ITALY
CYBER READINESS AT A GLANCE

Principal Investigator: Melissa Hathaway
Chris Demchak, Jason Kerben, Jennifer McArdle, Francesca Spidalieri

November 2016

POTOMAC INSTITUTE FOR POLICY STUDIES

Published by Potomac Institute for Policy Studies

Potomac Institute for Policy Studies
901 N. Stuart St, Suite 1200
Arlington, VA 22203
www.potomacinstitute.org
Telephone: 703.525.0770; Fax: 703.525.0299

Email: CyberReadinessIndex2.0@potomacinstitute.org

Follow us on Twitter:
@CyberReadyIndex

Cover Art by Alex Taliesen.

Acknowledgements

The Potomac Institute for Policy Studies and the authors would like to thank the following individuals for their contributions: Stefano Mele, Ph.D., Counsel at the Carnelutti Law Firm and co-founder of Moire Consulting Group; and Carola Frediani, journalist at *La Stampa*. The authors would also like to thank Alex Taliesen for cover art and Sherry Loveless for editorial and design work.

ITALY
CYBER READINESS AT A GLANCE

TABLE OF CONTENTS

ITALY

CYBER READINESS AT A GLANCE

Country Population	60.8 million
Population Growth	0%
GDP at market prices (current $US)	$1.815 trillion
GDP Growth	0.8%
Year Internet Introduced	1988
National Cyber Security Strategy	2013
Internet Domain	.it
Fixed broadband subscriptions per 100 users	23.5
Mobile broadband subscriptions per 100 users	70.9
Mobile phone subscriptions per 100 users	154.2

Information and Communications Technology (ICT) Development and Connectivity Standing

International Telecommunications Union (ITU) ICT Development Index (IDI)	**38**	World Economic Forum's Network Readiness Index (NRI)	**55**

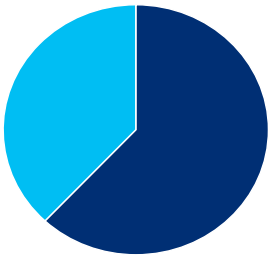
Sources: World Bank (2015), ITU (2015), NRI (2015), and Internet Society.

INTRODUCTION

Italy's first computer network emerged in 1980s, when a group of nuclear physicists connected all of the country's nuclear research institutes. In 1988, it became part of a broader scientific academic project to unify various scientific institutions and their large computers by means of a single network (Gruppo Armonizzazione Reti della Ricerca, GARR).[1]

The first commercial Internet service providers (ISPs) for residential users appeared several years later – from 1992-1993 – when Italy started to privatize its telecommunications industry. Until the 1990s, telecommunications services were provided by a collection of companies owned largely by the Italian government through the Institute for Industrial Reconstruction/Italian Telecommunications Society (Istituto per la Ricostruzione Industriale/Societa Italiana per l'Esercizio Telefonico, IRI-STET). In 1994, in compliance with the new "Rules for the Reform of the Telecommunications Industry," five of those companies merged to form Telecom Italia. Three years later, Telecom Italia merged with STET – retaining the Telecom Italia name – forming a privately owned company where government ownership phased out by the end of the 1990s. While Telecom Italia continues to be the country's largest telecommunications service provider, a number of other ISPs have emerged within a short period of time after the 1990s privatization.[2]

Since the 1990s, the Italian government supported Internet uptake as a catalyst for economic growth, increased tourism, reduced communication costs, and more efficient government operations. The Italian Internet penetration rate today, however, is still low compared to other European nations – 62 percent versus 79 percent, respectively[3] – and the availability of high-speed Internet connectivity is among the lowest in the EU.[4] On the contrary, mobile-broadband subscriptions have increased steadily to over 154 percent of the population – suggesting Italian citizens prefer mobile broadband connection.[5] The surge in mobile subscriptions may be due to the significant price decrease for mobile services by more than 52 percent between 2012 and 2014 in Italy – the largest decline in prices in all of Europe.[6]



Italy Internet Penetration: 62%

Nonetheless, Italian participation in e-government, e-banking, and e-commerce still lags behind much of Europe – ranging around 20 percent compared to a EU average of 40-50 percent – and less than 10 percent of the country's companies engage in online sales. These lower figures are due to infrastructure limitations, low availability of Next Generation Access (NGA) networks, and the fragmentation and duplication of past government investment strategies.[7] Other obstacles to greater Internet penetration include an aging population, a lack of advanced technical skills, mistrust of online transactions, and a persistent digital, educational, and income divide between northern and southern Italian regions. Together, past and continuing challenges have imposed limitations on the country's ability to reach EU targets of Internet speed and accessibility, digital literacy, and network modernization.

In 2015, the Italian government adopted a €6 billion (~$6.7 billion) "Digital Growth Strategy 2014-2020" ("Strategia per la Crescita Digitale 2014-2020"). The digital strategy is intended to expand and modernize Internet infrastructure, improve access to high-speed broadband, and expand e-government functions (e.g., "digital identity," public e-services, and "intelligent communities") as a mechanism to "ensure economic and social growth, through the development of skills in business and the dissemination of digital culture among citizens."[8] The national digital growth strategy acknowledges that Italy lags behind other European countries in economic development, Internet penetration levels, digitalization of public and business activities, and digital literacy. It also recognizes the need to use market interventions – such as those prescribed by the European Digital Single Market strategy – to grow national gross domestic product (GDP) by up to 3 percent.

In line with the objectives set by the 2010 European Digital Agenda – one of the seven pillars of the "Europe 2020 Strategy" – the 2015 Italian national digital growth strategy also identifies priorities and specific actions to help foster wider use of ICTs, ensure a safe and secure access to digital services, and encourage the cooperation among government agencies' information systems and between these systems and the EU. In addition, it sets clear objectives and deadlines indicating progress towards the goals of the digital strategy.[9] In particular, the digital strategy emphasizes improvements to the security of critical e-government and healthcare services – to be increasingly provided online – in order to ensure the privacy and integrity of communications and continuity of service for citizens.[10]

The Agency for Digital Italy (Agenzia per l'Italia Digitale, AgID) – established in 2012 within the Prime Minister's Office – is responsible for the implementation of the national digital strategy and is charged with a wide variety of related tasks, such as promoting and disseminating information initiatives; digital training of citizens and civil servants; monitoring the implementation of ICT plans in public administrations to improve efficiency and transparency; enhancing cooperation between public information systems; coordinating initiatives to provide network services for citizens and enterprise; and ensuring national interoperability of services through the development of technical requirements and guidelines. The Agency coordinates its efforts with the active participation of central and local governments, including autonomous regions and provinces, and other ministries as requested.[11]

In addition, the Office of the Prime Minister in collaboration with the Ministry of Economic Development, AgID, and the Agency for Cohesion are implementing additional projects, such as the "National Plan for Ultra-Wide Broadband" and the "Digital Growth" plan to accelerate the objectives of the national digital strategy.[12] The goals include provision of high-speed Internet access to at least 50 percent of Italians by 2020 and extension of fiber-optic network to rural areas. Major Italian ISPs like Fastweb, Vodafone, and Wind have also joined in a co-investment partnership – the "Fiber for Italy" project – which, together with another plan announced by Telecom Italia, aim to further extend fiber-optic networks to all of the largest cities by 2018.[13]

As in many other developed countries, cyber security is a major challenge for Italy. Assessing the severity and impact of malicious cyber activity on individuals and organizations in Italy has been somewhat difficult in the past because of the lack of official statistics and the propensity of victims not to report incidents or notify authorities. The Italian Security Intelligence Department (DIS) noted in its annual report that, in 2015, cyber espionage activities against both government entities and high-tech industry grew in scale, volume, and sophistication. It also estimated that almost seventy percent of cyber attacks in Italy were directed at public entities and that the prime threat actor (by percentage of activities registered, not by threat level) were groups of hacktivists.[14] In addition, in 2016, the Italian Association for Information Security (Associazione Italiana per la Sicurezza Informatica, CLUSIT) estimated that, in the first half of 2016, cyber crime grew by 9 percent and was the cause of 71 percent of all cyber attacks in Italy.[15] Their 2016 semiannual report stated also that economic losses due to cyber insecurity have quadrupled since 2013.[16] While Italy does not rank high on the list of countries identified as points of origin for cyber attacks,[17] it is the second most infected country across the European and Middle Eastern (EMEA) region. Countries like Turkey, Italy, and Hungary – the top three most-bot-populated countries in the EMEA region – in fact, are an attractive target for hackers because they have experienced a huge increase in high-speed Internet and connected devices in recent years, but this increased connectivity has not been accompanied by higher security awareness.[18]

The topic of cyber security was brought forward in 2009 by then Deputy Prime Minister and Chairman of the Italian Parliamentary Committee for the Security of the Republic (COPASIR), Francesco Rutelli. He initiated the first set of Parliamentary consultations on "the potential implications and threats to national security derived from the use of cyberspace."[19] The discussions and hearings undertaken by COPASIR continued and led to the publication of the first Report to the Parliament and the Government on Cybersecurity and its implication for national security in 2010. The report urged the government to develop a strategic plan and appropriate mechanisms to combat cyber crime and protect computer networks. In particular, the report recommended the development of a national cyber security strategy that would "ensure an adequate leadership and clear policy guidelines to combat [cyber] threats and to facilitate coordination among all interested stakeholders."[20] It also suggested identifying a competent authority under the responsibility of the cabinet office (Presidenza del Consiglio dei Ministri) charged with carrying out all cyber security-related activities. The strong recommendations in this report were largely ignored until Italy experienced a string of cyber incidents, including one major intrusion by Anonymous against the Italian Ministry of Interior, which exposed a wealth of sensitive documents and emails.[21]

Ultimately, it took the Italian government three more years to develop its first national cyber security strategy. The 2013 Prime Minister's "Decree Containing Strategic Guidelines for

