CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

National Cybersecurity Organisation: ITALY

Samuele De Tomas Colatin

National Cybersecurity Governance Series

Tallinn 2020

About this study

This publication is part of a series of country reports offering a comprehensive overview of national cyber security governance by nation. The aims are to improve awareness of cyber security management in the various national settings, support nations in enhancing their own cyber security governance, encourage the spread of best practice, and contribute to the development of interagency and international cooperation.

Primarily focusing on NATO nations that are Sponsoring Nations to the CCDCOE, each country report outlines the division of cyber security roles and responsibilities between agencies, describes their mandates, tasks, and competences and the coordination between them. In particular, it covers the mandates of political and strategic management; operational cyber security capabilities and cyber incident management; military cyber defence; and cyber aspects of crisis prevention and management. It offers an introduction to the broader digital ecosystem of the country and outlines national cyber security strategy objectives to clarify the context for the organisational approach in a particular nation.

CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is a NATO-accredited cyber defence hub focusing on research, training and exercises. It represents a community of 25 nations providing a 360-degree look at cyber defence, with expertise in the areas of technology, strategy, operations and law. At the heart of the Centre is a diverse group of international experts from military, governmental, academic and industrial backgrounds.

The Centre is home to the *Tallinn Manual*, the most comprehensive guide to how international law applies to cyber operations. It organises the world's largest and most complex international live-fire cyber defence exercise, Locked Shields. Every spring in Tallinn, the Centre hosts the International Conference on Cyber Conflict, CyCon, a unique event bringing together key experts and decision-makers of the global cyber defence community. Since January 2018, the Centre has been responsible for identifying and coordinating education and training solutions in the field of cyber defence operations for all NATO bodies across the Alliance.

The Centre is staffed and financed by its member nations, currently: Austria, Belgium, Bulgaria, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States. NATO-accredited centres of excellence are not part of the NATO Command Structure.

www.ccdcoe.org
publications@ccdcoe.org

Disclaimer

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use for non-profit and non-commercial purposes, provided that copies bear a full citation.

Reports in this series

National Cyber Security Organisation in Czechia

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Italy

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in Turkey

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the United States

China and Cyber: Attitudes, Strategies, Organisation

National Cyber Security Organisation in Israel

Series editor: Kadri Kaska (NATO CCDCOE)

Information in this document has been checked for accuracy as of March 2020.

Table of Contents

1. Digital society

Country indicators

60.4 million	Population
38.8 million (67.9%)	Internet users (% of population)
301.3 thousand	Area (km^2)
34.4 thousand	GDP per capita (USD)

International rankings*

47th	ICT Development Index (ITU 2017)
24th	E-Government Development Index (UN 2018)
25th	Digital Economy and Society Index (EU 2019)
28th	Global Cybersecurity Index (ITU 2018)
15th	National Cyber Security Index (eGA 2019)

1.1 Digital infrastructure availability and take-up

A basic fixed broadband connection is practically universally available in Italy, including in rural areas; 99% of households are connected[1] and 90.2% of households have access to high-speed broadband of 30 Mbps and higher.[2] Although Italy's total fixed broadband coverage is better than the EU average, the total ultrafast coverage lags below the EU average, with rural fibre to the premises (FTTP) coverage amounting to a mere 0.8% against the 14.2% EU average as of 2018.

In a bid to improve fast-broadband penetration across the whole country and launch Italy towards the 'gigabit society', in 2015 the Government approved the Italian Strategy for Ultra-broadband (Piano Strategico Banda Ultra Larga),[3] which seeks to bring fast internet coverage to 85% of the population by 2020. In line with the 2020 European Commission's Digital Agenda,[4] the Strategy aims to develop infrastructure capable of offering services at speeds of 100Mbps and above, while ensuring that all citizens have access to download speeds of at least 30Mbps. It also promotes optical fibre deployment

* Various international rankings rely on different methodologies and sources for their scores. They can vary widely as a result.

[1] Unless explicitly stated otherwise, the statistics in this section are taken from the EU Digital Agenda Scoreboard, 'Digital Economy and Society Index, Country Profile: Italy', https://ec.europa.eu/digital-single-market/en/scoreboard/italy (DESI Report).

[2] Next Generation Access includes the following technologies: FTTH, FTTB, Cable Docsis 3.0, VDSL and other broadband performing at least at 30 Mbps in download. EU Open Data Portal, 'NGA broadband coverage/availability' https://data.europa.eu/euodp/it/data/dataset/DpWNLE4HUdjQte15bq0tRQ.

[3] Italian Ministry of Economic Development (MISE), 'Italian Strategy for ultra-broadband' (available in English), http://bandaultralarga.italia.it/en/strategy-high-speed-broadband/intro/.

[4] European Commission, 'Shaping the Digital Single Market', https://ec.europa.eu/digital-single-market/en/europe-2020-strategy.

to ‘white areas’[5] which cover approximately a quarter of the Italian population.[6] Benefitting from EU structural funds,[7] the Italian government aims to bring a fast broadband connection to ‘market failure’ areas where commercially-driven investment in internet infrastructure is not expected.[8]

4G mobile coverage reaches 97% of households. Italy is a pioneer in readiness for fifth-generation (5G) mobile technology[9] and ranks second among EU member states for the assignment of 5G spectrum broadband. 94% of the 2090 MHz spectrum harmonised at the EU level for wireless broadband had already been assigned by April 2019. Italy’s **Telecommunications Regulator and Competition Authority** (Autorità per le Garanzie nelle Comunicazioni - AGCOM) held the latest 5G multi-band auction in October 2018, assigning spectrum in both the low, medium and high bands (the 700-MHz, 3.6-3.8 GHz, and 26.5-27.5GHz bands), with all of Italy’s five mobile network operators having obtained a 5G spectrum licence.[10] The two largest mobile carriers, TIM[11] and Vodafone,[12] have already launched their 5G commercial services in selected cities, and the remaining three, Wind-Tre, Iliad and Fastweb, are preparing to do so. The latter struck a deal with Wind Tre to share the 5G frequencies and build a joint proprietary 5G network reaching 90% of the nation by 2026.[13]

1.2 Digital public services

In 2017, Italy introduced the last in a series of reforms of the Digital Administration Code (Codice dell’Amministrazione Digitale, CAD) with Legislative Decree n. 217 of 2017.[14] The decree updated the existing E-Government Code which came into force in 2006.[15] The Digital Administration Code aims to provide a clear legal framework for the development of e-government and the creation of a user-friendly digital public administration. Italy ranks 18th among EU member states in the provision of digital public services. Although it performs very well in open data and e-health services, the level of online interaction between public authorities and the public is low and only 37% of internet users needing to submit forms did so online.[16]

[5] On white areas see, European Commission Press Release Database, ‘State aid: Commission adopts Guidelines for broadband networks – frequently asked questions’ https://europa.eu/rapid/press-release_MEMO-09-396_en.htm?locale=en, 17 September 2009.

[6] INFRATEL, ‘White Areas Plan’ (available in English), http://bandaultralarga.italia.it/en/white-areas-plan/introduction/.

[7] INFRATEL, ‘Objectives’ (available in English) http://bandaultralarga.italia.it/en/strategy-high-speed-broadband/objectives/.

[8] TeleGeography, ‘Open Fibre awarded third regional broadband tender’, https://www.telegeography.com/products/commsupdate/articles/2018/12/19/open-fiber-awarded-third-regional-broadband-tender/, 19 December 2018.

[9] In 2017, the Italian Ministry of Economic Development (MISE) launched the programme ‘5G in 5 Cities’, an early pre-commercial trial for testing 5G wireless communications; see, MISE, http://bandaultralarga.italia.it/en/5g-5-italian-cities/ (available in English).

[10] European 5G Observatory, ‘National 5G Spectrum Assignment: Italy’, https://5gobservatory.eu/5g-spectrum/national-5g-spectrum-assignment/#1533310457982-93376798-7871.

[11] European 5G Observatory, ‘TIM launches 5G services in parts of Rome and Turin with new 5G plans’ https://5gobservatory.eu/tim-launches-5g-services-in-parts-of-rome-and-turin-with-new-5g-plans/, 28 June 2019.

[12] European 5G Observatory, ‘Vodafone Italia switches on 5G in 5 cities’, https://5gobservatory.eu/vodafone-italia-switches-on-5g-in-5-cities/, 10 June 2019.

[13] TeleGeography, ‘Fastweb becomes Italy’s fifth MNO’ https://www.telegeography.com/products/commsupdate/articles/2019/07/31/fastweb-becomes-italys-fifth-mno/, 31 July 2019; Wind Tre, ‘Wind Tre and Fastweb announce a strategic agreement for the deployment of a nationwide state-of-the-art 5G network’ https://www.windtre.it/EN/Press-&-Events/press-releases/Istitutional-Press-Releases/2019/windtre-fastweb-agreement-5g.aspx, 25 June 2019.

[14] Gazzetta Ufficiale della Repubblica Italiana (available only in Italian), ‘DECRETO LEGISLATIVO 13 dicembre 2017, n. 217’, https://www.gazzettaufficiale.it/eli/id/2018/1/12/18G00003/sg.

[15] Gazzetta Ufficiale della Repubblica Italiana (available only in Italian), ‘DECRETO LEGISLATIVO 7 marzo 2005, n. 82’, https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2005-05-16&atto.codiceRedazionale=005G0104&elenco30giorni=false.

[16] 2019 EU DESI Country Report – Italy, 13.

