

# Cybersecurity in ITALY

The background features a dark blue grid of white lines that recede into the distance, creating a sense of depth. Overlaid on this grid are three horizontal stripes of the Italian flag: red, white, and green, arranged from top to bottom and slightly offset to create a layered effect.

**New opportunities for business**



PRESIDENZA DEL CONSIGLIO DEI MINISTRI



SISTEMA DI INFORMAZIONE  
PER LA SICUREZZA DELLA REPUBBLICA



Ministry of Foreign Affairs  
and International Cooperation



ITALIAN TRADE AGENCY



CONFINDUSTRIA





# Cybersecurity in ITALY

**New opportunities for business**

## ***Index***

Foreword	2
Cybersecurity: challenges and opportunities	4
Italian cybersecurity architecture	6
Research and Innovation	18
Economic trends	24

# Foreword



*Digital transformation has an impact on each and every piece of our economy and of our society. It broke down borders once insurmountable and it*

*permanently changed the way we see the world. It generated a new form of space –the “cyberspace”– that has become a central part of our life as well as a precondition for growth.*

*Cyberspace creates unforeseen opportunities but it also exposes us to disruptive consequences. Nevertheless, we must face the challenges of innovation.*

*Building a national cybersecurity structure means seizing the opportunities and mitigating the risks*

*through a more effective preparation at strategic and organizational level, and embracing technological innovation by implementing solid security principles.*

*Threats' prevention and response are essential, but not enough.*

*Governing bodies, companies, families, and citizens must all play their role in protecting the system.*

*I am honored to lead Italy's intergovernmental cybersecurity defense system. All initiatives,*

*both at public and private level, are part of a unique framework of intervention for a coordinated and sustainable growth of cybersecurity standards nationwide, especially for our strategic assets.*

*We push for a cultural change that involves our society as a whole, making cybersecurity part of our mind-set.*

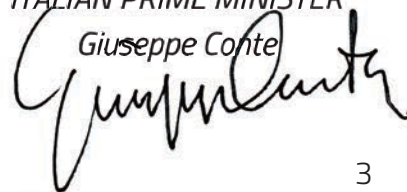
*We foster synergies between scientific and industrial champions to build a national cyber ecosystem aimed at increasing growth and*

*promoting ICT innovation for a more resilient country. The outcome is a "cyber made-in-Italy" that we promote through our diplomatic network and we are willing to share with our trade partners.*

*We cannot imagine the perfect recipe. In cyberspace zero-risk does not exist. But we have many reasons to look at the future with confidence.*

ITALIAN PRIME MINISTER

Giuseppe Conte







# Cybersecurity: challenges and opportunities

In times of ever-increasing dependence on digital solutions in an increasingly interconnected world, it has become apparent that society has become more vulnerable. The current technological revolution and its global effects imply the need in Italy and elsewhere to tackle common opportunities and challenges through a systemic approach that must include public institutions, companies, academia and individual citizens.

A common, general challenge when it comes to cybersecurity is creating a

clear legal framework and **institutional architecture**, so as to identify all entities responsible for cybersecurity issues. Italy made **tremendous advances in creating a cybersecurity ecosystem** and a **new cybersecurity governance/strategy** in the belief that a transparent and protected environment can contribute to creating a positive business environment favorable to the birth and development of new companies and to investments in innovation.

This last point, innovation, is key to the development of a



healthy cyber-economy. New investments play a key role in **activating a cyber-ecosystem**, allowing research worldwide to be transformed into business opportunities. In general, a set of organic actions is needed to **strengthen existing skills, intercept new talent and create new career paths** needed to meet the technological challenges posed by cybersecurity and to improve the relationships between academia and private companies.

Joint efforts of all cybersecurity players must aim to build strong and resilient capabilities, particularly in specific sectors of cyberspace.

Priority areas to develop cybersecurity know-how are connected to **defence and national security issues**, critical networks providing essential services to end users and the protection of national businesses.

When it comes to **ICT**, cybersecurity is also fundamental to the protection of citizen rights. We live in an era where state surveillance powers are expanded, where global internet giants collect and record **data** on our behaviour, holding a knowledge of our most intimate beliefs and conduct, which can allow others to manipulate (such as in the case of the well-known **"fake news"**

**phenomenon**) and intimidate us.

Cybersecurity is growingly focusing also on the **financial sector**, in which cyber attacks pursue three specific goals: organise large-scale theft of financial data, temporary impairment of banking and insurance services, and violation of the integrity of data present within the banking system.

**Italian companies are end-users** of sophisticated solutions for cyber-protection, and at the same time, **producers** and **exporters** of advanced technologies, which position Italy among the most important players in the world cyber market.



# Italian Cybersecurity Architecture

In 2017 and 2018, Italy streamlined and strengthened its cybersecurity structure in order to boost its cyber capabilities.

**The Security Intelligence Department (DIS) is at the center of the Italian cybersecurity ecosystem's governance, acting as:**

- Supporting body for the Prime Minister and the Inter-Ministerial Committee for the Security of the Republic (CISR) on cyber issues
- Chair of the Cybersecurity Management Board (NSC),