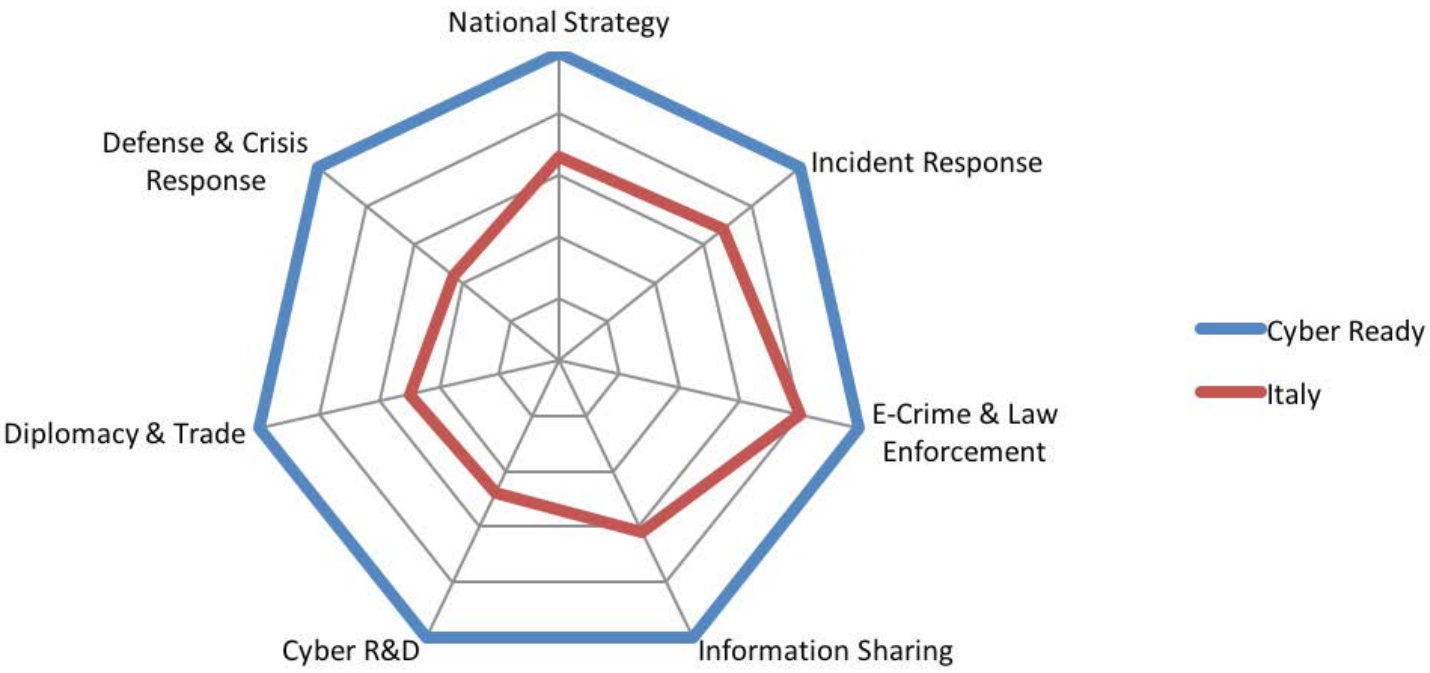
National Cyber Protection and Information Security" provided the first outline of the institutional and organizational structure for the national cyber security architecture, and assigned the Prime Minister direct responsibility for the cyber security of the Nation.[22] Following this decree, the "National Strategic framework for Cyberspace Security" and the accompanying implementation plan, the "National Plan for Cyberspace Protection and ICT Security" were published in 2013. The two documents taken together constitute a comprehensive strategy that includes: a description of the national security and economic risks of cyber insecurity; an assessment of Italy's cyber security capacity; a clear delineation of the roles and responsibilities of the different entities involved in national cyber security; and specific strategic and operational objectives to be implemented.[23]

In addition to the national cyber security strategy and implementation plan, the Italian Security Intelligence Department and AgID endorsed the 2015 "National Cyber Security Framework" – a voluntary guidance developed by the Italian Cybersecurity National Laboratory and the Cyber Intelligence and Information Security Center at the Sapienza University (CIS-Sapienza) – based on the 2013 US National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity." The voluntary framework, expanded and updated to reflect the Italian context, aims at providing organizations with "a homogeneous and volunteer approach to face up cyber security."[24] It is also intended as a reference guide to existing standards and regulations for entities to evaluate their current risk profile and maturity levels, identify priorities and targeted levels of cyber preparedness, and ultimately reduce risks associated with cyber threats. A key objective of this voluntary framework is offering guidelines to increase cyber security levels of Italian small and medium-sized businesses (SMEs) with recommendations for C-level executives in large companies and operators of critical infrastructures on cyber security risk management processes.

Despite the publication of a national cyber security strategy and the restructuring of the relevant national cyber security architecture, there is still a substantial gap in terms of national-level preparedness for cyber risks between Italy and comparable EU member states. While Italy has put forward a number of cyber security-related initiatives, many of those efforts are still fragmented and there does not appear to be a centralized coordination mechanism to ensure the economic and security objectives for the country are met. Yet, the Italian government recognizes the benefits and threats derived from the use of ICTs and both the 2013 national cyber security strategy and the 2015 national digital growth strategy clearly acknowledged the importance of Internet connectivity and ICT development as key drivers for economic growth. Moreover, the 2015 "White Paper for International Security and Defense" strategically prioritized cyber defense and defensive military operations in cyberspace as one of the main investment programs for 2016-2018.[25] With the decision to create a Cyber

Command within the Ministry of Defense, whose first unit may be operational by 2017, the Italian government appears to be gaining ground in defending itself and its economy in and through cyberspace.

The Cyber Readiness Index (CRI) 2.0 has been employed to evaluate Italy's preparedness levels for cyber risks. This analysis provides an actionable blueprint for Italy to better understand its Internet-infrastructure dependencies and vulnerabilities and assess its commitment and maturity in closing the gap between its current cyber security posture and the national cyber capabilities needed to support its digital future. A full assessment of the country's cyber security-related efforts and capabilities based on the seven essential elements of the CRI 2.0 (national strategy, incident response, e-crime and law enforcement, information sharing, investment in R&D, diplomacy and trade, and defense and crisis response) follows.



Italy Cyber Readiness Assessment (2016)

1. NATIONAL STRATEGY

Following the adoption of the Prime Minister's "Decree Containing Strategic Guidelines for National Cyber Protection and Information Security" in 2013,[26] a Cybersecurity Working Group (Tavolo Tecnico Cyber, TTC) was established under the auspices of the Interdepartmental Committee for the Security of the Republic (Comitato Interministeriale per la Sicurezza della Repbblica, CISR) and chaired by the Security Intelligence Department (Dipartimento delle informazioni per la sicurezza, DIS) to develop the first Italian national cyber security strategy.

In 2013, Italy published its first national cyber security strategy to enhance the country's preparedness to the security threats and challenges stemming from cyberspace.

In accordance with the 2013 Prime Minister's Decree and 2013 EU Cyber Security Strategy – that was followed by the 2016 EU Directive on Network and Information Security (NIS) – requiring each EU member state to create their own "network and information security strategy," Italy published both the "National Strategic Framework for Cyberspace Security" national strategy and the "National Plan for Cyberspace Protection and ICT Security" implementation plan in 2013. While the national strategy "highlights the nature and the evolving trends of the cyber threat as well as of the vulnerabilities to the national ICT networks, outlines roles and tasks of public and private stakeholders involved in cyber security, and identifies tools and procedures to enhance the country's preparedness," the implementation plan "identifies a limited set of priorities, and provides specific objectives and guidelines in order to give concrete implementation to the Strategic Framework."[27] The two documents taken together constitute a comprehensive national cyber security strategy "around which to coordinate all efforts, so that [Italy] can face with confidence the security threats and challenges stemming from cyberspace, and pursue [its] national interest where the wealth of nations will more and more prosper."[28]

Staying focused on the long-term goals and objectives of connecting Italy while reducing its cyber insecurity may be difficult vis-à-vis the other competing and long-standing structural challenges Italy faces. Balancing economic priorities and national security needs can be tricky. Italy is challenged by stagnant GDP growth, low productivity rates, a banking sector burdened with "bad" debt, and a high unemployment rate. The Italian government has put forth a series of solutions to revitalize the economy and address Italy's financial problems, but the success of these efforts remains to be seen.[29] Moreover, an impending constitutional referendum on the future of its Senate – the upper house of parliament – could further distract the government from key national cyber security priorities.[30]

The 2013 national cyber security strategy recognized that given the "current financial and economic tightening," the government and relevant stakeholders should not "allow for any duplication of efforts" and instead "seek any possible synergy, keeping in mind that the budget allocation will constitute not only a net saving if compared with the possible damage cyber attacks can entail, but also an extraordinary opportunity of cultural, social and economic growth."[31] The implementation plan set clear objectives, many of which have already been initiated, if not fully implemented, including strengthening intelligence, police, civil protection, and military defense capabilities; establishing a national Computer Emergency Response Team (CERT); conducting international exercises; and promoting *ad hoc* legislation and compliance with international obligations.