To coordinate the digitalisation of Italian public administration, in 2012 the Italian government established **the Agency for Digital Italy** (Agenzia per l'Italia Digitale - AgID).[17] AgID is the technical agency of the Presidency of the Council of Ministers and drafts and coordinates the implementation of the Three Year Plan for Information Technology in Public Administration, which sets the guidelines and actions for the digitalisation process.[18] AgID also hosts CERT-PA, the Public Administration Computer Emergency Response Team (see Section 3.2).[19]

Many eGovernment platforms and services have already been implemented. The e-Identification and e-Authentication services are maturing with the introduction of the electronic identity card[20] containing a set of personal data including the holder's fiscal code, blood group and fingerprint scan;[21] the qualified electronic signature[22] (digital signature); and the public digital identity system (Sistema Pubblico di Identità Digitale - SPID) which allows citizens to access the online services of the public administrations with a single digital identity.[23] Online portals have also been activated to give access to data and information such as services for businesses and entrepreneurs,[24] Italian normative legislation,[25] and open[26] and spatial or geographic data.[27] Enabling platforms for processing electronic payment to public authorities[28] and providing public administration electronic invoicing have also been introduced,[29] and a national resident and population register is under development.[30] The portal is owned and maintained by the Ministry of the Interior and is a single and centralised registry containing up-to-date information about addresses and civil states of Italian nationals at home and abroad.[31]

AgID is now committed to the creation of a public administration cloud[32] following the ongoing rationalisation of national public data centres.[33] National strategic nodes will use the public administration's physical infrastructure which will be certified by evaluation groups tasked by AgID. The preliminary evaluations are necessary to ensure a common security standard for infrastructure offering public administration cloud services. This is in progress and it is part of the 2019-2021 Three Year Plan for Information Technology in Public Administration.

[17] AgID, 'Responsibilities and functions' (available in English), https://www.agid.gov.it/en/agency/responsibilities-and-functions.

[18] AgID, 'Three-Year Plan for ICT in Public Administration 2017-2019' (available in English), https://www.agid.gov.it/en/node/1746/piano-triennale, 2017.

[19] AgID, 'CERT-PA' (available in English), https://www.agid.gov.it/en/security/cert-pa.

[20] Digital Transformation Team, 'Electronic Identity Card (EIC)' (available in English) https://teamdigitale.governo.it/en/projects/cie.htm, 2019.

[21] Personal data, biometric key and digital signature are only stored in the card and are not kept in any central database. They can only be released and used with the holder's permission via pin-code submission.

[22] AgID, 'Qualified Electronic Signature' (available in English), https://www.agid.gov.it/en/platforms/qualified-electronic-signature.

[23] The Public Digital Identity is provided by both public and private entities free of charge if the identity is ascertained in person and purchased if it is issued by webcam. AgID, 'SPID – Public Digital Identity System' (available in English), https://www.agid.gov.it/en/platforms/spid, 2019.

[24] Cliclavoro, https://www.cliclavoro.gov.it/Pagine/default.aspx, Impresainungiorno, http://www.impresainungiorno.gov.it/.

[25] Normattiva – Il portale della legge vigente, https://www.normattiva.it/.

[26] AgID, 'Open Data' (available in English), https://www.agid.gov.it/index.php/en/data/open-data.

[27] Geodati, 'Repertorio Nazionale dei Dati Territoriali' (available in English), https://geodati.gov.it/geoportale/eng/.

[28] AgID, PagoPA (available in English), https://www.agid.gov.it/index.php/en/platforms/pa-payment-system.

[29] AgID, Electronic Invoicing (available in English), https://www.agid.gov.it/index.php/en/platforms/electronic-invoicing.

[30] AgID, 'ANPR – National Registry of Resident Population' (Anagrafe Nazionale della Popolazione Residente) (available in English), https://developers.italia.it/en/anpr/.

[31] According to the 2019 EU DESI Country Report, so far, the register comprises the data from only 21% of Italian municipalities. *See*, 2019 EU DESI Country Report – Italy, 14.

[32] AgID, 'PA Cloud' (available in English), https://www.agid.gov.it/index.php/en/infrastructures/pa-cloud.

[33] AgID, 'Entra nel vivo il processo di razionalizzazione dei data center pubblici e formazione dei PSN' (available only in Italian), https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2019/07/05/entra-vivo-il-processo-razionalizzazione-data-center-pubblici-formazione-psn, 5 July2019.

1.3 Digitalisation in business

Italian enterprises are lagging behind in taking advantage of the opportunities offered by online commerce. Apart from the low level of Italian internet users shopping (47%) and selling (11%) online (the EU averages are 60% and 23%, respectively), only 10% of SMEs sell online, 6% sell cross-border, and the average turnover from online sales is around 8%. Despite these low figures, business-to-consumer e-commerce continues its upward trends, reaching a total of 41.5 billion revenues in 2018.[34] In terms of the integration of digital technology by businesses, Italy ranked 23rd among EU countries in both 2018 and 2019.[35]

2. National cybersecurity strategy and legal framework

2.1 National cybersecurity foundation

The original National Strategic Framework for Cyberspace Security (NSF)[36] and the attached National Plan for Cyberspace Protection and ICT Security[37] were released in 2013 following the adoption of the Prime Minister's Decree of 24 January 2013 ('Decreto Monti').[38] The decree and the two attached documents constituted the blueprint for the Italian national cybersecurity architecture. While the NSF identifies the roles and tasks for the public and private sectors in handling cyber threats and sets guidelines for the protection of cyberspace, the National Plan identifies a set of priorities for the correct deployment of the NSF.[39]

The 2013 prime ministerial decree introduced a complex crisis management structure, due to the high number of interactions between various public actors such as different departments of the Presidency of the Council of Ministers, several other ministries and AgID.[40] This, however, interfered with coordination initially, especially in the case of a wide-ranging crisis, which is why a new Prime Ministerial Decree (Decreto Gentiloni)[41] and an updated Action Plan[42] were adopted in 2017 to make the national cybersecurity architecture more efficient. The 2017 decree aimed at reorganising the entities

[34] CorCom, 'E-commerce italiano a quota 42 miliardi' (available only in Italian), https://www.corrierecomunicazioni.it/digital-economy/e-commerce-italiano-a-quota-42-miliardi-al-top-lo-shopping-su-smartphone/, 16 April 2019.
[35] 2019 EU DESI Country Report – Italy, 11.
[36] Italian Presidency of the Council of Ministers, 'National Strategic Framework for Cyberspace Security', https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf, 2013.
[37] Italian Presidency of the Council of Ministers, 'The National Plan for Cyberspace Protection and ICT Security' (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf (2013).
[38] Decreto del Presidente del Consiglio dei Ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.' (available only in Italian) http://www.sicurezzacibernetica.it/db/[2013]%20Decreto%20PCM%2024%20gennaio%202013%20-%20Direttiva%20recante%20indirizzi%20per%20la%20protezione%20cibernetica%20e%20la%20sicurezza%20informatica%20nazionale.pdf, 24 January, 2013.
[39] Decreto del Presidente del Consiglio dei Ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali', https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf, 17 February, 2017.
[40] Cyber Security National Lab – CINI, 'The Future of Cybersecurity in Italy: Strategic focus areas', https://www.consorzio-cini.it/images/Libro-Bianco-2018-en.pdf, 2018, 16.
[41] Decreto del Presidente del Consiglio dei Ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali', https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf, 17 February, 2017.
[42] Italian Presidency of the Council of Ministers, 'The Italian Cybersecurity Action Plan' (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf, 2017.

participating into the Italian cybersecurity architecture, while the Action Plan updates the 2013 National Plan's regulatory framework and objectives, setting out the operational guidelines and actions to be executed for the correct implementation of the National Strategic Framework. In addition, the 2017 decree and updated Action Plan were reviewed to incorporate the new cyber security requirements set by the EU NIS Directive, which had been transposed into the Italian national legislation in May 2018.

2.2 National cybersecurity strategy

The 2017 Action Plan takes the lessons learned from the first steps under the previous cybersecurity strategy, while recognising that the 2014-2015 efforts to protect networks and systems proved patchy, with discrepancies both horizontally – between public and private stakeholders – and vertically within the same domain.[43] To correct this, the plan outlines eleven 'Action Items' to strengthen cooperation between the two sectors:

1. **Strengthening intelligence, police, civil protection and military defence capabilities** to secure ICT cyber exploitations through improved cyber incident management.
2. **Enhancing organisational preparedness, coordination and dialogue between private and public stakeholders.** Interoperability among actors is paramount since critical infrastructures are managed and operated by private organisations.
3. **Promoting cybersecurity culture, education and training** to empower not only experts and cyber operators but also citizens, businesses and the public administration.
4. **Enhancing international cooperation and organising cyber exercises at national level**, as cyber threats are transnational, requiring a common level of competence and preparedness to counter them.
5. **Strengthening the readiness of competent national bodies for incident prevention, response and remediation.** The existing public Computer Emergency Response Teams (National CERT and PA-CERT) will merge their tools and procedures in a coordinated cyber incident management effort.
6. **Updating cybersecurity legislation according to technological developments and ensuring compliance with international obligations**, considering the high pace of regional and global legislative developments.
7. **Ensuring compliance with standard security requirements and protocols for the protection of high-levels of networks**, updating the national framework of information systems identifying basic security requirements and ICT security certifications, which consider international standards and best practices.
8. **Supporting industrial and technological development** by stimulating the creation of a secure and resilient supply chain for ICT components supported by an efficient evaluation and certification process.
9. **Fostering effective strategy and operational communication** and developing coordination capacity on situational awareness to facilitate response and remediation activities.
10. **Ensuring streamlining of financial resources,** not only to promote efficient cyber defence spending measures in the public, private and cooperation programmes but also to identify the economic impact of cyber incidents.
11. **Implementing a national system of cyber risk management** to be able to identify a unique and agreed cyber-risk management methodology for essential services, critical infrastructure and other national strategic actors.

[43] Italian Presidency of the Council of Ministers, 'The Italian Cybersecurity Action Plan' (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf, 2017, 9.

To facilitate the quick improvement of the national cybersecurity framework, the 2017 Action Plan identifies eight priorities, labelled 'core tasks':

1. review governance and responsibilities of the National Cyber Security Management Board (NSC);
2. simplify decision making procedure for cyber crisis management;
3. reduce complexity within the national cybersecurity framework through the consolidation of organisations;
4. the gradual merging of CERTs;
5. the creation of a National Cybersecurity Evaluation and Certification Centre;
6. the creation of a venture capital fund or foundation to support private companies, academic research, start-ups and other entrepreneurial activities;
7. the creation of a National Cybersecurity R&D Centre; and
8. the creation of a National Cryptographic Centre.