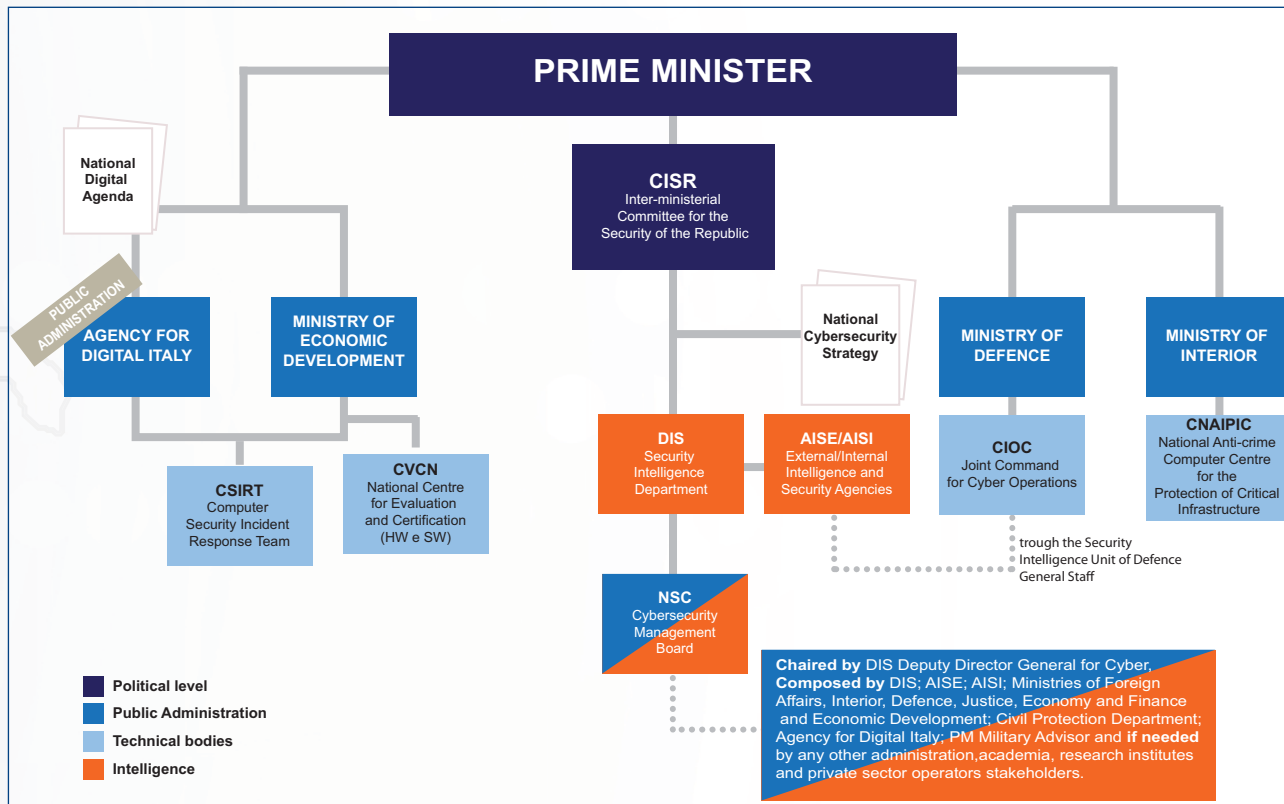
an interagency and intergovernmental operational body within the DIS tasked with cyber crisis prevention, preparation and management(**Fig. 1**)

- European Point of Contact under the Network and Information Security (NIS) directive (**Fig. 2**)

**The NSC is responsible for promoting Italy's participation in cyber activities** (such as Cyber Europe organized by ENISA, the European Network and Information Security Agency) and other initiatives aimed at



**Fig. 1 - Italian cybersecurity architecture**



# Italian Cybersecurity Architecture

Fig. 2 - European Points of Contact under the Network and Information Security (NIS) directive





**The Joint Command for Cyber Operations (CIOC)** was established in 2017 with two main operational objectives: cyber-defence and cyber network-defence. **Cyber-defence** is related to the static defence and protection of critical networks, carried out in coordination with the Ministry of Defence, to ensure their integrity. **Cyber network-defence** is the ability to carry out vulnerability assessments and penetration tests, in order to provide a quick intervention when needed. The CIOC will also contribute to the organization and training of the entire Italian Cybersecurity System.

increasing national cybersecurity. NSC also contributed to the creation of the National Laboratory for Artificial Intelligence and Intelligent System and the Italian Industry Plan 4.0 Funding Program launched by the Ministry of Economic Development.

## **THE ITALIAN STRATEGY**

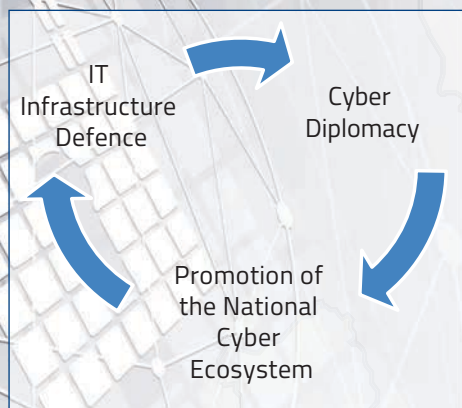
The Italian strategy provides **guidelines for collaboration among both private and public stakeholders**, as well as with **academia and research**. These guidelines aim to:

- Strengthen Italian critical infrastructures and other strategic players' defence capabilities;
- Improve cyber actors' technological, operational, and analytic capabilities;
- Boost public-private cooperation;
- Foster cybersecurity culture;
- Support international cooperation.

## **THE ROLE OF CYBER DIPLOMACY**

The main lines of action of the **Italian Ministry of Foreign Affairs** take into **account the complex, interdependent and continuously changing nature of the cyber domain**. Therefore, while we are dedicated to defending our own communication networks, we also cooperate in safeguarding a national security perimeter, promoting our research and industrial systems, and engaging in cyber-diplomacy while remaining committed to an accessible, open,

# *Italian Cybersecurity Architecture*



interoperable and reliable cyberspace. Italy keeps up its efforts to guarantee the safety and security of cyberspace, the promotion of economic and commercial growth, the protection of human rights and the promotion of fundamental freedoms in cyberspace.