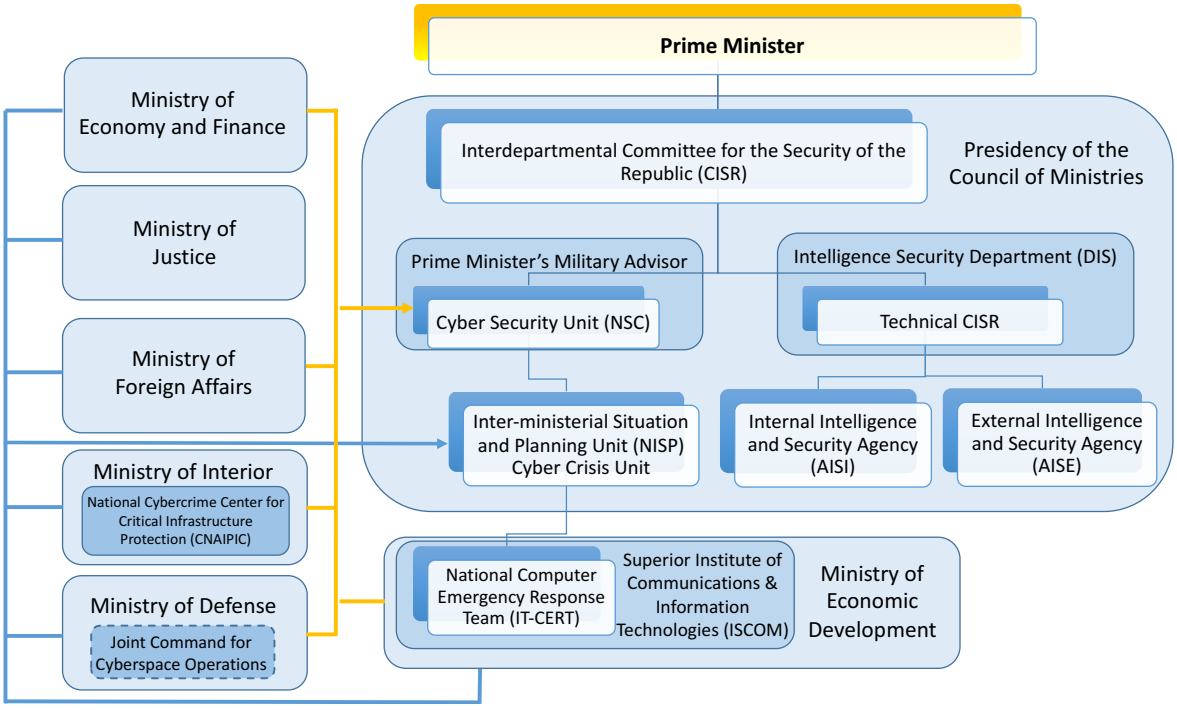
Cyber security coordination is directly under the responsibility of the cabinet office (Presidenza del Consiglio dei Ministri). The Italian Prime Minister's Office (or Presidency of the Council of Ministries) is formally responsible for the development and implementation of the national cyber security strategy and the implementation plan through the adoption of specific directives. The Prime Minister's Office is supported in this endeavor by the Interdepartmental Committee for the Security of the Republic (CISR), which advocates for the adoption of additional legislative initiatives, approves guidelines to foster private-public partnerships, introduces policies for enhancing information sharing arrangements and the endorsement of best practices, promotes collaboration among institutional bodies and private market players operating in the national cyber security realm, and approves other measures to strengthen national cyber security.[32] CISR is chaired by the Prime Minister and is composed by the Ministries of Foreign Affairs, Interior, Justice, Defense, Economy and Finance, and Economic Development. The Prime Minister's Military Advisor participates to CISR meetings whenever cyber security matters are discussed. The DIS Director General acts as the CISR Secretary. The CISR at Working Level – called "Technical CISR" – supports the work of CISR in verifying the timely and correct implementation of the strategy and related plan, which are regularly reviewed and assessed internally. In addition, the CISR at Working Level is assisted in its activities by various national intelligence public entities, including DIS, the External Intelligence and Security Agency (Agenzia informazioni e sicurezza esterna, AISE), and the Internal Intelligence and Security Agency (Agenzia informazioni e sicurezza interna, AISI). The Italian government is currently working on an updated implementation plan.

The 2013 Prime Minister's Decree established the Cyber Security Unit (Nucleo per la sicurezza cibernetica, NSC) a permanent body within the Prime Minister's Office comprised of representatives from the Ministry of Foreign Affairs, Interior, Defense, Economy and Finance, Eco-

The Cyber Security Unit (NSC), within the Prime Minister's Office, coordinates the activities of all the government agencies that compose the national cyber security architecture.

nomic Development, the Civil Protection Department, DIS, AISE, AISI, and the Agency for Digital Italy. This body reports directly to the Prime Minister's Military Advisor.[33] NSC coordinates the activities of the various institutions that compose the national cyber security architecture. In particular, it is responsible for all national cyber security prevention, risk assessment and mitigation, incident response and crisis management activities. The NSC is also responsible for restoring networks and systems functionality, and is the formal point of contact for national and international organizations.[34] In the event of a large-scale cyber incident that requires the involvement of multiple ministries, the NSC will activate the Inter-ministerial Situation and Planning Unit (Nucleo Interministeriale Situazione e Pianificazione, NISP) in the format of the Inter-ministerial Cyber Crisis Unit (Tavolo interministeriale di crisi cibernetica) to oversee response coordination.[35] The national CERT is responsible for technical response measures and supports citizens and companies through awareness, prevention, and cyber incident response activities (see "Incident Response" section for more information).

A 2015 Prime Minister's Directive provided additional implementation guidance to all major stakeholders for the 2013 national cyber security strategy, including increasing national-levels of cyber preparedness, security, and resilience, and "aligning strategic capabilities to international standards."[36] Other aspects in this Directive included directing the development of a more comprehensive institutional architecture, establishing stronger incident response capabilities, and fostering closer collaboration with both public entities and the private sector operators of telecommunications and critical infrastructures.



Italy Cyber Security Organizational Chart (2016).

While the 2013 national cyber security strategy mentioned the importance of allocating "adequate human, financial, technological and logistic resources" to achieve its goals, it did not pledge any specific funds. In the 2015 digital growth strategy, the Italian government committed €50 million (~$56 million) to securing citizens and businesses' digital identities and ensuring safe and secure access to digital services, including from mobile devices.[37] The 2016 Stability Law (Legge di Stabilitá 2016), approving the FY 2016 budget, allocated €150 million (~$166 million) for national cyber security efforts, of which €15 million (~$16.6 million) to the Italian Postal and Communications Police Service and its "National Cybercrime Centre for Critical Infrastructure Protection" (CNAIPIC) – a special unit responsible for all activities of prevention, containment, mitigation, and investigation of cyber crime and other malicious cyber activities conducted against critical infrastructure.[38] Finally, a recent September 2016 Prime Minister's Decree allocated the remaining €135 million (~$149 million) of the FY 2016 budget to national cyber security efforts under the responsibility of the DIS to strengthen both traditional preventive and defense measures against cyber risks that rise to the national level and to prioritize the protection of national cyberspace.[39]

2. INCIDENT RESPONSE

While Italy does not have a consolidated, single national incident response plan, both the 2013 Prime Minister's Decree on national cyber protection and information security and the 2013 national cyber security strategy assigned to the Cyber Security Unit (NSC) the responsibility to coordinate cyber incident response activities and restore networks and systems functionality. In addition, NSC can activate a non-permanent Inter-ministerial Situational and Planning Unit for Cyber Crisis (NISP) in the event of a cyber incident that is considered relevant to national security, or of such magnitude to require coordination with various ministers for the management of broader crises.

In addition, Italian private sector companies supplying information services and the operators of critical infrastructures, both at national and European levels, are required to notify the NSC of all relevant violations of their networks and to adopt specific cyber security measures.

The national Computer Emergency Response Team (CERT Nazionale or IT-CERT) was established in 2015 in response to the provisional guidelines of the 2013 national cyber security strategy and in line with the requirements of the 2013 EU strategy for "An Open, Safe and Secure Cyberspace" and subsequent EU Cyber Security Directive.[40] IT-CERT is embedded within the Ministry of Economic Development and headed by the Director of the Superior Institute

Italy established its first national Computer Emergency Response Team (IT-CERT) in 2015, tasked with facilitating containment of and response to large-scale cyber incidents.

of Communications and Information Technologies (Istituto Superiore delle Comunicazioni e delle Technologie dell'Informazione, ISCOM). IT-CERT is tasked with facilitating containment of and response to large-scale cyber incidents. It also provides a series of other proactive and reactive services to a broad domestic constituency, including: publishing timely alerts and advisories on cyber vulnerabilities and threats; promoting cyber security awareness and best practices; cooperating with CERT-equivalents both domestically and internationally; and supporting restoration activities.

In addition to IT-CERT's cyber security news and alerts, the DIS conducts regular analysis and assessments of cyber threats and publishes an annual "Report on Security Intelligence Policy and Results Achieved" in cyber security. The annual report highlights the activities for the defense of the critical, physical, and intangible infrastructures; the national cyberspace; and information security.[41]

In 2012, the Italian government passed a law requiring the DIS to provide technical guidance on security controls for critical infrastructures and share cyber threat and warning data with the private sector.[42] In addition, partially government-owned companies, such as ENEL (electricity), ENI (oil & gas), Poste Italiane (postal services), ENAV (air-traffic control), TrenItalia (rail network), and the Italian Central Bank, signed a cooperation agreement with DIS to voluntarily report breaches and share threat data. The 2013 Ministerial Decree updated the 2012 law and required all telecommunication providers and other operators of critical infrastructure to collaborate with DIS and other government entities responsible for national security (e.g., IT-CERT, CNAIPIC) to respond to cyber incidents and ensure the continuity of operations.

While data breach notification requirements still vary among European countries, the Italian government has already adopted many of the prescriptions contained in the 1995 EU Data Protection Directive and the 2016 EU Network and Information Security (NIS) Directive, aimed at improving cyber security capabilities and cooperation across Europe.[43] For example, Italy had already established a Data Protection Authority (Garante per la Protezione dei Dati Personali) in 1996. This four-person collegiate body, whose members are elected by the Parliament every seven years, is tasked with supervising compliance by both governmental and non-governmental entities with all Italian data protection and privacy laws.[44] The Data Protection Authority has adopted a series of provisions for public administration entities and other organizations, which detail specific data breach notification requirements. For instance, telecommunications and Internet Service Provides (ISPs) that have been breached are required to notify the Data Protection Authority within 24 hours from discovery of the incident and send additional information via a form available on their website within three days.[45]

In addition, two committees – the Industry Technical Working Group (Tavolo Tecnico Imprese) and the government's Cybersecurity Working Group (Tavolo Tecnico Cyber, TTC) provide additional contact points for critical industries and government entities essential to the operation and recovery of critical services and infrastructures. Moreover, all government agencies and offices involved in national security affairs,

including the Ministry of Interior, Ministry of Defense, Ministry of Public Administration and Innovation, Ministry of Infrastructure, police and other law enforcement agencies, Civil Protection Department, and intelligence agencies participate in a Critical Infrastructure Protection Coordination Working Group. Finally, the 2013 national cyber security strategy required Italy to conduct periodic national cyber security exercises with public sector stakeholders and relevant private sector operators.