2.3 Cybersecurity legislation

Network and information systems security

With the entry into force of Legislative Decree 65 on 18 May 2018,[44] Italy has implemented EU Directive 2016/1148[45] on the security of network and information systems (the NIS Directive), and adapted its cyber architecture to the new cyber security organisational standards provided by the EU. To improve preparedness and collaboration in preventing cyber threats against networks and information systems, the NIS Directive requires member states to designate one or more national competent authorities and, within one of them, to appoint a single point of contact[46] to ensure cross-border cooperation in case of a cyber event.

The Directive also requires member states to identify national public and private operators of essential services and digital service providers[47] which integrates certain security measures and reports on incidents to the national Computer Security Incident Response Team (CSIRT). The areas of competence identified by the EU NIS Directive are health, energy, transportation, banking, financial market infrastructures, water supply and distribution services and digital infrastructure.[48]

On 12 December 2018, the Italian Government adopted the Telecommunications Decree,[49] updating the 2003 Code on electronic communications and imposing on private Internet Service Providers (ISPs) providing internet access to the public, certain security measures and a duty to notify of relevant incidents. According to the new Decree, ISPs shall ensure:[50]

- the physical security of the premises where servers and strategic infrastructures are physically located;

[44] Gazzetta Ufficiale della Repubblica Italiana, 'Decreto Legislativo 18 maggio 2018, n. 65' (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg.

[45] Directive (EU) 2016/1148 of the European Parliament and of the Council,, https://eur-lex.europa.eu/eli/dir/2016/1148/oj, 6 July 2016.

[46] Ibid, Article 8.

[47] Ibid, Article 5.

[48] Ibid, ANNEX II.

[49] Gazzetta Ufficiale della Repubblica Italiana, MISE, Decreto 12 dicembre 2018, 'Misure di sicurezza ed integrita' delle reti di comunicazione elettronica e notifica degli incidenti significativi' (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2019/01/21/19A00317/sg.

[50] MISE, Audizione Commissione Finanze del Senato, Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione ISCTI, 'Reti 5G: Problematiche di Cyber Sicurezza ed Iniziative in Corso' (PDF available only in Italian), http://www.senato.it/application/xmanager/projects/leg18/attachments/documento_evento_procedura_commissione/files/000/001/554/DOCUMENTO_PERVENUTO.pdf, last accessed 14 March 2020.

- compliance with technological standards for what concerns procurement and adaptation or implementation of network infrastructure;
- preventive testing of networks and information systems and implementation of new versions of the software before the connection to the network and constant monitoring of critical systems;
- specific internal procedures are in place aimed at ensuring network security;
- duty to notify a cyber incident to the CSIRT.

In 2018, Italy designated the NIS competent authorities as the Ministry of the Economic Development, the Ministry of Infrastructures and Transport, the Ministry of Economy and Finance, the Ministry of Health and the Ministry of the Environment, Land and Sea Protection.[51] These ministries identified the national public and private providers of essential services and digital service providers which are required to adopt security measures and notify of relevant incidents affecting the availability of their service to the CSIRT. According to the 2018 Security Intelligence Department Report to the Italian Parliament,[52] Italy has identified 465 operators of essential services (Operatori di Servizi Essenziali - OSE)[53] in the areas of competences of the NIS authorities.[54] Due to its central main position in the Italian cyber security architecture, the Security and Intelligence Department has been appointed as the NIS single point of contact (see Section 3.1).

Cybersecurity certification

With the advent of new internet architectures in areas such as Machine-to-Machine (M2M) communication and the Internet of Things (IoT), new information and telecommunication technology (ICT) tools will be implemented in national infrastructure and by national strategic operators. Therefore, the cybersecurity certification framework within ICT procurement has become increasingly important. The 2017 Action Plan foresees a high level of network and information systems security, by strengthening the ICT security certification and stressing the need for a secure and resilient supply chain review.[55]

Since the 1990s, Italy has had a certification scheme for ICT products in place. This national assessment scheme (Schema Nazionale di Certificazione)[56] have been reviewed and expanded over the years to include the necessity for stringent security standards which are demanded by the latest development in technology. The national assessment scheme is active on three distinct levels. Since 1995, the **National Authority for the Security** (Autorità Nazionale per la Sicurezza - ANS) has ensured the security of ICT products and services that handle classified data. The technical evaluations are guaranteed by the **Defence Evaluation Centre** (Centro di Valutazione della Difesa - CE.VA)[57] which applies the European Information Technology Evaluation Criteria (ITSEC) and the international Common Criteria (CC).[58]

[51] Legislative Decree nr. 65, 'Implementing EU Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union' (available only in Italian), http://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg (18 May 2018), Article 7, para 1.

[52] Sistema di Informazione per la Sicurezza della Repubblica Italiana, 'Relazione al Parlamento sulla politica dell'informazione per la sicurezza 2018' (available only in Italian), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf (2019), see section 'Documento di Sicurezza Nazionale', 13-14.

[53] See graph in the Appendix section, 'European Points of Contact under the Network and Information Security (NIS) Directive'.

[54] The identified areas of competence are health, energy, transportations, banking, financial market infrastructure, water supplying and distribution services and digital infrastructures.

[55] See Action Item 7, Italian Presidency of the Council of Ministers, 'The Italian Cybersecurity Action Plan' (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf (2017).

[56] Ministero della Difesa Italiano, 'Schema di Certificazione' (available only in Italian), https://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pagine/Schema_certificazione.aspx.

[57] Ministero della Difesa Italiano, 'Ce.Va. Difesa' (available only in Italian), https://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pagine/default.aspx.

[58] Ministero della Difesa Italiano, 'Gli Standard di Valutazione' (available only in Italian), https://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pagine/standard_valutazione.aspx.

In 2003, the Prime Ministerial Decree of 30 October[59] approved the national evaluation scheme for ICT non-military products and services lying outside the national security context, valid for public, private and commercial spheres. The competent body for this certification is the **Computer Security Certification Organisation** (Organismo di Certificazione della Sicurezza Informatica - OCSI). It also selects and accredits **security evaluation laboratories** (Laboratori per la Valutazione della Sicurezza - LVS), which verify the integrity of ICT systems in accordance with the ITSEC and ITSEM and the CC criteria.

As provided for in the Gentiloni Decree,[60] in 2019 Italy activated a **National Centre for Evaluation and Certification** (Centro di Valutazione e Certificazione Nazionale – CVCN)[61] as part of the Ministry of Economic Development. It verifies the absence of vulnerabilities in third-party software and hardware used by organisations with critical or strategic functions. The functions of the CVCN have been confirmed by a recent law approved by the Presidency of the Council of Ministries.[62] It prescribes the establishment of a national cyber security perimeter (Perimetro di Sicurezza Cibernetico) made up of actors from the public and private sectors identified according to two specific criteria: they exercise an essential function for the state; and this function depends on networks, informatics systems or services whose availability, if affected by partial or total malfunction, disruption or improper use, may result in prejudice to national security. The law gives authority to the CVCN to impose software and hardware tests to verify the absence of vulnerabilities affecting the networks in question. The **Technical Committee for the Security of the Republic** (Comitato Tecnico Interministeriale per la Sicurezza della Repubblica - T-CISR), in collaboration with a representative from the Presidency of the Council of Ministries, defines the criteria to which the subjects will adhere and update their own networks and services.[63] Following evaluation tests, the CVCN may also impose conditions and specific protocols to be applied to ICT tools being used within the perimeter.[64] Specific conditions can also be applied to ICT tenders and they might suspend or render invalid a contract or assign it to a specific subject if needed.

The Decree also dedicates an article specifically to 5G. Referring to the special powers of the Italian government over companies of national interests,[65] the Decree extends the so-called 'Golden Power'[66] instrument to the procurement of 5G tools and technology.[67] Conditions on goods and services already

[59] Gazzetta Ufficiale della Repubblica Italiana, 'Decreto del Presidente del Consiglio dei Ministri 30 ottobre 2003' (available only in Italian), https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2004-04-27&atto.codiceRedazionale=04A04314&elenco30giorni=false (30 October 2003).

[60] Article 1, para 6(a).

[61] Ministero dello Sviluppo Economico, 'Centro di Valutazione' (available only in Italian), https://www.mise.gov.it/index.php/it/comunicazioni/istituto-superiore-comunicazioni/sicurezza-informatica/centro-valutazione.

[62] Gazzetta Ufficiale della Repubblica Italiana, 'Decreto Legge 21 settembre 2019, n.105' (available only in Italian), https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario;jsessionid=g6v+BHJq0BVT7oc+fikU6A__.ntc-as1-guri2a?atto.dataPubblicazioneGazzetta=2019-09-21&atto.codiceRedazionale=19G00111&elenco30giorni=true.

[63] Within this perimeter, the subjects providing services and products for the critical and essential functions of the state are obliged to report any incident to the CISR. Being unable to deliver the list of services, adhere to the criteria prescribed or unable to report relevant incidents according to the procedures set out by the Decree will result in administrative fines. Ibid, Article 1 para 8 and 9.

[64] Ibid, Article 1, para 6 and 7.

[65] Gazzetta Ufficiale della Repubblica Italiana, 'Decreto Legge 15 marzo 2012, n.21' (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2012/03/15/012G0040/sg.

[66] The Golden Power is a series of legislations that allows the public authority the exercise of special powers over public and private companies whose activities and sectors of competence are qualified as strategically relevant for the public interest. When a serious threat for the public interest subsists, depending on the circumstances and following reasonable grounds, objective criteria and the principle of proportionality, the government might intervene by, opposing equity investments, imposing conditions and regulations or vetoing the adoption of corporate decisions. See, Presidenza del Consiglio dei Ministri, 'Golden Power', (Available only in Italian), http://www.governo.it/it/dipartimenti/dip-il-coordinamento-amministrativo/dica-att-goldenpower/9296.

