CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Ludovica Glorioso

National Cyber Security Organisation: Italy

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Other reports in this series

National Cyber Security Organisation in Czech Republic

National Cyber Security Organisation in Estonia

National Cyber Security Organisation in France

National Cyber Security Organisation in Slovakia

National Cyber Security Organisation in the Netherlands

National Cyber Security Organisation in the United Kingdom

National Cyber Security Organisation in the USA

Upcoming in 2015

National Cyber Security Organisation in Germany

National Cyber Security Organisation in Hungary

National Cyber Security Organisation in Latvia

National Cyber Security Organisation in Lithuania

National Cyber Security Organisation in Poland

National Cyber Security Organisation in Spain

Series editor: Kadri Kaska (Researcher, NATO CCD COE)

Information in this study was checked for accuracy as of March 2015.

About this study

This report is a part of a NATO CCD COE project that assembles a comprehensive overview of existing national organisational models for ensuring cyber security in NATO Nations that are Sponsoring Nations to the NATO CCD COE.

The study outlines the division of cyber security tasks and responsibilities between different agencies, describes their mandate, tasks and competences, and coordination between them. In particular, it describes 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 crisis management. It also offers a summary of the national information society setting and e-government initiatives as well as the national cyber security strategy objectives in order to clarify the context for the organisational approach in a particular nation.

The result is a series of country chapters, outlining national cyber security management structures by nation.

The project contributes to awareness among NATO Allies about cyber security management in the varied national settings, thus supporting nations enhancing their own organisational structure, encouraging the spread of best practices, and contributing to the development of cooperation between different national institutions in NATO nations.

About NATO CCD COE

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is an international military organisation accredited in 2008 by NATO's North Atlantic Council as a 'Centre of Excellence'. Located in Tallinn, Estonia, the Centre is currently supported by the Czech Republic, Estonia, France, Germany, Hungary, Italy, Latvia, Lithuania, the Netherlands, Poland, Slovakia, Spain, the United Kingdom and the USA as Sponsoring Nations and Austria as a Contributing Participant. The Centre is neither part of NATO's command or force structure, nor is it funded by NATO. However, it is part of a wider framework supporting NATO Command Arrangements.

NATO CCD COE's mission is to enhance capability, cooperation and information sharing between NATO, NATO member states and NATO's partner countries in the area of cyber defence by virtue of research, education and consultation. The Centre has taken a NATO-oriented interdisciplinary approach to its key activities, including academic research on selected topics relevant to the cyber domain from the legal, policy, strategic, doctrinal and technical perspectives, providing education and training, organising conferences, workshops and cyber defence exercises, and offering consultations upon request.

For more information on NATO CCD COE, visit the Centre's website at http://www.ccdcoe.org.

ITALY

By Ludovica Glorioso
Researcher, NATO CCD COE

Table of Contents

1. Introduction: information society in Italy

1.1. Infrastructure availability and take-up

Fixed broadband internet access is available nearly universally throughout Italy: fixed access covered 99% of homes in 2013 (88% in rural areas); at the same time, Next Generation Access (NGA), capable of providing at least 30 Mbps download speed, was only available in 21% of homes.[1] Advanced third generation (3G) mobile broadband coverage was available to 97% of Italian households in 2013.[2]

The level of internet usage is low compared to the EU average – only 58% of the population uses the internet on a daily basis, against an EU average of 65% (2014). The country has some of the slowest internet speeds in the EU, with over 80% of subscribers contracted to a limit of 2 Mbps, while the share of high-speed connections (providing at least 30 Mbps) remains much lower than the EU average (2% compared to 22% in the EU in 2014). No ultra-fast connection subscriptions (download speed of 100 Mbps or higher) were available in 2014.

However, the Italian Government has published a new strategy[3] for broadband, looking at international examples that have implemented high-speed broadband in the rural areas.[4] The National Broadband Plan uses the financial means provided by the European Agricultural Fund for Rural Development (EAFRD) to support the deployment of broadband infrastructures in rural areas.[5]

1.2. E-government and private sector e-services

1.2.1. E-government

In 2006 the Italian *E-Government Code* came into force. It was intended to provide a clear legal framework for the development of e-government and the emergence of an efficient and user-friendly public administration.[6] In February 2007 the Minister for Reform and Innovation signed a Ministerial Order to implement the *E-Government Code* for improving administrative processes and accelerating technology in public offices.[7] In particular, the code regulates electronic signatures and confirms their legal validity (which was first defined in 1997 with Law no 57 on the Simplification of the Public Administration, which gave full legal force to electronic signatures).

