cini
Cybersecurity National Lab

The future of Cybersecurity in Italy: Strategic focus areas

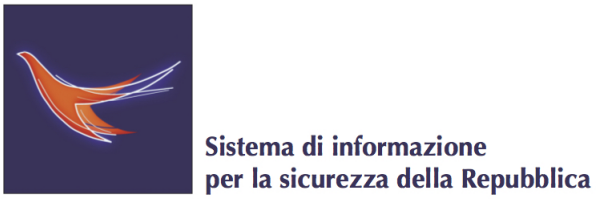
Projects and Actions to better defend our country from cyber attacks

Laboratorio Nazionale di Cybersecurity
CINI - Consorzio Interuniversitario Nazionale per l'Informatica

Edited by:
Roberto Baldoni, Sapienza Università di Roma
Rocco De Nicola, IMT School for Advanced Studies, Lucca
Paolo Prinetto, Politecnico di Torino

The volume has been produced by:

With the support of:



In collaboration with:

ISBN 9788894137347

Title: The future of Cybersecurity in Italy: Strategic focus areas

Translated from “Il futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici”, January 2018 – ISBN 9788894137330

Printed in Italy, May 2018

Last update: June 20th, 2018

Contents

Preface

At the end of 2015, the CINI Cybersecurity National Laboratory produced a White Paper [1] to present the main cybersecurity challenges that Italy had to face in the next five years. The volume focused mainly on the risks arising from cyber attacks and outlined a number of recommendations, including organisational ones.

The present volume is a continuation of the previous one, with the aim of outlining a set of *focus areas* and *actions* that the Italian research community considers essential to complement and support those foreseen in the executive decree on cybersecurity issued on February 2017, known as DPCM Gentiloni, by the Italian government. Reading the volume does not require any particular technical skills; the text is accessible to anybody who knows how to use a computer or surf the net.

The volume considers different aspects of cybersecurity, including: (i) the definition of infrastructures and centres necessary to organise defence; (ii) the actions and technologies to be developed to improve protection; (iii) the identification of the main technologies to defend; (iv) the proposal of a set of horizontal actions for training, awareness raising, and risk management.

The focus areas and the action, which we hope will be developed in the next few years in Italy, are complemented by a set of recommendations for the policy makers, in charge of dealing with the challenge of digital transformation at the country level. The recommendations are not intended to be exhaustive; they focus on issues that we consider essential for the correct implementation of a national cybersecurity policy. A policy that, by nature, must necessarily be dynamic and constantly evolving according to technological, regulatory, social, and geopolitical changes.

Inside the volume, the reader will find boxes with a violet or grey background; the former ones are used in the introductory chapter and in the conclusions to highlight some concepts considered important; the latter ones are used in other chapters to explain the meaning of some technical terms commonly used by professionals.

In conclusion, we would like to thank all the colleagues who have contributed to this volume: a group of over 120 researchers from about 40 research institutions and universities, unique in terms of number and excellence, representing the best of Italian research in the field of cybersecurity. Special thanks go to Gabriella Caramagno and Angela Miola who have contributed to all the phases of production of the book and to Sara Olson for her help in the translation from the Italian version. Finally, we would like to acknowledge the support from the FILIERASICURA project.

Finally, we would like to point out that our editorial work required a significant rephrasing of the texts provided by colleagues; this reworking may have partially misinterpreted their message or ignored some important aspects: we apologise in advance.

Roberto Baldoni
Rocco De Nicola
Paolo Prinetto

Rome, January 15th, 2018

CHAPTER

1 Role and Impact of Cybersecurity

Cybersecurity is the second emergency in Europe, after climate change and before immigration. The President of the European Commission, Jean-Claude Junker, pointed it out in his State of the Union address of 13 September 2017. In fact, for several years now, Chancelleries all over the world have put cybersecurity at the top of their agendas. The blocking of business operations, the surreptitious control of critical infrastructure services, the theft of intellectual property or information crucial to the survival of a company are examples of the major threats a country faces. The recent malware campaigns *wannacry* and *notpetya* were the visible events of an impressive series of attacks in every corner of the planet.

> *The **cyberspace** is the most complex thing that man has ever built: on one side, the union of thousands of networks that make it difficult to even have a snapshot of who is connected to it; on the other, the stratification of software programs and protocols developed in the last forty years. This complexity generates vulnerabilities (software errors, incorrect configurations and weaknesses in protocols) that are exploited by cyber criminals to steal data or cause damage.*

In an increasingly digitalised world, cyber attacks are alarming populations, causing huge damage to the economy, and endangering the lives of citizens when they affect distribution networks for essential services such as healthcare, energy, transport, i.e., critical infrastructures of modern society. Just imagine what might happen if all the traffic lights of a metropolis were suddenly turned off, if the elevators were stopped, and if the ambulances could no longer receive the right address to reach the injured. In addition, a successful cyber attack could also represent the point of no return for a company's credibility, the

development of its business and its ability to competitively sell products. A successful cyber attack could also destabilise the stock market by plunging entire countries into chaos, or block gas supplies in winter or the municipal waste collection system; the resulting political scenario would be tragic.

The damage caused by cyber attacks often depends on an identifiable weak link. The weak link of cybersecurity is the *human factor*. Man is now an integral part of cyberspace and therefore the human factor is the most important and unpredictable vulnerability of this macrosystem. One wrong click can in fact destroy any technological line of defence of a single apparatus, an organisation, or a country. It is people who are "fished" in a *phishing* campaign, who use the name of their cat or wife as their password, who access the company network with the same smartphone their children have played with. These people are the first to open the doors for criminals to their organisation's sites, networks and databases, with dangerous and unpredictable effects.

Before the advent of cyberspace, the world was based on information printed on paper or stored on isolated computers and placed in well-defined physical perimeters. This world had developed very precise threat models, allowing national, corporate and individual security, and protection policies to be defined with sufficient clarity and detail. In cyberspace, however, threats are constantly changing and many remain unknown for months or years before they emerge. We therefore have to define security policies in a world where information on the threat is highly incomplete.

When you are immersed in the cyberspace, looking at it from only one point of view signifies not truly being able to deal with the threat; vulnerabilities are potentially hidden in hardware, firmware, application software, in addition to organisational processes, contracts, and laws.

> *A country that does not put cybersecurity at the heart of its digital transformation policies is a country that puts its economic prosperity and independence at serious risk.*

In Italy, entire sectors of excellence, such as the mechanic and the shipbuilding industries, the made-in-Italy brand, tourism, agri-food commerce, and transport could suffer heavy downsizing of turnover due to attacks in the cyberspace by sovereign states or competitors.

Beyond industry, attacks can also be waged against democracy. *Fake news* is the evolution of attacks based on *social engineering*: created and disseminated through the cyberspace, false information tends to confuse and destabilise the citizens of a country by plunging them into an uncontrolled information space, with an almost endless set of sources of news.

We must therefore be ready to monitor, as citizens, businesses and public administrations (PA), our digital world. This monitoring must become our way of life, just as the advent of cars has made it natural to look left and right before

crossing a busy road. Keeping our devices under control, updating their software, and knowing our possible vulnerabilities are all actions that must be part of an endless monitoring process and continuous IT risk management.

The processes of monitoring and control cannot be uncoordinated, nor can they be isolated from each other. They must be linked and coordinated through multidimensional actions involving all the actors in play: public, private, research. Awareness raising, training, communication, a *common cyber language*, certification, and the use of *best practices* are just some of the cross-cutting aspects of this complex coordination.

In this context, the executive decree published in February 2017 and known as DPCM Gentiloni[1] comes into play in the area of cybersecurity. The text provides a strategic and operational national reference point where the public and the private sectors, both military and civil, from large organisations to citizens, can work in a coordinated way.

Coordination also allows for the development of projects aimed at guaranteeing the capabilities necessary for improving the country's response and resilience to cyber attacks. The executive decree offers an articulated and multidimensional range of actions, initiatives, and cutting-edge centres, such as the *Cyber Security Centre (NSC)*, the *National Centre for Research and Development in Cybersecurity*, the *National Laboratory for Encryption*, the *National Cyber Range*, and the *Centre for Evaluation and Certification*. They are all pieces of a complex mosaic that must be composed to support a *national cyber policy*. It is thus important that the executive decree be translated as soon as possible into concrete actions and that the necessary resources be made available in multiannual programmes, which, as will be seen in chapter 8, other countries have already started a long time ago.

The new white book This volume was created with the aim of outlining a set of *project areas* and *transversal actions* that the national research community considers essential to complement and support those foreseen in the February 2017 executive decree.

Areas and actions typically contain various *operational projects* aimed at both the public and private sectors. Each presentation includes motivations, a brief state of the art, and a set of challenges and objectives to be addressed. In this regard, it is assumed that a set of projects will be set up in order to provide adequate and sustainable responses to each of the challenges and to achieve the objectives.

The different project areas have been grouped into five operational areas:

[1] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf`

- *Infrastructures and Centres* — In this area, the tools and actions necessary to secure the national internet network and data centres of the PA are considered; in addition, some types of competence centres are presented to be activated on the national territory in order to strengthen the defences of the country.
- *Enabling actions* — In this area, actions necessary to make the threat management cycle safer are considered: from the protection of critical national applications to the creation of a national threat repository, from defence against different attacks (cybernetic, social, physical) to forensic analysis, from system-wide risk management to active protection.
- *Enabling Technologies* — In this area, the design areas aim to strengthen some of the basic technologies to be used to protect data, to limit attacks and their effects and, in general, to increase the resilience of systems, mostly resorting to the *security by design* paradigm. In particular, the area deals with hardware architectures to guarantee higher levels of security, encryption, blockchain, biometric, and quantum technologies.
- *Technologies to Protect* — This area presents the tools and actions needed to protect some key technologies, such as wireless communications, cloud services, functional system logic and, in the perspective of *Industry 4.0*, IoT, industrial control systems, and robots.
- *Horizontal Actions* — This area includes the tools and actions necessary to ensure the protection of personal data, to raise the level of knowledge and competence through training, awareness and certification projects and to improve risk management at the company level.

After the presentation of the project ideas, the volume analyses their impact on some of the cornerstones of digital transformation, highlighting how democracy, finance, industry, tourism, and culture can benefit from a national cybersecurity policy.

A chapter of the volume is then devoted to the presentation of the policies and actions undertaken by some key nations in European and international contexts.

