

CCSIRS | POLICY PAPER

ASSESSING THE ITALIAN NATIONAL CYBER SECURITY INDEX

Luigi Martino
Irene Spadaro



Center for Cyber Security and
International Relations Studies

ISSUE
DECEMBER 2020



Center for Cyber Security and International Relations Studies (CCSIRS)

Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII)

Department of Social and Political Sciences

University of Florence

Via delle Pandette 32

50127

Firenze

www.cssii.unifi.it

cyber@cssii.unifi.it

Contents, statements and views which are contained in this report are solely those of the authors and do not imply the vision or the endorsement by University of Florence, the Center for Cyber Security and International Relations Studies, or the CSSII.

Design and layout by Manuel Silvestro

Copyright 2020, CCSIRS-CSSII

ASSESSING THE ITALIAN NATIONAL CYBER SECURITY INDEX

Luigi Martino
Irene Spadaro



ABOUT THE CENTER

The Center for Cyber Security and International Relations Studies (CCSIRS) is part of the Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII) at the Department of Political Sciences of the University of Florence. Established in 2015, the CCSIRS aims at promoting and deepening the knowledge on cyberspace dynamics through a policy-oriented approach. More specifically, activities are focused on analyzing the influence that cyberspace exercises over both Italian national security and the international system's stability, peace and security.

The Center's multidisciplinary approach succeeds in integrating the traditional fields of Social Sciences (politics, economics, law, strategic and military studies) and Computer Science. The analyses are conducted by Italian and international experts from various sectors and countries. The Center shapes its international activities by creating an ever-increasing solid network of public and private partnerships, aiming at guaranteeing excellent research.

The Center's research focuses on comparative analysis of best cases and best practices in the fields of cyber strategy, governance and policy, critical infrastructures, economic and financial cybercrimes, privacy protection legislations and cyber intelligence structures. Complementarily, it carries out studies on the different approaches adopted internationally by both private and public actors.



TABLE OF CONTENTS

TABLE OF CONTENTS.....	1
EXECUTIVE SUMMARY.....	2
INTRODUCTION	3
1. ANALYSIS OF THE ITALIAN NATIONAL CYBER SECURITY INDEX	7
1.1. INTENT	11
1.2 CAPABILITIES.....	14
2. OVERVIEW OF ITALIAN CYBER PREPAREDNESS	17
3. STEPS FORWARD: THE NATIONAL CYBER SECURITY PERIMETER.....	21
CONCLUSION AND RECOMMENDATIONS.....	27
BIBLIOGRAPHY	30
APPENDIX A – OVERVIEW OF ITALIAN CYBER NORMS	34
APPENDIX B – ITALIAN CYBER ARCHITECTURE	37





Executive Summary

The concept of cyber power is comprised of several facets that go beyond the simply cyber capabilities of certain countries and present many difficulties when trying to define it. This partially explains why all the many indices that have been elaborated during the past few years consider different factors and present different outcomes. Indeed, Italy has not reached the top-level ranks in most of the major international cyber power and security index.

For instance, among all the most common classifications, the Belfer Center's National Cyber Power Index (NCPI) is currently the best and most inclusive attempt to categorize States' efforts and capabilities, without limiting the concept of cyber power to the mere ability to attack or defend. In this index, Italy ranks 29 out of 30 countries, and presents a low index both in the Intent and in the Capabilities indicators. However, a question arises: is this the real situation of the Italian Cyber Security Index?

This policy paper attempts to answer the above question with an analytical approach considering, inter alia, the Italian normative, institutional, and operational framework. For example, Italy – starting from 2013 – has structured a specific national architectural framework considering cyber security as a comprehensive part of the national security, also in compliance with the European Union constraints and its status as a member of NATO. At the same time, the establishment of the National Cyber Security Perimeter (Perimetro di sicurezza nazionale cibernetica) represents the last initiatives that could potentially reshape the Italian cyber security posture, in an innovative and appropriate way.

The policy paper presents a twofold perspective: a) frame Italy's cyber ecosystem and its deficiencies, and b) highlight some bias and lacks in the NCPI regarding the Italian cyber power index score. In light of this, the research proceeds to assess the Italian cyber security regulatory framework to highlight its strengths and weaknesses. As a result of the analysis, practical policy recommendations are given on updating the national strategy, implementing it effectively through the creation of a National Center for Cyber Security and funding on R&D programs.

Introduction

The exponential growth of the digital arena has called into question the traditional definition of spaces, borders, State power, and national security policies, all critical variables of international relations. If, on one hand, it is true that States remain the dominant actors in the international system, on the other hand, it is equally true that the cyber domain is changing the dynamic of actors involved in the international arena.

Power relationships have been heavily influenced by the morphology of digital society, which describes the social structure of the information age (Castells, 2006). This is because, as highlighted by many scholars, power depends on the context in which it is exercised. Therefore, for instance, cyber power is strictly connected to the resources linked to the new domain and the technological capabilities of the actor who intends to use the power. In other words, as explained by Nye, cyber power depends on the mechanisms of creation, control, and communication of information, notably electronic infrastructures, networks, communication technologies, human capabilities, but also the physical infrastructure on which cyberspace relies (Nye, 2010).

However, the capability to use appropriate tools to measure cyber power at the empirical level presents relevant difficulties. In particular, the concept of cyber power consists of several facets that go beyond the simple cyber capabilities. This partially explains why all the many indices that have been elaborated during the past few years consider different factors and contain different outcomes. This emerges clearly, for instance: by data contained in the Global Cybersecurity Index; the Global Cybersecurity Index & Cyberwellness profiles; the Potomac Institute's Cyber Readiness Index 2.0; the Economist Intelligence Unit and Booz Allen Hamilton's Cyber Power Index; the International Institute for Strategic Studies (IISS) Military Balance and the National Cyber Security Index 2018 and the National Cyber Power Index (NCPI).

As highlighted by data contained in the table below, these approaches are based on heterogeneous cataloging tools, employing different criteria and methods with different (and sometimes contrasting) results.

TOP 10

Countries in terms of cyberpower according to different indices

Global Cybersecurity Index (GCI) 2018	National Cyber Power Index 2020	National Cyber Security Index	Economist Intelligence Unit and Booz Allen Hamilton	Global cybersecurity index & cyber wellness profiles
<ul style="list-style-type: none"> United Kingdom United States France Lithuania Estonia Singapore Spain Malaysia Canada Norway 	<ul style="list-style-type: none"> United States China United Kingdom Russia Netherlands France Germany Canada Japan Australia 	<ul style="list-style-type: none"> Greece Czech Republic Estonia Lithuania Spain Belgium Finland Slovakia Croatia France 	<ul style="list-style-type: none"> United Kingdom United States Australia Germany Canada France South Korea Japan Italy Brazil 	<ul style="list-style-type: none"> United States Canada Australia Malaysia Oman New Zealand Norway Brazil Estonia Germany

Center for Cyber Security and International Relations Studies

Table 1: Top 10 countries in terms of cyber power according to different indices

Even though all the indices listed above define cyber power and preparedness in different terms, with different ranking, their analysis could help identify and assess the state of art of the Italian cyber security posture, in terms of institutional, legal, and governance frameworks. In particular, the **Global Cybersecurity Index (GCI)**¹, elaborated by the ITU, measures the commitment of countries to cyber security at a global level. The score is assessed along five pillars: Legal Measures, Technical Measures, Organizational Measures, Capacity Building, and Cooperation – which are then aggregated into an overall score. As complementary to the GCI, ITU has also developed the **Global cybersecurity index & cyberwellness profiles**², which is rooted in the Global Cybersecurity Agenda. The GCICP explores and analyzes at the level of commitment in five areas: legal measures, technical measures, organizational measures, capacity building, and international cooperation.

¹ ITU (2019), *Global Cybersecurity Index 2018*, ITU, Geneva.

² ITU (2015), *Global Cybersecurity Index & Cyberwellness Profile 2015*, ITU, Geneva.

The **Potomac Institute's Cyber Readiness Index 2.0**³ (CRI 2.0) is designed to evaluate a country's preparedness and commitment to protect its national cyber infrastructure and services. It does not include a ranking, but just an assessment of each country, assigning them a score.

The **Economist Intelligence Unit & Booz Allen Hamilton**⁴ (EIU & Booz) developed a "cyber power index" (CPI) in 2010, focusing on policy, organizational and technical aspects of cyber security. It is the first attempt to categorize cyber power outside the mere level of cyber offensive/defensive capabilities.

National Cyber Security Index⁵, by the e-governance academy, provides an overview of the cyber security capacity of countries, in terms of preparedness to prevent cyber threats and manage cyber incidents, pointing out good practices and aspects that can be improved.

The IISS **Military Balance**⁶ has been considering cyber capabilities in the assessment of its index – military-owned cyber capabilities – since its first edition in 2014. These capabilities are assessed following different indicators: political, military, economic, social, and infrastructural.

