central Public Administration CSIRTs and the ISAC Italia to coordinate information sharing, thanks also to the creation of sectoral ISACs; and
- the technological scrutiny and certification capabilities of national laboratories, centered around CVCN, which has progressively expanded to a network composed of 12 laboratories and 2 evaluation centers.

In addition to that, the Agency worked hand in hand with the national productive system, particularly in the framework of the Cyber Innovation Network (CIN), a collaboration program

aimed to foster the creation and development of startups active in the field of cybersecurity. The CIN constitutes an integrated system to identify startups that qualify for direct funding by the ACN. In 2024 the Agency subscribed agreements with 5 startup incubators and accelerators (Figure 2), leading the way for the kick-off of 3 programs to select the cybersecurity startups to be assisted. Further support has also been made available in the form of a match-making event to allow connections with potential investors, industrial partners and final users as well as other stakeholders of the innovation ecosystem.

Figure 2 – CIN agreements with startup incubators and accelerators

The Agency also contributed to endow Italy with cutting-edge equipment capable of improving the national cyber protection and of allowing to reap the opportunities offered by technological evolutions. Two important examples are being brought forward in cooperation with the non-profit consortium CINECA, a world-leader in High Performance Computing (HPC): setting up an HPC near Naples (San Giovanni a Teduccio) with the aim to enhance the HyperSOC and launching one of the few European AI factories – "IT4LIA AI-Factory" – with an AI-optimized supercomputer in Bologna. Such projects will allow firms and researchers to take advantage of the computational power created, enabling the growth of new startups and spin-offs.

The latter project can benefit from a very significant EU contribution (50% of the overall €430 mn), witnessing the relevance of European investments for the Italian digital and cybersecurity capacities. Further examples can be found in the financial leverage available through the Digital Europe Programme (DEP), which is allowing Italy, and its consortium partners, to go forward with the creation of a European network of SOCs (ENSOC project, granted in 2023, total budget €24 mn) and with services for small and medium enterprises needing to comply with the Cyber Resilience Act (SECURE, granted in 2023, total budget €22 mn).

Finally, the ACN considers the synergies with the academic and research sectors crucial to advance cybersecurity goals and it followed up on the launch of the Research and Innovation Agenda, drafted in 2023 with the Ministry of University and Research. In 2024, it launched a call to fund 30 PhD projects on the topics identified in the afore-mentioned Agenda, with a total budget of €3 mn. The selection process, which was highly competitive, allowed to identify aspiring researchers working in 17 Italian universities, which will be supported in the doctoral endeavor by the Agency.

6. INTERNATIONAL COOPERATION: THE ITALIAN G7 AS A BOOST FOR COLLABORATION BETWEEN CYBER AGENCIES

International cooperation on cybersecurity is an integral part of Italy's foreign and security policy and represents an essential tool for protecting national interests in cyberspace, in line with the country's international role. In coordination with the Ministry of Foreign Affairs and International Cooperation (MAECI), the Agency actively supports the promotion of national interests within key international cyber cooperation frameworks.

Italy's cybersecurity policy is closely aligned with that of the European Union, given the central importance the EU holds for our country, both in terms of regulation and operations. The ACN played an active and strategic role in numerous forums and working groups within the institutional framework of the European Union. Through its participation, the Agency contributed its specialized expertise on key cybersecurity topics, including but not limited to governance models, common standards and certifications and mechanisms for effective incident response. Its involvement extended beyond technical contributions to include policy-oriented inputs aimed at strengthening the overall cybersecurity posture of the EU (Figure 1). Additionally, the relationship with the European Commission has been reinforced, with meetings held with its Vice President, Věra Jourová, and the Director-General of DG CONNECT, Roberto Viola.