---

[1] European Commission, 'Digital Performance of Italy', 2014 <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5685>. While the broadband access indicator is over the European Union (EU) average (which was 97% in 2013), NGA is much lower compared to the EU average of 62%.

[2] Unless otherwise indicated, statistical data in this section is drawn from the EU Digital Agenda Scoreboard for Italy. EU Digital Agenda, 'Country Ranking Table, on a Thematic Group of Indicators — Digital Agenda Scoreboard', 2013 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"back","ref-area":"IT","time-period":"2013"}>.

[3] Presidenza del Consiglio dei Ministri, 'Strategia Italiana per la banda ultralarga', 2014 <http://www.agid.gov.it/sites/default/files/documenti_indirizzo/strategia_italiana_banda_ultralarga_nov._2014.pdf>.

[4] E.g. UK, USA and Sweden; in addition, countries such as France for the private and public partnership, or Japan for the financing model.

[5] Digital Performance of Italy (n 1).

[6] European Commission. eGovernment Factsheets, 'eGovernment in Italy', Edition 16.0, 2014 <https://joinup.ec.europa.eu/sites/default/files/6d/af/f3/eGov%20in%20IT%20-%20April%202014%20-%20v.16.0.pdf>.

[7] Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica, 'Direttiva Innovazione - Direttiva del Ministro per le riforme e le innovazioni nella Pubblica amministrazione in materia di interscambio dei dati tra le pubbliche amministrazioni e pubblicità dell'attività negoziale', Direttiva n. 2, 2007 <http://db.formez.it/fontinor.nsf/faf9e352d389be8fc1256bb900405812/3DDDC469CB9ABE6AC12572AD0055F2DD/$file/dir_cad200207.pdf>.

The Agency for Digital Italy (*Agenzia per l'Italia Digitale,* AgID)[8] was established within the Prime Minister's Office in 2012 for promoting innovation in public administration,[9] following the objectives of the Digital Agenda for Europe. With the Simplification Unit (under the Ministry for Simplification and Public Administration), it is responsible for coordinating central, regional and local administration activities regarding e-government tasks in order to improve efficiency and transparency in public administration.

Citizens' use of e-government services was at 23% in 2014 – still far from the EU average of 47%. On the positive side, quality indicators for public e-government services are equal to or higher than the EU average. This includes the 'transparent e-government' indicator, measuring the on-line transparency of the activity of the public sector, especially regarding the treatment of citizens' personal data (both Italy scored 49 points out of 100, which corresponds to the EU average value), and the 'user-centric e-government' indicator, measuring the availability of e-government services in terms of connectedness and user-friendliness (Italy 75, EU 70 in 2013).[10]

1.2.2. E-commerce

E-commerce is not much used by the citizens of Italy and only 22% of Italians use services online for buying products, which places Italy in 26th position in the EU (2014). Enterprise turnover from e-commerce was at 5% of total turnover for small and medium-size enterprises (SMEs) and 11% for large ones, which are both below the EU average. Only 5% of SMEs and 16% of large enterprises sold their products online in 2013, while online purchases were made by 15% and 25% of SMEs and large enterprises, respectively. While online sale activity is low in comparison to other EU countries, online purchasing is noticeably active (12th and 13th place among 28 EU countries).

The use of electronic commerce is regulated by a national Decree of 2003[11] which transposes the European directive on electronic commerce (Directive 2000/31/EC).

2. Strategic national cyber security objectives

2.1. National cyber security foundation

Following the adoption of the Prime Minister's Decree of 24 January 2013[12] containing strategic guidelines for national cyber protection and ICT security, the *National Strategic Framework for Cyberspace Security*[13] and the *National Plan for Cyberspace Protection*[14] were adopted to respond to the challenges affecting cyber security in Italy.

---

[8] Presidenza del Consiglio dei Ministri, Agenzia per l'Italia Dgitale (AgID), 'Il Paese che cambia passa da qui', <http://www.agid.gov.it/>.

[9] Parlamento Italiano, Camera dei deputati, 'Agenzia per l'Italia digitale', D.L. 83/2012, art. 19 <http://www.camera.it/leg17/1050?appro=826&Agenzia+per+l'Italia+digitale>.