3. E-CRIME AND LAW ENFORCEMENT

In 2001 Italy signed – and in 2008 ratified – the Council of Europe Convention on Cybercrime (commonly known as the 'Budapest Convention'). While Italy has amended and strengthened its Criminal Code to include comprehensive coverage of computer crimes and e-crime since the early 1990s,[46] it has yet to implement all of the cross-border assistance options contained in the Budapest Convention. Some of the government's early attempts to regulate the Internet relied on the same laws that apply to print and broadcast media, which do not have the same implications for human rights, privacy, and freedom of information.[47] For example, some of the earlier laws proposed in regards to data protection, which would hold publishers responsible for all the content of their publications – when applied to the Internet, and especially to websites with user-generated content – may be seen as online censorship and in contradiction with EU directives on Internet matters.[48]

A 2011 law repealed a controversial article in a set of anti-terrorism measures passed in 2005 after the London and Madrid terrorist attacks. The law, entitled the "Legge Pisanu" after the name of the then-Minister of Interior, restricted the opening of new wireless (Wi-Fi) hotspots and required entities offering public communication services (such as hotels and Internet cafés) to apply for licensing approval and keep photocopies of customers' identification and logs of websites visited.[49] The law was one of the most stringent among all Western countries and inhibited the opening of new hotspots all across Italy for several years, thus causing additional delays in closing the digital gap with the rest of Europe.[50] Another bill requiring ISPs to monitor Internet activity and store user data for five years failed to pass in 2003 after protests by activists and opposition parties.[51]

In the wake of the 2015 terrorist attacks in Paris, Italy passed a new anti-terrorism law that criminalizes online terrorist recruitment and the endorsement or incitement of terrorism online. The law also entrusts the public prosecutor (the Postal Police) with drawing up a blacklist of terrorist websites to be blocked or taken down by ISPs. In addition, the law extended the period ISPs must retain users' records of online traffic – "metadata" as opposed to the content of communications – until December 2016 despite a 2014 European court ruling that such measures would restrict the fundamental right to privacy.[52] Critics worry that the law may be applied broadly, thereby hampering legitimate instances of free expression that may fall within international norms for protected speech. Prior to becoming law, however, the government

did withdraw provisions from the bill that would have authorized law enforcement agencies to remotely break into private computers.[53]

Like much of the EU, Italy regulates certain categories of websites, including those that display child pornography and illegal online gambling, and some peer-to-peer (P2P) websites that infringe on copyright laws (e.g., "The Pirate Bay"). In 2006 and 2007, the Italian government introduced new Internet filtering laws requiring ISPs to block access to international or unlicensed gambling sites identified on a blacklist compiled by the Autonomous Administration of State Monopolies (AAMS, a central government agency regulating gambling and other monopolies), as well as those displaying child pornography within six hours of being notified of their existence.[54] The National Center for the Fight against Child Pornography, part of the Postal and Communications Police Service, is in charge of maintaining a list of blocked websites, and Italy's penal code includes severe punishment for the distribution and publication of child pornography.[55]

The Italian Postal and Communications Police Service, is the main law enforcement entity responsible for cyber crime prevention and for the protection of critical infrastructure in Italy. The Italian Postal Service had been delivering services online to millions of customers for decades and had developed a sophisticated system for monitoring and defending its electronic network against cyber attacks. Its police unit was therefore the agency best equipped to take on additional anti-computer crime responsibilities. In 2005, the aforementioned anti-terrorism law (Legge Pisanu) conferred the jurisdiction to the Italian Ministry of Interior and identified the Postal and Communications Police as the department responsible for law enforcement initiatives against cyber attacks on critical information infrastructures. In 2008, the Ministry of Interior established by decree a dedicated National Cybercrime Centre for Critical Infrastructure Protection (Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, CNAIPIC) as the branch of the Italian Postal Police directly responsible for all activities of prevention, containment, mitigation, and investigation of cyber crime and other malicious cyber activities against critical infrastructure. The CNAIPIC, as a law enforcement agency, is active on a 24/7 basis and comprises an operational, a technical, and an investigative unit. In addition, CNAIPIC is the national point of contact for the G-7 High-Tech Crime Network, as provided for by the Budapest Convention for all member states. The Network aims to improve collaboration and increase the effectiveness of cyber crime inves-

The National Cybercrime Centre for Critical Infrastructure Protection (CNAIPIC), within the Italian Postal and Communications Police Service, is responsible for cyber crime prevention and for the protection of critical infrastructure.

tigations and prosecution. With the 2016 Stability Law, the Italian government allocated €15 million (~$16.6 million) for the Postal and Communications Police and CNAIPIC's operational, technical, forensic, and training activities.[56]

There are other law enforcement entities that have responsibilities to combat cyber crime. The Italian police and the Carabinieri – a national gendarmerie charged with both military and civilian police duties – have established special units dedicated to combating cyber crime and conducting computer forensics and scientific investigations.[57] In addition, the Finance Guard (Guardia di Finanza, GdF) is responsible for enforcing decisions related to the blocking of websites for copyright violations and other cyber crime and fraud issues.

Italy is working to increase its capacity and has joined various law enforcement cyber training programs, such as the Council of Europe's "Cybercrime@Octopus" launched in 2014 to assist countries in implementing the Budapest Convention and strengthening data protection and rule of law safeguard.[58] Among other activities, the program includes courses for judges and law enforcement agents on cyber crime and electronic evidence.[59] In order to enhance the effectiveness of strategies against cyber crime, selected police representatives participate in permanent working groups, established by government or international organizations, including the Inter-ministerial Group for Network Security (Gruppo Interministeriale per la sicurezza delle reti), G-7, the European Community, the Council of Europe, the Organisation for Security and Co-operation in Europe (OSCE), Interpol, and Europol.

Additionally, Italy participates in various other interagency partnerships to increase cooperation on cyber security, information sharing, border security, and surveillance. For example, the Italian Ministry of Interior works closely with the US Secret Service and the Federal Bureau of Investigation (FBI) – two of the US federal law enforcement agencies tasked with preventing and combating financial crimes including cyber crime – to thwart transnational cyber crime. As part of this initiative, cyber-trained FBI investigators come to Italy every six months and share tools and information with Italian law enforcement agencies that can help with cyber crime investigation. In 2009, the Italian Postal and Communications Police Service joined forces with the US Secret Service to set up an international task force, called the European Electronic Crime Task Force (EECTF).[60] The agency focuses on a wide range of "computer-based criminal activity," including identity theft, network intrusions, and other computer-related crimes affecting the financial sector and other critical infrastructures. Headquartered in Rome, the EECTF monitors computer networks across Europe using the Italian Postal Service's (Poste Italiane S.p.A.) threat software, and gathers cyber crime information from law enforcement authorities, businesses, security-solution providers, intelligence agencies, and experts in Europe. Moreover, the EECTF actively shares information and alerts related to cyber crime and has established dedicated tools to exchange expertise, knowledge, best practices, and common solutions with other member organizations, including international law enforcement agencies (e.g., Bulgarian

Police, Romanian Police, and Spanish Police), financial institutions (e.g., American Express, Citibank, and MasterCard), international organizations (e.g., ENISA, Anti-Phishing Working Group [APWG], United Nations Interregional Crime and Justice Research Institute [UNICRI], and the Digital Crimes Consortium), ICT security vendors (e.g., Kaspersky, Symantec, and Verizon), and academia (e.g., Universitá di Bologna, Universitá di Salerno, and University College Dublin).[61] In 2010, the task force expanded its European involvement by creating a second unit in the United Kingdom.

Recognizing that cyber crime can increase as high-speed Internet becomes more available and as more connected devices become avenues for infection and exploitation, IT-CERT established the first Italian National Anti-Botnet Support Center (Centro Nationale AntiBotnet). It is part of the European Project Advance Cyber Defence Centre (ACDC), a non-profit initiative composed of 14 EU nations, funded by the European Commission to counter the spread of botnets.[62] Nonetheless, Italy's small and medium-sized companies – the backbone of Italian economy – continue to be plagued by intellectual property theft, ransomware, and business email compromise. This is caused by a combination of lack of awareness of the threats, a dearth of secure and resilient products and services, and a high rate of botnet infection of Italy's digital devices and infrastructures. Despite the efforts of the anti-botnet initiative, in fact, Italy is still facing one of the highest infection rates in Europe and the Middle East.[63] These infections enable illicit and illegal activities, thus calling into question Italy's commitment to reducing criminal activities that are emanating from its territory and to combating transnational crime. To effectively respond to these challenges, Italy may need to increase its efforts with law enforcement agencies and the ISPs to reduce the botnet pathway for cyber crime.

The Italian National Anti-Botnet Support Center actively counters the spread of botnets, as part of a broader European cyber defense initiative.

4. INFORMATION SHARING

As stated in the 2013 national cyber security strategy and its implementation plan, Italy recognizes the importance of private-public partnerships and is committed to working closely with the private sector to share information and collaborate in the area of crisis management planning.