The final chapter presents a number of recommendations which, if followed, will allow the country to properly respond to the challenge of digital transformation. While not exhaustive, these recommendations focus on aspects considered essential for a correct implementation of a cybersecurity policy at the national level.

Necessary Synergies The implementation of projects, given the diversity of the objectives and involved skills, will require a particular synergy between the

world of research, government and industry, leveraging the appropriate mechanisms of public-private partnerships as well. In particular:

- The role of research in this context is basically linked to the study of new solutions for each identified challenge. To complement theoretical results, it is necessary to create prototype systems aimed at a more rapid industrialisation of solutions.
- Companies will play a fundamental role in the subsequent prototyping and industrialisation within an integrated system of all the proposed solutions. The relationship between research and industry must be *circular*, in the sense that the definition of problems tackled must be shared; innovative approaches defined on the basis of scenarios and requirements should be identified collaboratively; solutions developed, modified, and refined on the basis of industrial experiences *in the field*. All of this will enable us to achieve a timely and effective technology transfer.
- On the government side, we expect a definition of the necessary regulatory frameworks and the implementation of appropriate financing programs.

1.1 Impact of cyber attacks in Italy

Finance Ministers and central bank governors of the G7 countries, at the end of the Bari meeting in May 2017, stressed the need to have statistically sound and public databases on cyber attacks: how many, who carried out the attack, whom and what they hit, the cost of the damage [2]:

> We acknowledge that *cyber* accidents are a growing threat to our economies, and *policy* responses are needed that involve the entire production system, ... based on reliable, impartial, comprehensive and widely accessible data. ... Definitions, methodologies for data collection and sharing should, where appropriate, be coordinated and consistent across countries and sectors, so that results be comparable.

Despite the fact that mass media periodically provide estimates of such data, these estimates are almost never based on scientific collection methods. There are some exceptions. In the United Kingdom the government led a sample survey covering the whole private sector: it shows that a little less than half

[2] `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf`

of all British companies were victims of at least one attack attempt in last year[3]. In Italy, the Bank of Italy estimated that between September 2015 and September 2016, 45% of national companies were hit by some type of attack. The most risky subjects are large companies, exporters, and operators working in a sector with high-end technological intensity. In this regard, Table 1.1, taken from [16], reports the percentages of Italian companies in the private non-financial industry and services sector, with at least 20 employees, affected by one or more cyber attacks between September 2015 and September 2016.

Table 1.1: Attacks suffered by Italian companies, September 2015 – 2016

Geographic area	
North-West	44.2
North-East	47.3
Centre	52.3
South and Islands	35.9
Number of employees	
20 – 49	42.7
50 – 199	48.4
200 – 499	56.0
500 or more	62.8
Technology intensity	
High and medium-high	48.8
Low and medium-low	43.8
Effect of exports on turnover	
Less than 1/3	43.0
Between 1/3 and 2/3	51.8
More than 2/3	48.5
Percentage on total number of companies	**45.2**

In the same target universe, in 2016 the expenditure on IT security was modest: the median enterprise devoted only EUR 4 530 to attack prevention, i.e., 15% of the gross annual retribution of a typical employee [16]. There were important differences between sectors: the figure went as high as EUR 19 080 among ICT companies, to decreased to EUR 3 420 among low technology companies. Almost all companies claim to use at least one anti-virus software, and two thirds of employees are trained in the safe use of information technology; less diffused is instead the practice of data encryption, performed by less than a third of non-ICT companies.

[3] `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/609186Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf`

Regarding damages caused by attacks, both British and Italian data show that in most cases the direct economic impact is limited; in Italy, the costs of repairing the affected systems and lost earnings resulting from the interruption of activities exceed EUR 50 000 in only one instance out of one hundred cases. The distribution of costs is highly asymmetric: on the one hand, the average dimension of the phenomenon is more limited than what has been reported from commercial sources, on the other hand few major accidents appear to be responsible for a very large proportion of the overall economic damage. Measuring the so-called *tail* phenomena poses methodology challenges; detection methods and models should be developed to accurately quantify the cost of the most serious attacks.

It is also necessary to take into account the fact that the economic impact of an attack is often not limited to the cost it imposes on the direct victim. In some cases, for example when an infrastructure is affected, the extent is also clear to non-specialists. In other cases, however, awareness is limited to specialists. In particular, not all seem to have understood the extent to which the techniques of indirect attacks are spread and leverage the vulnerabilities of a subject in order to affect another. In this regard, see the two cases described below.

1. *Indirect attacks involving Italian companies* [80] — A company in the city of Cuneo that produces pet food, with international customers, suffered the theft of a list of customers and information about their supply relationship. Cyber criminals then contacted customers to notify a change in the IBAN of the Piedmontese society; the plausibility of the communication was linked to the fact that to the e-mail an invoice with exact supply amounts was attached. Of the four companies contacted, all Asian, three credited the amounts requested to the IBANs indicated for a total of USD 200 000. Just one company, suspicious of the fact that the IBAN was not linked to an Italian bank, called the company in Cuneo to double-check, making it so aware of the fraud that took place.

2. *Identity theft*[4] — A company from Turin in 2013 received an e-mail from one of its (long-standing) Chinese suppliers, which communicated that the company had changed banks. Without any further verifications, the company paid to the would-be supplier about USD 60 000. Subsequent investigations identified a Nigerian citizen as the guilty party, who had managed to steal data from the Chinese company's email account. Fraudsters escaped any control by depositing the stolen money into a Thai account, from which the money was subsequently withdrawn in cash from an ATM.

[4] "So I steal your identity on the web'", la Repubblica, 24/11/2014, (A. Longo).

In many countries, including Italy, it is not clear who is responsible in cases like this, except in events linked to personal data protection, payment services and a few other economic activities. The possible reimbursements due from vulnerable subjects to third party victims can be established only at the end of long, complex and expensive legal proceedings. Therefore, many companies, which are not particularly attractive to attackers and do not operate within a regulated framework, are less motivated to protect themselves. The presence of thousands of weak rings in the value chain affects the security of the cyberspace as a whole and sets the conditions for the proliferation of accidents on a large scale, almost always conducted with indirect attack techniques (*targeted attack*).

Vulnerability – Weaknesses present in a software or hardware element of a system that can be exploited by an attacker to conduct an attack against the system itself.

Threat – Threats to the assets of a *target* entity which, based on malicious software agents (*threat agent*) and exploiting the vulnerabilities of the target, are able to penetrate its computer system and/or network.

Targeted Attack – Targeted and deliberate attacks against a defined target, be it an individual, an enterprise or a system.

There is a particular risk of weakening the competitiveness of small and medium size enterprises. They clearly see the economic advantages of digitisation, while they do not seem to fully understand the risks that the new instruments entail. As highlighted in sections 6.2 and 6.3, it is particularly important that appropriate *cyber-hygiene* practices are developed in these companies, i.e., behavioural habits which, at a very low cost, may nullify the most common attack attempts. It is also essential that they acquire at least a minimum awareness of their own vulnerabilities and of the operational modes typical of attackers.

Analysing the accidents reported in 2016, it is possible to provide a taxonomy of the main trends, see fig. 1.1 (resulting from the analysis of reports by ENISA[5,6,7] - apologies for some Italian text in the Table). This taxonomy is useful to both policy makers and potential victims.

[5] `https://www.enisa.europa.eu/publications/etl2015`

[6] `https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016`

[7] `https://www.enisa.europa.eu/publications/ce2016-after-action-report`

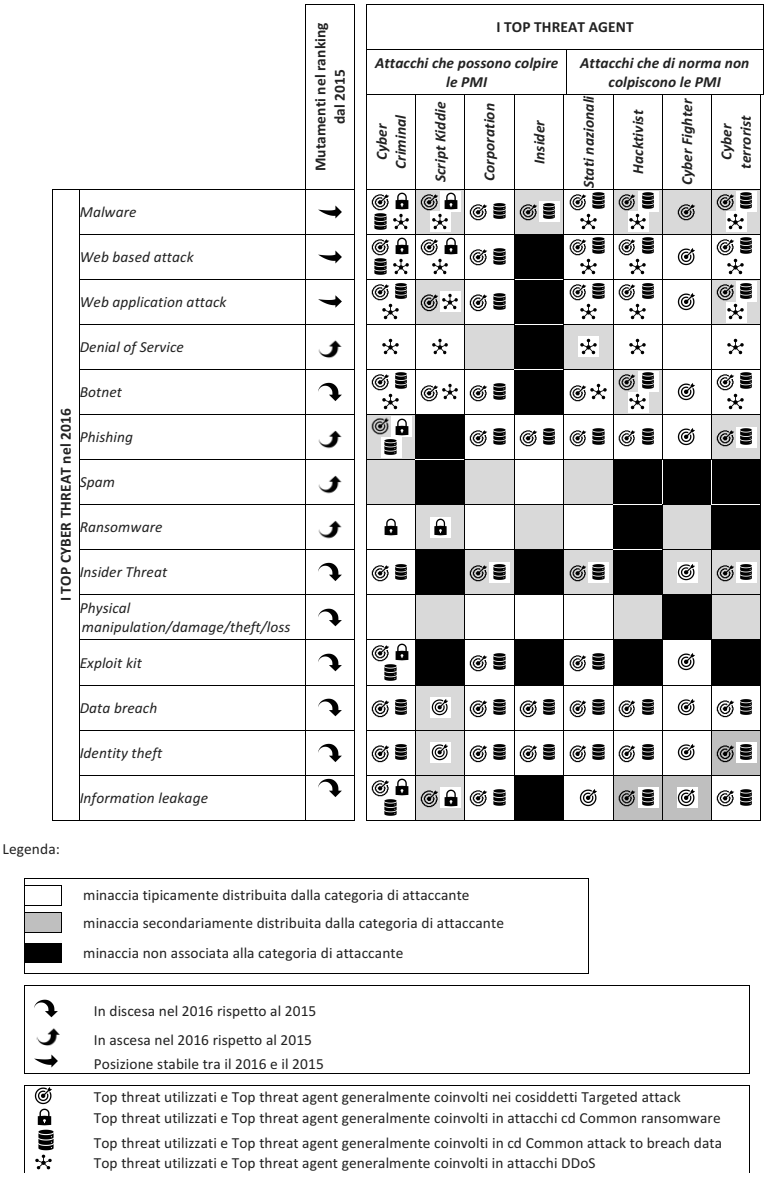


Figure 1.1: Threat Agent, Attack Vector and Threat: trends based on accidents reported in 2016

1.2 European legislation

A recommendation, two communications, a proposal for a regulation and a proposal for a directive: these are the legal instruments with which the European Commission, together with the High Representative, has updated and strengthened its cybersecurity strategy. Some of these instruments are immediately operational, others will become operational as soon as they are adopted following the initiated legislative procedure[8].