The **National Cyber Power Index** (NCPI)⁷, elaborated by the Belfer Center of Harvard Kennedy School, measures the cyber capabilities of thirty countries in the context of seven national targets, using 32 intent indicators and 27 capacity indicators, through a «*whole of country*» approach. The thirty countries include the five cyber superpowers, countries with attributed APT (Advanced Persistent Threats) groups, and rising cyber powers. This last index represents a *unicum* in the cyber power categorization approaches because it constitutes a new method in the conceptualization and measurement of national cyber capabilities. The NCPI considers cyber power through States' **intention** to achieve different national goals using cyber means and the national **capabilities** to achieve the objectives within the context of seven national aims:

- **surveillance** and monitoring of domestic groups;

³ Hathaway, Melissa, Chris Demchak, Jason Kerben, Jennifer McArdle, and Francesca Spidalieri, (2015) *Cyber Readiness Index 2.0*. Paper. Potomac Institute for Policy Studies.

⁴ Economist Intelligence Unit & Booz Allen Hamilton, (2011). *Cyber Power Index*.

⁵ E-governance Academy, (2020). *National Cyber Security Index*. [Index \(ega.ee\)](#) (Accessed 20 November 2020)

⁶ IISS, (2014), *The Military Balance*, Routledge.

⁷ Voo, Julia, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy and Anina Schwarzenbach, (2020). *National Cyber Power Index 2020*. Belfer Center for Science and International Affairs.

- strengthening of cyber national **defence**;
- **control** and mapping of the information environment;
- collection of **intelligence** information for national security;
- **commercial** gains and industry growth;
- ability to destroy or disable opposing infrastructure and capabilities (**offence**);
- definitions for international IT standards and technical standards (**norms**).

In light of this, it is possible to analyze, from an empirical point of view, the Italian cyber security index, comparing it to the results (and for certain aspects to validate or invalidate the ranking attributed to the Italian case) contained in the NCPI elaborated by the Belfer Center. To do so, the NCPI is used as an operational framework and its analytical dimensions are followed to assess the Italian cyber security preparedness.

1. Analysis of the Italian National Cyber Security Index

Italy has not reached the top ten rankings in most of the international cyber power and security indices. For instance, it positioned 25^o in the Global Cybersecurity Index (ITU); 20^o in the National Cyber Security Index, and 10^o in the Global Cybersecurity Index and Cyber Wellness Profiles, in which many countries share the same ranking so Italy is unofficially positioned 32^o.

According to the Potomac Institute's Cyber Readiness Index 2.0, which does not rank countries but just present an overview of their situation assigning them a score, Italy is a country which is not completely operational in any of the sector considered by the analysis (see Fig. I).

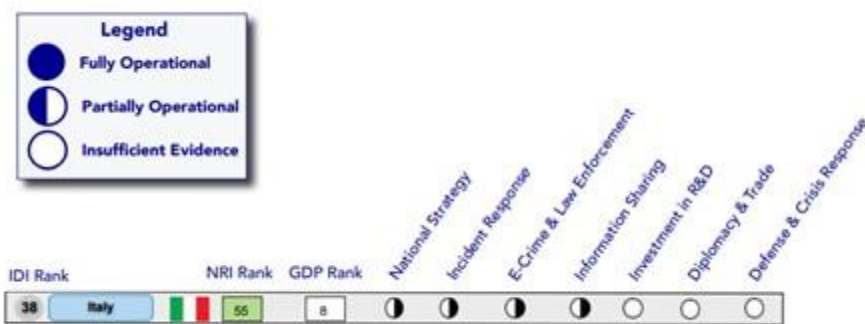


Fig. I. Italy's cyber readiness. Potomac institute, Cyber Readiness Index 2.0 (2016)

In particular, it is worth noting that Italy ranks 29^o in the NCPI of the Belfer Center, after Ukraine, Saudi Arabia, and Lithuania, with a National Cyber Power Score below 10. Other major European countries such as France and Germany are above the 20 thresholds, and the USA has a score of 50. This situation is represented in Fig. II which illustrates the NCPI general ranking, aggregating intent and capabilities scores on the aforementioned 7 national objectives.

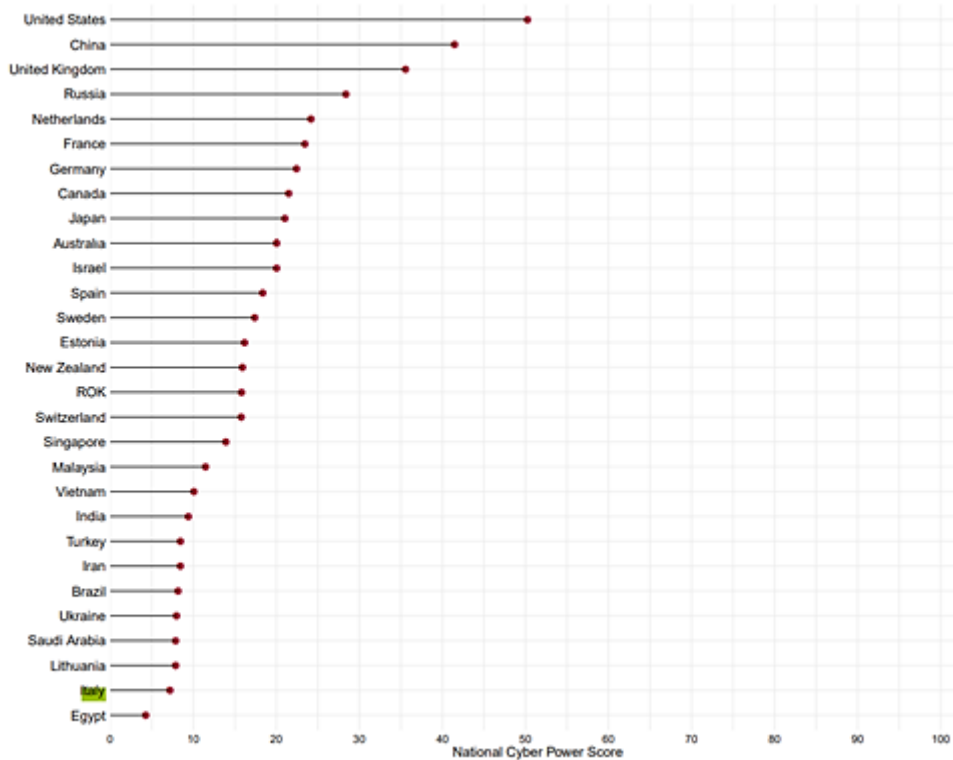


Fig. II. NCPI Most Comprehensive Cyber Powers. Source: NCPI, Belfer Center (2020)

Regarding cyber intent and cyber capability, Italy presents a low index for both. In other words, according to the NCPI index, Italy is one of those countries that either is not actively developing nor capabilities or intent to affirm its power in cyber space, either does not release an appropriate amount of information on its status.



Fig. III. Countries' position in relation to "Intent" and "Capabilities" categories. Source: NCPI, Belfer Center (2020)

Although work needs to be done in the development of capabilities and intent, this low score – and subsequent low ranks – of the Italian case could be better explained by the lack of available and clear data, especially in sensitive sectors such as intelligence and military sectors. For example, 13 countries' score on this indicator is close to zero, because of the lack of information, the uncertainty in attribution and the data which the study is based upon – that only considers official government statement and strategies. Regarding the offence indicator, Italy is placed 26° in the comprehensive rank and intent rank, whilst in the capabilities rank for the same indicator, it is positioned the highest (16°) among all indicators and categories, as highlighted by Table I. This sets out a plausible scenario of reticence in divulging information on State-sponsored cyber attacks accompanied by high-level military organizations, substantial participation in international and regional cyber exercises and well-defined cyber strategies. All these considerations match the empirical evidence. For comparison, Egypt is the State that has the lowest position in intent and capabilities in the cyber offence, although

State-sponsored cyber attacks have been attributed to the government, especially against internal political oppositions.⁸



Italy's position for different NCPI categories and indicators

TABLE 2	Surveillance	Defence	Information Control	Intelligence	Commerce	Offence	Norms	Total
Comprehensive Score	24	27	18	20	18	26	23	29
Intent	22	21	17	21	19	26	20	22
Capabilities	23	28	23	20	19	16	25	23



Table II: Italy's position for different NCPI categories and indicators

⁸ For example, according to a report published in 2019 by Check Point Software Technologies and another 2019 report published by Amnesty International, the cyber attacks of March 2019 targeting journalists and human rights activists were allegedly government-sponsored.