[67] Gazzetta Ufficiale della Repubblica Italiana, 'Decreto Legge 21 settembre 2019, n.105' (available only in Italian), https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario;jsessionid=g6v+BHJq0BVT7oc+f

acquired through contracts previously authorised by the government might be modified or integrated with additional security measures. If necessary, tools or products deemed seriously inadequate will be substituted for security reasons.[68]

3. National cybersecurity governance

3.1 Strategic leadership and policy coordination

The 2017 Decreto Gentiloni identifies the bodies participating in the Italian cyber security architecture, outlining their organisation and tasks.[69] The declared goal is to render the institutional cyber security architecture easier to coordinate, improving prevention of and response to cyber events.[70]

The Prime Minister is the highest authority in the Italian cybersecurity architecture[71] and is supported by the **Inter-Ministerial Committee for the Security of the Republic** (Comitato Interministeriale per la Sicurezza della Repubblica - CISR),[72] which works as an advisory board to the Prime Minister, including in cybersecurity matters. The CISR is composed of the Ministry of Foreign Affairs, the Ministry of Interior Affairs, the Ministry of Justice, the Ministry of Defence, the Ministry of Economy and Finance, and the Ministry of Economic Development. It can be summoned by the Prime Minister for advisory purposes and in the event of a cyber crisis which affects national security. The CISR also develops and adopts new strategies related to the national cyber security framework. The Director General of the **Security and Intelligence Department** (Dipartimento delle Informazioni per la Sicurezza - DIS) is also the secretary of the CISR.

3.2 Cybersecurity authority and cyber incident response

The work of the CISR is supported by the **Technical Committee for the Security of the Republic** (Comitato Tecnico Interministeriale per la Sicurezza della Repubblica - T-CISR),[73] which has been confirmed by the updated cybersecurity framework and is chaired by the Director General of the Security and Intelligence Department (DIS). The T-CISR is responsible for the correct implementation of the cybersecurity national plan. It collects and analyses data from public and private entities to target cyber threats and recognise critical vulnerabilities, and it carries out an in-depth analysis of specific cyber incidents.[74]

The **Security and Intelligence Department** (Dipartimento Informazioni per la Sicurezza - DIS) coordinates all intelligence activities including cybersecurity,[75] overseeing the activities of the External Intelligence and Security Agency (AISE) and the Internal Intelligence and Security Agency (AISI). The

ikU6A__.ntc-as1-guri2a?atto.dataPubblicazioneGazzetta=2019-09-21&atto.codiceRedazionale=19G00111&elenco30giorni=true, Article 3.

[68] Ibid.

[69] For a visual representation, see graph in the Appendix section ‘Crisis Management - Actors of the Italian Cybersecurity Architecture’.

[70] Cyber Security National Lab – CINI, ‘The Future of Cybersecurity in Italy: Strategic focus areas’ (available in English), https://www.consorzio-cini.it/images/Libro-Bianco-2018-en.pdf, 2018, 16-17.

[71] Decreto del Presidente del Consiglio dei Ministri, ‘Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali’, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf (17 February, 2017), Article 3.

[72] Ibid, article 4.

[73] Ibid, article 5.

[74] Ibid.

[75] Italian Security Intelligence Department – DIS, ‘About us’ (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/english/about-us.html#DIS.

Department has a primary role in national cyber architecture.[76] In addition to defining and implementing the national cyber governance by chairing the Cyber Security Unit (NSC, see below), it also serves as a link to manage the relationships with EU, NATO, OSCE and the UN. The Legislative Decree of 18 May 2018 also identifies the Intelligence Department as the NIS Single Point of Contact[77] which ensures cross-border cooperation by linking the NIS member states' competent authorities and the Cooperation Group established in the European Commission.

The **Cyber Security Unit** (Nucleo per la Sicurezza Cibernetica - NSC)[78] is the interagency and intergovernmental operational body for cybersecurity within the national cyber architecture. It is responsible for preventing and preparing for a national cyber crisis, for declaring such a crisis, and for coordinating the responses by competent bodies following the Prime Minister's decisions.[79] Established within the DIS, the NSC is chaired by a Deputy Director General from the DIS and made up of a Military Advisor and representatives from the Intelligence Department[80] and from the Ministries of Foreign Affairs, Interior, Justice, Economic Development, Economy and Finance and the Department of Civil Protection (to manage the kinetic effects of a cyber event).[81] The NSC meets at least once a month and informs the DIS General Director of its activities. Within the NSC, an Early Warning and Cyber Incident Response Unit is always active to detect and respond to a cyber crisis.[82] In addition, the NSC collects notifications of malicious cyber events from abroad[83] and evaluates the severity of the incidents. It is also the national focal point for managing all necessary contacts with the UN, NATO and the EU in case of a cybersecurity crisis management[84] (see Section 3.4). The NSC is also responsible for promoting Italy's participation in cyber activities such as ENISA's 'Cyber Europe', the EU 'Blue OLEx[85]' and 'EU ELEx[86]' and the 'G7 Cyberincident Cross-border Coordination Exercise'.[87] It also contributed to the creation of the National Laboratory for Artificial Intelligence and Intelligent System.[88]

[76] Decreto del Presidente del Consiglio dei Ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali', https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf (17 February, 2017), Article 7.

[77] Decreto Legislativo 18 Maggio 2018 nr. 65 'Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione' (available only in Italian), http://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg, 18 May 2018,, Article 7, para 3.

[78] Ibid, article 8 and 9.

[79] Decreto del Presidente del Consiglio dei Ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali', https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf (17 February, 2017), Article 8, para 1.

[80] DIS (Security Intelligence Department), AISE (External Intelligence and Security Agency) and AISI (Internal Intelligence and Security Agency).

[81] Ibid, Article 8, para 2.

[82] Ibid, Article 9, para 2 b).

[83] Ibid, Article 9, para 3.

[84] Ibid, Article 9, para 2 f).

[85] ENISA, 'ENISA plays an active role at the first of its kind cyber crisis exercise, Blue OLEx 2019' (available in English) https://www.enisa.europa.eu/news/enisa-news/enisa-plays-an-active-role-at-the-first-of-its-kind-cyber-crisis-exercise-blue-olex-2019, 1 July 2019.

[86] European Parliament, 'EU Member States test their cybersecurity preparedness for free and fair EU elections' (available in English), https://www.europarl.europa.eu/news/it/press-room/20190404IPR35103/eu-member-states-test-cybersecurity-preparedness-for-free-and-fair-eu-elections, 5 April 2019.

[87] Reuters, 'G7 countries to simulate cross-border cyber attack next month: France' (available in English), https://www.reuters.com/article/us-g7-france-cyber/g7-countries-to-simulate-cross-border-cyber-attack-next-month-france-idUSKCN1SG1KZ, 10 May 2019.

[88] Italian Ministry of Foreign Affairs and International Cooperation and Department of Information for the Security of the Republic at the Prime Minister's Office (DIS), 'Cybersecurity in Italy- New Opportunities for Business' (available in English), https://www.esteri.it/mae/resource/doc/2019/09/esteri_cibersecurity_web.pdf, September 2019, 6.

National and sectoral CSIRTs

Italy has around 20 sectoral CERTs, dedicated to different areas of operations or tasked with different specialised roles to monitor and defend the interested networks from cyber threats.[89]

The **National CERT** (CERT-N),[90] part of the Ministry of Economics and Development, supports both the private sector and the citizens by sharing data of recent vulnerabilities and coordinating the response to large-scale cyber incidents. For a selected and restricted group of private and public partners, the CERT-N acts as a point of contact offering an information-sharing platform to spread information and alerts about cyber threats and incidents.

The **Public Administration CERT** (CERT-Pubblica Amministrazione)[91] is operated and coordinated by AgID to support the civil administration. It is tasked with defining recommendations, strategies and technical standards to raise awareness and inform authorities about issues related to information security and connected emergencies, detection and risk analysis methodologies, and protection and performance measurement initiatives.[92] In October 2019, a pilot information-sharing platform was launched to promote the automated transmission of indicators of compromise (IoC) among the national public authorities.[93] The testing phase is directed by the Cyber Security Unit in collaboration with the Security Intelligence Department. The goal is to launch by the end of 2019 a Cyber-Threat Intelligence platform (CTI) able to receive relevant information for the prevention and monitoring of cyber attacks. The establishment of the CTI platform is part of the 2019-2021 Three Year Plan for Information Technology in Public Administration.[94]

To adapt the national cyber architecture to the EU NIS Directive, Italy is in the process of merging the CERT-N and the CERT-PA into the **Italian Computer Security Incident Response Team** (CSIRT-Italia)[95] which was formed by Decree in 2018[96] within the Security Intelligence Department.[97] It will inherit the tasks of both the CERT-N and the CERT-PA serving as a point of contact between the EU member states CSIRTs net and the Cooperation Group within the European Commission.[98] Currently, CSIRT-Italia is in the process of being established.[99] During this transitional phase, the CERT-N and the CERT-PA will carry out the tasks of preventing and responding to cyber incidents.[100] CSIRT-Italia will receive notifications from the operators of essential services and digital service providers and will collaborate

[89] CSIRTs by Country - Interactive Map. Italy. https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Italy.

[90] CERT-N, 'Italian CERT-N Profile' (available in English) https://www.certnazionale.it/content/uploads/2015/10/IT-CERT_RFC_2350_1_7_EN.txt.

[91] CERT-PA, 'Italian CERT-PA Profile' (available in English) https://www.cert-pa.it/wp-content/uploads/2018/07/CERT-PA_RFC_2350.txt

[92] AgID, 'CERT-PA' (available in English), https://www.agid.gov.it/en/security/cert-pa.

[93] AgID, 'Sicurezza cibernetica: il CERT-PA avvia la fase pilota della piattaforma nazionale di contrasto agli attacchi informatici' (available only in Italian), https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/10/25/sicurezza-cibernetica-il-cert-pa-avvia-fase-pilota-piattaforma-nazionale-contrasto, 25 October 2019.

[94] Ibid.

[95] NIS Directive, Article 9.

[96] Gazzetta Ufficiale della Repubblica Italiana, 'Decreto Legislativo 18 maggio 2018, n. 65', Article 8 (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg.

[97] Decreto del Presidente del Consiglio dei Ministri, 8 Agosto 2019, 'Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano' (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2019/11/08/19A06940/sg, Article 3.

[98] As provided by Articles 10-11-12, EU NIS Directive.