The initiative, announced by President Juncker in his speech on the "State of the Union", has a clear objective: to increase the resilience of the European Union (EU) against cyber attacks and to create an effective deterrent to protect the emerging cybersecurity single market with concrete actions, thus contributing to the construction of a solid and coordinated institutional structure at a European and a national level. This is based on:

- a European Agency already in operation, the *European Union Agency for Network and Information Security* (ENISA)[9], whose mandate will be made permanent and which is given new tasks and resources to take on a more operational role directly in support of the European Commission and Member States;

- a framework of rules for an EU security certification of ICT products, systems, and services, based on international standards on a voluntary basis;

- the *Blueprint*, i.e., principles and mechanisms, in terms of objectives and methods of cooperation, to respond in a coordinated way to large-scale cyber incidents and crises;

- the proposal to create a European network and a centre of research and expertise on cybersecurity.

To be added to this list is the proposal for a directive to combat fraud and counterfeiting by non-cash means of payment (credit and debit cards) in order to provide a more effective enforcement and criminal law response. This initiative is focused on the detection, tracking and repression of cyber criminals involved in activities that mostly have a transnational dimension, such as terrorism and drug and human trafficking. The proposal also aims at defining actions for a joint EU diplomatic response to harmful cyber activities and measures to strengthen international cooperation on cybersecurity.

[8] `https://ec.europa.eu/commission/state-union-2017_it`

[9] `https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014/`

The broad scope of the initiative is shown in particular by the contents of the communication devoted to the NIS Directive (see section 1.2.1) and its transposition, which includes a document full of operational indications. The Commission's concern, already expressed in its communication of 2016, is clear: as the NIS Directive is the cornerstone of the European strategy on cybersecurity, its implementation by the Member States must be based on a harmonised approach, aimed at avoiding misalignments and fragmentation that could compromise the efforts deployed thus far.

Hence, a series of concrete indications which constitute a kind of operational manual for the Member States in view of the deadlines of 9 May and 9 November 2018, for the transposition of the Directive and the designation of operators of essential services, respectively.

First, Member States need to have a national cybersecurity strategy at their disposal, aimed at defining both appropriate policy and regulatory objectives and actions on the basis of a holistic and coordinated approach.

Another important aspect, to which the Commission's document devotes particular attention, is the identification of the persons to whom the rules of the Directive apply. While Member States do not have to indicate digital service providers, the designation of operators of essential services is a complex and sensitive exercise. The Directive, in this respect, merely sets out the criteria to be applied at the national level, in the hope that this will happen everywhere in a consistent manner and that, where an operator provides services in different Member States, there will be an agreement between them to regulate their identification under the Directive. Regulatory approaches should not vary from country to country. Moreover, Member States have the possibility to extend the scope of the Directive and thus apply its rules (in terms of security requirements and notification requirements) to sectors not directly covered by the Directive as well, such as the PA (where these are essential services), the postal sector, the food sector, the chemical and nuclear industry, the environment and civil protection.

1.2.1 NIS Directive

The NIS Directive – *Network and Information Security*[10] on network and information system security is the first set of European security rules approved by the EU. The Directive, which was adopted on 6 July 2016 and entered into force in August 2016, deals mainly with three essential aspects: (i) strengthening cybersecurity management capacities in each EU Member State; (ii) increasing the level of cooperation between EU Member States; (iii) strengthening cybersecurity risk management and incident reporting strategies.

[10] `http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&rid=1`

The main objective of the Directive is to achieve a high common high level of network and information security in all EU Member States and to achieve greater cooperation between them to facilitate the information sharing on risks, with particular reference to the management of cybersecurity incidents and related risks. In particular, it applies to providers of "essential services" operating in critical sectors and to digital service providers and requires operators to take measures for the management of cyber risks and the timely, albeit not temporally quantified, reporting of security incidents.

The Directive must be transposed into national law by May 2018, and each Member State must identify the operators of essential services by November 2018.

More specifically, the NIS Directive sets out a number of network and information security requirements that apply to essential service operators and providers of digital services – DSP[11]. With the aim of establishing a security culture in sectors vital to the EU economy, these entities shall take appropriate security measures and report serious accidents to the competent national authority. Providers of essential services operate in the following sectors: energy, transport, banking and financial services, health, water, and digital infrastructures. Digital service providers include online markets, cloud services, and search engines[12].

One of the essential features of the NIS Directive is to build a solid foundation for forming a European framework for network and information security: it arises from the need for each Member State to secure its infrastructures and ensure their operation in accordance with common rules and requirements. To achieve this, each country must therefore align its security methods, approaches, and practices. This will prevent European companies from operating within a fragmented environment and will facilitate and improve their efforts to comply with these rules.

Finally, the Directive requires the designation at a national level of an IT security authority and of a national *Computer Security Incident Response Team* (CSIRT) for the management of cyber risks and notifications in case of major incidents involving the critical infrastructures of each Member State[13].

Essential and digital service providers are obliged to notify such events to the competent authorities without undue delay and such notification must include information to allow the determination of the severity of incidents and their possible impact[14].

[11] `https://www.enisa.europa.eu/publications/nis-directive-and-national-csirts`

[12] `http://europa.eu/rapid/press-release_IP-15-6270_it.htm`

[13] `https://clusit.it/wp-content/uploads/2017/02/direttiva_nis.pdf`

[14] `http://community.forumpa.it/system/files/file_upload/Direttiva%20NIS%20-%20allegato%201.pdf`

1.2.2 The GDPR legislation

On 27 April 2016, the EU adopted the EU Regulation 2016/679 on data protection, known as the *General Data Protection Regulation* (GDPR), applicable from 25 May 2018 and intended to replace the 1995 Data Protection Directive. Its main purpose is to reform, update and modernise European data protection legislation so as to make it more robust and coherent. Directly applicable without the need for any transposing legislation, it will have a significant impact on each Member State and on the rules in force at the national level. The GDPR is presented in detail in section 6.1.1.

1.2.3 The cPPP in cybersecurity

As part of the Digital Single Market Strategy, the European Commission set up a *contractual Public-Private Partnership* (cPPP) on cybersecurity, with the main objective of strengthening the EU cybersecurity industry and stimulating the European cybersecurity sector. This aim is pursued through several actions:

- bringing together industrial and public resources to improve European industrial policy on cybersecurity, focusing on innovation and following a jointly agreed strategic research and innovative path;
- promoting trust between Member States and industrial actors by fostering bottom-up cooperation in research and innovation;
- helping stimulate the cybersecurity industry by aligning offer and demand of products and services, enabling the industry to efficiently address the future needs of end users;
- using the Horizon 2020 funding to maximise the impact of available sector funds through better coordination and focus on some technical priorities;
- improving the visibility of European excellence in R&D in cybersecurity and the protection of digital personal data.

The public part of the cPPP is represented by the European Commission, while the private part by the Belgian law association *European Cyber Security Organization* (ECSO)[15], which currently has about 220 members.

The establishment of the cPPP has enabled the increase in the budget available in the remaining part of Horizon 2020 from EUR 200 million to EUR 450 million. A similar increase seems to be possible for the next framework programme.

[15] `www.ecs-ppp.eu`

The vastness and complexity of the problems related to cybersecurity require cooperation between subjects that, even if with distinct roles, operate in this sector, which is so strategic for the security and economy of the EU and Italy. There is no doubt that for a more effective management of the whole matter it is necessary to develop every possible synergy that facilitates such integrations. In this context, hence, the ECSO represents a strategic element of the utmost importance.

1.3 Italian legal framework

The entry into force of the NIS directive and GDPR - as well as the by now boundless potential extent of the damage that a cyber attack can cause - have imposed, at the Italian level, a revision of the so-called Monti's decree of 24 January 2013 (hereinafter *DPCM Monti*)[16] This Prime Minister's decree, together with the *National Strategic Framework for Cyberspace Security*[17] and the *National Plan for Cyberspace Protection and ICT Security* of 2013[18], essentially constituted the Italian national strategy for cybersecurity.

This section examines both the new Prime Minister's decree of 17 February 2017 (also called in Italian *DPCM Gentiloni*)[19], which replaces Monti's decree providing guidelines for cyberspace protection and ICT security, and the update of the *National Plan*, also published in 2017[20].

1.3.1 Prime Minister Paolo Gentiloni's Decree (February 2017)

The first Prime Minister's decree outlining a national cybersecurity architecture was the one adopted by Mario Monti in 2013. Monti's decree was extremely important because it came at a time when reaction activities against cyber threats were marginal and unstructured. However, the decree introduced a cumbersome crisis management, due to the high number of interactions among various public actors – among them, different departments of the Presidency of the Council of Ministers, several Ministries and the AgID (Agency for Digital Italy) –

[16] http://www.gazzettaufficiale.it/eli/id/2013/03/19/13A02504/sg

[17] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf

[18] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf

[19] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf

[20] https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf

which were hardly prone to be coordinated in short timeframes, as required by wide-ranging crises, thus slowing reactivity.

The revision of the Prime Minister's decree was therefore driven, on the one hand, by the need to reduce complexity and, on the other, by the necessity to prepare for the transposition of the NIS Directive. This Directive aims at systematising the various competences involved in crisis management.

Therefore, Gentiloni's decree is aimed to optimize crisis management and centralise responsibilities. This is achieved by strengthening the role of the *Security Intelligence Department* (DIS); the Italian Secret Services - as national cybersecurity governance holder. DIS hosts the *National Cybersecurity Board - Nucleo di sicurezza cibernetica* - (NSC), an interagency and intergovernmental cybersecurity operational body, chaired by one of the DIS Deputy General Directors.

The NSC is composed of representatives from the Interministerial Committee for the Security of the Republic (CISR)[21] Administrations, the Intelligence Community (DIS, AISE, and AISI), the Department of Civil Protection (to manage the kinetic effects of a cyber event) and AgID, as well as the Prime Minister's Military Advisor. In case of a national cyber crisis, the Board is also integrated with representatives from the Ministry of Health, the Ministry of Infrastructures and Transports, and the Fire Department. NSC competences on cyber crisis prevention, preparation and management, strengthened DIS role, posing it at the core of the national cybersecurity architecture, as shown in fig. 1.2.