1.1. Intent

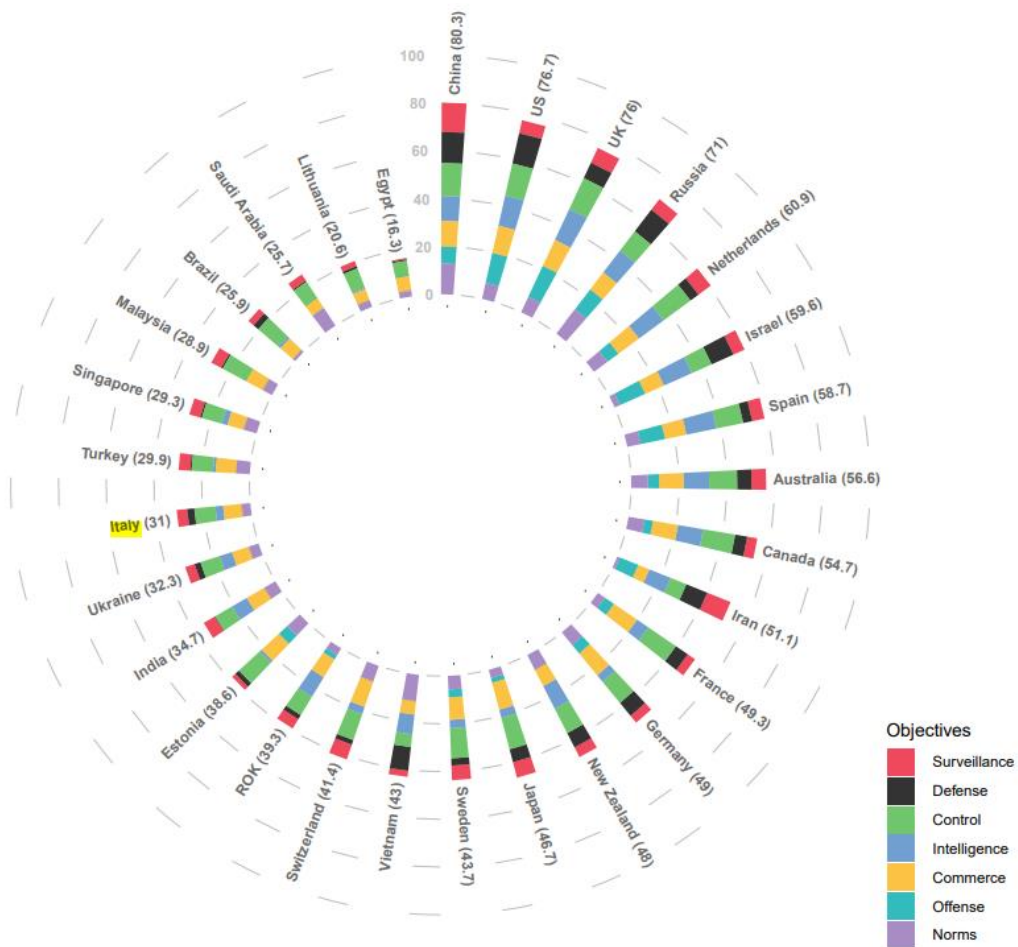


Fig IV. Countries scoring in the Intent indicator, divided in the 7 objectives. Source: NCPI, Belfer Center

The analysis of the intent is carried out considering national cyber strategies and other strategic documents. In this regard, the Italian national cyber strategy lacks in comprehensiveness, in the sense that it does not properly specify actions and operational factors – although these are better explained in other key institutional documents. Moreover, the first Italian strategy is not recent⁹ and has not been properly updated to reflect the current conditions of the cyber arena, nor has it been regularly modified in line with the national policies framework in this sector. Another key issue that can partially explain the Italian low score is the lack of a substantial increase in government funding for cyber security during the last few years.

⁹ The Italian national cyber strategy has been published in 2013.

The Italian Government has recognized the need to ensure the defence of cyber space since 2013, in the Ministerial Directive on the Military Policy¹⁰, and has reiterated the cruciality of the fifth domain in the White Paper for International Security and Defence (2015)¹¹ and in the Ministry of Defence Multi-Year Planning document 2019-2021¹², as well as in its other national strategic cyber security document.¹³

Even though Italy presents many documents on cyber security and cyber defence that explore the topic from multiple perspectives and that are generally more updated than other types of strategic documents, not many active cyber defence measures have been pursued. This could explain the gap between intent and capabilities scoring for the defence indicator. Italy has already set up in 2017 a military command in charge of conducting cyber operations – the Joint Cyber Command (Comando Interforze per le Operazioni Cibernetiche – CIOC)¹⁴ in compliance with its commitments outlined in its national strategy and in international forums¹⁵.

The Command has two operational objectives: defence and protection of the integrity of critical networks, in coordination with the Ministry of Defence, and assessment of vulnerabilities and implementation of penetration tests, to provide rapid intervention when required. Alongside the Joint Cyber Command, an Armed Forces Institute of Telecommunications has been established in 2017 in Chiavari.¹⁶ The Institute aims at providing joint military and civilian personnel of the Armed Forces with specialist training, qualifications, retraining and basic, as well as advanced, training.

The Project Group (Gruppo di Progetto) C5ISR, established by Decree of the Minister of Defence in January 2019, has created a Command for Network Operations (Comando per le Operazioni in Rete – COR) in March 2020. The COR merges the Joint Command for Cyber Operations (CIOC) and the Joint C4 Command and is structured into three Divisions (C4, Security and Cyber Defence, Cyber Operations). The Command, which will conduct operations

¹⁰ Italian Ministry of Defence, (2013). *Ministerial Directive on the Military Policy for the Year 2013*. https://www.difesa.it/Primo_Piano/Documents/2013/gennaio%202013/Direttiva%20Ministeriale_ENG.pdf.

¹¹ Italian Ministry of Defence, (2015). *White Paper for International Security and Defence*. https://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf.

¹² Ministero della Difesa, (2020). *Documento Programmatico Pluriennale per la Difesa per il Triennio 2020-2022*, Camera dei Deputati. <https://www.camera.it/leg18/494?categoria=234&idLegislatura=18>.

¹³ See Annex A for reference.

¹⁴ Italian Presidency of the Council of Ministers, (2017). *Italian Cybersecurity Action Plan*. <https://www.sicurezza-nazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan2017.pdf>

¹⁵ Notably, the NATO Warsaw Summit (2017) and the European Defence Agency

¹⁶ Stato Maggiore della Difesa, (2017). *Informazioni della Difesa. Cyber-Defence. Nasce il Comando Interforze per le Operazioni Cibernetiche*. https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID3_2017_ridotto.pdf.

in the cyber domain, will secure technical-operational management of all Defence Information and Communications Technology Systems / C4 Systems, to harmonize and promptly distribute the information produced by command and control systems, computing, intelligence surveillance and reconnaissance. This further step will impact both the intent and capabilities indicator, improving the Italian position in cyber defence.

The “intent” indicator also considers the level of State-sponsored initiatives on cyber awareness and the level of investments for defence activities. Whilst, as previously explained, poor scoring in the offence indicator could be attributed to the lack of data on offensive national cyber operations and attribution of at least one cyber attack, in line with constitutional and international obligations.¹⁷

¹⁷ According to articles 10, 11 and 117 of the Constitution of the Italian Republic.

1.2 Capabilities

The capabilities index assesses the ability of a State to achieve the intended goals, and it depends directly on the resources that the State deploys to do so. These are not just considered in terms of the creation and control of ICT infrastructures and software, but also in terms of human capital and influence on the international arena (norms, influence, and exports).

It is formulated upon 27 indicators, which are grouped by the seven national objectives. According to the Index Report: “The data collected on capabilities can be categorized into eight themes: Evidence of Attacks; National Online Content; Domestic State Cyber structures; Cyber Vulnerability Mitigation; Private Sector, Trade, and Innovation; Connectivity; Workforce; and Legal and Policy Frameworks” (p. 37, 2020).

Italy positioned the highest in offence (16°) and the lowest in defence (28°) whilst, for the other indicator, it is classified in the middle-low part of the ranking (Commerce 19°; Intelligence 20°; Surveillance 23°; Information Control 23°; Norms 25°). To better understand why these scores have been assigned, it is worth summing up the indicators considered for each objective.

Indicators considered for each objective

Offence	State-Sponsored Attacks, Cyber Military Doctrine, National Cyber Command, High-tech Exports, Cyber Military Staffing.
Commerce	Global Top 100 Technology Firms; High-tech Exports, Skilled Employees in the Tech Industry, Global Top 500 Cyber security Firms, ICT Imports, Patent Applications, Ecommerce Economy
Intelligence	State-Sponsored Attacks, Global Top 100 Technology Firms, High-tech Exports, Skilled Employees in the Tech Industry, Cyber Military Staffing, Existence of Private Sector Surveillance Technology

Surveillance	Cyber security Laws, Population % on the Internet, Population % on the Social Media, State-Sponsored Attacks, Existence of Private Sector Surveillance Technology, Freedom on the Net Score.
Information Control	State-sponsored attacks, Population % on Social Media, Population % on the Internet, Top Websites in Alexa top 50, Top News Sites in Alexa top 50, Successful Google Content Removal Requests.
Norms	Cyber security Laws, Bilateral Cyber Agreements, Multilateral Cyber Agreements, Global Top 100 Technology Firms, High-tech Exports, ICT Imports, Global Soft Power
Defence	Cyber security Laws, Skilled Employees in the Tech Industry, Global Top 500 Cyber security Firms, Computer Infection Rates, Mobile Infection Rates, Population % on the Internet, ICT Imports, Speed of broadband and mobile, Vulnerabilities listed in Shodan affecting domestic machines, Existence of Cyber Security Incident Response Teams (CSIRTs)



Table III. Indicators considered for each objectives. Source: NCPI, Belfer Center (2020).