[99] The Presidential Decree provides the full activation of the CSIRT by May 2020. See, Article 9, Decreto del Presidente del Consiglio dei Ministri, 8 Agosto 2019, 'Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano' (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2019/11/08/19A06940/sg.

[100] CSIRT Italia, 'La NIS in Pillole' (available only in Italian), https://www.csirt-ita.it/nis.html.

with the representatives of the other EU member states' CSIRTs, exchanging information on cyber threats or incidents.[101]

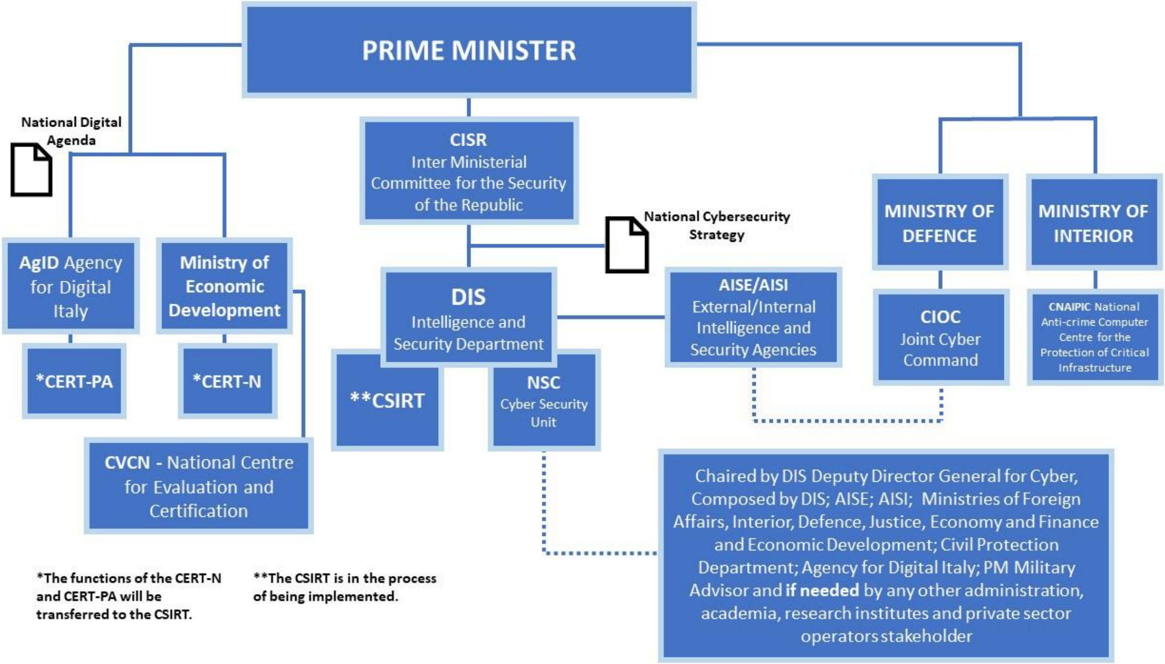

PRIME MINISTER
National Digital Agenda
CISR Inter Ministerial Committee for the Security of the Republic
National Cybersecurity Strategy
MINISTRY OF DEFENCE
MINISTRY OF INTERIOR
AgID Agency for Digital Italy
Ministry of Economic Development
DIS Intelligence and Security Department
AISE/AISI External/Internal Intelligence and Security Agencies
CIOC Joint Cyber Command
CNAIPIC National Anti-crime Computer Centre for the Protection of Critical Infrastructure
*CERT-PA
*CERT-N
**CSIRT
NSC Cyber Security Unit
CVCN - National Centre for Evaluation and Certification
Chaired by DIS Deputy Director General for Cyber, Composed by DIS; AISE; AISI; Ministries of Foreign Affairs, Interior, Defence, Justice, Economy and Finance and Economic Development; Civil Protection Department; Agency for Digital Italy; PM Military Advisor and if needed by any other administration, academia, research institutes and private sector operators stakeholder
*The functions of the CERT-N and CERT-PA will be transferred to the CSIRT.
**The CSIRT is in the process of being implemented.

Figure 1. Italian cybersecurity architecture[102]

Cybersecurity of critical infrastructure

Italy's dedicated entity overseeing the protection of national critical infrastructure against cyber-attack is the **National Anti-Crime Centre for the Protection of Critical Infrastructure** (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - CNAIPIC),[103] part of the Postal and Communication Police Department.[104] The Centre is a law enforcement agency and comprises an operational, a technical and an investigative unit. The CNAIPIC is in charge of preventing and repressing both common and terrorist cybercrimes; it is part of the Interpol and Europol collaboration and information exchange formats and it constitutes the Italian point of contact with foreign police departments. The CNAIPIC is constantly expanding its capacities by stipulating protocols and agreements with private sector entities to ensure an efficient and coordinated protection of national critical infrastructures across the whole national network.[105]

[101] Decreto del Presidente del Consiglio dei Ministri, 8 Agosto 2019, 'Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano' (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2019/11/08/19A06940/sg, Article 4.

[102] The figure consideres latest developments within the Italian cybersecurity architecture as of March 2020. The author's adaptation of the original scheme (partially outdated) at Ministry of Foreign Affairs and International Cooperation and Department of Information for the Security of the Republic at the Prime Minister's Office (DIS), 'Cybersecurity in Italy – New Opportunities for Business' (available in English), https://www.esteri.it/mae/resource/doc/2019/09/esteri_cibersecurity_web.pdf (September 2019), 7.

[103] Ministero dell'Interno, 'Decreto del 9 gennaio 2008' (available only in Italian). http://www1.interno.gov.it/mininterno/site/it/sezioni/servizi/old_servizi/legislazione/sicurezza/0994_2008_05_06_decreto_del_ministro_9_gennaio_2008.html.

[104] Commissariato di Polizia di Stato - 'CNAIPIC' (available only in Italian) https://www.commissariatodips.it/profilo/cnaipic/index.html.

[105] According to the latest report of the Postal and Communication Police Department, in 2018 eight new conventions have been agreed with WindTre, Sky Italia, Fincantieri, MM S.p.A., Monte dei Paschi di Siena, Consip, S.p.A., Nexi S.p.A. and BT Italia. See the report Questura di Roma, 'Resoconto attivita' della Polizia

3.3 Cyber crisis management

The Italian 2017 model of cybersecurity introduces a focused way to handle a cyber crisis, simplifying the crisis management structure and decision-making processes and streamlining both ordinary and emergency procedures.

The 2017 Decreto Gentiloni identifies the NSC as the body established within the DIS to handle a cyber crisis. The NSC substitutes for the NISP and is chaired by the DIS. The Board is supported by an early warning and cyber incident response unit, constantly able to receive information related to relevant cyber events for prevention and response, and any information useful for cyber situational awareness. The NSC analyses threats and alerts received from National CERT together with the Public Administration CERT, private operators, the CNAIPIC, Interpol and Europol, the **National Defence CERT** (CERT-Difesa), and the Intelligence Community.

The NSC, through the DIS Director General, keeps the Prime Minister up-to-date on any ongoing crisis and coordinates responses to the cyber events according to the Prime Minister's decisions. The Prime Minister is supported by the CISR, which is responsible for providing guidance in a cyber crisis (see Section 3.2).

It is also worth mentioning that, in case of a grave and imminent cybernetic crisis affecting networks providing an essential function of the state,[106] the Cyber Security Perimeter Decree provides that the Presidency of the Council of Ministry holds the capacity to order the partial or total deactivation of one or more tools used in the affected networks if it is necessary to mitigate or solve an ongoing emergency.[107] This authority is granted by deliberation of the CISR Committee and needs to take into account the principle of proportionality.[108]

3.4 Military cyber defence

The Italian Ministry of Defence has recognised cyber attack as a threat to national defence and security from the fifth domain of warfare, cyberspace. The Ministerial Directive on the Military Policy for the Year 2013 acknowledges the hybrid nature of modern conflict and underlines the need for Italy to strengthen both conventional and non-conventional capabilities, including in the cyber spectrum.[109] Additionally, through the 2015 White Paper for International Security and Defence, Italy recognises the urgency and need for creating 'specific defensive operational capabilities into the domain of cybernetics to preserve the safety of the national system and increase the solidity of the political, economic and social structures'.[110] Cyber defence is also addressed in the official Ministry of Defence Multi-Year Planning document 2019-2021 (Documento Programmatico Pluriennale – DPP),[111] which recognises the

Postale e delle Comunicazioni 2018', CNAIPIC section (available only in Italian), https://questure.poliziadistato.it/statics/35/comunicato-stampa---resoconto-polizia-postale-e-delle-comunicazioni-anno-2018.pdf?lang=it (31 December 2018).

[106] Gazzetta Ufficiale della Repubblica Italiana, 'Decreto Legge 21 settembre 2019, n.105' (available only in Italian), https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario;jsessionid=g6v+BHJq0BVT7oc+fikU6A__.ntc-as1-guri2a?atto.dataPubblicazioneGazzetta=2019-09-21&atto.codiceRedazionale=19G00111&elenco30giorni=true

[107] Ibid, Article 5.

[108] Ibid.

[109] Italian Ministry of Defence, 'Ministerial Directive on the Military Policy for the Year 2013' (available in English), https://www.difesa.it/Primo_Piano/Documents/2013/gennaio%202013/Direttiva%20Ministeriale_ENG.pdf, page 8.

[110] Ministero della Difesa Italiano, 'White Paper for International Security and Defence' (available in English) https://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf, 49.