[10] 'Digital Performance of Italy' (n 1).

[11] Gazzetta Ufficiale Della Repubblica Italiana n. 87 del 14 aprile 2003, Decreto Legislativo 9 aprile 2003, n. 70 'Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico' - Supplemento Ordinario n. 61 <http://www.camera.it/parlam/leggi/deleghe/03070dl.htm>.

[12] Gazzetta Ufficiale, Della Repubblica Italiana, 'Decreto del Presidente del Consiglio dei ministri 24 Gennaio 2013', n 66, 19 marzo 2013 <http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg>.

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

[14] Presidency of the Council of Ministers, 'The National Plan for Cyberspace Protection And ICT Security', 2013 <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf>.

The Decree of the President of the Council of Ministers of 24 January 2013 defines the institutional architecture tasked with safeguarding national security in relation to critical infrastructure and intangible assets, with particular attention to the protection of cyber security and national security.

2.2. Cyber security strategy objectives

The National Strategic Framework for Cyberspace Security identifies the roles and tasks for the public and private sectors in handling cyber threats, while the National Plan identifies a set of priorities for implementing the National Strategic Framework. The tasks assigned to each component and the mechanisms and procedures are intended to reduce vulnerability, improve risk prevention, provide timely response to attacks, and permit the immediate restoration of the functionality of systems in the event of a crisis.

In the National Strategic Framework, six strategic guidelines are listed to enhance the cyber capability of Italy and maintain a safe cyberspace for the public:

1. *Analyse, prevent, mitigate and react to cyber threat*, which entails enhancing the technical, operational and analytic capabilities;
2. *Ensure business continuity of the critical infrastructures and full compliance with security standards*, with the task of protecting critical infrastructures and strategic assets from cyber attacks;
3. *Protect the national intellectual property and technological innovation*, which has the task of facilitating public and private partnership;
4. *Leverage the expertise of academia*, with the task of promoting the culture of security among citizens and institutions;
5. *Counter online criminal activities in compliance with national and international law*, which is primarily focused on reinforcement of the capability; and
6. *Support international cooperation*, which looks at initiatives underway in the international organisations of which Italy is a member, and with its allies.

In accordance with these six strategic guidelines, the National Strategic Framework identifies eleven operational guidelines:

1. *Develop the capabilities of the Armed Forces* to plan and conduct computer network operations (CNO), improving the expertise of the intelligence community, police and civil protection department;
2. *Identify the network and information security (NIS) authorities* that will be engaged at the European level for information-sharing purposes to improve public and private partnerships by the creation of joint working groups, periodic national exercises, compulsory reporting to the competent authorities and information-sharing;
3. *Develop a shared cyber taxonomy* to promote the use of questionnaires, sponsor training and education campaign and courses;
4. *Participate in international forums and working groups* at the European level reinforcing the protection of critical ICT communications, support the full integration of the cyber domain in NATO defence planning process and in military doctrine, and participate in the exercises organised by ENISA and NATO;
5. *Achieve full operational capability of the CERT* (identified by art. 16 of legislative decree no. 259/2003), which works as a cooperative public-private partnership, in order to react to potential threats to and actual attacks on the national infrastructure;
6. *Adapt existing legislation* to technological evolution in order to create a legal framework for cyber security;
7. *Ensure security standards for systems and procedures*, maintaining interoperability with international organisations such as NATO;
8. *Support small and medium enterprises* and develop the R&D for software and other ICT products;

9. *Develop institutional communication* as a dissuasion strategy against potential criminals in cyberspace;
10. *Implement the National Strategic Framework* with human and financial resources in the sectors within the Public Administration dedicated to reaching the strategic objectives; and
11. *Establish a national structure for information risk management* and connected policies and procedures.

Following the adoption of the guidelines, specific measures have been identified for implementing them at the operational level. In the assessment of vulnerabilities and the action against the threats, the efforts of the Italian institutions are to concentrate on:

- cyber situational awareness, creating a coordination between the Ministry of Defence and Ministry of Interior;
- cooperation with academia and the private sector in research and study of new methodology for the assessment of vulnerabilities;
- exchange of information between different institutions, developing inter-ministerial programs;
- implementation of early warning procedures, creating partnership with the public sector;
- Response to cyber incidents and cybercrimes, developing capabilities and procedures against such threats; and
- training and exercises. Italy takes part in national and international exercises, such as the NATO Cyber Coalition exercise and Locked Shields, organised by the NATO CCD COE in Tallinn.