If we proceed to compare the categories which score the least (defence and norms) with the highest (offence), assuming that Italy partially satisfied the offence indicators, at first glance emerges a situation of vulnerability and deficiencies in cyber security laws implementation and the international arena. It also highlights high rates of computer and mobile infection and the percentage of the population on the Internet exposed to these vulnerabilities.

The scoring in the commerce indicator – as well as the better positioning in indicators that implies Tech import/export and high-level technology firms – provides an overview that partially represents the Italian excellence in the sector. Italy presents interesting and dynamic actors, although not giants, in software integration, communication infrastructures and specific niche markets that can be useful for the development of pieces of a national architecture (CINI, 2015). On the other hand, it has been empirically proven a lack of human capital properly equipped and an underfunding of programs of cyber awareness and R&D, which represent a common challenge to many countries. This point was also confirmed by the annual Information

Security Policy Report¹⁸ which highlights a “vast problem concerning cyber security education” that affects the Italian cyber resilience.

Furthermore, the reality of the Italian private sector, which is characterized by the presence of small and medium-sized enterprises which have not yet adequately equipped for the contemporary cyber arena, creates multiples weak links in the supply and industrial chain. The situation affects the Italian cyber space as a whole and creates the environments for the rise of larger-scale cyber incidents. In Italy, entire sectors of excellence, the so-called *Made-in-Italy* brand, could suffer heavy downsizing of turnover due to attacks in cyber space by sovereign States or competitors, in particular in case of cyber espionage¹⁹.

To better comprehend the different levels of Italy’s strategic preparedness, the next section is going to briefly analyze the Italian cyber ecosystem created by the different national documents on this subject.

¹⁸ Sistema di Informazione per la sicurezza della Repubblica, (2018). *Relazione sulla politica dell'informazione per la sicurezza, Allegato: Documento di sicurezza nazionale*.

¹⁹ Which remains, as highlighted by the Department for Information Security (DIS) annual relations: “The Primary objective of the intelligence” (p. 5, annex to the annual report to the parliament, 2019)

2. Overview of Italian cyber preparedness

Italian policies, norms, and institutions have focused, during the past few years, on national cyber security, to maintain Italy in compliance with European Union constraints, international and regional principles and obligations.

The first Italian cyber policy – the “Directive containing guidelines for national cyber security” (so-called Monti Decree)²⁰ – was published in January 2013 and has defined the first institutional architecture for the protection of national security from to cyber threats. It also defined the subjects included in the institutional architecture and the governance model, identifying the Prime Minister as the authority in charge of cyber security – as this is included in the broader concept of national security. This step was extremely important because it came at a time when reaction activities against cyber threats were marginal and unstructured. In this regard, the decree introduced a crisis management approach which, after an assessment conducted at the political and operational level, was considered as inadequate due to its “slow” nature and the command-control fragmented approach. This consideration was highlighted in light of the high number of interactions among various public actors –different departments of the Presidency of the Council of Ministers, several Ministries and the AgID (Agency for Digital Italy)²¹ – which were difficult to coordinate in short timeframes, as required by the nature of the cyber crises.

In light of the National Strategic Framework for Cyber Space Security²² and the National Plan for Cyber Protection and ICT Security²³ – both elaborated and released in December 2013 – the next step taken to define a national cyber security framework was under Renzi Cabinet in August 2015. The “Directive on cyber protection and national IT security”²⁴ aimed to consolidate an efficient reaction system to ensure the resilience of the national IT infrastructure, through greater coordination and integration between the public entities involved and of the partnerships with private operators who are involved in the national cyber security ecosystem. It also aimed to frame the flaws of the first national architecture based on

²⁰ Presidenza del Consiglio dei Ministri, (2013). *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale*.

²¹ Cyber Security National Lab – CINI, (2018). *The Future of Cybersecurity in Italy: Strategic focus areas*.

²² Presidency of the Council of Ministers, (2013). *National Strategic Framework for Cyberspace Security*.

²³ Presidency of the Council of Ministers, (2013). *The National Plan for Cyberspace Protection and ICT Security*.

²⁴ Presidency of the Council of Ministers (2015). *Directive on cyber protection and national IT security*.

the Monti Decree and identifies the operational level in the intelligence context, in direct coordination with the Prime Minister.

The 2017 “Directive containing guidelines for cyber protection and national IT security”²⁵ (DPCM Gentiloni) has reformed the Monti architecture as well as reformulated the role of the Cyber security Management Board (Nucleo per la Sicurezza Nazionale, NSC) to manage cyber crises and coordinate an overall response and governance among the various actors involved. In this way, the DPCM Gentiloni has strengthened the role of the intelligence services (in particular, the role of the DIS) in the national cyber security context, establishing a direct chain of command with the Prime Minister, as the competent authority responsible for national security assisted by the intelligence services.

Furthermore, from a governance perspective, the DPCM Gentiloni has offered a strategic and organizational national focal point where the public and private sectors, both military and civil, from major corporations to individuals, could operate in a synchronized manner. Coordination also promoted the implementation of programs aimed at maintaining the skills needed to strengthen the country's response and resilience to cyber attacks.

At the same time, an additional Executive Decree – the Italian cyber security action Plan²⁶ – approved by the Prime Minister in March 2017, has provided an articulated and multi-dimensional set of actions, programs and cutting-edge centers, such as the National Center for Cyber Security Research and Development, the National Cryptography Laboratory, the National Cyber Range, and the Center for Assessment and Certification. They were both parts of a nuanced mosaic composed to promote a national cyber strategy.

At the operational level, the DIS hosts the Cyber security Management Board (Nucleo di sicurezza cibernetica, NSC) – an interagency and intergovernmental cyber security institutional entity, headed by the DIS Deputy Director. In the event of a national cyber crisis, the Board is equipped with members from the Ministry of Health, the Ministry of Infrastructure and Transport. At the same time, a National Assessment and Certification Center (Centro di valutazione e certificazione nazionale – CVCN) was established within the Ministry of Economic Development, to assess and verify the security conditions and the absence of vulnerabilities on

²⁵ Presidenza del Consiglio dei Ministri, (2017). *Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali*. <https://www.sicurezza-nazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf>.

²⁶ Presidency of the Council of Ministers, (2017). *The Italian Cybersecurity Action Plan*. <https://www.sicurezza-nazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italiancybersecurity-action-plan-2017.pdf>

products (software and hardware), equipment and IT systems which are used in the field of national critical infrastructures and strategic sectors.

In 2018, the NIS EU Directive was implemented by the Legislative Decree no. 65 of 18 May 2018 containing measures for a common high level of security of networks and information systems.²⁷ The implementation of the NIS Directive in Italy has created a mechanism in which incidents that have a significant impact on the continuity and provision of the service must be notified to the Computer Security Incident Response Team (CSIRT) which was created in 2019 and the national single contact point which is the Department for Information Security – (Dipartimento delle informazioni per la sicurezza – DIS).

The latest policy on the subject – Law Decree 18 November 2019 no. 133/2019²⁸ (Urgent provisions on the perimeter of national cyber security), implemented in November 2020 – will be discussed in the next section, as an instrument for the partial resolution of the Italian deficiencies previously highlighted.

These strategic documents have created a cyber institutional architecture composed of multiple agencies, which are briefly described in the infographic below.

²⁷ The NIS Directive – first set of European security rules approved by the EU on 6 July 2016 – is intended to define the measures necessary to achieve a high level of security of networks and information systems in all Member States. The decree applies to Operators of Essential Services (OESs) and to Digital Services Providers (DSPs). The latter are called upon to adopt adequate and proportionate technical and organizational measures for risk management and to prevent and minimize the impact of accidents affecting the security of networks and information systems. The NIS Directive guarantees the alignment to EU security methods, approaches, and practices, and allows to prevent European and Italian companies from operating within fragmented environment.

²⁸ Gazzetta Ufficiale della Repubblica Italiana, (2019). *Legge 18 novembre 2019, n. 133. "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, n. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (GU Serie Generale n.272 del 20-11-2019)".* <https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg>