CERT – Computer Emergency Response Team – Official bodies responsible for providing assistance on risk prevention and incident response, whose priority tasks are::

- taking charge of requests for assistance in case of security incidents (attacks) on networks and information systems;
- processing of alerts and responding to cyber attacks: developing technical analysis, exchanging information with other CERTs, contributing to technical studies;
- creating and maintaining vulnerability databases;
- disseminating best practices on risks reduction measures;
- coordinating with other entities: operators and Internet service providers, and international CERTs.

This is reflected in the Italian transposition law of the NIS Directive, which foresees that a "single point of contact" will be established within the DIS in or-

[21] Ministry of Internal Affairs, Ministry of Justice, Ministry of Defense, Ministry of Internal Affairs, Ministry of Economic Development, Ministry of Economy, Ministry of International Affairs, Intelligence System.

der to facilitate cross-border cooperation and communication at EU level. The law also foresees the establishment of an Italian CSIRT that will take up the duties of the National CERT and of the Public Administration CERT.

The Prime Minister's decree also introduces a *National Evaluation and Certification Centre - Centro Nazionale di Valutazione e Certificazione* - (CVCN) to be set up at the Ministry of Economic Development (MISE), to evaluate the security of products and devices to be deployed within national critical infrastructures.

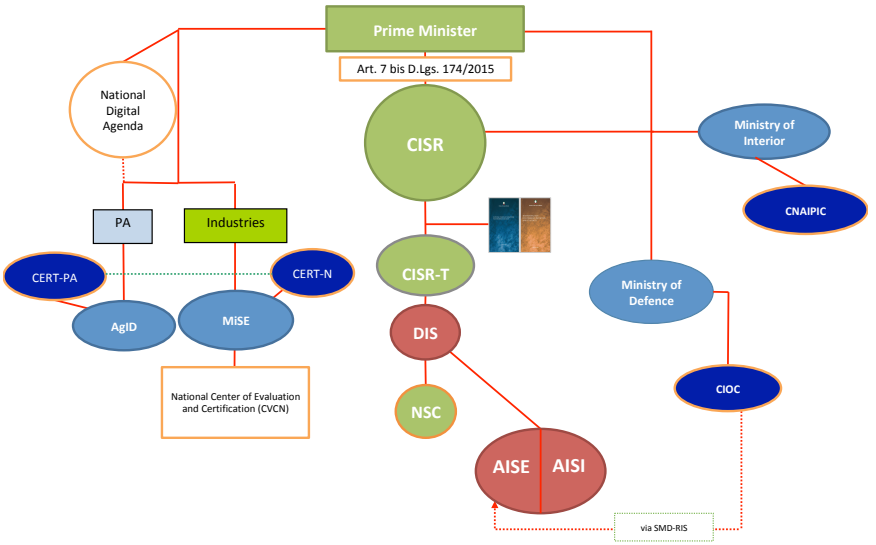


Figure 1.2: National architecture for cybersecurity as provided by Paolo Gentiloni's executive decree (2017)

1.3.2 National Plan for Cyberspace Protection and ICT Security

The new *National Plan for cyber protection and information security*[22] ((hereinafter referred to as the National Plan) implements the Gentiloni's decree and aims to update and simplify national cyber crisis management and reaction procedures. In this regard, the National Plan states the following:

[22] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf`

> The need to allow a rapid and effective qualitative leap of the national cyber architecture has made it necessary to identify an essential nucleus of priority initiatives, selected on the basis of the needs that have informed the activity of revision of the National Strategic Framework and National Plan and taking into consideration the evolving national and international legal requirements.

The awareness that cyber threats and risks cannot be addressed through a bureaucratic and slow decision-making process is at the basis of the abovementioned initiatives. An *action plan* was therefore created with the aim of making the national cybersecurity architecture more effective and efficient; the box below summarises the main actions.

Action Plan – from executive decree by Gentiloni

- Revision of the National Cyber Security Management Board (NSC)
- Shortening of the chain of command for cyber crisis management
- Optimisation of the national cybersecurity architecture, through the suppression/merger of bodies
- Progressive unification of CERT-N and CERT-PA
- Establishment of a National Evaluation and Certification Centre at the Ministry of Economic Development
- Creation of a Foundation or a Venture Capital Fund
- Establishment of a National Centre for Research and Development on Cybersecurity
- Institution of a National Cryptography Centre.

This action plan aims to increase both cyberspace protection through the implementation of appropriate security policies and to streamline decision-making in the event of a cyber crisis. Both operational lines call for developing organizational, procedural and technical tools. These include: the certification of ICT devises, the development of a public-private partnership through forms of venture capital funding, the launching of *National Centre for Research and Development in Cybersecurity* and of a *National Cryptography Centre*.

In addition, the National Plan aims at stimulating a further qualitative leap in terms of cooperation capabilities between public actors and private sector operators. The detailed list of the eleven operational guidelines of the National Plan is reported in the next box.

Operational guidelines of the Italian National Plan

1. Strengthening intelligence, police, civil protection, and military defence capabilities
2. Enhancing organisational preparedness of, coordination and dialogue between private and public stakeholders
3. Promoting cybersecurity culture, education and training
4. Enhancing international cooperation and organising cyber exercises at National level
5. Strengthening the readiness of national bodies competent for incident prevention, response and remediation
6. Updating the legislation according to technological developments and ensuring compliance with international obligations
7. Granting compliance with standard security requirements and protocols
8. Supporting industrial and technological development
9. Fostering effective strategic and operational communication
10. Ensuring rationalisation of financial resources
11. Implementing a national system of Cyber Risk Management.

1.3.3 National Cybersecurity Management Board - Nucleo per la Sicurezza Cibernetica - (NSC)

According to Gentiloni's decree, the Cybersecurity Management Board (NSC) is responsible for preventing, preparing for a national cyber crisis, for declaring such a crisis, as well as for coordinating the response and recovery activities carried out by competent administrations in compliance with Prime Minister's decisions.

The NSC, through the DIS Director General, keeps the Prime Minister constantly informed on crisis developments. The Prime Minister is supported by the Inter-ministerial Committee for the Security of the Republic (CISR), which is responsible for providing guidance in case of national security crisis.

The Unit ensures all the necessary contacts, for crisis management, with cybersecurity entities of other States, the NATO, the EU, and other international organisations.

The Board can declare a situation of cyber crisis whenever a cyber event, for its dimension, intensity or nature cannot be dealt with by the single Administration concerned but it requires a coordinated approach, which is ensured by the NSC.

The Board is supported by an "Early warning and Cyber Incident Response Unit", to operate 24/7, that receives information related to relevant cyber events

for prevention and reaction initiatives, as well as any information useful for a cyber situational awareness. This information currently come from:

- National CERT together with the Public Administration CERT: they get alert respectively from private operators, the European Union and national CERTs, and from Central and Local Public Administrations;
- National Cybercrime Centre for Critical Infrastructures Protection (CNAIPIC): other than Interpol and Europol, it gets alerts from national critical infrastructures;
- Defence CERT: it receives information about cyber events from the NATO Computer Incident Response Capability (N-CIRC);
- Intelligence Community.

1.4 Protection of Italy's assets

The cyber threat has in fact created a time-space collapse that has essentially destroyed the threat management models as conceived so far. The enemy can be anywhere, at no more than a hundred milliseconds away from you; a single enemy, with even only an average cyber capability, can simultaneously attack thousands of a country's strategic assets. This is why we need a new way of interpreting national security, which should also consider the cyber protection of the country by an operational coordination plan that must be flexible, adaptable and have a very short chain of command, i.e., fast in the response. Although it can be improved in some respects, the above mentioned points are all qualities found in the executive decree by Gentiloni.

Figure 1.3 represents the overall picture of the public and private assets of Italy: from the Ministries constituting the CISR, from critical infrastructures to the industrial system, and finally to the citizens. Raising the country's level of security and resilience necessarily requires an increase in the level of security and resilience of each of the components of the overall framework. The closer you are to the middle of the picture, the more you need to increase response coordination and speed. The sector with inadequate defences becomes, in fact, the weak link of the entire country system. The levels of security are peculiar to the specific asset. While, for example, citizens are required to maintain an adequate form of cyber-hygiene, the CISR is required to have an extremely sophisticated and articulated security infrastructure with rapid response times.

It is advisable to immediately highlight how, in order to minimise the consequences of an attack, a sequence of operations must be activated in the shortest possible time by the NSC and by its operational players (see fig. **??**) as stated in the National Plan. These actions include, for example, the detection by the target asset of the ongoing attack, the notification of the attack to the NSC, the

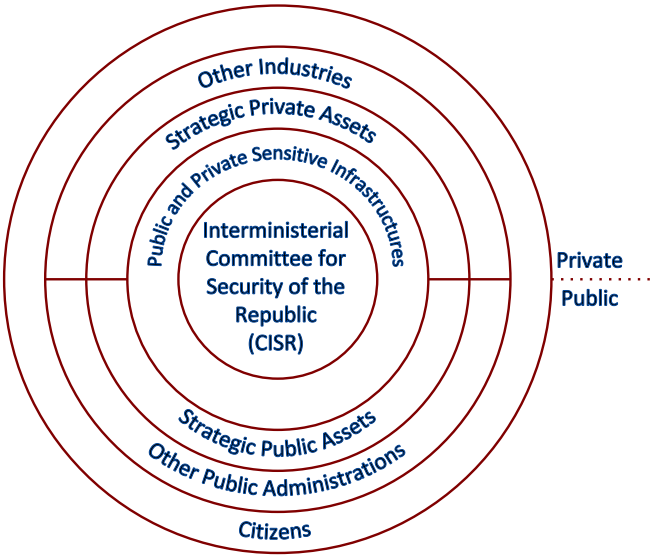


Figure 1.3: Overview of public and private Italian assets

assessment done of the threat entity, the identification of potentially attacked assets and actions to be taken, their communication by the NSC to the assets involved, and the application of appropriate countermeasures by these assets.

To deal with the threat caused by the collapse of the cyberspace, it is necessary to reduce the transit times of relevant information from any point in fig. 1.3 to the point where it can be handled appropriately, bringing to the heart of the system only those events that threaten national security in terms of the economic, political and scientific interests of the country. A sort of nervous system of the Italian platform overlying the assets shown in fig. 1.3. This nervous system is formed by the constituencies of NSC operational players and by the *Centres of Competence* dealt with in section 2.3.

In general, the operational projects within the various focus areas presented in this volume are aimed, in their entirety, at raising the level of security and/or the resilience of one or more national assets.