3. National organisational structure for cyber security and cyber defence

3.1. Policy coordination and setting strategic priorities

The National Strategic Framework confirms the roles determined in the Decree issued in January 2013, describing the responsibilities of a number of entities in the public sector in ensuring cyber security.[15]

The overall responsibility for national cyber security is held by the **Prime Minister**, who is supported by the **Committee for the Security of the Republic** (*Comitato Interministeriale per la sicurezza della Repubblica*, CISR), which functions as an advisory body to the Prime Minister. The CISR was created by law in 2007,[16] with authority to propose the adoption of legislative measures. It also has a decision-making role in the approval of measures to improve cyber security. In line with the implementation of the *National Plan For Cyberspace*, CISR promotes initiatives for participating in international cooperation, such as with the European Union or NATO. The Technical CISR – the Committee for the Security of the Republic at Working Level – was created in 2013 and supervises the timely and correct implementation of the National Plan for Cybersecurity.

The **Security Intelligence Department** (*Dipartimento Informazioni per la Sicurezza*, DIS)[17] supports the political level by conducting analysis and assessments of cyber threats. DIS has an important role in supporting cyber security awareness and has a link with the Cyber Security Unit providing warnings and information on cyber threats. The Department works with the Agency for Internal Information and Security (*Agenzia Informazioni e Sicurezza Interna*, AISI)[18] and the Agency for External Information and Security (*Agenzia Informazioni e*

[15] 'National Strategic Framework for Cyberspace Security' (n 13) Annex I, 27-39.
[16] Parlamento Italiano, 'Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto', Legge 3 agosto 2007 n. 124 <http://www.camera.it/parlam/leggi/07124l.htm>.
[17] Sistema di informazione per la sicurezza della Repubblica, 'DIS' <https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/dis.html>.
[18] Sistema di informazione per la sicurezza della Repubblica, 'AISI' <https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aisi.html>.

Sicurezza Esterna, AISE)[19] for ICT security and interacts with public authorities, academia, and public electronic communications networks and service providers.

The **Cyber Security Unit** (*Nucleo per la Sicurezza Cibernetica*) coordinates the activities of the institutions responsible for cyber security, handles cyber incidents and restores network functionality, and interacts with NATO, the European Union, and other international organisations as a point of contact during a crisis. The Unit evaluates and promotes procedures for information-sharing and early warning for crisis management. It also promotes and coordinates the execution of cyber security exercises on the national level and coordinates the nation's participation in international exercises. The Unit is established within the Prime Minister's Military Advisor's Office and is comprised of representatives of the Ministries of Economy and Finance, Health, Foreign Affairs; Interior; Defence, Justice, the AISE, AISI, DIS, and the Department of Civil Protection.

In the event of a large-scale cyber incident that requires coordinated response by multiple ministries, the Cyber Security Unit activates the **Interministerial Situation and Planning Unit** (*Nucleo Interministeriale Situazione e Pianificazione*, NISP) in the format of the **Interministerial Cyber Crisis Unit** (*Tavolo interministeriale di crisi cibernetica*), which oversees response coordination, while the national **Computer Emergency Response Team** (CERT) is responsible for technical response measures (see section 3.4 in this paper for more detail).

3.2. Operational cyber security capabilities, cyber incident management and coordination

The Ministry of Economic Development is the central regulatory body for matters of security and integrity in regard to electronic communications systems. The Ministry hosts the **National Computer Emergency Response Team** (CERT-N), which is tasked to prevent cyber incidents and coordinate the national response to such incidents. The main role of the CERT-N is to ensure the state's crisis management capability and interaction with the private sector where necessary.[20]

A Computer Emergency Response Team was created in 2003 to protect national infrastructure and be a platform for exchanging information, and today the CERT-N holds the responsibility on the national level for sharing information and acting as a point of contact. CERT-N participates in European exercises[21] practising handling crisis situations in the cyber domain.