The NSC is responsible for both incident response coordination and for promoting information sharing with public and private stakeholders during crisis and emergencies. The Security Intelligence Department (DIS) shares intelligence information deemed significant for the purpose of cyber security with the NSC and other public and private interested stakeholders. The DIS also promotes cyber security awareness and education nationwide. In addition to the NSC, IT-CERT acts as a whole-of-society information gathering and sharing center with more technical expertise. IT-CERT provides a dedicated "info-sharing" service to a restricted group of users across critical public and private organizations in order to facilitate the interaction among them. Access to this platform allows users to exchange information and experiences related to cyber threats and incidents, expand their collective "knowledge base," and improve their overall response time in case of large-scale incidents.

The Cyber Security Unit (NSC) is the competent authority responsible for both incident response coordination and information sharing during crisis and emergencies.

In addition, the government's Public Administration's CERT (CERT-PA) – established in 2014 as an expansion of the tasks performed by the superseded CERT for System of Public Connectivity (CERT-SPC) – provides a clearing house for internal cyber information sharing among Italian government agencies. It is also the central contact point for other Public Administrations' CERTs at the European level for the exchange of information and agreed procedures.

The Italian Postal Police's National Cybercrime Centre for Critical Infrastructure Protection (CNAIPIC) has developed its own dedicated and protected network for information sharing enabling a bi-lateral exchange of information on cyber threats prevention, assessment, and repression with operators of critical infrastructure.[64] Moreover, a special "Computer Crime Analysis Unit" (Unità di analisi del crimine informatico – UACI) was established to study and analyze cyber crime in partnership with major Italian universities, companies, and public entities, and to develop new computer crime investigation tools and techniques.[65] Local territorial units provide similar services to UACI and can be operationalized to manage legal cases and emergencies arising from citizen reports to police hotlines. In addition, Italy is a member of the National Cyber Forensics and Training Alliance (NCFTA), a US non-profit corporation with a mission to facilitate collaboration and information sharing among private industry, academia, and law enforcement to identify, mitigate, and neutralize complex cyber-related threats.

While Italian telecommunication providers and other operators of critical infrastructure have been required to share information about cyber-related incidents and breaches with government entities responsible for national security, Italy has yet to establish a unique, dedicated institutional structure that provides mechanisms for cross-sector incident information exchange, both operational (near-real-time) and forensic (post-facto). Moreover, there is requirement for certain critical sector companies to establish information sharing partnerships with each of the government agencies responsible for cyber security (e.g., DIS, IT-CERT, CNAIPIC) which causes duplication of efforts and an inefficient allocation of resources. Telecommunication providers and operators of critical infrastructure, among others, would prefer to have a single point of contact with the government to increase the flow of information while reducing the administrative costs of reporting.[66]

Finally, in 2013, a unique information sharing initiative was established with funding from the European Commission through the EU Programme on the Prevention of and Fight against Crime (ISEC). The Postal and Communication Police, in partnership with the Global Cyber Security Center, Abi Lab, Unicredit, Booz & Company, the General Inspector of the Romanian Police, and the National Crime Agency, created an information exchange platform for banks and law enforcement agencies to share information on suspicious transactions, financial fraud, and potential cyber attacks against the banking system.[67] This Online Fraud Centre and Expert Network (OF2CEN) facilitates information exchanges, analyzes information, and provides timely communication about suspicious criminal activities to all its stakeholders. The positive outcomes of this initiative led Italy to start a second project in 2015 (OF2CEN v.2), in partnership with Europol and the European Banking Association. This next generation information sharing platform extended operations to all EU member states.

5. INVESTMENT IN RESEARCH AND DEVELOPMENT

The 2013 national cyber security strategy and the accompanying implementation plan both state an intent to facilitate investment in research and development (R&D) and recognize the need to "cooperate with universities and public and private research centers to elaborate innovative methodologies and technologies for the detection and the analysis of threats and vulnerabilities."[68] However, the 2013 strategy did not clearly state how the government would support, advance, and sustain these efforts. In the 2015 "Digital Growth Strategy 2014-2020," the Italian government committed €12 million (~$13.4 million) to develop ICT-related skills as a key to increasing job opportunities. The funds are intended to: increase digital literacy levels especially among civil servants; widen the curricula of topics related to digital skills; increase the number of ICT skills training courses; and boost the number of graduates in fields related to ICT.[69] In addition, different governmental entities are individually and more directly involved in cyber R&D efforts. For example, the Italian government's Ugo Bordoni Foun-

dation – an ICT research institution within the Ministry of Economic Development – has recently launched a new strategic parstnership with the US-based National Cyber Forensics and Training Alliance (NCFTA) to promote research activity aimed at e-commerce activities, protect trademarks and patents, and strengthen the fight against counterfeiting.[70] Nonetheless, actual R&D expenditures are still low compared to other European countries.

Italy, like all EU countries, participates in the EU's Horizon 2020 program for research and innovation. Italy is one of the top EU countries participating in this program, and has received significant funding to carry out some of its technological development initiatives.[71] While the Italian government has not developed a unified program or set of incentives to encourage cyber security education and applied research at universities and academic institutions, it does support and fund all public universities and national laboratories – some of which have developed their own research projects in this field. In particular, the Ministry of Education, University and Research (MIUR) funds and supervises the National Inter-university Consortium for Informatics (Consorzio Interuniversitario Nazionale per l'Informatica, CINI). The Consortium links public universities, institutes of higher education, and research institutions in a joint Cybersecurity National Lab (Laboratorio Nazionale di Cybersecurity), which includes thirty-eight public and private universities and research centers across Italy.[72]

The Cybersecurity National Lab promotes and coordinates basic and applied scientific research and technological transfer in several fields of computer science, computer engineering, and information technology, and leads several nationwide research projects on supply chain security of critical infrastructure, analysis of malware, and intelligence gathering over the web.[73] Bilaterally with the US, the Cybersecurity National Lab is partnering with NIST to facilitate a Joint Commission Meeting on Science and Technology Cooperation with a focus on cyber security. On the Italian side, this working group includes the National Research Council (CNR) and ENEA.[74] The Cybersecurity National Lab has also played a key role in the development of the 2015 "National Cyber Security Framework" – a voluntary guidance, based on the 2013 US NIST "Framework for Improving Critical Infrastructure Cybersecurity." It expand-

The Cybersecurity National Lab includes thirty-eight public and private universities and research centers across Italy, and promotes and coordinates basic and applied scientific research and technological transfer in computer science, computer engineering, and information technology.

ed and updated the Framework and tailored it to Italy's specific business sectors. Finally, the Cybersecurity National Lab is developing a new cyber security plan to expand the cyber security workforce in Italy, and has recently published a White Paper on the national security and economic implications of cyber insecurity. The White Paper, authored by over fifty scientists from more than twenty top Italian universities, discusses some of the main cyber security challenges Italy will face in the upcoming years and makes specific recommendations for policy makers to tackle them.[75]

In addition, the Prime Minister's Office through CINI supports the Research Center of Cyber Intelligence and Information Security (CIS) at the Sapienza University of Rome – a multidisciplinary center focused on developing information security methodologies, threat profiles, and better preventive and defense strategies.[76] One of CIS' most relevant projects – the TENACE Project – is dedicated to researching technical and organizational methodologies for protecting critical infrastructures from cyber threats.[77] CIS and the Cybersecurity National Lab publish also a yearly "Italian Cyber Security Report." Other Italian public universities have developed advanced cyber security programs and Italian coders and developers rank among the best in the world.[78]

The Global Cyber Security Center (GCSEC) – a non-for-profit organization funded by Poste Italiane and other member companies – is tasked with advancing and disseminating cyber security knowledge and awareness in order to improve capabilities, skills, cooperation, and communication among different stakeholders involved in the use and protection of the Internet. GCSEC collaborates with other Italian and international government institutions, private companies, international organizations, and research institutions, and promotes a variety of programs including training activities, advanced research efforts, information exchanges between specific sectors, capacity building projects, and international engagements.[79]

Moreover, the Italian Postal Police has established different partnerships with Italian universities to both develop innovative solutions to combat cyber crime and to develop a pipeline of cyber security professionals interested in joining specialized cyber crime units upon graduation.

The Italian government has approved in recent years R&D tax credits for different industries and some specific tax incentives for private citizens and corporations investing in innovative star-ups.[80] In addition, in September 2016, the government unveiled a new "Industry 4.0" national stimulus plan aimed at preparing Italian industry for the digital age and supporting investment in research and innovation. The plan is a mix of tax breaks and other incentives and additional measures to ensure all startups and businesses have access to Internet and broadband technology. The Italian government has committed €13 billion (~$14.6 billion) in new funding dedicated to this initiative and plans to "mobilize an additional €10 billion ($11.2 billion) in private investments in 2017."[81]

In addition, a new project, promoted by a non-profit association (CyberPARCO) of cyber security professionals and academics, plans to transform the broad area outside of Milan's city center used for the 2015 World Exhibition (Expo Milano 2015) into a cyber technology park and establish a center of excellence for cyber security. The regional government of Lombardia – the region where Milan is located – has recently created a dedicated cyber security working group to discuss and assess various cyber security-related projects, including the creation of the first Euro-Mediterranean Hub for Cyber Security.[82] The so-called "Cyber Park" plans to create new jobs and attract investments and talent for an expanding cyber security industry in Italy; encourage the development of innovative startups; promote closer cooperation among cyber security companies, investors, entrepreneurs, and academic research organizations; and facilitate the collaboration with international organizations, associations, and similar centers worldwide.[83]

Italy's R&D initiatives must overcome a legacy of R&D stagnation and find mechanisms to encourage the creation of a vibrant startup community underpinned by increased investments by service providers and others. The government's limited implementation and funding to advance its digital growth strategy, combined with its dependence on Horizon 2020 funding, may not be enough to accelerate the digitalization of public and private activities while at the same time reducing the country's cyber insecurity.