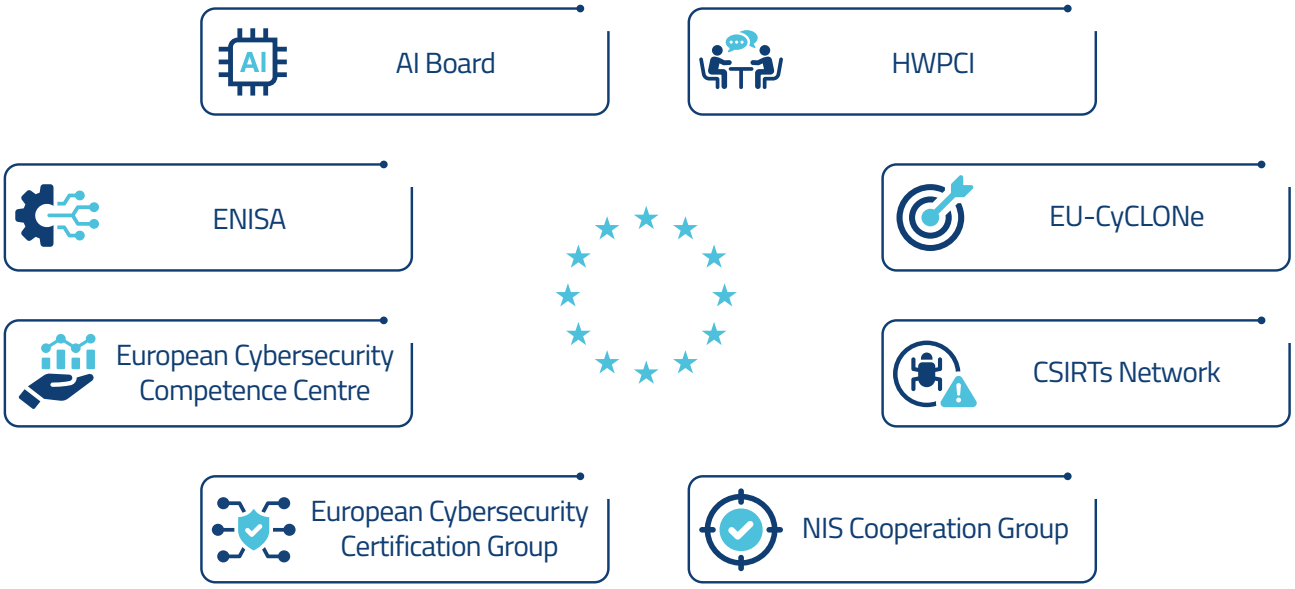


Figure 1 – Selected EU cyber forums and working groups

By engaging in regular, constructive dialogue with representatives of other EU Member States, the ACN facilitated the exchange of information, best practices and lessons learned. It also articulated national strategic perspectives on emerging challenges in the digital domain. This collaborative approach enabled the Agency to support the progressive alignment of cybersecurity policies across the Union, helping to foster a more harmonized and resilient European cybersecurity ecosystem capable of addressing cross-border threats in a coordinated and timely manner.

Besides the European Union dimension, the Agency's action was structured along three main geographical axes (Figure 2):

- G7 countries, with which Italy shares strategic goals related to cybersecurity and the protection of critical infrastructures;
- the broader Mediterranean and the Balkans, regions that are historically central to Italy's geopolitical interests; and
- the IMEC corridor (India-Middle East-Europe Economic Corridor), with the aim of strengthening ties with key countries through the Mediterranean and the Gulf region, all the way to India.

The Agency's commitment along these three axes was consolidated through its main international policy initiative in 2024: the establishment of the G7 Cybersecurity Working Group.