In addition to the national CERT, Italy has several sectoral CERTs which are dedicated to specialised roles or areas of operation. The CERT of the Public Administration, CERT-PA, is tasked with preventing, responding to and recovering from cyber incidents within the Public Administration. CERT-PA is complemented by the CERT of the System of Public Connectivity (CERT SPC) which is responsible for preventing, monitoring, information sharing, and assessing ongoing and terminated security incidents within the public administration. The Italian Armed Forces have a CERT capacity of their own.

There is also a dedicated entity called the National Anti-Crime Computer Centre for the Protection of Critical Infrastructure (*Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche*, C.N.A.I.P.I.C.) for the prevention and the fight against cybercrime and critical ICT infrastructure attacks.

[19] Sistema di informazione per la sicurezza della Repubblica, 'AISE' <https://www.sicurezzanazionale.gov.it/sisr.nsf/chi-siamo/organizzazione/aise.html>.
[20] 'National Strategic Framework for Cyberspace Security' (n 13) 23.
[21] CERT nazionale Italia, 'Cyber Europe 2014 : conclusa la terza e ultima fase', 2015 <https://www.certnazionale.it/news/2015/02/27/cyber-europe-2014-conclusa-terza-ultima-fase/>.

3.3. Military cyber defence

The **Ministry of Defence** coordinates Italy's military capabilities in the cyber domain. The most recent doctrinal update for the armed forces, the *Ministerial Directive on Military Policy for the Year 2013*,[22] recognises the hybrid nature of modern conflict and notes that conventional and non-conventional capabilities, including cyber domain operations, are a reality for Italy. Accordingly, the National Strategy Framework states that the Italian Armed Forces may carry out Computer Network Operations (CNO) to defend against threats in the cyber domain. To enable this, the capabilities of the National Armed Forces to plan and conduct cyber operations are to be improved. The Directive notes that cyber defence activities will be coordinated with NATO, the EU and forces of allied and friendly countries.

CERT DIFESA, the CERT of the Italian Armed Forces,[23] provides technical assistance and defends all computer systems and networks against malicious activities. The Coordination Centre of CERT DIFESA links to the national CERT and cooperates with the CERTs of all services of the armed forces[24] and with civilian CERTs, such as those of the private sector and academia, sharing information about threats to critical infrastructure. In line with the strengthening of cyber operations capability as described in the National Strategic Framework, CERT DIFESA's activity is to be 'fully integrated in the military operational planning'.[25]

At the international level, the CERT DIFESA Coordination Centre interacts with the NATO Computer Incident Response Capability (NCIRC) and participates in the annual NATO Cyber Coalition Exercise which is organised every year to encourage communication between NATO bodies and the CERTs of the armed forces in case of cyber crisis.

Further military cyber defence establishments include the **Defence Innovation Centre**[26] and the Division for Information Security, established within the Defence Staff. Additionally, the Telematics Department of the military police (**Carabinieri** General Staff) has been established with the task of combatting cybercrime and terrorism.[27]

3.4. Crisis prevention and crisis management

The Decree of the President of the Council of Ministers of 5th May 2010 on National Organisation for Crisis Management set up two bodies: the **Political Strategic Committee** (*Comitato Politico Strategico*, CoPS) as the political authority for crisis management, and the **Interministerial Situation and Planning Unit** (NISP) as the central coordinating authority for the Italian Government.[28]

---

[22] Ministry of Defence, 'Ministerial Directive on the Military Policy for the Year 2013', 8 <http://www.difesa.it/Primo_Piano/Documents/2013/gennaio%202013/Direttiva%20Ministeriale_ENG.pdf>.

[23] CERT DIFESA Coordination Centre is also organised with a Technical Centre, with which it works in coordination for the analysis of cyber threats.

[24] CERT Esercito Italiano, CERT Marina Militare, CERT Aeronautica Militare, CERT Arma dei Carabinieri.

[25] 'National Strategic Framework for Cyberspace Security' (n 13) 24.

[26] Ministero della Difesa, 'I compiti' <http://www.difesa.it/SMD_/Staff/Reparti/III/CID/Pagine/Cosafacciamo.aspx>.

[27] Carabinieri, Ministero della Difesa, 'Indagini Scientifiche' <http://www.carabinieri.it/arma/oggi/indagini-scientifiche/indagini-scientifiche>.