6. DIPLOMACY AND TRADE

The 2013 national cyber security strategy explicitly states that "Italy is fully engaged in multilateral institutions, first of all within the European Union (EU) and the North Atlantic Treaty Organization (NATO), as well as with [other] bilateral partners." In addition, the strategy highlights the Italian government's intention to fully "support international cooperation initiatives in the field of cyber security" and "to promote the endorsement and respect of a set of rules of behavior in the digital arena that is consistent with our values, and to facilitate the emergence of a shared approach to cyberspace governance, so that the International Community as a whole can effectively cope with the challenges laying ahead."[84] Indeed, one of the strategy's key objectives is to "foster Italy's participation in international initiatives to enhance cyber security both by joining endeavors underway in the international organizations of which Italy is a member and by strengthening ties with friendly and allied nations."[85]

In line with the objectives described in the national cyber security strategy, Italy regularly participates in multinational negotiations and discussions on cyber security and is a member of all major international bodies addressing cyber-related matters, including the EU, the Council of Europe, NATO, the G-7, the United Nations Group of Governmental Experts (UN GGE), the Organisation of Economic Cooperation and Development (OECD), OSCE, and the Network and Information Security Platform (NIS Platform) established by the European Commission. Italy became also the first European country in 2015 to publish a non-binding parliamentary statement, the "Declaration of

Internet Rights," which promotes the right to internet access, data protection, net neutrality, anonymity, and the so-called "right to be forgotten."[86] An inter-parliamentary committee released the document in a bid to increase public awareness of digital rights and influence legislators tasked with amending the country's current set of laws.

Cyber security issues are often entangled in trade negotiations and security treaties as well. While Italy may not play a leading role in these discussions, it does participate in all such dialogues and negotiations in the various international forums mentioned above and has been implementing and enforcing international agreements at the domestic level. For example, in March 2016, the Ministry of Economic Development – the national authority that oversees the export of "dual use" technologies, such as those covered in the "Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies" – revoked the "global authorization" of the Italian-based Hacking Team to export its spyware based on the export restrictions under the Wassenaar Agreement.[87] Hacking Team – a company best known for its surveillance and hacking tools sold to governments – had been accused of exporting some of its products to countries that may have used those products to violate human rights.

Italy engages more at the bilateral level. Recently, an Italian cyber security trade mission to Israel resulted in an agreement to strengthen business and academic collaboration between the two countries. Additionally, the Italian Ministry of Interior has actively engaged US law enforcement agencies to increase cooperation on cyber security, information sharing, border security, and surveillance.

The Italian Ministry of Foreign Affairs serves as the office responsible for coordinating Italian participation and efforts in the various multilateral forums of discussion on cyber security issues. Italy has also established a dedicated Cyber Security Coordinator position within this ministry with the direct responsibility of negotiating cyber security-related foreign policy and trade agreements, and to represent the ministry within the government's Cybersecurity Working Group. In addition, the Cyber Security Unit within the Prime Minister's Office acts as "the national point-of-contact in cyber crisis situations involving the UN, the EU, NATO, as well as other international organizations and countries."[88]

The Italian Ministry of Foreign Affairs has established the role of Cyber Security Coordinator, responsible for negotiating cyber security-related foreign policy and trade agreements.

7. DEFENSE AND CRISIS RESPONSE

The Italian Ministry of Defense (MoD) has defined cyber security as a threat to national defense and security and acknowledged that cyberspace is now the fifth domain of warfare,[89] which has been reiterated in the declaration made by NATO member states at the July 2016 Warsaw Summit. The "Ministerial Directive on the military policy for the year 2013" recognized the hybrid nature of modern conflict and stressed the need for Italy to strengthen both conventional and non-conventional capabilities, including "in the cyber spectrum."[90] The 2015 "White Paper for International Security and Defense" (Libro Bianco per la Sicurezza Internazionale e la Difesa) highlighted the potentially destructive effects of cyber attacks on the whole-of-society, comparable to those caused by conventional conflicts, and made clear the government's intention to develop Italian Armed Forces' "defense capabilities to counter cyber attacks that might overwhelm civilian agencies' existing capabilities."[91] In particular, the White Paper noted that cyber defense and defensive military operations in cyberspace would be one of Italy's strategic priorities and one of the main investment programs for 2016-2018.[92]

To implement the ambitious goals related to cyber defense stated in the 2015 White Paper, Italy has begun the process of standing up a Joint Command for Cyberspace Operations (Comando Interforze per le Operazioni Cibernetiche, CIOC), which is expected to be operational by 2017. The Command will have two functions. First, it will concentrate and enhance all cyber defense capabilities to protect military networks and the nation at large from cyber attacks. Second, it will develop a Computer Network Operations (CNO) unit with planning and management capabilities in support of military operations within Italy and abroad.[93]

Although limited information is currently available on this new command, recent statements by officers of the Italian Armed Forces suggest that the first unit of this cyber command-equivalent may be operational by mid-2017. Those involved in the development of this new entity are discussing three main activities: (1) the establishment of an organizational structure; (2) the identification of the technological capabil-

Italy has begun the process of standing up a Cyber Command, expected to be operational by 2017.

ities needed to operate it; and (3) the training of the workforce. [94]

The new Command will be physically co-located with the Italian Defense CERT (CERT Difesa) and plans to operationalize some of the Defense CERT technical center's capabilities to be able to conduct defensive cyber operations. CERT Difesa is currently responsible for defending military networks, providing alerts and warnings of threats and possible solutions, managing incident response, and promoting information sharing and collaborations with other civilian CERTs.[95] Cyber Command will be part of the MoD but will also collaborate directly with other government agencies and international organizations.

While the final organization is still being developed, the Italian Cyber Command will most likely be placed within the existing Ministry of Defense's Command, Control, Communications, and Computers Command (Joint C4 Command) answering to the Chief of Defense Staff (Capo di Stato Maggiore della Difesa, CaSMD) – in his capacity as technical and military head of the Italian Defense – through the Vice Commander for Operations (Vice Comandante per le Operazioni, VCOM-OPS), who is responsible for operational planning and deployment of forces in military operations, including cyber operations. The Defense Joint C4 Command already exists within the Italian Ministry of Defense, with the purpose of managing joint activities aimed at ensuring the efficiency of command, control, telecommunications, and ICT. This Cyber Command may also assume the IT missions within the Defense Joint C4 Command. Appropriate laws would have to be created for regulating the new Cyber Command.

Funding for Cyber Command is not specifically called out in the MoD's multi-year economic planning document but it is included as part of the funding allocated for "Joint C4I Systems." The MoD budget defines the enhancement of cyber defense capabilities as one of the most significant funding programs for the Italian Defense. These cyber defense capabilities may receive as much as €22.4 million (~$25 million) in "Joint C4I Systems" funding in the period 2016-2018.[96]

The Italian Armed Forces in general are an active participant in multi-national cyber exercises organized by the EU (e.g., Cyber Europe exercise), NATO (e.g., Cyber Coalition and Cyber Atlantic exercise), and the European Network and Information Security Agency (ENISA) with the goal of testing and improving national preparedness levels. In particular, CERT-IT and the Ministry of Defense's Joint C4 Command participate jointly in all domestic and international cyber security exercises.

Italy is just beginning to establish its national defensive capabilities for cyberspace. During the July 2016 Warsaw Summit, NATO member states agreed to enhance the cyber defenses of national networks and infrastructures, improve their resilience and ability to respond quickly and effectively to cyber attacks, and adapt their cyber defense capabilities.[97] As a

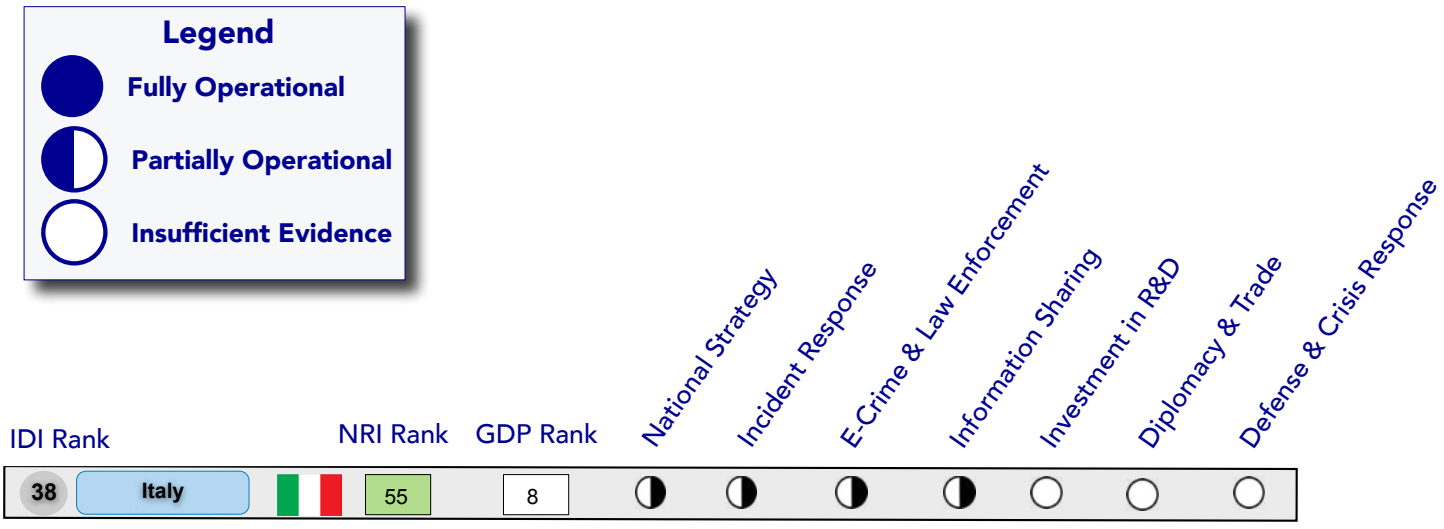
result of this agreement, Italy may accelerate its activities and investments in cyber defense to reinforce its commitment to NATO.

CRI 2.0 BOTTOM LINE

According to the CRI 2.0 assessment, Italy is on a path to becoming cyber ready, and is currently partially operational in many of the seven CRI essential elements.