[111] Ministero della Difesa Italiano, 'Documento Programmatico Pluriennale per la Difesa per il Triennio 2019-2021', Camera dei Deputati, DOC. CCXXXIV, N. 2 (available only in Italian). https://www.camera.it/leg18/494?categoria=234&idLegislatura=18.

extension of military operations into the cybernetic domain which must be protected and defended from the effects of cyber attacks on network or computer services and critical infrastructure.[112]

As a result, in 2017, in compliance with the National Defence White Paper guidelines and in line with the NATO Alliance commitments in the field of cyber defence,[113] Italy set up a military command exclusively in charge of conducting cyber operations, the **Joint Cyber Command** (Comando Interforze Operazioni Cibernetiche - CIOC). The main task of the Cyber Command is to protect the national Ministry of Defence systems and networks from cyber threats.[114] The Command set to achieve full operational capability by the end of 2019. Currently, the Cyber Command is physically co-located within the Italian Armed Forces CERT (CERT Difesa - CERT-D) and is tasked with conducting defensive cyber operations and cyber network defence and vulnerability assessments and penetrations tests.[115]

To enhance the work of the Joint Cyber Command, a Cyber Lab has been established within it to generate the tools required to study cyber vulnerabilities and training cyber capabilities in a controlled virtual environment.[116] In addition, preliminary testing for the development of a live-fire range has been conducted within the **Italian Armed Forces School of Telecommunications** (Scuola delle Telecomunicazioni delle Forze Armate, STELMILIT) in Chiavari, Genova. The purpose is to create a suitable environment for technical cyber training.[117]

Further operational developments in the Italian Ministry of Defence's cyber organisation are included in the document Strategic Concept of the Chief of the Italian Defence General Staff, (Il Concetto Strategico del Capo di Stato Maggiore della Difesa).[118] The creation of a new Joint Command has also recently been approved.[119] The Ministry of Defence, through the Italian Defence General Staff, is organising the **Joint Command for Network Operations** (Comando Operazioni in Rete – COR). This will become the lead cyber department available to the **Defence's Joint Operational Command** (COI - Comando Operativo Interforze) tasked with conducting defensive operations to protect the cyberspace of the Italian national military apparatus and the Ministry of Defence.[120] The COR will be able to ensure a better-coordinated approach in response to cyber attack by gathering under a common command chain the Italian Joint Cyber Command (CIOC), the C4 Command and the CERT-D, and will collaborate with the relevant cybersecurity departments of the Air Force, Navy and Army.[121]

[112] Ibid, 'Potenziamento 'Cyber Defence'' parte 2, 28.
[113] NATO, 'NATO Warsaw Summit 2016', 'Cyber Defence', https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
[114] Italian Presidency of the Council of Ministers,,'Italian Cybersecurity Action Plan' (available in English) https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf (2017), 13-14.
[115] CyCon 2019, 'Cyber Commanders Panel', https://www.youtube.com/watch?v=qDslaTRKPx8 see, speech delivered by former Italian Cyber Commander Air Vice-Marshal Francesco Vestito.
[116] Stato Maggiore della Difesa, 'Informazioni della Difesa' (available only in Italian), https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf, 12-16, March 2017.
[117] Ministero della Difesa Italiano, 'Forze Armate: testato il poligono cibernetico UNAVOX' (available only in Italian) https://www.difesa.it/SMD_/Eventi/Pagine/Difesa_testato_il_poligono_cibernetico_UNAVOX.aspx, 6 February, 2019.
[118] Chief of the Italian General Staff, Chief of Defence General Enzo Vecciarelli, 'Il Concetto Strategico del Capo di Stato Maggiore della Difesa' (available only in Italian), https://www.difesa.it/SMD_/CaSMD/concetto_strategico_casmd/Pagine/default.aspx.
[119] Ministero della Difesa Italiano, 'Comando per le Operazioni in Rete (COR)' (available only in Italian), https://www.difesa.it/Protocollo/AOO_Difesa/SMD/Pagine/SCOR.aspx.
[120] *See*, 'Obiettivi di Breve Termine' in, 'Il Concetto Strategico del Capo di Stato di Stato Maggiore della Difesa', Chief of Defence General n Enzo Vecciarelli, 'Il Concetto Strategico del Capo di Stato Maggiore della Difesa' (available only in Italian), https://www.difesa.it/SMD_/CaSMD/concetto_strategico_casmd/Pagine/7_Obiettivi.aspx, document officially presented on 30 January 2020 at the Italian Centre for Defense Higher Studies. See, Andrea Mottola, 'Il nuovo concetto strategico del CSMD' (available only in Italian), https://www.difesa.it/SMD_/CaSMD/Eventi/Pagine/Generale_Enzo_Vecciarelli_al_Centro_Alti_Studi_Difesa.aspx, Portale Difesa, 30 January 2020.
[121] *Ibid*.

3.5 Engagement with the private sector

A National **Inter-University Consortium for Informatics** (Consorzio Interuniversitario nazionale per l'informatica - CINI) has been active since 1989 under the supervision of the Italian Ministry for University and Research.[122] CINI is the main point of reference for Italian national academic research in the field of computer science, computer engineering and information technology. Since 2015, in collaboration with the DIS, CINI has published a yearly White Book[123] to describe the Italian legal framework, technical challenges and latest developments in the field of cybersecurity. From 2017, the consortium has also organised training programmes aimed at reducing the current shortage of IT workers. Worth mentioning is the CyberChallenge.IT programme,[124] which represents the major Italian effort to identify, attract and recruit university students talented in cybersecurity and make their capabilities available to the nation.

To promote a culture of cybersecurity, DIS and Samsung Electronics Italia (SEI) signed a Memorandum of Understanding in September 2018 to encourage the spread of basic knowledge related to the risks of a digitalised world.[125] They will collaborate to create events and activities directed to citizens to promote more responsible use of technology.

The Italian Government is supporting the 4.0 industrial revolution process. Since 2016, the National Industry 4.0 Plan (Impresa 4.0)[126] has offered a series of conjunctional measures, funds and tax relief for companies intending to invest in digital technology and innovation. Focusing on increasing competitiveness by investing in R&D and the development of skills, the measures are beneficial for companies of any size, sector or location.

Finally, it is worth mentioning the public/private collaboration called 'ASSET per le imprese'.[127] The initiative has been promoted by the Italian Intelligence and Security Department to raise awareness of the strict relationship between economic security and cyber security. Through a series of roadshows touching many Italian regional capitals, high-level representatives from the Intelligence Department and private sector have gathered to share knowledge and increase awareness on the interconnection of the fields of cyber security and economy. The initiative aims to bolster the partnership between private economic operators, informing on the latest developments in the Italian cybersecurity architecture and of the role of the public sector bodies in tackling threats that can take place in both the analogue, digital and hybrid dimensions.

[122] National Interuniversity Consortium for Informatics – CINI (available in English) https://www.consorzio-cini.it/index.php/en/about-us.
[123] CINI, 'White Book: The Future of Cybersecurity in Italy: Strategic project areas' (available in English), https://www.consorzio-cini.it/index.php/en/labcs-home/labcs-news/1269-white-book-cybersecurity-highlight.
[124] CyberChallenge.IT (available in English), https://cyberchallenge.it/info (last accessed 14 March 2020).
[125] La Repubblica, *'Intesa Dis-Samsung Italia per promuovere la cultura della sicurezza'* (available only in Italian), https://www.repubblica.it/tecnologia/sicurezza/2018/09/19/foto/intesa_dis-samsung_italia_per_promuovere_la_cultura_della_sicurezza-206872064/1/#1 (19 September 2019).
[126] EU Digital Transformation Monitor, 'Italy: Industria 4.0' (available in English), https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Industria4.0_IT%20v2wm.pdf, August 2017.
[127] Sistema di Informazione per la Sicurezza della Repubblica (DIS) (available only in Italian), https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/asset-lintelligence-in-campo-per-le-imprese.html (26 November 2019).

References

Policy

AgID, ‘ANPR – National Registry of Resident Population’ (Anagrafe Nazionale della Popolazione Residente), (available in English), https://developers.italia.it/en/anpr/

AgID, ‘Entra nel vivo il processo di razionalizzazione dei data center pubblici e formazione dei PSN’, (available only in Italian), https://www.agid.gov.it/index.php/it/agenzia/stampa-e-comunicazione/notizie/2019/07/05/entra-vivo-il-processo-razionalizzazione-data-center-pubblici-formazione-psn

AgID, ʻPA Cloudʼ, (available in English), https://www.agid.gov.it/index.php/en/infrastructures/pa-cloud

AgID, ‘Three-Year Plan for ICT in Public Administration 2017-2019’, (available in English), https://www.agid.gov.it/en/node/1746/piano-triennale, 2017

AgID, Electronic Invoicing, (available in English), https://www.agid.gov.it/index.php/en/platforms/electronic-invoicing

AgID, PagoPA, (available in English), https://www.agid.gov.it/index.php/en/platforms/pa-payment-system

AgIGID, ‘SPID – Public Digital Identity System’, (available in English), https://www.agid.gov.it/en/platforms/spid

Chief of the Italian General Staff, Chief of Defence General Enzo Vecciarelli, ‘Il Concetto Strategico del Capo di Stato Maggiore della Difesa’, (available only in Italian), https://www.difesa.it/SMD_/CaSMD/concetto_strategico_casmd/Pagine/default.aspx

Decreto del Presidente del Consiglio dei Ministri, ‘Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali’, (available only in Italian), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf, (17 February, 2017)

Digital Transformation Team, ‘Electronic Identity Card (EIC)’, (available in English) https://teamdigitale.governo.it/en/projects/cie.htm, 2019

‘Shaping the Digital Single Market’, European Commission, 2020 https://ec.europa.eu/digital-single-market/en/europe-2020-strategy

‘Qualified Electronic Signature’. Agencia per l’Italia digitale, https://www.agid.gov.it/en/platforms/qualified-electronic-signature

INFRATEL, ‘Objectives’, (available in English) http://bandaultralarga.italia.it/en/strategy-high-speed-broadband/objectives/

INFRATEL, ‘White Areas Plan’ (available in English), http://bandaultralarga.italia.it/en/white-areas-plan/introduction/

Italian Ministry of Defence, ‘Ministerial Directive on the Military Policy for the Year 2013’, (available in English), https://www.difesa.it/Primo_Piano/Documents/2013/gennaio%202013/Direttiva%20Ministeriale_ENG.pdf

Ministero della Difesa Italiano, ʻWhite Paper for International Security and Defenceʼ, (available in English) https://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf

Ministero della Difesa, Documento Programmatico Pluriennale per la Difesa per il Triennio 2019-2021, Camera dei Deputati, DOC. CCXXXIV, N. 2, (available only in Italian) https://www.camera.it/leg18/494?categoria=234&idLegislatura=18.