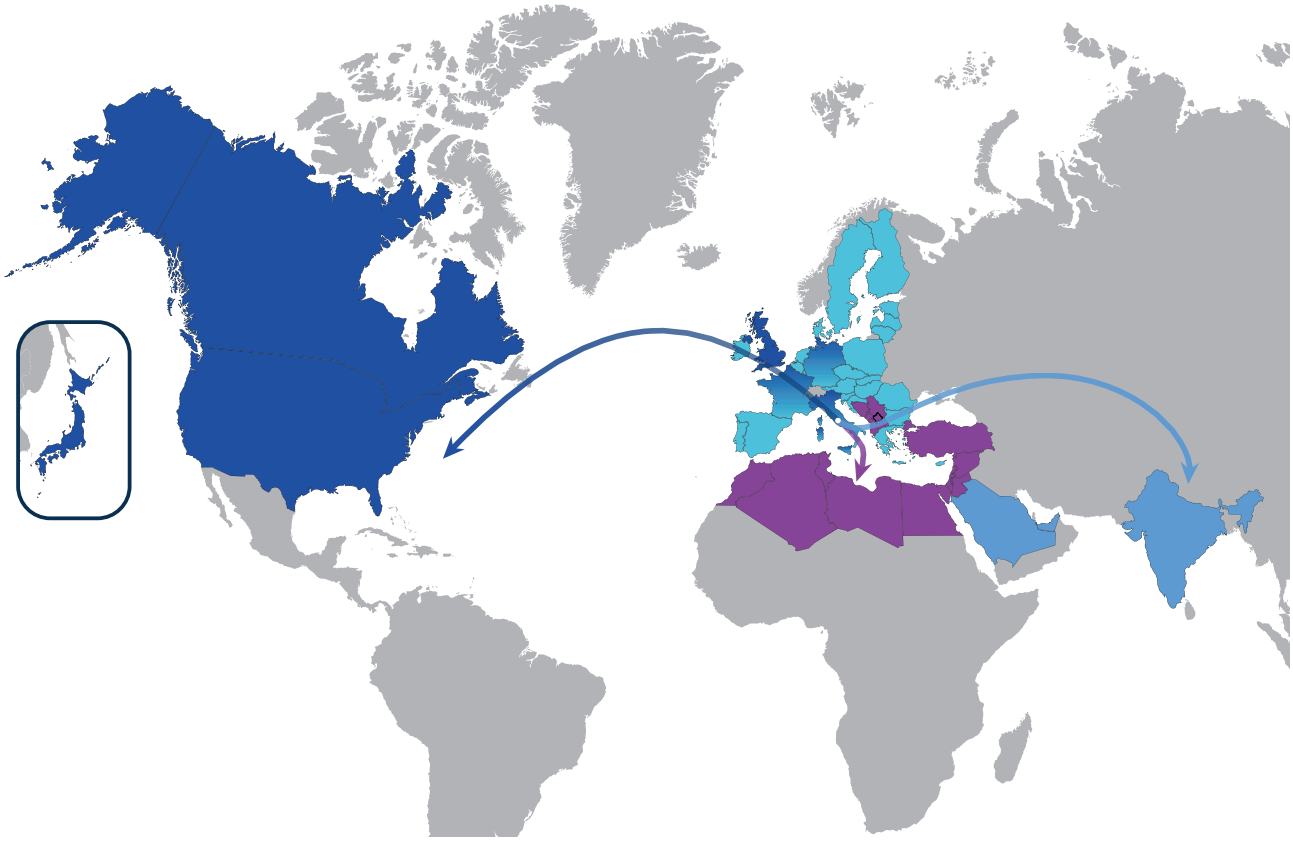


Figure 2 – 2024 international cooperation's main axes

The G7 Cybersecurity Working Group, composed of the leading cybersecurity agencies and centers from the G7 nations and the EU, was convened by ACN during Italy's 2024 G7 Presidency. Its goal is to strengthen cybersecurity and cyber resilience both at the national level and among G7 countries and the European Union and to advance the political mandate defined by the leaders during the Borgo Egnazia Summit (13-15 June 2024). On that occasion, a shared commitment

was expressed to take specific steps to enhance cyber resilience. The Working Group's activities are therefore complementary to ongoing efforts in areas such as cyber diplomacy, the security of financial infrastructure, technological innovation and the fight against cybercrime.

Over the year, the Working Group focused on protecting critical infrastructure supply chains, especially in the energy sector and addressing cybersecurity risks linked to artificial intelligence. It reviewed international and national cybersecurity laws and standards, identifying shared approaches among G7 countries for securing the digital supply chain in energy. On AI, the Group focused on two key areas: ensuring the security of AI system components and protecting infrastructure from cyberattacks involving malicious AI use.

The Agency has been particularly active in other multilateral fora as well, such as participating in the Counter Ransomware Initiative (CRI), contributing to negotiate the final declarations of the CRI Summit. It also supported the MAECI in the discussions at the UN level, including the negotiation of the Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. In terms of NATO activity, the ACN continued to work alongside the MAECI and the Ministry of Defense, following development of cyber defense policies, particularly those concerning resilience and cybersecurity.

At the bilateral level, in addition to strengthening the ties with the cyber agencies of the G7 partners, the ACN signed new memorandum of understandings to strengthen relations with Romania, Spain, the Vatican City State Governorate and Albania, while also initiated negotiations with other strategic countries for the Agency's international outlook. These agreements defined a cooperation framework aimed at strengthening cybersecurity in Europe and the Mediterranean, promoting common regional objectives. Furthermore, the Agency deepened contacts with executives from an array of other countries, with a view to broaden its bilateral relations.

The ACN's focus on international cooperation also aims to support technological research and development as well as cyber capacity building – that is, initiatives to strengthen the cyber skills and technological capabilities of countries, organizations, or communities to help them face cyber challenges. For this reason, in collaboration with the MAECI, the ACN organized the first National Conference on Cyber Capacity Building, held on 2 July 2024. The event brought together representatives from public institutions, businesses and universities with the aim of creating a national ecosystem to support third countries.