To reach these main goals, Italy relies on the importance of international cooperation, and also aims to implement "Confidence Building Measures" among States and shape effective partnerships in promoting security and stability in cyberspace. At the same time, we underscore the risks, in particular for those activities that could have a destabilizing effect on international peace and security, including massive denial-of-service attacks, critical infrastructure damage, or other malicious cyber activities that compromise the use and





## The European Initiatives

In October 2018, the European Council called for measures to build **strong cybersecurity in the European Union**, which should have been able to respond to and to deter cyber-attacks.

The **Cybersecurity Act**, effective since June 2019, reinforces the current European Network and Information Security Agency (ENISA) as a solid and permanent EU Agency for Cybersecurity, granting the agency a clear mandate and role. A further goal of the Cybersecurity Act is to equip Europe, where the level of standardization in cybersecurity is still too low, with a **framework of cybersecurity certification** for specific ICT processes, products, and services. Such certificates will be **valid in all EU countries**, making it easier for users to gain trust in these technologies, and for companies to carry out their business across borders.

With the Cybersecurity Act, the Directive on Security of Networks and Information Systems (NIS Directive - 2018) and the proposed **European Cybersecurity Competence Centre**, the EU put forward a strong commitment in cybersecurity based on the need to stay competitive while safeguarding common democratic values and the interests of EU citizens.

The EU's strategic aim is indeed to ensure that all the member states **develop essential cyber-capabilities** and to promote investments that could **make the EU's digital Single Market more secure and overcome the fragmentation of the european research**.

The **Public Private Partnership on Cybersecurity (cPPP)**, launched in 2016 as the first EU-wide attempt to bring together the industry, the demand side and the research community, was followed by the new **Digital Europe programme** (2021-2027), which with an overall budget of 9.2 billion € will boost frontline investments in this sector. To encourage and increase investment in research and innovation, the next framework programme (**Horizon Europe 2021-2027**) has an estimated budget of 97.6 billion € to support EU Member States in their efforts to make the most of their national research and innovation potential.

Cybersecurity has also been identified as one of the new six strategic value chains by the Strategic Forum for Important Projects of Common European Interest (IPCEI), promoted by the EU Commission.

# *Italian Cybersecurity Architecture*



operation of critical infrastructures.

Based on this platform, Italy remains committed to **playing a pivotal role in many international fora**, with a view to addressing the major threats in cyberspace.

During the G7 Italian presidency in 2017, the so-called **"Lucca Declaration"** was adopted "on Responsible States Behavior in Cyberspace" – although a non-binding statement, it remains an important commitment to tackle "the risk of escalation and retaliation in cyberspace".

This same approach has

inspired Italy's Chairmanship-in-Office of the OSCE: we hosted the **2018 OSCE-wide Conference on Cyber/ICT Security** in Rome, aimed at providing a platform for exchanging views on digital security and highlighting the positive impact that could arise by a full implementation of Confidence Building Measures on transparency, predictability and International stability. As a **member State of both the EU and NATO**, Italy supports **closer cooperation to promote security and stability in the cyberspace realm**.



## NATO

For more than 10 years, NATO has continued to adapt its collective defense posture to address evolving cyber security threats, **implementing cyberspace as a domain of operations**. The role of the Alliance in the cyber realm is first and foremost to **defend the networks that protect the headquarters and all NATO sites, missions and operations from cyber threats**, recognizing that such attacks have become more frequent, complex, disruptive and potentially destructive.

NATO provides support to its members through: real-time information-sharing; exchange of best practices; maintaining rapidly deployable crisis response teams; facilitating the development of a common approach to cyber defense throughout the Alliance; and investing in education, training and exercises.

**NATO continues to develop its partnership with industry and academia** from all Allies to keep pace with technological advances, including through the **NATO Industry Cyber Partnership**, which supports NATO's efforts to protect networks, increase resilience and help Allies develop their cyber capabilities.

**Italian companies already support NATO efforts in partnership with the Organization and relevant Agencies**; notably, Leonardo Company partners with the NATO Communications and Information Agency (NCI) to provide cyber defense support through the NATO Computer Incident Response Capability (NCIRC). The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn contributes to analysis and evolution of international legal norms pertaining to cyber activities, and the NATO School in Oberammergau and **the NATO Defense College in Rome** conduct **cyber-related education** and foster strategic thinking on cyber-defence related issues.

# *Italian Cybersecurity Architecture*

## **CYBERSECURITY PROMOTION**

The Italian national strategy for cybersecurity promotes the integration and a synergistic approach between cyber security companies with different expertise with two main objectives. First, to develop new means and solutions at the national level to tackle cyber challenges. Second, create national “champions” to be able to compete at the highest international level. In this context, the Ministry of Foreign Affairs and International Cooperations,

together with other competent institutions, facilitates the development of a cyber supply chain, promoting national and international Business to Business (BtoB), Business to Government (BtoG), and Government to Government (GtoG) cooperation agreements, and contributing to exporting Italian capabilities and strategic know-how globally.

**Italian Economic Diplomacy** is involved in supporting cybersecurity companies that are approaching foreign markets, thanks to the work of the wide network of





Embassies and Consulates around the world. Each year, the **Steering Committee for international promotion of Italian companies**, co-chaired by the Minister of Foreign Affairs and International Cooperation and the Minister of Economic Development, sets Italy's priorities for bilateral commercial relations with other Countries. This activity includes the definition of target markets and export sectors, the organization of training activities for entrepreneurs, facilitating financial support for export strategies, monitoring opportunities in international



### International Promotion checklist

- 1) Market knowledge
- 2) Economic Diplomacy
- 3) Developing business opportunities
- 4) Consolidation and growth

markets and organizing dedicated **systemic missions** to enter emerging and innovative markets abroad, including the cyber security market.