Ministry of Economic Development (MISE), 'Italian Strategy for ultra-broadband' A(available in English), http://bandaultralarga.italia.it/en/strategy-high-speed-broadband/intro/

'Cybersecurity in Italy- New Opportunities for Business', Ministry of Foreign Affairs and International Cooperation and Department of Information for the Security of the Republic at the Prime Minister's Office (DIS), (available in English), https://www.esteri.it/mae/resource/doc/2019/09/esteri_cibersecurity_web.pdf, (September 2019)

Presidency of the Council of Ministers, 'National Strategic Framework for Cyberspace Security', (2013) https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

Presidency of the Council of Ministers, 'The Italian Cybersecurity Action Plan', (2017) (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf

Presidency of the Council of Ministers, 'The National Plan for Cyberspace Protection and ICT Security', 2013 (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf)

Law

Decreto del Presidente del Consiglio dei Ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale.', 24 January, 2013 (available only in Italian), http://www.sicurezzacibernetica.it/db/[2013]%20Decreto%20PCM%2024%20gennaio%202013%20-%20Direttiva%20recante%20indirizzi%20per%20la%20protezione%20cibernetica%20e%20la%20sicurezza%20informatica%20nazionale.pdf.

Decreto del Presidente del Consiglio dei Ministri, 'Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali',, 17 February, 2017. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf

Decreto del Presidente del Consiglio dei Ministri, 8 Agosto 2019, (available only in Italian), 'Disposizioni sull'organizzazione e il funzionamento del Computer security incident response team - CSIRT italiano' https://www.gazzettaufficiale.it/eli/id/2019/11/08/19A06940/sg

Directive (EU) 2016/1148 of the European Parliament and of the Council, 6 July 2016 https://eur-lex.europa.eu/eli/dir/2016/1148/oj

Gazzetta Ufficiale della Repubblica Italiana, (available only in Italian), 'Decreto Legislativo 13 dicembre 2017, n. 217', https://www.gazzettaufficiale.it/eli/id/2018/1/12/18G00003/sg

Gazzetta Ufficiale della Repubblica Italiana,, 'Decreto Legislativo 7 marzo 2005, n. 82', (available only in Italian), https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2005-05-16&atto.codiceRedazionale=005G0104&elenco30giorni=false

Gazzetta Ufficiale della Repubblica Italiana, 'Decreto Legge 21 settembre 2019, n.105', (available only in Italian), https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario;jsessionid=g6v+BHJq0BVT7oc+fikU6A__.ntc-as1-guri2a?atto.dataPubblicazioneGazzetta=2019-09-21&atto.codiceRedazionale=19G00111&elenco30giorni=true

Gazzetta Ufficiale della Repubblica Italiana, ‘Decreto Legge 21 settembre 2019, n.105’, (available only in Italian), https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario;jsessionid=g6v+BHJq0BVT7oc+fikU6A__.ntc-as1-guri2a?atto.dataPubblicazioneGazzetta=2019-09-21&atto.codiceRedazionale=19G00111&elenco30giorni=true

Gazzetta Ufficiale della Repubblica Italiana, ‘Decreto Legislativo 18 maggio 2018, n. 65’, (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2018/06/09/18G00092/sg

Gazzetta Ufficiale, MISE, Decreto 12 dicembre 2018, ‘Misure di sicurezza ed integrita' delle reti di comunicazione elettronica e notifica degli incidenti significativi’, (available only in Italian), https://www.gazzettaufficiale.it/eli/id/2019/01/21/19A00317/sg

Italian Presidency of the Council of Ministers, ‘National Strategic Framework for Cyberspace Security’, (2013). https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

Italian Presidency of the Council of Ministers, ‘The Italian Cybersecurity Action Plan’, 2017 (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf

Italian Presidency of the Council of Ministers, ‘The National Plan for Cyberspace Protection and ICT Security’, (2013) (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf

Ministero dell’Interno Italiano, ‘Decreto del 9 gennaio 2008’ (available only in Italian). http://www1.interno.gov.it/mininterno/site/it/sezioni/servizi/old_servizi/legislazione/sicurezza/0994_2008_05_06_decreto_del_ministro_9_gennaio_2008.html.

Presidency of the Council of Ministers, ‘The Italian Cybersecurity Action Plan’, 2017 (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf

Other

AgID, ‘CERT-PA’, (available in English), https://www.agid.gov.it/en/security/cert-pa

AgID, ‘PA Cloud’, (available in English), https://www.agid.gov.it/index.php/en/infrastructures/pa-cloud

AgID, ‘Qualified Electronic Signature’, (available in English), https://www.agid.gov.it/en/platforms/qualified-electronic-signature.

AgID, ‘Responsibilities and functions’, (available in English), https://www.agid.gov.it/en/agency/responsibilities-and-functions.

‘Sicurezza cibernetica: il CERT-PA avvia la fase pilota della piattaforma nazionale di contrasto agli attacchi informatici’. AgID, 25 October 2019 (available only in Italian), https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2019/10/25/sicurezza-cibernetica-il-cert-pa-avvia-fase-pilota-piattaforma-nazionale-contrasto

CERT-PA, ‘Italian CERT-PA Profile’, (available in English) https://www.cert-pa.it/wp-content/uploads/2018/07/CERT-PA_RFC_2350.txt

Commissariato di Polizia di Stato - ‘CNAIPIC’, (available only in Italian) https://www.commissariatodips.it/profilo/cnaipic/index.html

Cyber Security National Lab – CINI, ‘The Future of Cybersecurity in Italy: Strategic focus areas’, 2018. (available n English), https://www.consorzio-cini.it/images/Libro-Bianco-2018-en.pdf

CyCon 2019, ‘Cyber Commanders Panel’, Head of the Italian Joint Cyber Command https://www.youtube.com/watch?v=qDslaTRKPx8. See the speech delivered by former Italian Cyber Commander Generale Francesco Vestito.

Digital Transformation Team, ‘Electronic Identity Card (EIC)’, (available in English) https://teamdigitale.governo.it/en/projects/cie.htm, 2019

Italian CERT-N Profile, (available in English), https://www.certnazionale.it/content/uploads/2015/10/IT-CERT_RFC_2350_1_7_EN.txt

Italian Ministry of Economic Development (MISE), ‘Centro di Valutazione’, (available in Italian), https://www.mise.gov.it/index.php/it/comunicazioni/istituto-superiore-comunicazioni/sicurezza-informatica/centro-valutazione

Italian Security Intelligence Department – DIS, ‘About us’, (available in English), https://www.sicurezzanazionale.gov.it/sisr.nsf/english/about-us.html#DIS.

Ministero della Difesa Italiano, ‘Ce.Va. Difesa’, (available in Italian), https://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pagine/default.aspx

Ministero della Difesa Italiano, ‘Gli Standard di Valutazione’, (available in Italian), https://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pagine/standard_valutazione.aspx

Ministero della Difesa Italiano, ‘Schema di Certificazione’, (available only in Italian), https://www.difesa.it/SMD_/Staff/Reparti/II/CeVa/Pagine/Schema_certificazione.aspx

Ministry of Foreign Affairs and International Cooperation and Department of Information for the Security of the Republic at the Prime Minister’s Office (DIS), ‘Cybersecurity in Italy- New Opportunities for Business’, (available in English), https://www.esteri.it/mae/resource/doc/2019/09/esteri_cibersecurity_web.pdf, 6, (September 2019)

NATO, Warsaw Summit 2016, ‘Cyber Defence’, https://www.nato.int/cps/en/natohq/official_texts_133169.htm

Questura di Roma, ‘Resoconto attivita’ della Polizia Postale e delle Comunicazioni 2018’, CNAIPIC section, (available only in Italian), https://questure.poliziadistato.it/statics/35/comunicato-stampa---resoconto-polizia-postale-e-delle-comunicazioni-anno-2018.pdf?lang=it, (31 December 2018).

Sistema di Informazione per la Sicurezza della Repubblica Italiana, ‘Relazione al Parlamento sulla politica dell’informazione per la sicurezza 2018’, (available only in Italian), https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf, (2019)

Stato Maggiore della Difesa, ‘Informazioni della Difesa’, (available only in Italian), https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID-3_2017_ridotto.pdf, March 2017.