International exercises had a meaningful impact as well. At the EU level, the Agency was involved in the main EU exercise dedicated to managing cyber crises, "Cyber Europe 2024", and in the EU-CyCLONe exercise "BlueOLEx" 24. The latter exercise was held for the first time at the ACN's headquarters. At the NATO level, in coordination with the Italian Ministry of Defense, the Agency contributed to the planning and execution of several exercises, including cyber-range exercises which focused on cyber threat intelligence and situational awareness aspects. The ACN also participated in other international exercises, such as in the G7 framework, with regard to the financial sector and as part of the CRI, simulating a ransomware attack on the healthcare sector.

7. THE HUMAN FACTOR: EDUCATION AND PROMOTION OF A CYBERSECURITY CULTURE

The human factor is crucial for protecting the country's digital surface, in fact, the most advanced technology requires the involvement of people, both as professionals and as users. The ACN is committed to spreading cybersecurity skills at all levels to ensure a well-trained workforce and a citizenry aware of how to use digital tools securely. Education and the promotion of cybersecurity culture were identified by the 2022-2026 National Cybersecurity Strategy as enabling factors in achieving the protection, response and development goals set out by the strategy.

The Agency focused its efforts on the education of the Public Administration and young people. For the latter cooperation continued with the Italian National School of Administration (SNA), with basic and advanced courses delivered to over 500 employees from both central and local Administrations. Different initiatives were also launched in collaboration with the National Association of Italian Municipalities (ANCI). As part of this effort, the Agency supported the launch of ANCI's online education platform, the "*Accademia dei Comuni digitali*," and organized seminars to explain the new provisions introduced by Law No. 90/2024.

The already mentioned MoU with the Ministry of Education and Merit (Chapter 3) plays a key role in advancing cybersecurity education among young people. It encompasses a broad set of initiatives aimed at students, teachers and parents, with the objectives of: increasing awareness of digital risks such as cyberbullying, exposure to inappropriate content and privacy threats; promoting cyber-safety and digital hygiene by encouraging safe practices when using technology and digital devices; integrating cybersecurity into civic education to strengthen digital citizenship; and inspiring students to explore STEM careers, especially in the field of cybersecurity, through dedicated educational programs and competitions.

To raise cybersecurity awareness, several initiatives were organized targeting key sectors such as Public Administration and healthcare, given their central role in protecting the country from cyber threats. In particular, the Agency partnered with the Department of Public Administration of the Presidency of the Council of Ministers to launch a course aimed at public sector employees, made available on the Syllabus platform. Furthermore, the Agency started a series of events aimed at raising cybersecurity awareness in the healthcare sector, with the aid of a publication dedicated to the specific cyber threats identified in the sector.

At the same time, the ACN continued to focus on strengthening the cybersecurity posture of small and medium-sized enterprises. An awareness campaign was launched for Italian SMEs, featuring ads broadcasted on public and commercial TV and radio channels as well as guides and video tutorials for managers, employees and IT professionals. As part of the same campaign, a series of in-person events was launched across the country to promote a cybersecurity culture and raise awareness among SMEs. The roadshow, organized with the support of Confindustria and Confartigianato, kicked off in Naples in December 2024 and will continue in 2025 in various Italian cities.

8. 2022-2026 NATIONAL CYBERSECURITY STRATEGY: IMPLEMENTATION STATUS

The 2022–2026 National Cybersecurity Strategy is a cornerstone for strengthening the country's cybersecurity posture. Since its adoption in May 2022, the Agency has played a leading role in its implementation, coordinating activities, monitoring progress and supporting the various stakeholders involved.

In 2024, the ACN intensified its collaboration with Public Administrations, helping them define priorities and design targeted actions to enhance their cybersecurity posture, with an integrated vision that considers the resilience of the entire national ecosystem.

To finance the activities set out in the National Cybersecurity Strategy, the Agency can rely on two dedicated funds: the Fund for the implementation of the National Cybersecurity Strategy and the Fund for the management of cybersecurity. The resources of these funds are allocated on a yearly basis amongst the various Administrations responsible for implementing the Strategy through a Decree of the President of the Council of Ministers (Figure 1).