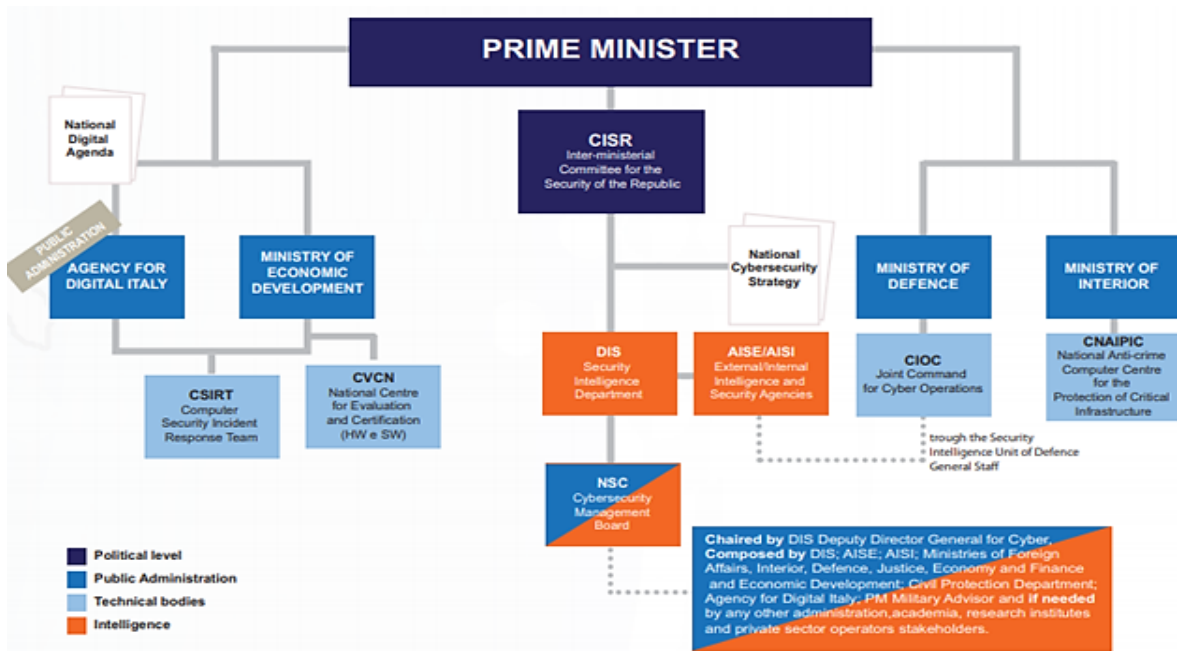


Fig. V. Italian Cyber Architecture. Source: Italian Ministry of Foreign Affairs (2019)

3. Steps forward: The National Cyber Security Perimeter

Law no.105 enacted on 21 September 2019²⁹, converted with amendments into Law on 18 November 2019, no. 133³⁰, established the **National Cyber security Perimeter** to ensure a high level of security of the networks, information systems, and IT services of public administrations, bodies and national operators, public and private, on which depends the exercise of an essential function of the State and society.

In other words, the final aim of the perimeter is to protect the subjects that provide essential services whose malfunction, interruption, even partial, or improper use could result in damage to national security.

According to Art. 1 paragraph 2 of the Law, within four months from the date of entry into force, the President of the Council of Ministers must adopt a Prime Ministerial Decree (DPCM), on the proposal of the Interministerial Committee for the Security of the Republic (Comitato interministeriale per la sicurezza della Repubblica - CISR), to identify the subjects included in the national cyber security perimeter which are required to comply with the measures and obligations envisaged.

The criteria for identifying the aforementioned subjects and the criteria by which these subjects prepare and update the list of networks, information systems, and IT services of their respective relevance are also stated in Art. 1, paragraph 2(a).

Moreover, within 10 months of the entry into force of the law, another Prime Ministerial Decree has to be adopted – on the proposal of the CISR, after obtaining the opinion of the competent parliamentary committees – to determine the notification procedures for accidents produced on networks, information systems and information systems national cyber security perimeter and security measures.

The aforementioned Prime Ministerial Decrees are updated – at least every two years – with the same procedure envisaged for their adoption. The provision also contains a detailed system

²⁹ Gazzetta Ufficiale della Repubblica Italiana, (2019). *Decreto Legge 21 settembre 2019, no.105*. "Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica". <https://www.gazzettaufficiale.it/eli/id/2019/09/21/19G00111/sg>

³⁰ Gazzetta Ufficiale della Repubblica Italiana, (2019). *Legge 18 novembre 2019, no. 133*. "Conversione in legge, con modificazioni, del decreto-legge 21 settembre 2019, no. 105, recante disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica (GU Serie Generale n.272 del 20-11-2019)". <https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg>

of sanctions for cases of violation of the obligations envisioned and identifies the competent authorities to ascertain the violations and to impose sanctions.

Two main aspects of the national perimeter concern the reinforcement of the role of the National Center for Evaluation and Certification (Centro di Valutazione e Certificazione Nazionale - CVCN) and the extension of the so-called Golden Power, also concerning the implementation and adoption of 5G networks.

The decree deepens the structuring of the role and the organization of the National Assessment and Certification Center (CVCN), which is required to develop and adopt cyber certification schemes, assess the risk and verify the security conditions, as well as the absence of vulnerability, and to contribute to the development of security measures. The systems and equipment subject to CVCN evaluations are specified with technical criteria and categories.

The Law no. 133 also extends the Law Decree no. 21 of 2012³¹ on 'special' prerogatives – the so-called golden power that the State can use to defend operators in the defence and national security sectors – to new areas of strategic importance such as energy, transport, communications (it has recently been extended to 5G).

These special powers essentially allow the Government to impose conditions on, or veto, certain transactions whenever the Government estimates that these would result in serious harm to Italian public interests, national defence and homeland security and, in certain circumstances, in the telecommunications, energy and transportation industries, including critical hi-tech infrastructures and 5G technologies. The 5G element was introduced through amendments in the Law no.133, which recognize that broadband electronic communications services based on 5G technology are activities of strategic importance for the national defence and security system.

The first implementing DPCM³² no. 131, approved on 30 July 2020 – **Regulation on the perimeter of national cyber security** – came into force on November 5, 2020.

³¹ Gazzetta Ufficiale della Repubblica Italiana, (2012). *Decreto Legge 15 marzo 2012, no. 21*. "Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.". <https://www.gazzettaufficiale.it/eli/id/2012/03/15/012G0040/sg>

³² Presidenza del Consiglio dei Ministri, (2020). *Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020 , no. 131*. "Regolamento in materia di perimetro di sicurezza nazionale cibernetica". <http://www.infoparlamento.it/Pdf/ShowPdf/7602>

Article 1 of the new Prime Ministerial Decree defines, for the first time, some fundamental concepts for the establishment of the national cyber security perimeter. Various central elements are clarified for the implementation of the provisions of the regulatory framework; it details the concepts of network, information system, and IT service as well as those of "ICT assets" and "architecture and components".

Although the concepts of "network" and "information system" were previously defined in Legislative Decree no. 65 of 2018 (implementation of NIS directive), the definition and framing of the remaining crucial concepts stands as a key innovative element for an effective understanding of the subject of analysis of the national cyber "perimeter".

It is worth highlighting the definition of ICT asset, which is understood as a "set of networks, information systems and IT services, or parts of them, of any nature", and which constitute the basis of two crucial activities regarding the criteria upon which the list is prepared and updated. These actions constitute the assessment of a cyber event in terms of impacts, the identification of dependent and relevant networks, information systems, IT services or physical infrastructures.

Another relevant point is contained in the Art. 2 which, *inter alia*, identifies the subjects involved in the perimeter, grouping them in two macro-categories:

- a subject who exercises **an essential function of the State**, which ensure the continuity of the action of the Government and Constitutional bodies; internal and external security and defence of the State, international relations, security and public order, the administration of justice, the functionality of economic systems and financial and transport;
- a subject - public or private - that **provides an essential service** for the maintenance of civil, social or economic fundamental **for the State**, specifying the definition of essential service.³⁵

The DPCM also identified the sectors relevant to the Italian national cyber security, in which the subject will be identified. Art. 3 provides more details on these sectors and identifies as

³⁵ (1) activities instrumental to the exercise of essential functions of the State; (2) activities necessary for the exercise and enjoyment of fundamental rights; (3) activities necessary for the continuity of supplies and the efficiency of infrastructure and logistics; (4) research and activities relating to production realities in the field of high technology and in any other sector, where they have economic and social importance, also for the purpose of guaranteeing national strategic autonomy, competitiveness and development of the economic system national.

relevant the State administration bodies that constitute the Interministerial Committee for the Security of the Republic (CISR)³⁴ and private and public subjects operating in 11 key sectors, which are identified by the respective Ministries of competence.


KEY SECTOR	MINISTER OF COMPETENCE
 Internal Affairs	Ministry of the Interior
 Defence	Ministry of Defence
 Space and Aerospace	Presidency of the Council of Ministers
 Energy	Ministry of Economic Development
 Telecommunications	Ministry of Economic Development
 Economics and Finance	Ministry of Economy and Finance
 Transport	Ministry of Infrastructures and Transport
 Digital Services	The Ministry of Economic Development, in conjunction with the structure of the Presidency of the Council of Ministers responsible for technological innovation and digitization
 Critical Technologies	The structure of the Presidency of the Council of Ministers responsible for technological innovation and digitization, in conjunction with the Ministry of Economic Development and the Ministry of Education, University and Research
 Social Security Labor Institutions	Minister of Labour and Social Policies

Table IV. Perimeter's key sectors and competent Ministers

The Art. 4 of the Decree provides that, for each sector, the Ministry of competence acts in four directions:

- a) First of all, it has to identify the essential functions and services performed by the aforementioned subjects, which depend on networks, information systems or IT services and whose interruption or impairment could compromise national security.³⁵

³⁴ Which are: Presidency of the Council of Ministers, the Ministry of Foreign Affairs and International Cooperation, the Ministry of the Interior, the Ministry of Defense, the Ministry of Justice, the Ministry of Economy and Finance, the Ministry of Economic Development.