**The Ministry of Foreign Affairs and International Cooperation** in cooperation with the Security Intelligence

Department and the Ministry of Defence, has organized **systemic missions in Washington, London**, and many other relevant markets in order to foster the international promotion of national companies specialized in cybersecurity related fields, such as **fintech, defence, energy** and **ICT**.

# *Italian Cybersecurity Architecture*

## **THE MINISTRY OF DEFENCE AND THE ITALIAN OPEN LAB EXPERIENCE**

---

In the past few years, the Italian Government implemented specific initiatives to support companies, in particular Small and Medium Enterprises (SMEs) and start ups, in their digitization and technological progress.

In 2019, the Ministry of Defence launched a program to support companies in the sectors of innovation and cybersecurity. This initiative, called **Italian Open Lab**, represents a **new model of interaction between public institutions, private stakeholders and citizens**. Its goal is to achieve, through

structured brainstorming sessions, **an improvement in the business environment** to enable an **increasing competitiveness** of this sector in Italy and abroad.

Italian Open Lab **seminars** concern different subjects, such as **network security** and **defence of critical infrastructures**, with particular attention to the promotion of Italian strategic know-how and production capacity on cybersecurity.

## **THE ITALIAN TRADE AGENCY AND CYBERSECURITY**

---

The Italian Trade Agency (ITA) is the Governmental agency that supports business development of Italian companies abroad



**and promotes the attraction of foreign investments in Italy.**

With a motivated and modern organization and a widespread network of overseas offices, it provides information, assistance, consulting, promotion and training to Italian small and medium-sized businesses. Using the most modern multi-channel promotion and communication tools, it acts to assert the excellence of Made in Italy in the world.

**ITA's promotional strategy and activity for the cybersecurity sector have significantly increased over the past few years** as a result of a careful analysis and understanding that includes the needs of the start-up

## **The Global Start-up Program**

The **Global Start-up Program 2019** is the first specific Italian Trade Agency (ITA) course to train Italian Start-ups when approaching foreign markets. Up to 120 startups are selected through a specific public competition and are **trained on innovative subjects, such as Medtech, ICT, Cybersecurity, Circular Economy and Automotive**. The program continues with a three-month incubation and/or acceleration stage in selected foreign incubators in Japan, China, USA, UK, South Korea and Slovenia. Through this program, Italian start-ups have the opportunity to meet international counterparts potentially interested in financial or technological collaborations and partnerships.

world. ITA pays continuous attention to the evolution of this domain (including Fintech and blockchain) in international markets and in specific sub-sectors; it organized and participated in events in the USA and UK and is planning promotional actions in the most developed countries when it comes to IT security.

**Promotional initiatives include participation at major international events, invitation of foreign**

**delegations to Italy at specialized fairs and forums, and organization of workshops, seminars and B2B initiatives in specific markets** on particular topics identified by the ITA's Innovation Desks in London, Los Angeles, Mumbai, Singapore, Moscow and Paris. ITA regularly involves Italian Universities, accelerators and incubators in selecting Italian start-ups with innovative cybersecurity software and hardware solutions.



# Research and Innovation



The Italian strategy on cybersecurity considers **research a pillar for a reliable cyberspace**. Universities, research centres, innovative start-ups and other Italian players involved in the development of cybersecurity technologies interact with public institutions and private companies to **ensure the development of resilient capabilities** and let Italy take a primary role as an attractive and competitive player in cybersecurity.



Established in 1989 under the supervision of the Ministry for Education, University and Research, **CINI (National Interuniversity Consortium for Informatics)** is a consortium of Italian universities that involves 1,300+ professors of both Computer Science and Computer Engineering from 45 public universities. It also supports joint research activities with universities, institutes of higher education, research institutions, industries, and public administrations. Finally, CINI facilitates access and participation in R&D projects, scientific activities, and technology transfer.





The **Cybersecurity National Laboratory** is the primary lab in the CINI network. The Lab is composed of **53 major Italian universities and research institutions** that include more than 500 professors and researchers.

The Lab works towards the creation of a cybersecurity technical workforce, the selection and training of cybersecurity talent and other aspects that may improve domestic resilience to cyber-attacks. The Lab is also actively involved in large research projects tackling different aspects of the cybersecurity domain, such as setting up **federated cyber ranges** (virtual environments used for cyberwarfare training and cyber technology development); establishing a **network of Regional Centers**; and developing **tools for evaluating cyber readiness** of firms and public administrations.

Together with Confindustria, the Cybersecurity Lab is currently designing **specific curricula to meet market needs and tackle the problem of skill shortage through initiatives such as the CyberChallenge**. Finally, the Lab organizes **ITASEC**, the Italian conference on cybersecurity.




## **CYBER-ALPHABETIZATION. THE EXPERIENCE OF *CYBERCHALLENGE.IT*: ETHICAL HACKING FOR YOUNG TALENT**

---

In order to grow the cyber-defender community, Italy is investing in young talent and stimulating their interest in cybersecurity issues. A **gamification-oriented approach** is used to complement the more traditional training activities, which simulate real cyber-security scenarios in which participants are called upon to solve cyber challenges, defend compromised services or attack opponents.

## Research & Innovation



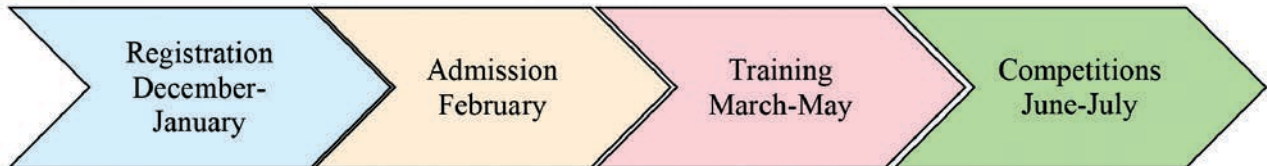
The CINI Cybersecurity National Laboratory set up the *CyberChallenge.IT* project, which offers a **free training course** and the possibility to become a member of the **Italian national cyber-defender team**, which takes part in international competitions, such as the European Cybersecurity Challenge (ECSC) organized by ENISA.