1.5 Deterrence in cyberspace

Deterrence plays an important role in the preparation of cybersecurity tools. It aims to curb an attacker by making him think about the cost of his attack and

is characterised by two components: the *defence* and the *counter-attack*[23]. The first tends to raise the level of defence of a system with the aim of increasing the cost of the attack disproportionately, in order to make it unprofitable. The second serves to "scare" the attacker, who must be sure that his attack will trigger an answer (retaliation) capable of inflicting a punishment on him that is greater than what he himself considers acceptable.

Deterrence – Prevention of an action through a credible threat of retaliation with consequences of unacceptable size to the attacker and/or through operations that lead to the belief that the cost of the action exceeds the perceived benefits.

The component of the *counter-attack* in the deterrence concept worked well in the nuclear context as the punishment the attacker would suffer could be catastrophic for him. Furthermore, the investment in nuclear weapons is such that only a few countries are able to possess them and the attribution of an attack becomes a relatively simple matter. This has led to the establishment of international treaties on the non-proliferation of nuclear weapons.

Nuclear power is very different from cyberspace, where cyberspace weapons can potentially be in anybody's hands, copied and spread throughout every part of the planet in just a few hundred milliseconds. In addition, in the cyberspace, an individual can launch a huge number of attacks and the attribution of responsibilities is a very complex and error-prone process thanks to the possibilities of anonymity that the network offers. These characteristics make it difficult to set up cyber weapon non-proliferation treaties. Finally, even if an attack can be attributed, the damage that could be inflicted with a cyber counter-attack would not be as catastrophic as a nuclear counter-attack and the attacker could accept to take the risk.

As a result, to date *defence* represents the only possible deterrent in the cyber world. The project areas and actions presented in the following chapters are a way to raise the level of cybersecurity (the defences) of the country and therefore act as an implicit deterrent to a cyberspace, where attacks are already an endemic factor.

[23] `https://www.hsdl.org/?view&did=798700`

CHAPTER

2 Centres and Infrastructures

To make Italy more resilient to cyber attack campaigns, a robust national cyberspace must be developed. This can by done by strengthening the national internet service and consolidating PA data centres to reduce the attack surface area and secure both data and applications of national interest. In addition, the country's defence capacities must be developed by creating a network of cybersecurity centres, distributed throughout the country and, in some cases, specialised in specific market sectors. The centres must range from R&D to competence and support centres for industrial sectors, from information analysis centres to CERTs. These centres must be equipped with an adequate critical mass in terms of resources and staff, with appropriate professional profiles. Finally, centres pursuing similar goals should be networked and their operations orchestrated in order to amplify their resilience effect on the country as a whole.

2.1 Italian Internet

We are now so used to having easy access to the internet that the lack of connectivity represents a major inconvenience in living our daily life. This makes the internet an indispensable asset for social life and for most of the country's strategic activities, characterising it as an indispensable service of public utility and as a critical infrastructure, on a par with distribution networks for electricity, water, and so forth.

The internet is a great network, indeed, an immense network and being able to have a complete map of it is very difficult if not impossible, due to the completely decentralised and highly dynamic nature that characterises its growth, as well as to the multiplicity and heterogeneity of the technological solutions

and parties involved. This makes it extremely hard to define a security perimeter and, consequently, to identify protection strategies and the points for their implementation.

To understand the reason behind the above statement and to assess its consequences, it is necessary to understand how the internet is structured and how it has evolved over time. The components that constitute the network are the so-called *Internet Service Providers* (e.g., TIM, France Telecom, Unidata, Deutsche Telekom, Fastweb, Interoute, Tiscali) hereinafter called ISPs. The links constituting the meshes of the net are links between ISPs (e.g., a link could exist between Fastweb and Interoute or between TIM and France Telecom). For economic, technical, and logistical reasons, these links are constantly changing over time. In addition, the existence of each link is known, in principle, only to the two parties who implement it. Some of these connections are made in places designed to be meeting points (IXP - *Internet eXchange Point*) between ISPs, while others are set up in places known only to stakeholders.

The presence of the myriad of connections set up as described above, using the most disparate transmissive technologies (fibre optic, radio, satellite, etc.), ensures that the internet is extraordinarily effective in adapting to faults and failures and to the geomorphological characteristics of the sites. On the other hand, the internet's fully distributed nature and the lack of a global vision of the network expose it to attacks which bring about two types of adverse effects: the fraudulent diversion of traffic, in order to analyse it without the need for direct access to equipment or terminal lines (with an obvious impact on the confidentiality and/or integrity of data), and the disruption of critical services (*Denial of Service*) for significant time periods. The asymmetric nature of the threat, the complexity of the infrastructures involved and the porosity of the security perimeter make it essential to strengthen the defence, containment, and response capabilities of the system.

2.1.1 State of the art

The protocol used for routing traffic between internet ISPs is the *Border Gateway Protocol* (BGP)[1]. Within the scope of monitoring methodologies, the collection of the traffic routes defined by BGP is a key and enabling tool for improving knowledge of the structure of the internet. At present, among the few BGP data sources available on connectivity among the approximately 60,000 ISP internet components are the *Route Views* project at the University of Oregon [2] and the RIPE-NCC project[3]. The routing data made public by these projects are, how-

[1] https://tools.ietf.org/html/rfc4271

[2] http://www.routeviews.org/

[3] https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris

ever, partial (as they mostly represent the point of view of large ISPs) and incomplete, both in terms of the internet as a whole and in terms of the specific features of the Italian internet infrastructure.

Considerations of this kind lead various organisations to carry out continuous monitoring of the internet and to equip themselves with increasingly sophisticated analysis instruments, including tools for predictive analysis. For example, in the USA the CAIDA (Center for Applied Internet Data Analysis) [4], which is largely funded by the DHS and the NSF, continuously monitors the internet with tools ranging from routing traffic control to the analysis of suspicious signals picked up by the network, with systems that recall the ones adopted in radar signals analysis. In Europe, the RIPE-NCC provides a wide range of services to the community, ranging from data on reachability of some points in the network to data on the actual use of IP addresses.

2.1.2 Challenges

Unfortunately, there are no services that allow for the following actions to be carried out at a national level:

- Continuous surveillance of particular portions of the internet considered to be critical (e.g., related to energy, transport, transport, financial services, information) in order to promptly detect early preparatory experiments for targeted or large-scale malicious attacks;
- Highlighting internet traffic routing anomalies which may be caused by operations aimed at information theft;
- Checking the status of key points in the network, such as IXPs or the *landing stations* of the major intercontinental traffic routes;
- Detecting, in real time, actions aimed at preventing large sections of the population from using the internet.

The realisation of services such as those mentioned above requires addressing numerous research challenges, encompassing both methodological and technological-application issues.

First of all, there is a scale problem due to the impossibility, or extreme difficulty, in implementing traffic inspection and filtering controls and policies at a central level (and therefore on a limited number of strategic points of the network), as a result of the traffic volumes involved and the technological limits of the current security enforcement equipment (NG firewall, Intrusion & anomaly detector, etc.) with respect to transmission technologies. In other words, if on

[4] http://www.caida.org/home/

the one hand it would be perhaps effective (although in many ways highly questionable) to introduce control points on trans-frontier links, limiting the size of the intervention perimeter, the technologies used on such links (to the state-of-the-art multiples of 100 Gbps, soon tera-speed connections), which by their very nature are intended to support large volumes of traffic, make both an online (and wire-speed) deep payload inspection of the packets transmitted and any selective blocking/filtering of those packets unfeasible. In practice, at the state-of-the-art there is at least one order of magnitude difference between the processing capacity of security equipment and the forwarding capacity of transmission equipment. The same applies to IXPs. This implies the need to shift the focus of security, and therefore the control and intervention points, towards the periphery of the network, typically on the distribution component, and therefore in greater proximity to the resources to be protected. This essentially introduces three needs:

- to multiply the number of security monitoring and management devices, with more *pulverisation* of the resulting architectures;
- to provide for the coordination of these systems with a view to implementing defence and containment strategies and policies that are both unitary and effective, and based on a sufficiently large scale;
- to introduce algorithmic intelligence and advanced analysis capabilities in monitoring, detection of anomalies and threat containment activities, in order to overcome the current technological limits through a better vision and understanding of phenomena, through the adoption of a *situation awareness* logic.

Phishing – Internet fraud in which the attacker tries to deceive the victim by inducing him/her to provide personal information, such as access credentials, bank account and credit cards details. It is typically done by sending e-mails, which may be more or less targeted, that imitate the graphics and settings of banking or postal sites with which you are required to provide your personal data.

2.1.3 Objectives

It is important to develop a holistic, coordinated and multi-dimensional approach to protecting the internet infrastructure at a national level. This approach must also be characterised by a unity of intent among the actors involved and must be able to automatically (or at least semi-automatically) detect, contain and, where possible, prevent attacks in a timely manner, making it possible to identify their real origins, facilitating backward tracking and the identification of their responsibilities.

Spear Phishing – A particular type of phishing carried out by sending fraudulent e-mails to a specific organisation or person. The purpose of these attacks is typically to gain access to confidential financial information or to industrial, state, or military secrets.

Three major design objectives are identified and described below, to be achieved over a period of three to five years:

- *Collection of the BGP routing of Italian ISPs* — In order to eliminate polarisation problems and due to the lack of BGP routing information, it is necessary to increase the number of routing collection points, involving small and medium ISPs - which make up the leaf nodes on the internet - in the process as much as possible. This is to outline the BGP peering ecosystem by creating a complete description of the Italian internet network from the BGP point of view. Achieving this goal means, therefore, having reliable data to which algorithms can be applied for the correlation and extraction of reliable and securely usable information.

  To achieve this objective, a number of actions must be taken gradually. The first step would involve building an architecture expressly aimed at collecting the Italian ISPs' BGP routes. At a later stage, it will be necessary to set up a collection system on a statistical basis of the traffic exchanged between ISPs, in order to get a clear and accurate picture of the Italian BGP ecosystem, including peering data, and therefore of the paths actually covered by traffic among Italian ISPs.

  Having acquired a solid knowledge of the Italian internet infrastructure and the paths covered by the traffic that runs on it, it makes sense, in the first place, to implement a monitoring and alerting system for the most critical Italian targets. The alerts generated by this system must be collected, analysed in real time, and correlated with each other in appropriate traffic control/monitoring centres able to reliably detect attacks such as hijacks, route flaps, and hostile traffic routes and, consequently, to apply threat mitigation and containment strategies. The BGP protocol could still be used to implement deflection mechanisms by providing for *blackholing* or cleaning and re-injection of affected traffic flows into the network.