³⁵ Art. 4, Paragraph 1(a)

- b) Second, in the case of an interruption of the essential function or service, the Ministry must assess the territorial extension of the essential function, the number of users involved and the possible economic consequences, as well as any other relevant element. As for the effects of the interruption of the essential function or service, the administration will have to consider the consequences of the loss of availability, integrity or confidentiality of the data. Finally, it is necessary to evaluate the mitigation possibilities for restoring the operativity of the function or service.³⁶
- c) Third, the DPCM requires the competent Ministry to identify the essential functions and services for which, in the event of interruption or compromise, the damage to national security is maximum and the mitigation possibilities minimum.³⁷
- d) Finally, the administrations are required to identify the persons who perform the functions indicated by the previous point.³⁸

Art. 5 gives the competent authorities the task of preparing the list of identifiable subjects and transmitting it to the technical CISR, as a collegiate body for coordinating and supporting the activities of the CISR. The list of subjects is contained in an administrative document, adopted and periodically updated by the President of the Council of Ministers, on the proposal of CISR.

Another new element is introduced by Art. 6, which establishes an inter-ministerial table for the implementation of the national cyber security perimeter, to support the technical CISR. The "Table" will be chaired by a deputy director-general of the DIS and composed of two representatives of each CISR administration, by a representative of the Information and External Security Agency (AISE) and by one of the Information and Internal Security Agency (AISI), as well as by two representatives of the other Ministries concerned from time to time. The latter are "called to participate in the meetings, also upon their motivated request, in relation to the topics to be discussed, of which at least one possesses technical-specialist skills in the field of cyber security" (DPCM no. 131, p. 14). The inter-ministerial table for the implementation of the national cyber security perimeter will meet periodically, every six months, but can also be convened on initiatives of the President or a designated member.

³⁶ Art. 4, Paragraph 1(b)

³⁷ Art. 4, Paragraph 1(c)

³⁸ Art. 4, Paragraph 1(d)

The first DPCM represents an essential step towards the construction of the national cyber security perimeter and, consequently, a great step forward for the defence of the ICT infrastructure. However, the real potential of the perimeter will be assessed after the adoption of future implementation decrees, especially at the operational level. Therefore, the concrete results of this regulatory framework will only be visible in the medium-long term.

Moreover, although the establishment of an advanced perimeter constitutes a step forward towards a stronger cyber security and a greater cyber defence, it still does not provide solutions for many of the deficiencies highlighted in the first part of this paper. In particular, it is still unclear if the perimeter should provide the normative and regulatory basis to respond with a counterattack (i.e. hack back) in case of a high-structured cyber attack.

Conclusion and recommendations

Defining cyber power or cyber security preparedness is a challenging task that becomes even more difficult when trying to rank countries worldwide. Every index present deficiencies and difficulties that could partially invalidate their outcomes. Given the sensitive nature of some aspects of the matter, data are difficult to gather and even more difficult to analyze comprehensively and coherently.

The NCPI, even though some bias and lacks were identified, is currently the best and most inclusive attempt to categorize States' efforts and capabilities, without limiting the concept of cyber power to the mere ability to attack or defend. It provides a general overview of States' cyber power, upon which governments can establish the next steps to take to better their cyber profile.

Following the indicators that were highlighted by the NCPI, in the political or normative sphere, Italy has developed in 2013 a comprehensive approach to cyber security matters, which was further improved from the adaptation of European directives, the implementation of the new decrees and the increased centralization of the intelligence service at the operational level.

At the same time, in the military field, it was established the Joint Command for Cyber Operations (CIOC) in 2017 and in 2020 was established the Command for Network Operations (COR), which will conduct and coordinate operations in the cyber domain and secure technical-operational management of all Defense Information & Communications Technology Systems.

Moreover, in the Italian political-legal context, since 2005 an ad hoc structure has been created for the protection of critical infrastructures from cyber crime (i.e. Polizia Postale – CNAIPIC, art. 7-bis, Law 144/2005 and Decree of the Minister of the Interior of 9 January 2008 "Identification of critical IT infrastructures of national interest"). In the context of the Ministry of Foreign Affairs and International Cooperation, a Unity for cyber space policies and security has been established in the General Directorate for Political and Security Affairs.

Nevertheless, some recommendations are needed to enhance the Italian cyber security posture, at the national and international levels.

In particular, the Italian Government should implement different measures to bridge the gap that has been highlighted both by the NCPI and by this policy paper:

- The first step should be the priority to update the national strategy to reflect the current challenges and opportunities in cyber space, and to formulate the strategic goals more comprehensively, by integrating it with other strategic documents (such as the national strategy on AI and 5G). This should also be accompanied by an annual document to highlight the progresses that have been made, to promote transparency and inform international partners and to enhance national awareness.
- Italy still lacks a National Center for Cyber Security, which is present in almost every country with a high cyber power score (in particular European Union Member States and G7 partners). The lack of a National Center dedicated to enhancing cyber capabilities might jeopardize the efforts which have been structured at the institutional and normative level. At the same time, the creation of an *ad hoc* structure could favour the appropriate centralization mechanisms of information sharing, avoid cases of ubiquity and fragmentation in the institutional architecture. In this sense, a National Center should play a central role in the relationship with the private sector and, in general, with the cyber security multi-stakeholders, promoting not only the exchange of information but the establishment of a cyber ecosystem for the development of national technologies. Awareness-raising, exchange of best practices, training, networking, education and R&D projects are just some of the cross-cutting facets of this dynamic ecosystem.
- One of the main issues that this policy paper has highlighted is the underfunding of the cyber security R&D, and the lack of public initiatives to raise the cyber-awareness of the population, at all levels. This can be solved through the allocation of specific budgets to implement specific awareness and cyber hygiene programs, encourage the education and specialization of the next generation in cyber-related fields and expand the R&D projects to also become more competitive in the high-tech market, especially in the emerging technologies sector (e.g. AI, 5G, quantum computing, robotics).
- Another related issue is the migration of professional profiles in the field of security towards companies that, across borders, offer better wages. Furthermore, the number of professional profiles related to cyber security that have graduated from Italian

universities is still too low. The combination of these two factors makes it necessary to develop appropriate policies and strategies for talent promotion and retention. In this specific case, the National Center for Cyber security should be the milestone to achieve this aim.

- The government should also be even more engaged at the international level, through the negotiation and signature of partnership agreements, Memorandum of Understanding, bi and multilateral agreements, but also by providing solutions and by proposing norms and agreements in the UN, EU, OSCE, G7 and NATO contexts, to raise its soft power in the cyber space arena. In this perspective, the new Cyber Unit created at the Ministry of Foreign Affairs and International Cooperation will play a key role but, at the same time, should involve academic actors to include in its vision the technological landscape and be able to understand how the emerging technologies could have impacts on international security and stability.

This paper has also underlined how Italy should cover a proactive role in the digital field. Nevertheless, to achieve this aim, some improvements can be done, in particular regarding the definition of clear Italian national interests related to its posture in cyber space. One of the major issues is related to the current Italian position as an importer of technology. In light of this, the Italian decision-makers should revert this trend through an approach able to replace foreign products with specific initiatives that can favour domestic technologies and products. Defining these priorities can help in promoting and supporting the national excellences and can put Italy in a more competitive position in the international market, already dominated by “giants” and “cyber superpowers”.

Bibliography

- Amnesty International, (2019). *Phishing attacks using third-party applications against Egyptian civil society organizations.*
- Castells, M. (2006). Communication, power and counter-power in the network society. *International journal of communication*, 1(1), 29.
- Check point research, (2019). *The Eye on the Nile.*
- Consorzio Interuniversitario Nazionale per l'Informatica, (2018). *The Future of Cybersecurity in Italy: Strategic project areas*, White Book.
- Economist Intelligence Unit & Booz Allen Hamilton, (2011). *Cyber Power Index.*
- E-governance Academy, (2020). *National Cyber Security Index.*
- Gazzetta Ufficiale (2019), *Legge 18 novembre 2019 n.133*. Retrieved from: <https://www.gazzettaufficiale.it/eli/id/2019/11/20/19G00140/sg>. (Accessed 20 November 2020)
- Gazzetta Ufficiale della Repubblica Italiana, (2012). *Decreto Legge 15 marzo 2012, n. 21*. "Norme in materia di poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale, nonché per le attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni.". Retrieved from: <https://www.gazzettaufficiale.it/eli/id/2012/03/15/012G0040/sg> (Accessed 20 November 2020)
- Hathaway, M., Demchak, C., Kerben, J., McArdle, J., Spidalieri, F., (2015). *Cyber Readiness Index 2.0*. Paper, Potomac Institute for Policy Studies.
- IISS, (2014). *The Military Balance*, Routledge
- Italian Presidency of the Council of Ministers, (2017). *Italian Cybersecurity Action Plan*. Retrieved from: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan2017.pdf>. (Accessed 20 November 2020).
- ITU (2015). *Global Cybersecurity Index & Cyberwellness Profile*, ITU, Geneva.
- ITU (2019). *Global Cybersecurity Index*, ITU, Geneva.

Ministero della Difesa, (2013). *Ministerial Directive on the Military Policy for the Year 2013*. https://www.difesa.it/Primo_Piano/Documents/2013/gennaio%202013/Direttiva%20Ministeriale_ENG.pdf. (Accessed 20 November 2020).