The findings in this analysis represent a snapshot in time of a dynamic and changing landscape. As Italy continues to develop and update its economic (digital agenda) and national cyber security strategies, policies, and initiatives to reflect a more balanced approach that aligns its national economic visions with its national security priorities, updates to this country profile will reflect those changes and monitor, track, and evaluate substantive and notable improvements.

The CRI 2.0 offers a comprehensive, comparative, experience-based methodology to help national leaders chart a path towards a safer, more resilient digital future in a deeply cybered, competitive, and conflict prone world. For more information regarding the CRI 2.0, please see: http://www.potomacinstitute.org/academic-centers/cyber-readiness-index.



ENDNOTES

1. Wolter Lemstra and William H. Melody, "The Dynamics of Broadband Markets in Europe: Realizing the 2020 Digital Agenda," (Cambridge University Press, 2015): 205.

2. "Italy," *OpenNet Intitiative*, December 15, 2010, https://opennet.net/research/profiles/italy.

3. World Bank, "Internet users (per 100 people)," 2014, http://data.worldbank.org/indicator/IT.NET.USER.P2.

4. Ludovica Glorioso, *National Cyber Security Organization: Italy*, NATO Cooperative Cyber Defence Centre of Excellence, (March 2015): 5, https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_ITALY_032015_0.pdf.

5. World Bank, "Mobile cellular subscriptions (per 100 people)," 2014, http://data.worldbank.org/indicator/IT.CEL.SETS.P2.

6. OECD, "OECD Digital Economy Outlook 2015," (OECD Publishing: Paris): 46, http://ec.europa.eu/eurostat/documents/42577/3222224/Digital+economy+outlook+2015/db-dec3c6-ca38-432c-82f2-1e330d9d6a24.

7. European Commission, "Digital Single Market – Italy," https://ec.europa.eu/digital-single-market/en/scoreboard/italy.

8. Presidency of the Council of Ministers, "Strategia per la Crescita Digitale 2014-2020," (March 2015): 9, http://www.agid.gov.it/sites/default/files/documentazione/strat_crescita_digit_3marzo_0.pdf.

9. *Ibid*, 114.

10. *Ibid*, 50-51 and 73-79.

11. *Ibid*, 41-42.

12. Agenzia per l'Italia Digitale, "Agenda Digitale Italiana," February 2016, http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana.

13. "Will Italy have the best FTTH network in Europe?," *FTTH Council of Europe*, December 2, 2012, http://www.ftthcouncil.eu/documents/PressReleases/2011/PR2011_Italian_Panorama_FINAL.pdf.

14. Sistema di Informazione per la Sicurezza della Repubblica, *Relazione sulla Political dell'Informazione per la Sicurezza – Documento di Sicurezza Nazionale Allegato alla Relazione Annuale al Parlamento*," (2015): 22-23, https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2016/03/Relazione-2015.pdf.

15. Security Summit 2016, "Rapporto CLUSIT 2016," October 5, 2016.

16. Steve Morgan, "Cyber Crime Costs Projected to Reach $2 Trillion by 2019," *Forbes*, January 17, 2016,

http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#2bfa6573bb0c.

17. For more on the countries identified as points of origin for cyber crimes, see the Global Security Map, "Italy," http://globalsecuritymap.com/#it.

18. Danny Palmer, "These ten cities are home to the biggest botnets," *ZDNet*, October 4, 2016, http://www.zdnet.com/article/these-ten-cities-are-home-to-the-biggest-botnets/.

19. Comitato Parlamentare per la Sicurezza della Repubblica, *Relazione sulle possibili implicazioni e minacce per la sicurezza nazionale derivanti dall'utilizzo dell spazio cibernetico*, (July 2010): 13, http://www.camera.it/_dati/leg16/lavori/documentiparlamentari/indiceetesti/034/004/d020.htm.

20. *Ibid*, 49.

21. Matteo Campofiorito, "Anonymous, attacco al Ministero dell'Interno: pubblicati sul blog documenti e email," *La Repubblica*, May 28, 2013, http://www.repubblica.it/tecnologia/2013/05/28/news/anonymous_attacco_ministero_interni-59869466/.

22. Gazzetta Ufficiale della Repubblica Italiana, "Decreto del Presidente del Consiglio dei Ministri 24 Gennaio 2013," n. 66, March 19, 2013, http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

23. Presidency of the Council of Ministers, "National Strategic Framework for Cyberspace Security," http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf, and "National Plan for Cyberspace Protection and ICT Security," December 2013, http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-cyber-security-plan.pdf.

24. Roberto Baldoni and Luca Montanari, "2015 Italian Cyber Security Report – A National Cyber Security Framework, version 1.0," (February 2016), http://www.cybersecurityframework.it/sites/default/files/CSR2015_ENG.pdf.

25. Ministry of Defense, "Libro Bianco per la Sicurezza Internazionale e la Difesa" (July 2015), http://www.difesa.it/Primo_Piano/Documents/2015/04_Aprile/LB_2015.pdf.

26. Gazzetta Ufficiale della Repubblica Italiana, "Decreto del Presidente del Consiglio dei Ministri 24 Gennaio 2013," n. 66, March 19, 2013, http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg.

27. Presidency of the Council of Ministers, "National Plan for Cyberspace Protection and ICT Security," 7.

28. Presidency of the Council of Ministers, "National Strategic Framework for Cyberspace Security," 6-7.

29. Giovanni Legorano, "Bad Debt Piled in Italian Banks Looms as Next Crisis," *The Wall Street Journal*, July 4, 2016, http://www.wsj.com/articles/bad-debt-piled-in-italian-banks-looms-as-next-crisis-1467671900.

30. Will Martin, "Forget Brexit – Italy is poised to tear Europe apart," *Business Insider*, July 5, 2016, http://www.businessinsider.com/italys-political-and-economic-crisis-threatens-europes-stability-2016-7.

31. Presidency of the Council of Ministers, "National Strategic Framework for Cyberspace Security," 7.

32. Presidency of the Council of Ministers, "National Strategic Framework for Cyberspace Security," 27.

33. Gazzetta Ufficiale della Repubblica Italiana, "Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013, art. 8 & 9" (2013), and Stefano Mele, "I principi strategici delle politiche di cybersecurity," Intelligence System for the Security of the Republic, December 5, 2013, https://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/principi-strategici-delle-politiche-di-cyber-security.html.

34. *Ibid.*

35. Ludovica Glorioso, "National Cyber Security Organization: Italy," 7.

36. Matteo Renzi, Italian Prime Minister, "Direttiva 1 Agosto 2015," Intelligence System for the Security of the Republic, August 1, 2015, http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/direttiva-1-agosto-2015.html.

37. Presidency of the Council of Ministers, "Strategia per la Crescita Digitale 2014-2020," (March 2015): 50.

38. Gazzetta Ufficiale della Repubblica Italiana, "Legge di Stabilitá 2016," December 30, 2015, http://www.altalex.com/documents/leggi/2015/10/15/legge-di-stabilita-2016.

39. Camera dei Deputati, "Interrogazione a risposta immediatan. 5-09876 Sisto e Palmieri sulle risorse stanziate per la sicurezza cibernetica," October 26, 2016, http://www.interno.gov.it/sites/default/files/sisto_on_0.pdf.

40. CERT Nazionale, "Chi Siamo," https://www.certnazionale.it/chi-siamo/.

41. Intelligence System for the Security of the Republic, "Annual Report," https://www.sicurezzanazionale.gov.it/sisr.nsf/category/relazione-annuale.html.

42. Sistema di Informazione per la Sicurezza della Repubblica, "Legge 133/2012," August 7, 2012, https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/riferimenti-giuridici/normativa-di-riferimento/legge-133-2012.html, and Melissa Hathaway's discussion with Ambassador Giampiero Massolo, Director of the Italian Security Intelligence Department, in Rome, Italy, December 4, 2012.

43. For more see: Data Protection Authority, "Legislative Decree No. 69/2012" implementing the Directive 2009/12/EC and amending the 2003 Privacy Code provisions in relation to data protection, breach notification, and privacy, May 28, 2012, http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1910654.

44. Garante per la Protezione dei Dati Personali,"The Italian Data Protection Authority: Who We Are," http://www.garanteprivacy.it/web/guest/home_en/who_we_are.

45. Garante per la Protezione dei Dati Personali,"Violazione di dati personali," http://194.242.234.211/documents/10160/0/Violazioni+di+-dati+personali+-+Gli+adempimenti+previsti+(infografica).pdf.

46. Gazzetta Ufficiale della Repubblica Italiana, "Legge n. 547 del 23 dicembre 1993 – Modificazioni ed integrazioni alle norme del codice penale e del codice di procedura penale in tema di criminalità informatica," December 30, 1993, http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:Legge:1993-12-23;547.

47. Ronald Deibert et al., "Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace," (MIT Press: Cambridge, MA. 2010): 319.

48. The most visible incident related occurred in November 2006, when prosecutors began an investigation of two representatives of Google after a violent video of four Italian teenagers attacking a disabled student was posted on Google Video. Italian media law restricts the press from publishing anything that might be deemed "counter to morality," a restriction Google allegedly violated by failing to check the content of the video before it was posted.

49. Sofia Celeste, "Want to check your e-mail in Italy? Bring your passport," *The Christian Science Monitor*, October, 4, 2015, http://www.csmonitor.com/2005/1004/p07s01-woeu.html.

50. Alessandro Gilioli, "Libero web senza fili," *L'Espresso*, November 26, 2009, http://espresso.repubblica.it/palazzo/2009/11/26/news/libero-web-senza-fili-1.17080

51. "Internet Under Surveillance 2004 – Italy," *Reporters Without Borders*, 2004, http://www.refworld.org/docid/46e6918b21.html.

52. Aldo Sghirinzetti, "Italy: Anti-terrorism decree to strengthen government surveillance," European Digital Rights (EDRI), April 22, 2015, https://edri.org/italy-anti-terrorism-decree-strengthen-government-surveillance/.