The first edition of CyberChallenge.IT was organized in **2017** by the Sapienza University in Rome and gathered the interest of **683 students and young professionals** from all over Italy. In **2019** there were **3203 registrations, of which 42% from high schools**.

Young people aged between 16 and 23 go through an

admission test used to select candidates with good reasoning skills and a strong problem-solving attitude; **no previous knowledge in cybersecurity is assumed**. The three-month training is offered in different universities scattered along the peninsula, and provides technical, scientific and ethical preparation on cybersecurity issues, including cryptography, binary exploitation and web security.

In July of each year, teams from all participating universities compete in a national attack/defence contest. Performance in the final competition is the base for selecting the **members of the national team for international competitions**.



## The White Book

In 2018, the Cybersecurity National Lab published the **White Book on “The Future of Cybersecurity in Italy: Strategic project areas”**, which aims at presenting the main cybersecurity challenges that Italy has to face and outlines a set of focus areas and actions that the Italian research community considers essential to implement Italy’s<sup>1</sup> and the EU<sup>2</sup> regulations on this subject. The White Book’s main suggestion is **that raising the country’s level of security and resilience** requires increasing the level of security and resilience of each of the components of the overall framework, and in this context it proposes a set of recommendations for the policy-makers in charge of dealing with the challenge of digital transformation at the national level. Policies must necessarily be dynamic and must evolve constantly in parallel to technological, regulatory, social, and geopolitical changes.



<sup>1</sup> Presidency of the Council of Ministers, *The Italian Cybersecurity Action Plan*, 2017

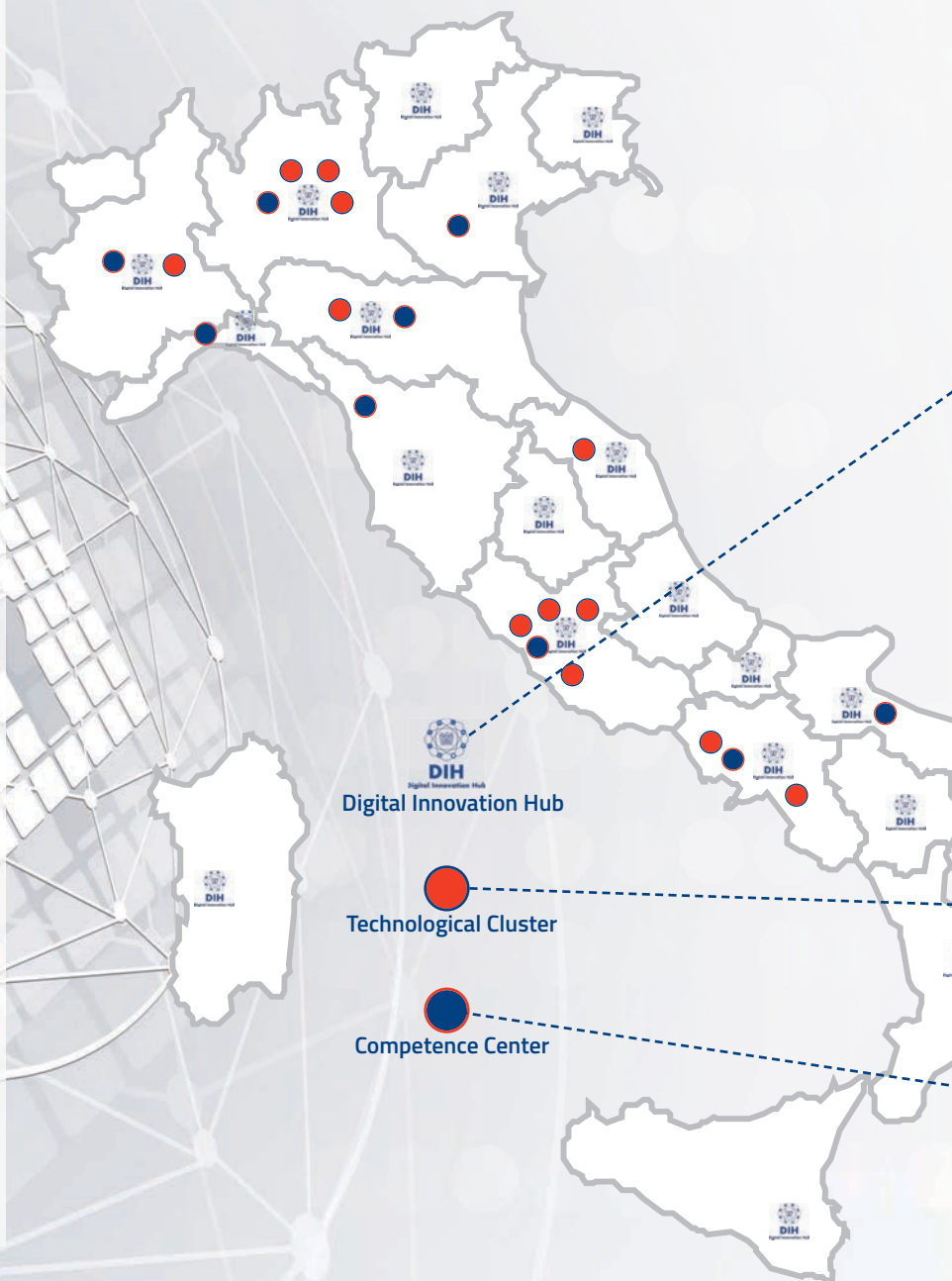
<sup>2</sup> European Commission Digital Single Market, *The EU directive on Security of Network and Information Systems*, 2016

## THE ITALIAN INNOVATION NETWORK

Italy has equipped itself with an efficient and functional innovation ecosystem in order to create and manage an **integrated research program** on the main technological drivers and to develop services and applications for businesses, institutions and citizens.