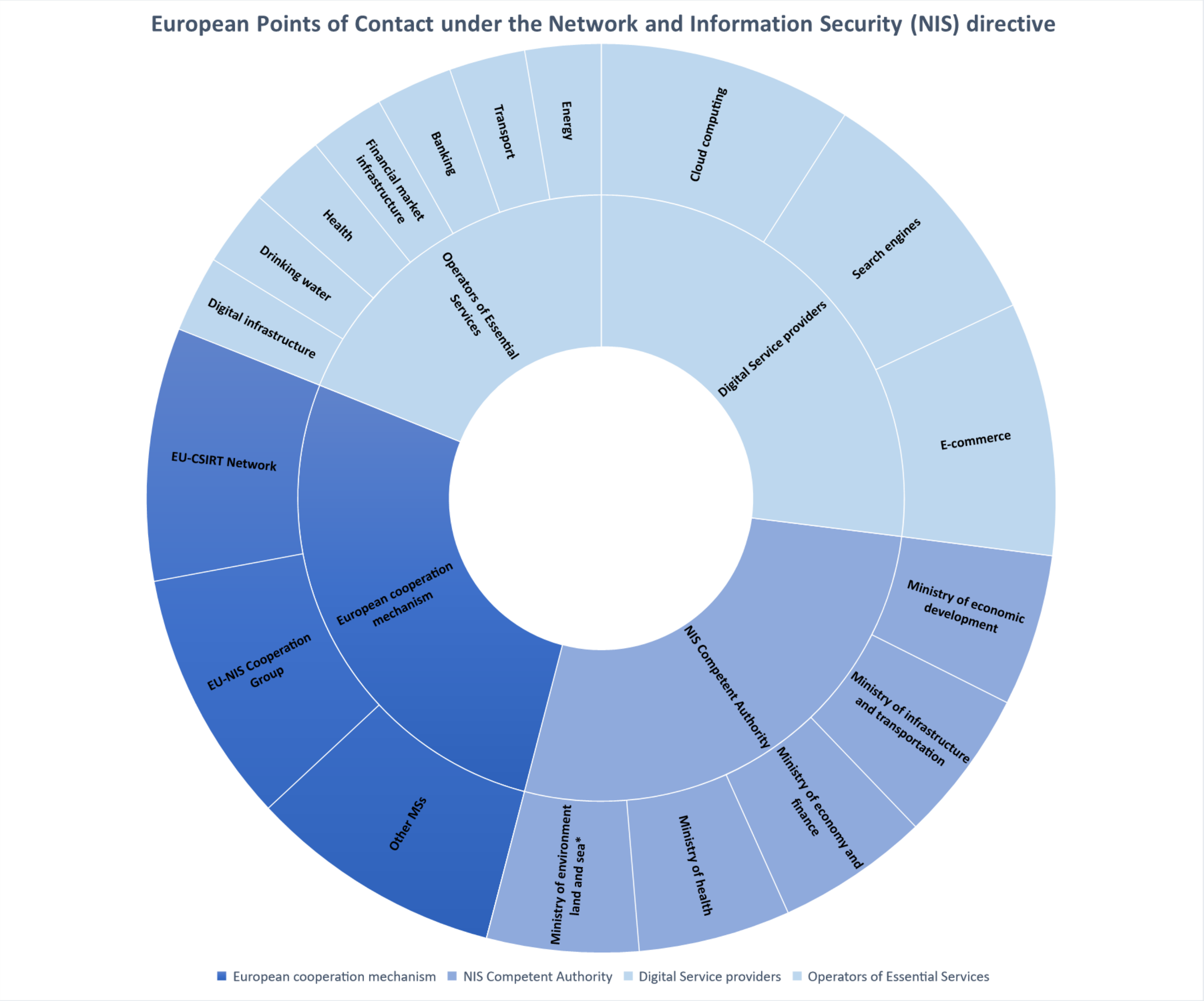
Acronyms

AGCOM	Autorità per le Garanzie nelle Comunicazioni
AgID	Agency for Digital Italy - Agenzia per l'Italia Digitale
ANS	Autorita Nazionale per la Sicurezza - National Authority for the Security
CAD	Codice dell'Amministrazione Digitale - Digital Administration Code
CC	Common Criteria
CE.VA	Centro di Valutazione della Difesa - Defence Evaluation Centre
CERT-D	CERT Difesa - Italian Armed Forces CERT
CERT-N	CERT Nazionale - National Computer Emergency Response Team
CERT-PA	CERT per la Pubblica Amministrazione - Public Administration Computer Emergency Response Team
CINI	Consorzio Interuniversitario Nazionale per l'Informatica - National Inter-University Consortium for Informatics
CIOC	Comando Interforze Operazioni Cibernetiche - Joint Cyber Command
CISR	Comitato Interministeriale per la Sicurezza della Repubblica - Committee for the Security of the Republic
CNAIPIC	Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche - Cybercrime Centre for Critical Infrastructure Protection
COR	Comando Operazioni in Rete – Joint Command for Network Operations
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence Platform
CVCN	Centro di Valutazione e Certificazione Nazionale - National Centre for Evaluation and Certification
DPP	Documento Programmatico Pluriennale - Multi-Year Planning Document
DIS	Dipartimento delle Informazioni per la Sicurezza - Security Intelligence Department
FTTP	Fibre to the Premises
ICT	Information and Communications Technology
IoT	Internet of Things
ITSEC	European Information Technology Evaluation Criteria
LVS	Laboratori per la Valutazione della Sicurezza - Security Evaluation Laboratories
M2M	Machine to Machine
N-CIRC	NATO Computer Incident Response Team
NIS	Directive on Security of Network and Information Systems
NISP	Nucleo Interministeriale Situazione e Pianificazione
NSC	Nucleo per la Sicurezza Cibernetica – Cyber Security Unit

NSF	National Strategic Framework for Cyberspace Security, Framework Nazionale per la Sicurezza Cibernetica
OCSI	Organismo di Certificazione della Sicurezza Informatica - Computer Security Certification Organisation
SPID	Sistema Pubblico di Identità Digitale, Public Digital Identity System,
STELMILIT	Scuola delle Telecomunicazioni delle Forze Armate – Armed Forces School of Telecommunications
T-CISR	Comitato Tecnico Interministeriale per la Sicurezza della Repubblica - Technical Committee for the Security of the Republic

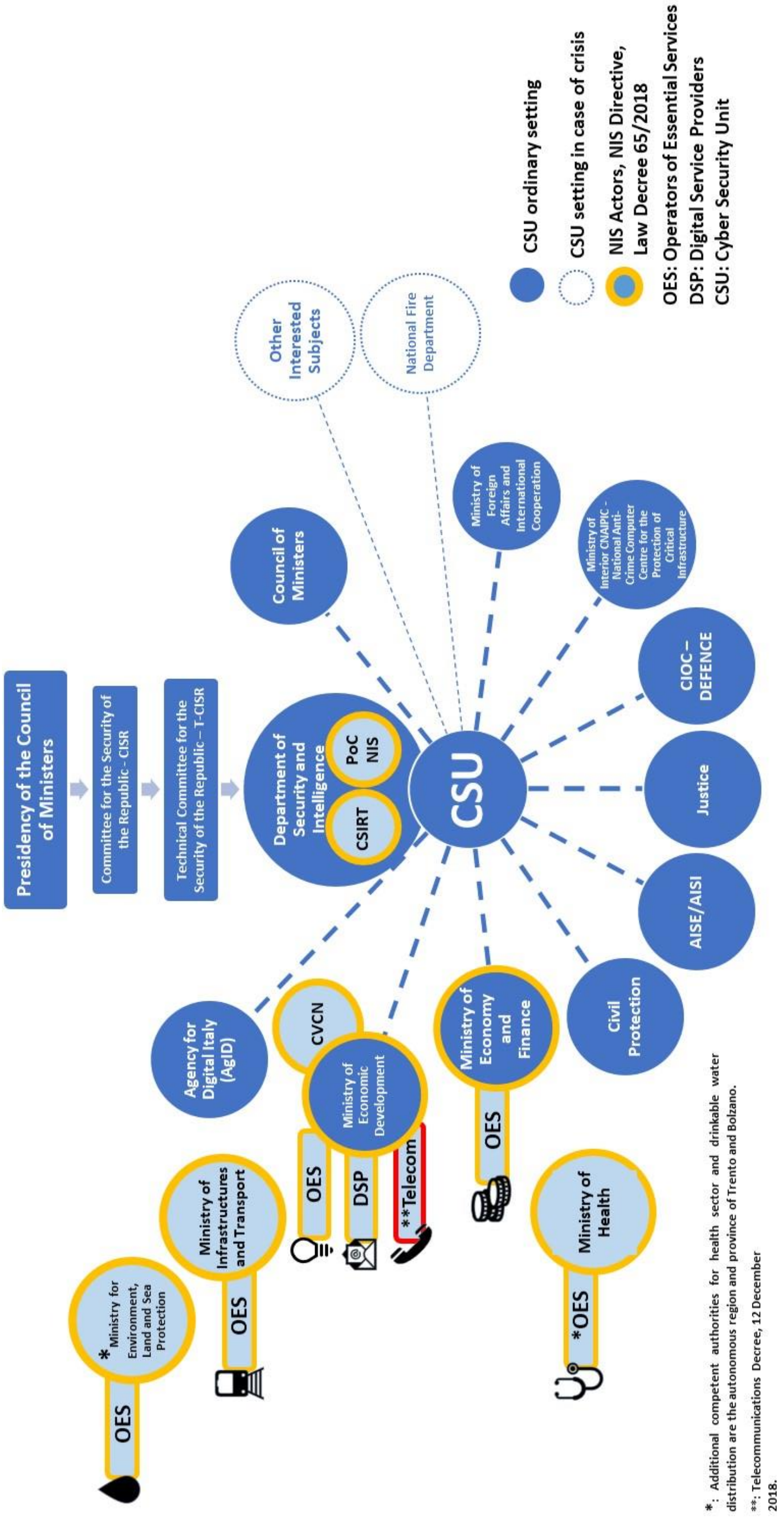
Appendix

European Points of Contact under the Network and Information Security (NIS) Directive[128]



[128] Scheme adapted by the author from the 2018 Security Intelligence Department Report to the Italian Parliament, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/02/Relazione-2018.pdf (2019) *s*ee section ‘Allegato alla Relazione sulla Politica dell’Informazione per la Sicurezza’, 13. (Available only in Italian.)

Crisis Management - Actors of the Italian Cybersecurity Architecture [129]


Presidency of the Council of Ministers
Committee for the Security of the Republic - CISR
Technical Committee for the Security of the Republic – T-CISR
Department of Security and Intelligence
CSIRT
PoC NIS
CSU
Council of Ministers
Other Interested Subjects
National Fire Department
Ministry of Foreign Affairs and International Cooperation
Ministry of Interior CNAIPIC - National Anti-Crime Computer Centre for the Protection of Critical Infrastructure
CIOC – DEFENCE
Justice
AISE/AISI
Civil Protection
Ministry of Economy and Finance
OES
Agency for Digital Italy (AgID)
CVCN
Ministry of Economic Development
OES
DSP
**Telecom
Ministry of Infrastructures and Transport
OES
*Ministry for Environment, Land and Sea Protection
OES
Ministry of Health
*OES
CSU ordinary setting
CSU setting in case of crisis
NIS Actors, NIS Directive, Law Decree 65/2018
OES: Operators of Essential Services
DSP: Digital Service Providers
CSU: Cyber Security Unit

*: Additional competent authorities for health sector and drinkable water distribution are the autonomous region and province of Trento and Bolzano.

**: Telecommunications Decree, 12 December 2018.

[129] Graph adapted by the author from ‘Relazione al Parlamento sulla politica dell’informazione per la Sicurezza 2019’, Italian Intelligence and Security Department 2020. https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2020/03/RELAZIONE-ANNUALE-2019-4.pdf, see Annex, 17. (Available only in Italian.)