- *Monitoring of traffic insisting on DNS* — In order to improve the stability and security of the Italian internet infrastructure, with modalities related to those described in the previous point, we need to monitor and collect the traffic that insists on DNS, with the intent to detect *phishing campaigns* and identify the traffic that can be traced back to botnets and DDoS attacks. In Italy, a similar project has been started by the .it Registry

of the Istituto di Informatica e Telematica of the CNR of Pisa, while, at the European level, by the Dutch ccTLD organisation.

- *Information Correlation* — Methodologies and tools already available on the market, based on data mining and machine learning techniques, should be enhanced in order to enable the extracting information of various kinds from the many available data sources. This information should include traffic routing data, data from active measurement networks, data from passive readings, data related to DNS operation and background activities on unused address areas (internet radiation), and data on traffic flows. In addition, the proposed solutions should make it possible to target anomalies in specific areas of the internet and/or specific traffic routes. Getting such in-depth data could involve, for example, placing targeted active measurement devices in strategic points.

2.2 National Network of Data Centres

European public administrations are investing a large amount of resources to digitalise all of their processes and services. In doing so, they are facing disparate and sometimes antithetical challenges. In fact, governments need to invest a significant proportion of taxpayers' money to consolidate and expand their service portfolio, but, at the same time, their budgets are increasingly tighter. In order to strike a true balance between these requirements, it is imperative to provide services based on new technologies and on their effective and efficient use.

> **Data Center Consolidation** – The use of technologies, methodologies and strategies to make IT infrastructures more efficient. In general, the objective is to reduce the footprint of one or more data centres, streamlining the use of hardware resources in order to reduce operating costs and the chances of successful cyber attacks.

Very often, however, the framework of the actual technological assets in use is quite different. The reality is that the IT infrastructures available to many governmental organisations are outdated and, in many cases, fragmented between several local departments. In these instances, the technical staff in charge of infrastructure management do not have access to an appropriate training program to acquire the expertise needed to use next-generation technologies, and there appears to be a lack of development projects in line with the latest technological and methodological innovations. In some cases, it is therefore difficult to implement policies aimed at standardising the systems and applications used in different territorial departments, a situation that often prevents even a mere reliable census of the applications or the versions/setups in use.

Similar considerations apply to the data acquired, processed, and stored in the current IT systems of many government organisations. There is actually a high degree of heterogeneity in the organisation and management of data, with twofold consequences: on the one hand, it is difficult to make applications used by different organisations interact and exchange data and, on the other hand, the confidentiality and security of critical data are at risk from a procedural and legal point of view.

A major challenge faced by the public sector, both at the national and European level, is therefore to undertake a process of digitisation aimed at the creation of a national network of data centres based on cutting-edge information technology and methodologies. This process of infrastructure *consolidation* will enable more consistent services, in which it will be easier to implement effective management/evolution and security policies, thanks to the reduction of surfaces and possibilities of attack from the outside, while at the same time allowing government organisations to implement interoperability processes that are of real benefit to citizens. This consolidation process will furthermore significantly reduce public spending.

Consolidation is already recognised as a key aspect for the modernisation of public administrations. The *Three-Year Plan for Informatics in Public Administration 2017–2019*, created by the AgID and by the Digital Transformation Team[5,6], coordinates a group of activities whose investment amounts to about EUR 4.6 billion. In this plan, processes to consolidate the hardware and software infrastructure are seen as one of the tools to reduce, earlier than expected, the annual expenditure related to ICT infrastructure in the PA by at least 50%.

Consolidation is also a great opportunity to raise the quality standards of the national IT infrastructure, with significant impacts on many fronts. In the field of security, for example, moving applications to a confined environment through consolidation can allow for the implementation of effective access control policies and reduce the number of attack vectors and exposure to vulnerabilities. When implementing these measures aimed at increasing the level of security, care must be taken not to affect the responsiveness of applications and services and the quality of the end-user experience.

2.2.1 State of the art

Technical tools such as virtualisation, which currently forms the basis for the *Cloud Computing* paradigm and consolidation projects in a wide range of application fields, have been available since the 1960s [42]. They allow you to put into

[5] `https://pianotriennale-ict.italia.it/`

[6] `http://www.agid.gov.it/sites/default/files/documentazione/circolare_three-yearplan_24.6.2016._def.pdf`

operation, on the same physical machine, multiple "virtualised execution environments" in complete isolation, giving the impression that each application is running on a dedicated physical environment. This is a fast-growing practice, in the world of the PA as well, to the point where it can be estimated that by 2020 there will be a global increase of at least 16% in critical systems migrated to Cloud environments, with the aim, among others, to increase security levels [57].

Many of the major organisations providing services to large user bases are concentrating the commissioning of their respective applications on no more than 3-4 data centres, which in turn can be expanded. At the European level, by the end of 2013, Spain and the UK had shifted more than 40% of their PA infrastructure to virtualised IT systems[7]. According to the same estimates, in the same year, France had already begun a transformation process that demonstrated the migration to centralised virtualised systems at more than 30% complete, while Italy was only at 13%. However, Italy can aim for a reduction from more than 4,000 data centres to less than 100 in the coming years.

At the same time, implementing a consolidation project without knowing in detail which applications should be consolidated and why is a process destined to fail. It is estimated that in 2014 more than 30% of consolidation projects worldwide did not achieve their objectives [27].

In Italy, as part of the three-year plan, the AgID has set stringent targets for 2018. In particular, it is expected that it will be necessary to identify the minimum requirements for SaaS solutions for the PA to be deployed on the Cloud infrastructure by the end of the year. This infrastructure will be subject to a strategic study during the year to define its technical and organisational requirements. At the same time, public organisations with an infrastructure that is eligible to be shortlisted to become a "National Strategic Hub" will be identified, and a few of them will be selected to start a pilot project for testing the infrastructure and migration (or adaptation) of data centres.

2.2.2 Challenges

Consolidation projects for large scale applications and systems are difficult, complex, expensive and not immune to failure. Their success typically results from detailed and coordinated planning between key parties: network, application, infrastructure and human resource managers.

Technically, there are a number of false beliefs that often undermine the success of consolidation projects. An important aspect, in fact, is that consolidating towards an infrastructure that is constituted by the theoretical minimum

[7] IDC: "Business Strategy: Western Europe Government Sector IT Cloud Computing Trends", 2012-2013,2013.

of computational resources is not necessarily the optimal solution. Often, in fact, acting in this way does not leave room for future growth, or it could be discovered later that optimisation is not guaranteed, for example, by the number of software licenses needed to support the operation of services. At the same time, it is essential to identify the operating characteristics of the applications hosted, in order to determine which and how many of them can be consolidated on the same physical environment, while ensuring the non-interference of the respective performance indexes. This characterisation must be performed vertically, taking into account computational resources, storage space, bandwidth availability at the level of the network infrastructure, available hardware and the features of all middleware components that support the operation of a modern portfolio of software applications.

Similarly, it seems important to rationalise the range of software applications used by PAs, in order to support the development of certified software according to defined and integrated standards. To this end, Consip has already created guidelines [8] for the adoption of applications supplied according to the *Software as a Service* paradigm, which takes into account the current transitional situation in which the technical/organisational directives for a single market for the PA are still being defined.

When we talk about massive consolidation projects, it is critical to be able to take complete inventory of what is necessary to migrate to the new infrastructure, document the metrics of the use of services and performance, and estimate the usage and load growth trends. It is important to consider solutions that will limit the future expansion of the data center surface area from the outset, because such an expansion would entail critical security flaws. The "forward consolidation", i.e., the one that also takes into account future prospects, allows for substantial savings and a high profitability index of the invested capital, even many years after the conclusion of the consolidation plan.

2.2.3 Objectives

For the effective implementation of a multi-level national data centre network for the PA, taking into account all the strategic and methodological possibilities described above, several objectives need to be pursued:

- Carrying out a large-scale census of the physical infrastructures owned by the PAs and the most common middleware components used to support the provision of offered services[9]. In this regard, the AgID explicitly

[8] Consip: "Provisions for the Procurement of Services "Software as a Services" for the Cloud of Public Administration" October 10, 2017.

[9] `http://www.gazzettaufficiale.it/eli/id/2017/12/14/17A08400/sg`

clarifies[10] the need to carry out a census in order to produce statistical information regarding the main IT installations at a national, regional, and local level, to identify all the main hardware and software components and to provide data/ information useful for the rationalisation of infrastructures. It will thus be possible to outline a medium-term strategy to enhance and rationalise the information assets of PAs and to drastically reduce infrastructure costs, so that efforts to secure applications can be concentrated on a limited number of products.

- Developing new methodologies and techniques to assist experts in understanding the characteristics of the workload of applications that will have to be involved in a consolidation process, considering the infrastructure vertically, from physical hardware to virtualised hardware, up to the single application, including the various middleware components. This can be done on several fronts, using both more traditional modelling techniques, such as analytical or simulative, and techniques based on machine learning.

- Promoting the training of new generations of system engineers (including through the creation of ad hoc study tracks) who understand the workings of complex systems in a vertical way and are familiar with the characteristics of real systems (physical ones), who comprehend the support provided by Operating Systems for running applications in virtualised environments and modern software stacks that allow for services to be provided to PA users. This training path will allow public organisations to make use of the skills of the new generations to maintain the complex and critical infrastructure of a network of national data centres, whose implementation is essential to allow significant economic savings, provide increasingly higher security levels, and ensure responsiveness, high performance, and scalability towards ever increasing growth.

2.3 National, Territorial, and Vertical Competence Centres

This section presents all the structures deemed necessary to increase the resilience of companies, public organisations, and the country as a whole, in relation to cyber attacks. These structures will be the basis for the coordination work needed to strengthen Italy's cybersecurity. Specifically, three different types of centres should be created:

[10] `https://www.censimentoict.italia.it/it/latest/docs/circolari/2017113005.html`

- *National Centre for Research and Development in Cybersecurity* (CNRSC) — Its main tasks are advanced research, the development of architectures and applications, and various kinds of actions on a national scale;
- *Territorial Competence Centres in Cybersecurity* — Distributed throughout the territory, covering metropolitan, regional and interregional areas, they should mainly manage innovation in the cyber field and take care of technology transfer, training, consultancy, and support to local companies, local authorities, and citizens;
- *Vertical Competence Centres in Cybersecurity* — Each of them should focus on specific market sectors such as, for example, energy, transport, financial markets, etc.