Ministero della Difesa, (2015). *White Paper for International Security and Defence*. Retrieved from: https://www.difesa.it/Primo_Piano/Documents/2015/07_Luglio/White%20book.pdf. (Accessed 20 November 2020).

Ministero della Difesa, (2020). *Documento Programmatico Pluriennale per la Difesa per il Triennio 2020-2022*, Camera dei Deputati.

Ministero dello Sviluppo Economico, (2019). *Programma di supporto tecnologie emergenti nell'ambito del 5G*. Retrieved from: <https://www.mise.gov.it/images/stories/documenti/Programma%20supporto%20tecnologie%20emergenti%205G.pdf>. (Accessed 20 November 2020)

Ministero per l'Innovazione tecnologica e la digitalizzazione (2020). *2025, Strategia per l'innovazione tecnologica e la digitalizzazione del Paese*.

NATO, (2016). "NATO Warsaw Summit, Cyber Defence". Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm. (Accessed 20 November 2020).

Nye Jr, J. S. (2010). *Cyber power*. Harvard University. Belfer Center for Science and International Affairs.

Presidency of the Council of Ministers (2013). *The National Plan for Cyberspace Protection and ICT Security*. Retrieved from: <https://www.sicurezza nazionale.gov.it/sisr.nsf/wpcontent/uploads/2014/02/italian-national-cyber-security-plan.pdf> (Accessed 20 November 2020).

Presidency of the Council of Ministers, (2013). *National Strategic Framework for Cyberspace Security*. Retrieved from: <https://www.sicurezza nazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategicframework-for-cyberspace-security.pdf> (Accessed 20 November 2020).

Presidency of the Council of Ministers, (2017). *The Italian Cybersecurity Action Plan*. Retrieved from: <https://www.sicurezza nazionale.gov.it/sisr.nsf/wp-content/uploads/2019/05/Italian-cybersecurity-action-plan-2017.pdf>. (Accessed 20 November 2020).

Presidenza del Consiglio dei Ministri (2013), *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*. Retrieved from: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf> (Accessed 20 November 2020)

Presidenza del Consiglio dei Ministri (2013), *Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico*. Retrieved from: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf>. (Accessed 20 November 2020)

Presidenza del Consiglio dei Ministri (2017), *Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica*. Retrieved from: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf>. (Accessed 20 November 2020)

Presidenza del Consiglio dei Ministri (2018). *Direttiva NIS- Decreto Legislativo 18 maggio 2018 n.65 in Attuazione della direttiva UE 2016/1148*. Retrieved from: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2018/06/La-NIS-in-pillole.pdf>. (Accessed 20 November 2020)

Presidenza del Consiglio dei Ministri, (2020). *Decreto del Presidente del Consiglio dei Ministri 30 luglio 2020 , n. 131. "Regolamento in materia di perimetro di sicurezza nazionale cibernetica"*. Retrieved from: <http://www.infoparlamento.it/Pdf/ShowPdf/7602>. (Accessed 20 November 2020).

Republic of Italy (1947). *Constitution of the Italian Republic*. 22 December 1947. Retrieved from: https://www.senato.it/documenti/repository/istituzione/costituzione_inglese.pdf (Accessed 20 November 2020).

Sistema di Informazione per la sicurezza della Repubblica, (2019). *Relazione sulla politica dell'informazione per la sicurezza, Allegato alla relazione annuale al Parlamento*. Retrieved from: <https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2020/03/RELAZIONE-ANNUALE-2019-4.pdf>. (Accessed 20 November 2020)

Stato Maggiore della Difesa, (2017). *Informazioni della Difesa. Cyber-Defence. Nasce il Comando Interforze per le Operazioni Cibernetiche*. Retrieved from: https://www.difesa.it/InformazioniDellaDifesa/periodico/Periodico_2017/Documents/Numero3/ID3_2017_ri-dotto.pdf.(Accessed 20 November 2020).

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., Schwarzenbach, A., (2020). *National Cyber Power Index 2020*. Belfer Center for Science and International Affairs.

Appendix A – Overview of Italian Cyber Norms

Cyber Norms

<p>Directive containing guidelines for cyber protection and national IT security (Monti Decree) January 2013</p> <p>DPCM - Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale (Decreto Monti)</p>	<p>It defines the institutional architecture for the protection of national security in relation to critical infrastructures regarding cyber protection and national IT security. It also defines the subjects included in the institutional architecture and the organizational-functional model.</p>
<p>National Strategic Framework for Cyber Space Security December 2013</p> <p>Quadro Strategico Nazionale per la Sicurezza dello Spazio Cibernetico</p>	<p>The Framework was developed by the Cyber Technical Work Table (Tavolo Tecnico Cyber-TTC) operating at the Information Security Department (Dipartimento Informazioni per la Sicurezza). Chapter I provides an overview of the main threats and vulnerabilities exploited to conduct cyber attacks against Italy and defines the roles and tasks of the various subjects, public and private, even those operating outside the country, to increase the country's ability to prevent and respond to events in the cyber space. In Chapter II, strategic guidelines are identified, including tools and procedures to enhance the country's cyber capabilities.</p>
<p>National Plan for Cyber Protection and Information Security December 2013</p> <p>Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica</p>	<p>The National Plan aims to develop, for the two-year period 2014-2015, the six strategic directions identified in the National Strategic Framework (2013). The Plan establishes the roadmap for the adoption of the priority measures for the implementation of the QSN by public and private entities, as framed by the Prime Minister's Decree of 24 January 2013.</p>
<p>Directive on cyber protection and national IT security (Renzi Directive) August 2015</p> <p>Direttiva 1° agosto 2015- Direttiva sulla protezione cibernetica e la sicurezza informatica nazionale (Direttiva Renzi)</p>	<p>In light of the two aforementioned existing planning documents, the directive aims to consolidate an efficient reaction system to ensure the resilience of the national IT infrastructure, through greater coordination and integration between the public entities involved and the of partnerships with private operators who manage the IT infrastructures</p>
<p>Directive containing guidelines for cyber protection and national IT security (Gentiloni Decree) February 2017</p> <p>DPCM - Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale (Decreto Gentiloni)</p>	<p>The DPCM replaces the previous "Monti Decree". The Decree reaffirms the main role of the CISR. The role and responsibilities of the DIS in the field of cyber security are redefined. A National Assessment and Certification Centre is established to verify the security conditions and the absence of vulnerabilities on products, equipment and IT systems.</p>

National Plan for Cyber Protection and Information Security
March 2017

Piano Nazionale per la Protezione Cibernetica e la Sicurezza Informatica

The National Plan replaces the previous one for the two-year period 2014-2015 and identifies the operational guidelines and objectives to be achieved to concretely implement the National Strategic Framework for the security of the cyber space (QSN). The Operational Guidelines (IIOO) are eleven, with consequent lines of action:

- Enhancement of intelligence, police, and civil and military defence capabilities.
- Strengthening the organization and methods of coordination and interaction at national level between public and private entities.
- Promotion and dissemination of the IT security culture. Education and training.
- International cooperation and exercises. Operation of the national incident prevention, response, and remediation structures.
- Legislative interventions and compliance with international obligations.
- Compliance with security standards and protocols.
- Support for industrial and technological development.
- Strategic and operational communication.
- Resources.
- Implementation of a national cyber risk management system

NIS Directive - Legislative Decree no. 65 of 18 May 2018 in Implementation of EU Directive 2016/1148 containing measures for a common high level of security of the Union's networks and information systems.

The NIS Directive is intended to define the measures necessary to achieve a high level of security of networks and information systems. The decree applies to Operators of Essential Services (OSE) and to Providers of Digital Services (FSD). The latter are called upon to adopt adequate and proportionate technical and organizational measures for risk management and to prevent and minimize the impact of accidents affecting the security of networks and information systems.

Notify the incidents that have a significant impact on the continuity and provision of the service to the Computer Security Incident Response Team (CSIRT) and the competent authority of the Dipartimento delle informazioni per la sicurezza (DIS).

Legislative Decree 10 August 2018 n.101 - Provisions for the adaptation of Italian national legislation to the provisions of the GDPR (General Data Protection Regulation) EU Regulation 2016/679

With the Legislative Decree, while not completely abolishing the Legislative Decree no. 196 of 2003 (Privacy Code), the national legislative sources are harmonized with the EU GDPR. The content concerns provisions on the protection of natural persons regarding the processing of personal data, as well as the free circulation of such data.