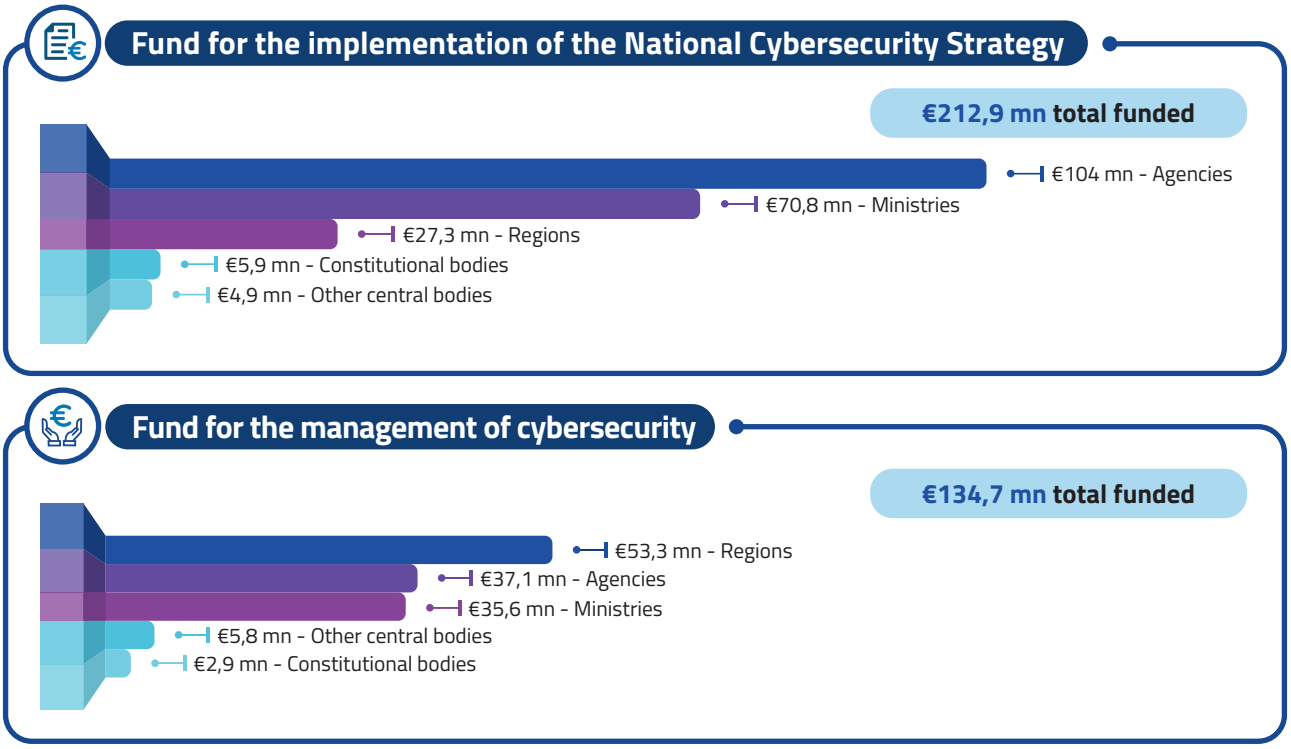


Figure 1 – Allocation of the 2024-2026 Strategy Funds

A key development this year was the direct involvement of the Italian Regions, which are benefitting of dedicated investments and working alongside Central Administrations to implement the Strategy. This expansion serves a dual purpose: on the one hand, it strengthens cybersecurity at the local level; on the other, it allows for a more accurate understanding of territorial specificities, enabling the adaptation of measures to different operational realities. The direct involvement of the Regions enhances the country's overall cyber protection by fostering a truly distributed and collaborative cybersecurity system, in which every institutional level actively contributes. Moreo-

ver, it may fill the gap between those organizations which have a small presence in remote areas of the country such as small and medium enterprises and the Government that is responsible for the national cybersecurity. Regions will benefit from €80,6 mn from these Funds, accounting for 21% of the total available resources.

The National Cybersecurity Strategy's Implementation Plan foresees 82 measures with the goal of acquiring, developing and strengthening the necessary national cyber capabilities to be implemented by various stakeholders. As of December 2024, 69 measures had been initiated: 63 were in progress and 6 had been fully achieved (Figure 2).