The Italian innovation network aims at seizing and exploiting the opportunities offered by digitization and to ensure the country's medium- and long-term competitiveness.

In order to support investments in digitization, the system integrates public and private subjects' networks, which are functional and complementary, so as to experiment and test digital innovations for the market: **Competence Centers (CC), Digital Innovation Hubs (DIH) and National Technological Clusters (TC).**





## Digital Innovation Hub

In line with the European strategy on industrial digitization, the Government promotes the **Digital Innovation Hub (DIH)** network at the regional level as a gateway for companies to access digital transformation. Its purpose is to set up competence centers, technology experts, suppliers, end-users of technological solutions and investors to **support the access of enterprises to the EU market. DIHs are the contact point among companies, research institutions and both public and private investors at regional level.**

## National Technology Clusters

To boost innovation processes and increase Country's industrial competitiveness through a more effective integration between national and regional policies on research and innovation, Italy has promoted the development of **12 National Technology Clusters**. The clusters are formed by companies, universities, research institutions, technology districts, start-up incubators and other stakeholders in the field of innovation.

In the framework of the National Smart Strategy, according to EU guidelines, **each Cluster is focused on a specific technology field:** aerospace, agrifood, green chemistry, intelligent factory, transport, life sciences, technologies for living environments, technologies for smart communities, cultural heritage, design, creativity and Made in Italy, sea economy and energy. The aim of each Cluster is to develop "technology roadmaps" to meet, **through specific industrial strategies, the challenges raised by** worldwide socio-economic changes. Clusters represent structural collaboration platforms for enterprises and R&D entities that help enhance research and technology transfer to the business system.

## Competence Centers


**The Competence Centers (CCs)** are public-private partnership centres, **vertically specialized in the technological fields of industry 4.0** to facilitate technology transfer to Italian companies. The centers offer training and support activities in the implementation of innovative projects, industrial research and experimental development of new technologically advanced products and services.

Two of these Competence Centers are focused on wide-ranging cybersecurity:

**Cyber 4.0, the Competence Center of central Italy**, is dedicated to data security and focused on solutions for the strategic sectors of **automotive, space and healthcare. Start 4.0 is the Competence Center for Security and Optimization of Strategic Infrastructures, based in Genoa.**

This CC focuses on enabling technological application of Industry 4.0 (IoT, blockchain, big data) in the field of security (security, safety and cyber), on the application domains of **infrastructures for transport (including ports), energy and water and production systems.**

# Economic trends



**It is estimated that by 2023 there will be over 30 billion connected devices, of which around 20 billion will be related to the IoT.**

*Source: Ericsson Mobility Report, 2017*

**The EU data market value is expected to exceed 79,5 billion euros by 2020**

*Source: The European Data Market Monitoring Tool*

**Global investments in blockchain will reach over 9.7 billion euro in 2021**

*Source: IDC, 2018*

**The global cybersecurity market value is expected to exceed 172,5 billion euro by 2021**

*Source: IMAP, 2018*

## WORLD MEGATRENDS ON CYBERSECURITY

**Innovation is the most powerful driver to develop the world economy.** New technologies, platforms, automation and networks are the enablers of the digital economy that, combined with

the potential offered by the "Internet economy" and Data and Internet of Things (IoT), allow the development of new business models that increase firms' competitiveness and foster countries' growth, improving government services and international cooperation.

The quick and continuous integration between the virtual and physical worlds in which people, objects and devices are increasingly connected, will bring **clear advantages for business but will also make them more vulnerable to cyber attacks.**



**The global cybersecurity market size** (security-related hardware, software, and services) is expected to grow from over 137 billion USD of investments in 2015 **to more than 248 billion by 2023**

*Source: statista, 2019*

**The cost of cybercrime worldwide** is expected to exceed **6 trillion USD annually by 2021**, up from 3 trillion USD in 2015

*Source: Cybersecurity Ventures, 2019*

## *Economic trends*



Every day 6.4 billion fake emails are sent worldwide. Furthermore, almost 2 billion records containing personal and other sensitive data were compromised between January 2017 and March 2018 (Ernst & Young, 2018-2019)

Implementing effective cybersecurity measures is particularly difficult today since **cybercriminals are becoming more experienced in their attacks**. The **number of cybercrimes and targeted attacks are rising rapidly, leading to a considerable growth in demand for services and security solutions.**

Nevertheless, cybersecurity can also be an opportunity. There will be **1.5 million cybersecurity job openings by 2019**, and by 2025 the demand for cybersecurity professionals will increase to approximately 6 million globally.<sup>1</sup>

---

<sup>1</sup> Bure Valley Group, 2019





From 2017 to date, Italian companies **producing cybersecurity solutions** have increased by over 300%, from 700 units to over 2,800 and a four-time growth was also detected in the **number of employees, which increased from 5,600 to 23,300 units** (Unioncamere-InfoCamere, 2019).