[28] Gazzetta Ufficiale, Della Repubblica Italiana, 'Decreto del Presidente del Consiglio dei ministri 5 maggio', n. 139, 17 giugno 2010 <http://www.gazzettaufficiale.it/gunewsletter/dettaglio.jsp?service=1&datagu=2010-06-17&task=dettaglio&numgu=139&redaz=10A07594&tmstp=1276847998921>.
For an overview about the Italian crisis management organizational approach, see: Federica Di Camillo et al, 'The Italian Civil Security System', Roma: Edizioni Nuova Cultura for Istituto Affari Internazionali (IAI), 2014 <http://www.iai.it/sites/default/files/iairp_11.pdf>.

CoPS involves the Ministers of Foreign Affairs, the Interior, Defence, and Economy and Finance, and serves as an advisory body for the President of the Council of Ministers, offering situation evaluation and making proposals regarding mitigation measures to the Council of Ministers.[29]

In support of CoPS, the NISP is chaired by the Secretary of State and involves representatives from the Ministries of Defence, Foreign Affairs and the Interior as well as from other agencies and administrative bodies including AISI and the Department of Fire, Rescue and Public Civil Defence.[30]

NISP supports inter-ministerial coordination in crisis prevention and emergency preparedness by harmonising common procedures and capabilities (information sharing, intelligence-gathering, inter-ministerial and operational planning, international collaboration), and by developing crisis exercises. In the event of a crisis, NISP maintains a coordinating role, but also acts to examine the situation, to identify and propose measures to be taken by CoPS and the President of the Council of Ministers, and to formulate the national position and collaborative efforts *vis-à-vis* international actors. In the execution of its crisis preparation and response mandate, NISP relies on approval and support from the Ministry of the Interior and its **Interministerial Technical Commission for Civil Defence** (*Commissione Interministeriale Tecnica per la Difesa Civile*, CITDC).[31]

3.5. Cooperation with the private sector

The 2013 Decree defines obligations for private operators regarding cooperation between internet service providers and public institutions. The ISPs have a duty to report any violations of their systems to the Cyber Security Unit. The Decree also requires them to share information and collaborate with the cyber crisis management.

The private sector is increasing its investments in the cyber domain and creating partnerships with the public sector at national and international level to take the measures necessary for cyber protection.[32] In June 2014 Selex ES, an electronics and information technology company which is part of Finmeccanica S.p.A., Italy's leading high-technology industry group, inaugurated the company's new Cyber Security Centre of Excellence in Chieti, Italy, with the aim of defining a strategic model for cyber security and enhancing the level of cyber threat prevention and defence activities. Finmeccanica-Selex ES was awarded the contract to develop, implement, and support the NATO Computer Incident Response Capability – Full Operating Capability (NCIRC FOC).

[29] Kadri Kaska and Lorena Trinberg, *Regulating Cross-Border Dependencies of Critical Information Infrastructure*, Tallinn: NATO CCD COE Publication, 2015.
[30] ibid.
[31] 'Decreto del Presidente del Consiglio dei ministri 5 maggio' (n 28) art 6 § 4 l; Governo Italiano, Presidenza del Consiglio dei Ministri, 'Decreto legislative: Attuazione della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione', 7 aprile 2011, art 4 § 5-6 <http://www.governo.it/Governo/Provvedimenti/testo_int.asp?d=63162>.
[32] Selex ES, a Finmeccanica Company, 'Finmeccanica - Selex ES Cyber Security Centre of Excellence Is Inaugurated in Chieti, Italy in the Presence of the Minister of the Interior', 2014 <http://www.selex-es.com/-/chieti>; Northrop Grumman, 'NATO Computer Incident Response Capability' <http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/NATO_CIRC.pdf>.

References

CERT nazionale Italia, 'Cyber Europe 2014 : conclusa la terza e ultima fase', 2015 <https://www.certnazionale.it/news/2015/02/27/cyber-europe-2014-conclusa-terza-ultima-fase/>.

Di Camillo, Federica, et al, 'The Italian Civil Security System', Roma: Edizioni Nuova Cultura for Istituto Affari Internazionali (IAI), 2014 <http://www.iai.it/sites/default/files/iairp_11.pdf>.

EU Digital Agenda, 'Country Ranking Table, on a Thematic Group of Indicators – a Digital Agenda Scoreboard', 2013 <http://digital-agenda-data.eu/charts/country-ranking-table-on-a-thematic-group-of-indicators#chart={"indicator-group":"back","ref-area":"IT","time-period":"2013"}>.

European Commission, 'Digital Performance of Italy', 2014 <http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=5685>.