Cyber Range – Virtual ranges dedicated to the training of security professionals, consisting in controlled environments and systems, typically based on virtualisation, that lend themselves to a wide variety of uses:

- Individual training and refresher courses on cybersecurity through practical exercises;
- Training and assessment of the skills of operators' teams through exercise;
- Design, development and testing of new cybersecurity tactics, techniques and procedures;
- Evaluation of the defence capabilities of a system.

Territorial and vertical centres can include one or more elements, such as *CERT*, *Cyber Range* (institutional, academic or specialist), cybercrime law enforcement structures, *Information Sharing and Analysis Organization* (ISAO), certification laboratories, and *Hardware Security and Trust* specialist laboratories (analysed in detail in section. 4.1). This would lead to the creation of specific networks of CERTs, ISAO, structures dedicated to countering cybercrime and dedicated and/or certification laboratories that should have, as their star point, the appropriate national body: the postal police for combatting cybercrime, intelligence agencies in the case of ISAOs, MISE in the case of certification laboratories, the unified CERT in the case of the CERT network, and the CNRSC for dedicated specialised laboratories.

In addition to the territorial support centres, it would be desirable if, following the example of the English, the French and the Germans (see chapter 8), a number of research centres of excellence, located throughout the national territory, were identified and financed, whose star point would be the National Centre for Research and Development in Cybersecurity. These centres should also focus on basic technologies essential for cybersecurity, such as artificial intelligence, machine learning, data analytics, operating systems, compilers, software engineering, distributed systems, hardware architectures, etc.

2.3.1 National Centre for Research and Development

According to the provision in the executive decree by Gentiloni, it is imperative to activate a *National Centre for Research and Development in Cybersecurity*: a centralised, multidisciplinary structure, with an adequate critical volume of resources and staff, partly governmental and partly linked to the world of research, able to carry out activities that can only be implemented by such a structure, to start the process of implementation of the *National Plan for cybernetic protection and cyber security* (illustrated in section 1.3.2). This centre should have no commercial purpose and should assist the government in activities of analysis, scientific research, technological scouting, and system engineering, following the example of the US *Federally Funded Research and Development Centers* (FFRDC). Such a structure will have to attract researchers and public and private (national) investors to develop cutting-edge research on topics of strategic national interest in the cyber domain.

The CNRSC will have to work in close synergy with universities and scientific research centres, cooperating with centres of excellence scattered throughout the country, in order to make the best use of their expertise and to provide highly innovative services to government organisations, public administrations, and the research system. In doing so, it should take into account the international reference landscape and the industry's best practices.

The CNRSC must be the national flagship and work closely with its counterpart centres in England, France, Germany, and the United States. In addition, it should play the role of a National Centre of Excellence in Europe in the context of the EU cybersecurity programmes as established, for instance, in the *Cybersecurity package*[11] and in the *EU cybersecurity certification framework*[12].

2.3.2 Territorial Competence Centres

In order to adequately support digital innovation in enterprises and in the public administrations and to enable them to face the challenges that cybersecurity poses, it is necessary to start effective mechanisms of technology transfer, training, consultancy, and support to local companies, local public administrations, and citizens. To this end it is necessary to activate a network of *Territorial Competence Centres in Cybersecurity* (CTCC) distributed throughout the territory, at metropolitan, regional or interregional levels, according to the needs of the territory in question.

[11] `https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en`

[12] `https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework`

These centres will need to leverage the close partnerships established at the local level between universities, public research institutions, private companies, and public organisations. Such collaboration is certainly a key success factor, as it is able to not only reduce the costs of the innovation process, but also to extend the scope of innovative projects, taking advantage of the complementarities of the involved realities, through appropriate synergies.

To achieve these objectives, it is necessary that each CTCC has an adequate number of researchers, operators, and technicians able to guarantee the spectrum of multidisciplinary skills needed to face and master the complexity of innovation in the cyber environment. Each centre must have initial financial support guaranteed for staff and infrastructures for at least five years. This support can then be scaled down, assuming that, from at least the third year onwards, each centre will have acquired a significant co-financing capacity through services to enterprises and the PA and through technology transfer activities.

The main tasks of each CTCC shall be defined according to the specific local production activities and could include:

- *Services and Consultancy* — (i) Providing services and advice to companies, in order to support them in their innovation processes and help them to protect their know-how, physical and virtual assets, and intellectual property, as well as to improve their offering and competitiveness; (ii) Managing local cybersecurity observatories for sharing information on attacks between government bodies, ensuring proper data confidentiality.

- *Support* — (i) Supporting operators/managers of critical infrastructures, according to the criticality of provided services; (ii) Supporting the efforts of businesses and local authorities, aimed at obtaining security certifications for hardware and software components.

- *Strategic Territorial Projects* — (i) Identifying and managing research and technology transfer projects of local strategic interest, which may involve setting up consortia of research institutions, universities, and industrial organisations; (ii) Participating, including through the consortia mentioned above, in national and international initiatives and calls for proposals.

- *Training* — (i) Organising various levels of local courses and seminars and promoting lifelong learning activities for local businesses and local authorities; (ii) Contributing to the increase of knowledge at all levels, including citizens' awareness of cybersecurity issues; (iii) Providing support to companies regarding the strengthening of their defence capabilities, and the testing and evaluation of their defence tools, in part potentially through the creation and management of local Cyber Ranges.

2.3.3 Vertical Competence Centres

The *Vertical Competence Centres in Cybersecurity* (CVCC) are the answer to the need, expressed by some specific sectors (energy, transport, healthcare, finance, etc.), to have ad hoc centres for the development of dedicated activities, such as CERT, ISAO, Cyber Range, Research Centres, Certification laboratories, cybercrime, business support, etc.

ISAC USA: Main sectors covered – Automotive, Aviation, Communication, Defense Industrial Base, Defense Security Information Exchange, Downstream Natural Gas, Electricity, Financial Services, Emergency Management & Response, Healthcare Ready, Information Technology, Maritime, Multi-State, National Health, Oil & Gas, Real Estate, Research & Education Network, Retail, Supply Chain, Transportation, Water.

As an example, the tasks related to the development of an ISAO are summarised below, while other activities mentioned above are dealt with in other parts of this volume. Information sharing is the basis of any cybersecurity strategy: the availability of timely, complete, and reliable information enables decisions that are more informed and accelerates protection actions in steady-state conditions, as well as detection, response, containment, and recovery actions in times of crisis. For this reason, many countries have set up coordination structures between the public and the private sectors, tasked with exchanging, analysing, and sharing information on cybersecurity. Examples include the *Information Sharing and Analysis Centre* (ISAC) established in the Netherlands[13] and in the USA, the *Information Sharing and Analysis Organization* (ISAO)[14] and the nodes of the British *Cyber Security Information Sharing Partnership* (CISP) program[15].

ISAO USA: Interest Information – Key Factors Indicators, Vulnerability Information, Courses of Action, Incidents, Threat Actors, Tactics Techniques and Procedures, Campaigns, Analytical Reports, Threat Intelligence Reports, Security Advisories and Alerts, Operational Practices.

In the United States, ISACs were first established as a private initiative brought together by category to share industry information on best practices and on security in general. Above the ISACs, the *National Council of ISACs* was founded, which guarantees inter ISAC sharing and connection with government bodies. President Obama then founded the ISAO, which are also sector-specific, but coordinated by the federal government.

[13] `https://www.ncsc.nl/english/Cooperation/isacs.html`

[14] `https://www.dhs.gov/isao`

[15] `https://www.ncsc.gov.uk/cisp`

In Italy, the Italian Ministry of Communications founded in 2006, at the *Istituto Superiore delle Comunicazioni*, a Telecommunications ISAC, which acted as a third party guarantor and in which all Italian telecommunications operators participated. This ISAC operated for one year in the form of a "pilot", after which it should have been officially regulated. The technologies available at that time did not allow for automated anonymisation; sharing and analysis were therefore carried out manually, which was feasible thanks to the limited amount of data to be processed. These were problems that have now been overcome.

2.3.4 Objectives

Raising the level of protection of the cyberspace is a long-term operation, in which it is important to act gradually, but within a clear and well-defined strategical framework. Avoiding excessive redundancy is indeed one of the first objectives. For example, in the Italian financial sector we registered the important birth of the CERTFin[16]; this does not, however, preclude the creation of specific additional centres in the financial sector, characterised by one or more specific elements, such as: ISAOs, cyber ranges, research centres, and certification laboratories or structures for countering cybercrime. These centres could be developed by public, private or public-private stakeholders in a territorial context. For instance, local or national production chains could be involved. In these initiatives, it is essential to define clear objectives for each centre, in order to avoid overlaps and a waste of resources. All of these considerations highlight the importance of a *national cybersecurity policy*, which will be addressed in the conclusions of this volume (chapter 9).

[16] `https://www.certfin.it`

CHAPTER

3 Enabling Actions

Once the cybersecurity centre-based infrastructure is in place, *enabling actions* should be developed to raise the level of security. These actions are aimed at strengthening specific parts of the attack management cycle within a complex system: from minimising the discovery time of the attack to data protection and applications of national interest (which can be active or preventive), from the creation of a of a national database of threats, capable of guaranteeing a certain autonomy in the recognition of malware found within national organisations, to forensic analysis and evidence management.

As far as the anticipation of the response is concerned, the chapter deals with three types of situations: (i) the anticipation of the response to classical cyber attacks, such as malware campaigns; (ii) the anticipation of the response in case of attacks based on social engineering, whose most important evolution has led to the deployment of fake news campaigns to accelerate polarisation and the conditioning of citizens' opinions; (iii) anticipating the response to physical attacks, such as terrorist attacks, which exploit the potential of cyberspace to carry out their actions.

Finally, three interrelated enabling actions are presented. The first concerns forensic analysis and its explosion, in recent years, due to the exponential increase in data and evidence sources due to the inflation of the number of IoT devices (analysed in section 5.4). The second is the definition of a systemic risk management process through new tools for the development of a comprehensive framework of public-private governance for cyber risk. The third and last enabling action focuses on active defence techniques, i.e., how to attack one's own systems to discover possible security flaws and then remedy them.