<p>Emerging technologies support program in the context of 5G.</p> <p>March 2019</p> <p>Programma di supporto tecnologie emergenti nell'ambito del 5G</p>	<p>The program, based on the CIPE Resolution 6/2018, for a total amount of up to 45 million euros, aims to carry out experimentation, applied research and technology transfer projects to be developed in collaboration with local authorities, relating to emerging technologies (Blockchain, AI, IoT) connected with the development of next generation networks. There are two axes of intervention:</p> <ul style="list-style-type: none"> • choosing among the 5G experimentation municipalities, technology transfer centres will be developed towards start-ups and SMEs. • Public administrations, public bodies, agencies, research bodies and universities can apply for the implementation of specific experimentation and applied research projects connected to the development of new generation networks.
<p>Italy 2025³⁹</p>	<p>Released by the Ministry for technological innovation and digitisation – based on UN's SDGs – identifies three main challenges for the next five years: creation of a digital society, innovation of the State and development of sustainable and ethic innovations. Between the 20 strategies to solve these issues, many are based on AI technologies [8, 13, 14, 20] in compliance with the social, cultural and democratic sustainability and ethics, already established in the national strategy draft and European Commission strategy [17].</p>
<p>National Strategy for Artificial Intelligence</p> <p>September 2020</p> <p>Strategia Nazionale per l'Intelligenza Artificiale</p>	<p>The Italian Strategy on AI proposes an ethic and normative framework coherent with the goal of the European Union White Paper, further elaborating on the governance of the Artificial Intelligence technologies. It proposes the creation of an interministerial cabinet to harmonize research, innovation and policies on the matter, in order to create a sustainable national.</p> <p>The Italian approach is moreover very human-centric and focused on sustainability. The strategy, after analysing the global and European trends and the threat and challenges that come from AI, is structured in four parts: AI and the human being, AI for a reliable and competitive ecosystem, AI for a sustainable development and strategy governance, followed by recommendations on these four macro sections.</p>
<p>National Cyber security Perimeter</p> <p>September 2019</p> <p>Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica</p>	<p>Established in order to ensure a high level of security of the networks, information systems and IT services of public administrations, bodies and national operators, public and private, on which depends the exercise of an essential function of the State and society. In other words, the final aim of the perimeter is to protect the subjects that provide essential services whose malfunction, interruption, even partial, or improper use could result in damage to national security.</p>

Appendix B – Italian Cyber Architecture

Cyber-Architecture

<p>Agency for Digital Italy Established with Legislative Decree 22 June 2012 n. 83</p> <p>AGID- Agenzia per l'Italia Digitale</p>	<p>The Agency for Digital Italy is the technical agency of the Presidency of the Council which has the task of guaranteeing the achievement of the objectives of the Italian Digital Agenda and contributing to the diffusion of the use of information and communication technologies, favouring the innovation and economic growth. Furthermore, it draws up guidelines, technical rules, and guidelines on the homogeneity of languages, procedures and standards for the full interoperability and uniformity of the IT systems of the public administration.</p>
<p>Cybersecurity Management Board DPCM 24 January 2013</p> <p>NSC - Nucleo per sicurezza cibernetica</p>	<p>The nucleus provides for the prevention and preparation of any risky situations and for the activation of the alert procedures.</p> <p>For the purposes of prevention and preparation for any crisis situations, the Nucleus promotes the programming and operational planning of the response to cyber crisis situations by public subjects and private operators concerned, and the development of inter-ministerial coordination procedures for crisis management; keeps an alert and response unit active (24/7); evaluates and promotes information sharing procedures for the dissemination of alarms and crisis management.</p> <p>To activate the response and recovery actions, however, the Nucleus receives the reports of a cybernetic event and issues the related alarms. Where the event takes on dimensions, intensity or nature such as to affect national security or cannot be dealt with by the individual competent administrations, but requires the taking of coordinated decisions in the inter-ministerial context, it declares the situation of cyber crisis and activates the NISP, which "Interministerial table of cyber crisis".</p>
<p>Department for Information Security Responsibilities in the field of cyber security: Law n.124/2007 and Law n.133/2012</p> <p>DIS - Dipartimento per le Informazioni e la Sicurezza. Competenze in ambito della sicurezza cibernetica.</p>	<p>The DIS, through its offices, ensures support to the General Director for the performance of coordination activities; on the basis of information, analyses and reports from security information services and entities of various kinds, formulates analyses, assessments and forecasts on the cyber threat; defines the cyber security measures that must be adopted to protect the IT systems and infrastructures that handle information classified or covered by State secrets.</p> <p>The DIS draws up the national security document concerning activities relating to the protection of critical, tangible, and intangible infrastructures, as well as cyber protection and information security, to be attached to the annual report to Parliament on information security policy. it entails two agencies: one for internal intelligence (AISI) and one for external intelligence (AISE).</p>

<p>Interministerial Committee for the Security of the Republic DPCM 13 April 2017 n. 87</p> <p>CISR - Comitato Interministeriale per la sicurezza della Repubblica</p>	<p>CISR is a body of consultancy, proposals and deliberations on the general guidelines and purposes of the information policy for safety. In particular, the committee:</p> <ul style="list-style-type: none"> • Resolution on the division of financial resources and on the budget and balance sheets of DIS, AISE and AISI • Indicates the information requirements needed by ministers to carry out government activities
<p>CSIRT- Computer Security Incident Response Team Established with the Legislative Decree of 18 May 2018 n.65 3 the DPCM 8 August 2019 art.4</p>	<p>The CSIRT provides proactive support through the dissemination of specific alerts and bulletins, through accident monitoring activities at national level, dynamic risk analysis, sharing of common or standardized practices in the classification and treatment of cyber events, risks, and information.</p> <p>The CSIRT also ensures, by virtue of its location at the DIS, close cooperation with the single point of contact established by the NIS Directive for receiving notifications of cross-border incidents and with the Cyber Security Nucleus, which intervenes in the event of any crisis situations that present risk profiles for national security. With respect to the role that the CSIRT will play in the national cyberspace, the conscious participation of all public and private entities, as contributors to strengthening the cyber security of the entire country system, will also be fundamental.</p>
<p>CVCN - National Centre for Evaluation and Certification Established on February 19, 2019, as part of the qualifying actions for the construction of the national cyber national security architecture (DPCM January 24, 2013)</p>	<p>The CVCN has the task of verifying the security conditions and the absence of vulnerability of products, equipment, and systems intended to be used for the operation of networks, services and strategic infrastructures, as well as of any other operator for which there is a national interest. Furthermore, the CVCN elaborates and adopts cyber certification schemes for the purpose of protecting the national security perimeter.</p>
<p>Joint Forces Command for Cybernetic Operations 2017</p> <p>CIOC- Comando Interforze per le Operazioni Cibernetiche</p>	<p>The Command has the task of countering and neutralizing the cyber threat to defend military networks and the information that travels on them both in Italy and abroad, where there are ongoing operations and where the networks are extensive. The Command is ready to respond to the 4th institutional mission of the Armed Forces, that is to support the nation for any need, with the most varied capabilities, such as those of digital forensics.</p> <p>The command has two main operational objectives:</p> <ul style="list-style-type: none"> • cyber defence: relating to static defence and the protection of critical networks, carried out in coordination with the Ministry of Defence, to guarantee their integrity. • Cyber network defence: the ability to carry out vulnerability assessments and penetration tests, to provide rapid intervention when necessary. The CIOC will also contribute to the organization and training of the entire Italian Cyber security System

**Postal Police - National
Cybercrime Centre
for the Protection of Critical
Infrastructures**

Polizia Postale—CNAIPIC
Centro Nazionale Anticrimine
Informatico per la Protezione
delle Infrastrutture Critiche

The C.N.A.I.P.I.C. is exclusively responsible for the prevention and repression of computer crimes, of a common, organized or terrorist matrix, which have as their objective the computerized infrastructures of a critical nature and of national importance.

The added value that the Centre represents, in the panorama of the protection of Critical Infrastructures derives:

- from the creation of an Operations Room, available 24 hours a day, 7 days a week, as a single point of contact dedicated both to ICs and to any other actor, including internationally, engaged in the protection of ICs.
- from the exclusive, dedicated, and protected telematic connections between the C.N.A.I.P.I.C. and the I.C., for the shared, mutual and constant transfer of data and information useful for the performance of the functions of evaluation, prevention and repression of threats and cybercrimes.

It makes use of high-level technologies and highly qualified personnel, specialized in the fight against cybercrime, who has also gained concrete experience in the so-called sectors. cyberterrorism and industrial espionage.

The operations of the C.N.A.I.P.I.C. it is satisfied through the exercise of an Operating Sector and a Technical Sector.

**Network
operations command**

Comando
operazioni di rete

The Command for Network Operations guarantees, with a unified and coherent vision, the conduct of operations in the cyber domain, the secure technical-operational management of all defence Information & Communications Technology / C4 Systems, in order to harmonize and distribute promptly the information produced by the command and control, computing, Intelligence Surveillance & Reconnaissance systems necessary to enable the functions of the CINC and the Commands concerned.

Structured in three Divisions (C4, Security and Cyber Defence, Cyber Operations), it reports directly to the Chief of the Defence Staff; it merges previous organizations, the Joint Command for Cyber Operations (CIOC) and the Joint C4 Command; it ensures the Operation and Maintenance (O&M) and security framework of the joint capability assets aimed at conducting Cyber Network Operations and it manages the Defence Network, the joint Information Communication Technology (ICT) services and several centralized ICT capabilities.



Center for Cyber Security and International Relations Studies (CCSIRS)

Interdepartmental Center for Strategic, International and Entrepreneurial Studies (CSSII)

Department of Social and Political Sciences

University of Florence

Via delle Pandette 32

50127

Firenze

www.cssii.unifi.it

cyber@cssii.unifi.it