European Commission. eGovernment Factsheets, 'eGovernment in Italy', Edition 16.0, 2014 <https://joinup.ec.europa.eu/sites/default/files/6d/af/f3/eGov%20in%20IT%20-%20April%202014%20-%20v.16.0.pdf>.

Carabinieri, Ministero della Difesa, 'Indagini Scientifiche' <http://www.carabinieri.it/arma/oggi/indagini-scientifiche/indagini-scientifiche>.

Gazzetta Ufficiale Della Repubblica Italiana, 'Decreto del Presidente del Consiglio dei ministri 5 maggio', n. 139, 17 giugno 2010 <http://www.gazzettaufficiale.it/gunewsletter/dettaglio.jsp?service=1&datagu=2010-06-17&task=dettaglio&numgu=139&redaz=10A07594&tmstp=1276847998921>.

Gazzetta Ufficiale Della Repubblica Italiana, 'Decreto del Presidente del Consiglio dei ministri 24 Gennaio 2013', n 66, 19 marzo 2013 <http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg>.

Gazzetta Ufficiale Della Repubblica Italiana n. 87 del 14 aprile 2003, Decreto Legislativo 9 aprile 2003, n. 70 'Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico' - Supplemento Ordinario n. 61 <http://www.camera.it/parlam/leggi/deleghe/03070dl.htm>.

Governo Italiano, Presidenza del Consiglio dei Ministri, 'Decreto legislative: Attuazione della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione', 7 aprile 2011 <http://www.governo.it/Governo/Provvedimenti/testo_int.asp?d=63162>.

Kaska, Kadri, and Trinberg, Lorena 'Regulating Cross-Border Dependencies of Critical Information Infrastructure', Tallinn: NATO CCD COE Publication, 2015.

Ministero della Difesa, 'I compiti' <http://www.difesa.it/SMD_/Staff/Reparti/III/CID/Pagine/Cosafacciamo.aspx>.

Ministry of Defence, 'Ministerial Directive on the Military Policy For the Year 2013' <http://www.difesa.it/Primo_Piano/Documents/2013/gennaio%202013/Direttiva%20Ministeriale_ENG.pdf>.

Northrop Grumman, 'NATO Computer. Incident Response. Capability' <http://www.northropgrumman.com/Capabilities/Cybersecurity/Documents/Literature/NATO_CIRC.pdf>.

Parlamento Italiano, Camera dei deputati, 'Agenzia per l'Italia digitale', D.L. 83/2012, art. 19 <http://www.camera.it/leg17/1050?appro=826&Agenzia+per+l'Italia+digitale>.

Parlamento Italiano, 'Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto', Law n. 124, 3 agosto 2007 <http://www.camera.it/parlam/leggi/07124l.htm>.

Presidency of the Council of Ministers, 'National Strategic Framework For Cyberspace Security', 2013 <http://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 National Plan For Cyberspace Protection And ICT Security', 2013 <http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf>.

Presidenza del Consiglio dei Ministri, Agenzia per l'Italia Dgitale (AgID), 'Il Paese che cambia passa da qui', <http://www.agid.gov.it/>.

Presidenza del Consiglio dei Ministri, Dipartimento della Funzione Pubblica, 'Direttiva Innovazione - Direttiva del Ministro per le riforme e le innovazioni nella Pubblica amministrazione in materia di interscambio dei dati tra le pubbliche amministrazioni e pubblicità dell'attività negoziale', Direttiva n. 2, 2007 <http://db.formez.it/fontinor.nsf/faf9e352d389be8fc1256bb900405812/3DDDC469CB9ABE6AC12572AD0055F2DD/$file/dir_cad200207.pdf>.

Presidenza del Consiglio dei Ministri, 'Strategia Italiana per la banda ultralarga', 2014 <http://www.agid.gov.it/sites/default/files/documenti_indirizzo/strategia_italiana_banda_ultralarga_nov._2014.pdf>.

Selex ES, a Finmeccanica Company, 'Finmeccanica - Selex ES Cyber Security Centre of Excellence Is Inaugurated in Chieti, Italy in the Presence of the Minister of the Interior', 2014 <http://www.selex-es.com/-/chieti>.

Sistema di informazione per la sicurezza della Repubblica <http://www.sicurezzanazionale.gov.it/sisr.nsf/index.html>.