## NATIONAL TALENTS

The Italian cybersecurity industrial landscape is very rich and it consists of companies specialized in a full range of products and services. The supply chain sees the coexistence of big firms, medium and small ones and start-ups that provide **pioneering and forward-looking solutions, technologies and services in the wide domain of cybersecurity, for both the defence and civilian sectors.**

The change of perspective on cybersecurity - no longer only considered a cost, but also a competitive factor for

companies - has contributed to enlarging and customizing the supply of products and services in this sector. Today it is possible to **identify areas of business where Italy offers state-of-the-art and innovative solutions for cyber problems.** In Italy, the market of solutions for information security accounted for more than **1 billion euro in 2018, while spending on cybersecurity increased by 13.3%<sup>2</sup> in the same year.**

<sup>2</sup> Anitec-Assinform, 2018

The **production value of the Italian cybersecurity supply chain** was almost 2 billion euro in 2017, with a growth of 10.6% compared to achievements of the same companies in 2015. Lombardy is the leading region, with a share of 42.5% of the total (835 million euro), followed by Lazio (307 million euro) and Emilia-Romagna (233 million euro).<sup>3</sup>

Italian **companies** are, on the

<sup>3</sup> Unioncamere-InfoCamere, 2019

## *Economic trends*



On the one hand, the first **to use** sophisticated solutions of cyber protection. On the other hand, they are **producers and exporters** of advanced technologies that position Italy among the most important players in the world cyber market. Critical sectors like utilities, energy, transport, oil & gas, finance and health, are becoming progressively digitized and our firms are developing expertise to protect their infrastructures from cyber-attacks, guaranteeing thereby the continuity of essential services. Our companies are specialized in solutions to

protect mobile and IoT applications, based on encryption, blockchain, biometric, and quantum technologies.

Italy, undoubtedly, has a **significant number of leading cyber companies with high expertise in software development, software integration and cyber threat intelligence solutions**, the new predictive paradigm based on Machine Learning and Artificial Intelligence technologies to enforce the cyber resilience of the ICT systems.

**The Defence industry sector is one of the most important**



Social media users in Italy are 34 million people, 59% of the whole population, while internet users are more than 54 million (92% of the population) (Data Report, Digital 2019).

**in which Italian companies have developed in-house technologies in the past few years** to cope with new threats and cyberwarfare challenges. To give an example, one of our main defence industries has collaborated since 2012 with the NATO Communication and Information Agency (NCIA) to protect NATO's communication infrastructures from cyber attacks and provide a **rapid-response cyber defence capability to more than 70,000 NATO users** around the world.

Regarding the

**Telecommunications industry**, government efforts and company investments have helped create a strategic, attractive and secure business ecosystem. This is particularly important since Italy is the **fourth-largest market for both ICT and telecommunications equipment and services in the European Union**<sup>4</sup>. Italy is also one of the largest and most advanced mobile communication markets in Europe.<sup>5</sup> Smartphone users in Italy have grown to 41.55 million in 2018 (around 2/3 of

<sup>4</sup> ITU, 2019

<sup>5</sup> R&S Mediobanca, 2019

the Italian population) and this number is expected to rise to almost 48 million by 2024<sup>6</sup>.

In the field of **Fintech**, as more and more end-users resort to online solutions for their daily financial transactions, cybercrimes grow proportionately. Consequently, a growing number of large, medium and small companies and startups focus on information security for the fintech service chain, **providing solutions to prevent hacker actions, anticipate possible data**

<sup>6</sup> Statista, 2019

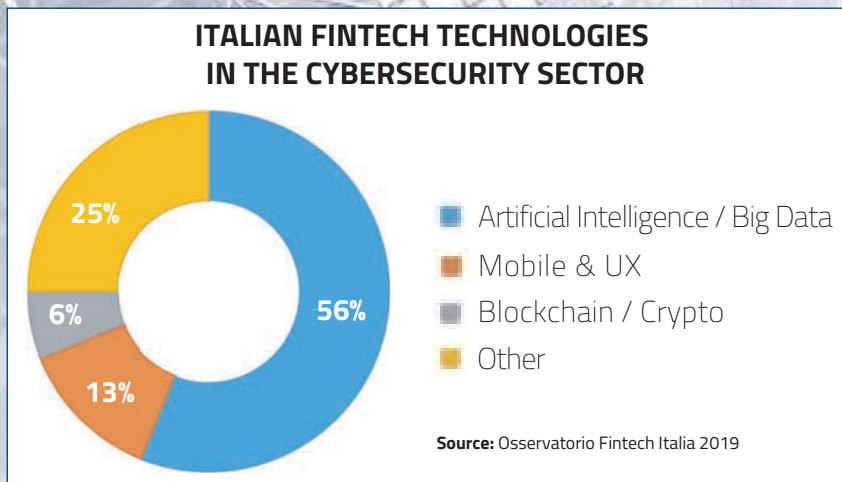
## Economic trends

breaches, intercept attacks and prepare appropriate reactions. Large Italian banks and innovative fintech start-ups offer services focused in particular on **Anti-fraud, Mobile Security, Web**

**Security, Endpoint Security, Infrastructure Security and Cryptography**<sup>7</sup>.

The **Energy sector** is actively working to respond to the need to **protect critical Italian infrastructures** from possible interferences caused by state and non-state actors to guarantee the continuity of electricity and oil and gas delivery. Companies have therefore adopted best practices to guide and manage cybersecurity activities<sup>8</sup>, embedded security measures throughout the design and

Fig. 3 Italian Fintech technology in the cybersecurity sector



<sup>7</sup> Pwc, 2019

<sup>8</sup> [www.agendadigitale.eu](http://www.agendadigitale.eu)



Fig. 4 Main Italian cybersecurity solutions

Cybersecurity Areas	Main technologies provided
Application Security	Software - Platforms
DDoS Protection	Security services in Cloud
End Point Detection	Software
End Point Protection	Software - security in Cloud
IoT Security	Managed Security Services con SOC - Security services in Cloud - Platforms
Messaging Security	Appliances - Software - security services in Cloud
Mobile Security	Software - Platforms
Risk & Compliance	Cybersecurity Consulting - Software
Security Consulting	Cybersecurity Consulting
Security Professional Services	System Integrator - Software
Security Operation Center	Managed Security Services with SOC - security services in Cloud - Platforms
Threat Intelligence	Software - Platforms
Transaction Security - Fraud	Software
Vulnerability Assessment	Software - Security services in Cloud
Web Security	Security services in Cloud

development of applications, processes and services, and created cyber emergency readiness teams, which intervene in case of cyber incidents<sup>9</sup>.