53. "Freedom on the Net: Italy," *Freedom House*, May 2015, https://freedomhouse.org/report/freedom-net/2015/italy.

54. Catherine Benson, "Italy enacts law to block child porn Web sites," *Reuters*, January 2, 2007, http://www.reuters.com/article/us-italy-internet-idUSL0227310120070102.

55. State Police, "National Center for the Fight against Child Pornography," https://www.commissariatodips.it/profilo/centro-nazionale-contrasto-pedopornografia-on-line.html.

56. Gazzetta Ufficiale della Repubblica Italiana, "Legge di Stabilitá 2016."

57. Ministry of Defense, "Carabinieri – Indagini Scientifiche," http://www.carabinieri.it/arma/oggi/indagini-scientifiche/indagini-scientifiche.

58. Council of Europe, "Global Project Cybercrime@Octopus," http://www.coe.int/en/web/cybercrime/cybercrime-octopus.

59. Council of Europe, "Trainings on cybercrime and electronic evidence," http://www.coe.int/en/web/cybercrime/trainings.

60. Philip Willam, "U.S. teams with Italy to fight cyber crime," *Computer World*, June 30, 2009, http://www.computerworld.com/article/2526301/security0/u-s--teams-with-italy-to-fight-cyber-crime.html.

61. Stefano Grassi, "International Collaboration against Cyber Crime," European Electronic Crime Task Force, July 7, 2011, https://www.gcsec.org/keyportal/uploads/stefano-grassi_presentation_001.pdf, and Roberto Baldoni and Gregory Chockler, "Collaborative Financial Infrastructure Protection," (Springer-Verlag Berlin Heidelberg, 2012), 34.

62. Centro Nazionale AntiBotnet, "Welcome to antibot.it," http://www.antibot.it/en.

63. Danny Palmer, "These ten cities are home to the biggest botnets," *ZDNet*, October 4, 2016, http://www.zdnet.com/article/these-ten-cities-are-home-to-the-biggest-botnets/.

64. Polizia di Stato, "Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche," https://www.commissariatodips.it/profilo/cnaipic.html.

65. Polizia di Stato, "Computer Crime Analysis Unit," https://www.commissariatodips.it/profilo/unita-di-analisi-sul-crimine.html.

66. Francesca Spidalieri's interview with Avv. Stefano Mele, in Rome, Italy, June 12, 2016.

67. Polizia di Stato, "Un passo avanti contro il cyber-crime," October 30, 2013, http://www.poliziadistato.it/articolo/30630.

68. Presidency of the Council of Ministers, "National Plan for Cyberspace Protection and ICT Security," (2013): 9.

69. Presidency of the Council of Ministers, "Strategia per la Crescita Digitale 2014-2020," (2015): 33.

70. "Italy and US United Against Counterfeiting," *NCFTA.net*, https://www.ncfta.net/Home/News.

71. European Commission, "Horizon 2020: First Results," (2015) https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/horizon_2020_first_results.pdf.

72. Intelligence System for the Security of the Republic, "Pansa; per l'Italia un progetto forte di cybersecurity," September 29, 2016, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pansa-per-litalia-un-progetto-forte-di-cybersecurity.html.

73. National Interuniversity Consortium for Informatics, "About us," https://www.consorzio-cini.it/index.php/en/about-us.

74. "Transferta a Washington per il CINI. Confronto Italia-USA su cybersecurity,"*Key 4 Biz*, April 4, 2016, https://www.key4biz.it/trasferta-a-washington-per-il-cini-confronto-italia-usa-su-cybersecurity/155527/.

75. Roberto Baldoni and Rocco De Nicola, "Il futuro della Cyber Security in Italia," *CINI* (October 2015), https://www.consorzio-cini.it/index.php/it/component/attachments/download/416.

76. Sapienza University of Rome, "Research Center of Cyber Intelligence and Information Security," http://www.cis.uniroma1.it/en.

77. Sapienza University of Rome, "Tenace Project," http://www.dis.uniroma1.it/~tenace/.

78. Karen Turner, "Who would win the coding Olympics?," *The Washington* Post, August 30, 2016, https://www.washingtonpost.com/news/the-switch/wp/2016/08/30/who-would-win-the-coding-olympics/.

79. Global Cyber Security Center, "About GCSEC," https://www.gcsec.org/about-gcsec.

80. Barbara Weisz, "Startup innovative, incentivi fiscali 2016," *PMI.it*, March 3, 2016, http://www.pmi.it/impresa/contabilita-e-fisco/news/114753/startup-innovative-via-incentivi-fiscali-2016.html.

81. "Renzi sees Italy 'land of opportunity' with Industry 4.0," *ANSA*, September 21, 2016, http://www.ansa.it/english/news/2016/09/21/renzi-sees-italy-land-of-opportunity-with-industry-4.0_7d601115-9e85-4d67-9301-edc81f7cb4ce.html.

82. "Del Gobbo insedia Tavolo Cyber Security," Regione Lombardia, July 11, 2016, http://www.regione.lombardia.it/cs/Satellite?c=News&cid=1213816605256&childpagename=Regione%2FDetail&pagename=RGNWrapper.

83. "A Cyber Technology Park in the Milan Expo 2015 Area," CyberPARCO, http://www.cyberparco.com/english-one.

84. Presidency of the Council of Ministers, "National Strategic Framework for Cyberspace Security," 6.

85. *Ibid*, 22.

86. Camera dei Deputati, "Declaration of Internet Rights," (2015), http://www.camera.it/application/xmanager/projects/leg17/commissione_internet/testo_definitivo_inglese.pdf.

87. John Zorabedian, "Hacking Team loses global license to sell spyware," *Naked Security*, April 8, 2016, https://nakedsecurity.sophos.com/2016/04/08/hacking-team-loses-global-license-to-sell-spyware/.

88. Presidency of the Council of Ministers, "National Strategic Framework for Cyberspace Security," 28.

89. Remarks by The Honorable Domenico Rossi, Italian Undersecretary of Defense, at the *Cyber Strategy and National Security Conference* in Rome, Italy, June 12, 2016.

90. Ministry of Defense, "Ministerial Directive on the Military Policy for the Year 2013," 21, http://www.difesa.it/Primo_Piano/Documents/2013/gennaio%202013/Direttiva%20Ministeriale_ENG.pdf.

91. Ministry of Defense, "White Paper for International Security and Defense," (July 2015): 38.

92. *Ibid*, 51.

93. Stefano Mele, "Cyber Strategy & Policy Brief, vol. 6 – June 2016," (June 2016): 6, http://stefanomele.it/news/dettaglio.asp?id=459, and remarks by Maurizio La Puca, Vice-Chief of the Italian Defense Staff, at the *Cyber Strategy and National Security Conference* in Rome, Italy, June 12, 2016.

94. *Ibid.*

95. Ministry of Defense, "CERT Difesa – Chi Siamo," http://www.difesa.it/SMD_/Staff/Reparti/II/CERT/Pagine/Chi_Siamo.aspx.

96. Stefano Mele, "Cyber Strategy & Policy Brief, vol. 6" (June 2016), 6.

97. NATO, "Warsaw Summit Communiqué," Press Release, 9 July, 2016, http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en.

For more information or to provide data to the CRI 2.0 methodology, please contact:

CyberReadinessIndex2.0@potomacinstitute.org

ABOUT THE AUTHORS

Melissa Hathaway is a leading expert in cyberspace policy and cybersecurity. She serves as a Senior Fellow and a member of the Board of Regents at Potomac Institute for Policy Studies and is a Senior Advisor at Harvard Kennedy School's Belfer Center for Science and International Affairs. She served in two Presidential administrations where she spearheaded the Cyberspace Policy Review for President Barak Obama and led the Comprehensive National Cybersecurity Initiative for President George W. Bush. She developed a unique methodology for evaluating and measuring the level of preparedness for certain cybersecurity risks, known as the Cyber Readiness Index. She publishes regularly on cybersecurity matters affecting companies and countries. Most of her articles can be found at the following website: http://belfercenter.ksg.harvard.edu/experts/2132/melissa_hathaway.html.

Chris Demchak is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. Her research areas are digital resilience, cyber conflict, and the structures and risks of cyber space. She designed a digitized organization model known as "Atrium" that helps large enterprises respond to and accommodate surprises in their systems. She is also the author of *Wars of Disruption and Resilience: Cybered Conflict, Power and National Security*.

Jason Kerben is a subject-matter expert on the Potomac Institute for Policy Studies' Cyber Readiness Index project. He also serves as senior advisor to multiple Departments and Agencies in matters related to information security and cyber security. In particular, he focuses on legal and regulatory regimes that impact an organization's mission. He develops methodologies and approaches to assess and manage cyber security risk and advises on a myriad of specific cybersecurity activities including international principles governing information and communications technologies, identity and access management, continuous diagnostics and mitigation and cyber insurance.

Jennifer McArdle is a Non-Resident Fellow at the Potomac Institute for Policy Studies and an Assistant Professor of Cybersecurity at Salve Regina University in Newport, RI. Jennifer's academic research and publications focus on cyber conflict, escalation management, and military innovation. She is a PhD candidate in War Studies at King's College London.

Francesca Spidalieri is a subject-matter expert at the Potomac Institute for Policy Studies' Cyber Readiness Index Project. She also serves as the Senior Fellow for Cyber Leadership at the Pell Center, at Salve Regina University, and as a Distinguished Fellow at the Ponemon Institute. Her academic research and publications focus on cyber leadership development, cyber risk management, cyber education, and cyber security workforce development. She also published a report, entitled *State of the States on Cybersecurity*, that applies the Cyber Readiness Index 1.0 at the US state level.

POTOMAC INSTITUTE FOR POLICY STUDIES
901 N. Stuart St. Suite 1200, Arlington, VA 22203
www.potomacinstitute.org