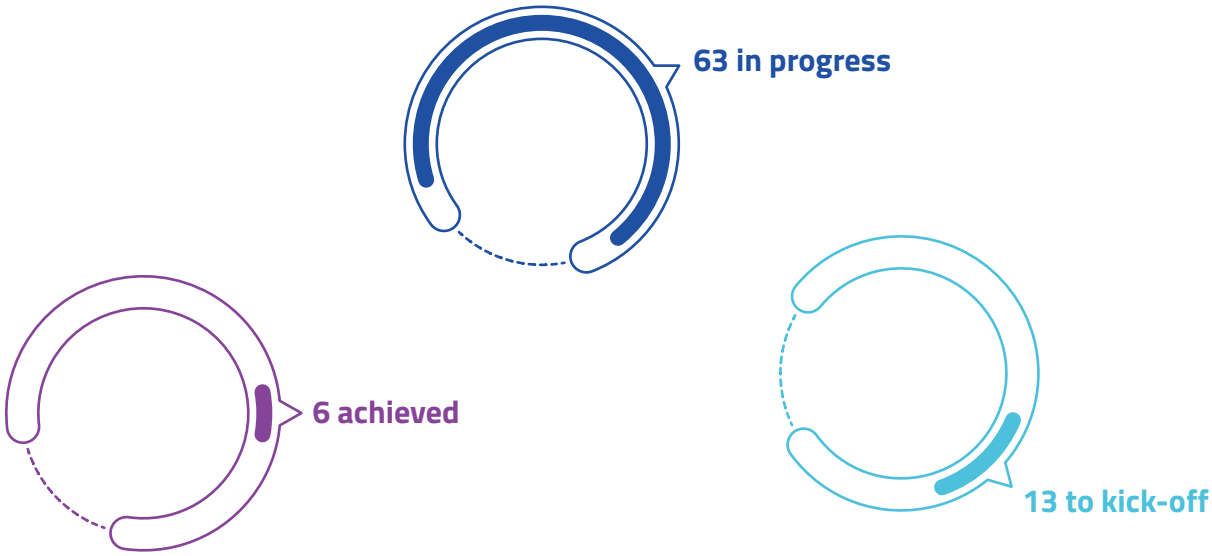


Figure 2 – implementation status of the 82 measures

It is worth noting that 33 measures were initially scheduled to begin in 2025; however, thanks to the collaboration with all the stakeholders involved and the coordinating role of the ACN, many were launched ahead of schedule. The remaining 13 measures will be initiated by 2026.

9. THE AGENCY IN 2024: STRENGTHENING THE STRUCTURE

In 2024, the Agency continued to strengthen its internal organization to meet the many challenges outlined in this Review. This development process spanned several areas – organizational structure, staff, financial resources, technological tools and communication activities – all contributing to the fulfilment of the Agency's mission.

In light of its expanding institutional role, the ACN continued recruiting highly qualified professionals through various channels, confirming its status as one of the youngest and most specialized public bodies in the country. Internal organization and processes were revised to simplify operations and improve their effectiveness and efficiency. As part of this effort, the Agency completed the acquisition of a new headquarters, in order to better suit its operational needs.

To respond effectively to current challenges and to define its objectives in a more structured manner, the Agency adopted the 2024-2026 Strategic Plan. This instrument serves as a unified document for governance, planning and coordination, setting out five strategic goals and identifying the key priorities and guiding principles that will shape the Agency over the next three years.

The 5 goals of the 2024-2026 Strategic Plan

1. *Protection of national strategic assets*
2. *Response to national and transnational cyber threats, incidents and crises*
3. *Secure development of digital technologies*
4. *Strengthening cybersecurity cooperation*
5. *Becoming a centre of excellence with flexible organizational model*

With reference to economic and financial aspects, the budget has seen a gradual increase in available resources. This growth has been driven both by its ordinary allocation and by new spending authorizations introduced through specific legislation, in line with the expanding responsibilities and duties assigned to the ACN. Special attention was also devoted to the responsible management of financial resources, with procurement activities carried out in compliance with the new Public Procurement Code and the specific regulations concerning national cybersecurity.

The year in review was also crucial to develop and enhance the IT systems of the Agency to make institutional activities more secure and efficient, while also ensuring compliance with data pro-

tection and document management regulations. Additionally, in order to operationalize the new requirements imposed by the NIS2 Directive a dedicated platform was developed to allow entities to comply with registration obligations, which must be fulfilled in the first months of 2025.

Lastly, the Agency strengthened its communication capacity by expanding the use of institutional channels, consolidating and spreading its voice towards the general population. Communicating its activities and positioning itself within the public debate required numerous initiatives. These efforts allowed the Agency to emphasize its role in addressing cybersecurity challenges and its contributions to national and international efforts in safeguarding digital infrastructures. The data in Figure 1 offers a snapshot of the main activities carried out in terms of media relations. These activities helped enhance the ACN's visibility and fostered stronger connections with various media outlets, ensuring a broad understanding of its ongoing efforts in cybersecurity and its role in the national security landscape.

Figure 1 – Media relations at a glance