The Italian Cybersecurity network has developed, in particular, resilient know-how and strong capabilities to be able to promptly respond with customized solutions to

the different needs expressed by end-users of every dimension and sector, through a flexible and strong supply chain. Italian firms increasingly perceive **cybersecurity as a core business requirement**. In fact, in 2018, 88% of Italian companies dedicated a specific budget to cybersecurity (increasing from 58% in the previous year).

<sup>9</sup> World Economic Forum, 2019

**September 2019 issue.**

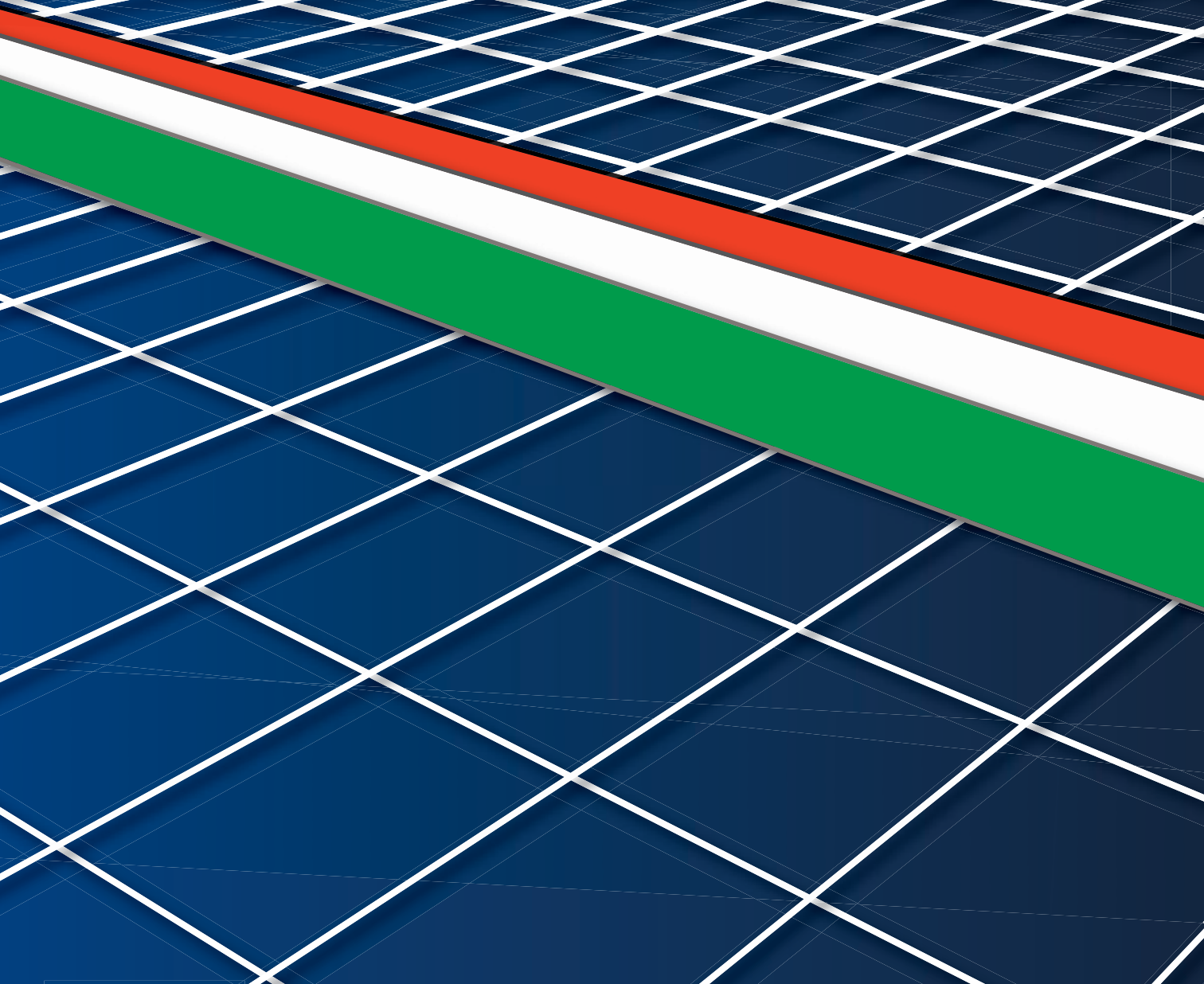
Written by Presidency of the Council of Ministers (Sistema di Informazione per la Sicurezza della Repubblica), Ministry of Foreign Affairs and International Cooperation, Italian Trade Agency, Confindustria and National Interuniversity Consortium for Informatics - CINI.

Edited by Andrea Mazzella, Chiara Ratzenberger, Giacomo Mennuni and Giada Castellan, International promotion of the aerospace, defense and cyber security industries, Directorate General for Economic Promotion and Innovation, Ministry of Foreign Affairs and International Cooperation.

PROGETTAZIONE GRAFICA E IMPAGINAZIONE  
Loretana Alivernini

STAMPA E CONFEZIONE  
**SOLARIGRAFICHE**  
info@solarigrafiche.com





PRESIDENZA DEL CONSIGLIO DEI MINISTRI



SISTEMA DI INFORMAZIONE  
PER LA SICUREZZA DELLA REPUBBLICA



Ministry of Foreign Affairs  
and International Cooperation



ITALIAN TRADE AGENCY



CONFINDUSTRIA



consorzio  
interuniversitario  
nazionale  
per l'informatica