3.1 Security analysis of applications and services

Networked applications and services are rapidly becoming the preferred channel for users to access digital services provided by PAs and businesses. Take, for example, the services provided by the INPS (the Italian welfare national institute) and by the Agenzia delle Entrate (the Italian revenue agency) portals, the digital ticketing service adopted by Trenitalia and the unstoppable rise in home banking offered by banks. These applications make it possible to carry out operations that require high security standards, both because of the sensitivity to the data processed, as in the case of the filling out of an on-line income tax statement form, and because of the economic or reputational impact that an abuse of the service by malicious persons would entail, as in the case of home banking. It is not by chance that security certifications and assessments are identified as priority measures within the framework of the *National Plan for cyber protection and information security* (shown in section 1.3.2) and among these, the following is explicitly mentioned:

> the assessment of cyber defence measures applied by key service providers, including the performance of periodic testing of protection systems and the definition of an independent assessment system.

Consistently with this approach, the Italian *Three-Year Plan for Information Technology in Public Administration 2017–2019*[1] provides a set of measures to raise the level of security of the digital services provided, such as *assessment* and *testing*, which include activities to verify the correct implementation and compliance with the standards of security functions of system components or PA service components. Of particular importance among these are the *Digital Public Identity Service* – SPID[2], the *Electronic Identity Card* – CIE[3], and the service for electronic payments – PagoPA[4] for the "enabling" nature and centralisation that they represent in the strategic model of evolution of the PA information system.

Advanced services are often provided by combining different systems that interact with one another, producing real ecosystems. A particularly relevant ecosystem from different points of view is the healthcare ecosystem, where the

[1] `https://pianotriennale-ict.italia.It/`

[2] `http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid`

[3] `http://www.cartaidentita.interno.gov.It/elements-securityelements/`

[4] `http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/pagamenti-elettronici`

so-called *patient empowerment*[5] promises to reduce costs and increase efficiency thanks to the contribution of ICT technologies. A typical example is represented by the (often combined) use of the *Electronic Health Record* – EHR[6] (in Italy *Fascicolo Sanitario Elettronico – Electronic Health File*[7]) and of the *Personal Health Record* – PHR[8]. The former conveys information generated by healthcare professionals to the patient, while the latter allows the patient to share information with physicians and specialists.

As data in ecosystems are generated by interoperable applications with different levels of sophistication, complexity, and security, the risks of their subtraction are amplified. The security analysis of these ecosystems is therefore particularly complex, as security problems may arise due to the interaction between components even when each of them has been well designed, tested, and implemented. In fact, even if all components have a specific *security level*, the system resulting from their interaction may have a much lower one, due to abnormal or malicious interactions between the components themselves.

It is therefore important to have methodologies, tools, and environments to assess, analyse, and measure the level of security of individual components, of the systems obtained through their interaction, and of the ecosystems resulting from the composition of other systems.

3.1.1 State of the art

With regard to the security analysis of interoperable systems, ANSSI[9] supports a particularly relevant initiative in France: the *EIC (Environment for Cybersecurity Interoperability and Integration)*[10] managed by the Institute for Technological Research SystemX.

To analyse the security of applications and interoperable systems, a number of approaches have been proposed; the main ones are:

- *Vulnerability Assessment and Penetration Testing* — The *Open Web Application Security Project* (OWASP)[11] significantly contributes to the definition of these checks, through the development and dissemination of methodologies and tools for the production of secure software by the

[5] https://joinup.ec.europa.eu/sites/default/files/document/2014-12/media2499.pdf

[6] https://ec.europa.eu/health/ehealth/projects/nationallaws_electronichealthrecords_en

[7] https://www.fascicolosanitario.gov.it

[8] http://europepmc.org/articles/pmc2605603;jsessionid=E16BF856642E785880C17373E53DA3CB?pdf=render

[9] https://www.ssi.gouv.fr/

[10] http://www.irt-systemx.fr/en/project/eic/

[11] https://www.owasp.org/index.php/OWASP_Testing_Project

community of experts and developers. The *OWASP Testing Guide* is the de facto standard for the "Security and penetration testing" guide to web applications. Although it has brought important benefits, the proposed methodologies still rely on manual execution by expert analysts. For this reason, there is a strong interest in the development of new tools for the automatic identification of vulnerabilities.

VAPT – Vulnerability Assessment and Penetration Testing – It is based on the systematic execution of procedures and test cases aimed at detecting the presence of known vulnerabilities. By just interacting with the perimeter (inputs and outputs) of the target system, the methodology usually does not require a particular knowledge of the running software (black box approach). The procedures can be partially automated under appropriate conditions, but, in general, they require supervision and often the direct intervention of an experienced *penetration tester*.

Static and dynamic analysis of applications – Techniques that analyse the (source or executable) code of applications in order to assess the absence of vulnerability and the correct use of the information they manipulate. The static analysis performs these checks before executing the application, while the dynamic analysis is based on observing the behaviour of the application during its execution. In principle, static analysis allows the security of the program to be proved for any future execution, while dynamic analysis only guarantees that the executions considered have not violated the requested security requirements.

Formal Verification – Combining theoretical methods and results (coming from logics, graph theory, automata theories, etc.) with advanced algorithmic solutions, formal methods allow to detect errors in the various phases of the application life cycle (design, implementation, and execution) certifying the absence of vulnerability with an extremely high level of reliability. The common mathematical basis ensures the accuracy and completeness of the analytical results. However, their application to large systems is particularly burdensome because of shared data, side effects, competition, etc., which lead to the increase of possible situations to be considered.

Another interesting initiative is the *CBEST Intelligence-led testing guide*[12], written by the *Sector Cyber Team* (SCT) of the *Bank of England*, which

[12] `http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx`

defines guidelines and best practices for the evaluation of the security of digital services, with particular attention to e-banking services. The guide describes a multi-step process, including threat identification and penetration testing, but does not define the technical details of the checks to be performed.

- *Static and dynamic analysis of applications* — The most widely used static analysis techniques to assess application security allow for the control of information containment (*taint analysis*), the assessment of the non-interference between confidential and public data (*information flow analysis*), and the analysis of the performed sequence of operations (*control flow analysis*). It is now possible today to apply these techniques to *mainstream* programming languages such as Java, as shown in the case of the OWASP [31] test security analysis. However, there are theoretical limits (e.g., in terms of complexity) that curb the applicability of these techniques. The dynamic analysis may overcome some of these limitations and is applicable in most contexts. In any case, techniques based on software execution cannot exhaustively cover all possible behaviours, thus providing only partial guarantees. Recent developments are exploring the benefits of hybrid techniques that suitably combine phases of static and dynamic analysis.

- *(Semi)automatic tools* — System analysis, especially due to the increasing use of concurrency for applications running on multi-processor architectures, which may even differ from one another, is a major scientific challenge. Recent developments in this respect, based on advanced techniques and models, are already used by large IT companies such as Facebook, Google, and Microsoft. In order to minimise the costs associated with verification, the international scientific community is developing and testing increasingly sophisticated and effective automatic analysis and verification techniques. For example, software tools for the automatic analysis of authentication protocols have been successfully used for the discovery of serious vulnerabilities of network services [6, 71]. Tools for automatic security analysis of mobile applications are already on the market. In all cases, these tools use techniques capable of automatically carrying out an exhaustive analysis of application behaviour when performed on malicious inputs and/or in hostile execution environments.

3.1.2 Challenges

Among the most important scientific and technological challenges to be addressed are the following:

- *Verification costs* — Verification methodologies necessarily entail a cost in terms of time required and staff qualification. The higher the level of warranty required, the higher the cost. This also depends on the precision of the techniques used: a technique that produces a high number of false alarms (false positives) requires the manual intervention of specialised operators to identify alarms that require attention. For example, the application of static analysis methodologies, besides being particularly burdensome from a computational point of view, can produce false alarms, requiring the additional analysis by an expert.
- *Certifiability and verifiability of analysis* — Some verification techniques can formally guarantee the absence of certain vulnerabilities in applications and services. However, these guarantees must be made available so as to facilitate the secure and verifiable integration of software and services. In this sense, it is necessary to investigate new methodologies for the certification of software security properties in order to foster the development of an ecosystem of reliable applications and services.
- *Limits of automatic tools* — Automatic analysis tools must be able to analyse complex applications in terms of size, heterogeneity of languages, data flow and control. In particular, web and mobile applications pose new challenges related to event-driven programming, which makes it difficult to track data within the application itself. The use of dynamic languages, particularly in web programming, makes applications more vulnerable to malicious external code insertion and, at the same time, makes their security analysis more complex.
- *Environments for the security analysis of interoperable systems* — A significant shortage has been observed of environments that allow for the:
  - integration of third-party cybersecurity products and solutions with the existing ones, experimentally evaluating their security level and the resilience to possible attacks to the resulting system;
  - analysis of components and systems developed abroad and/or by untrusted third parties, in order to verify that they do not carry out, in addition to the intended tasks, unwanted, illegal, or fraudulent operations.

3.1.3 Objectives

The following objectives should be pursued:

- *Certification of applications with sensitive data* — For applications that capture and transmit sensitive medical and healthcare-related data via

personal devices, it is necessary to initiate a project that implements all the necessary measures to consider such devices as real medical devices, subjecting them, consequently, to the appropriate certification regimes before their use.

- *Automatic Analysis Tools* — There is a need to develop automatic methodologies for security analysis, configuration, management and testing, capable of analysing real applications, i.e., complex in size, heterogeneity of languages, data flow and control. The results of the analysis shall be readily understandable (in such a way as to facilitate the identification of the most appropriate remedy or countermeasure) and integrable with existing VAPT procedures, providing, where possible, an indication of the risk associated with identified vulnerabilities. The project should aim to include formal methods in the development process and promote the definition of minimum safeguards on the security of applications and on-line services based on formal methods.
- *Environments for security analysis of interoperable systems* — It is necessary: (i) to develop methodologies and tools for certifying integrity at the level of both components (applications, operating systems, virtualisation managers, security protections, embedded systems, etc.) and infrastructure (physical and virtual networks, cloud and edge computing, etc.); (ii) to develop environments that allow the integration of cybersecurity products and solutions, with particular emphasis on the automatic management of operational aspects, ensuring the protection of personal data in the interaction between distributed systems such as those that manage the digital identity federated with legal value (SPID) and commercial systems used, for example, for network or mobile applications.
- *Integration with Cyber Ranges* — It is desirable that the above environments are able to be placed within a suitably adapted Cyber Range (see box on page 35). This is to allow, among other things: (i) the joint validation of defence capabilities of interoperable systems; (ii) the effectiveness of the analysis methodologies developed when applied to real complex systems; (iii) the training of new security experts in the use of state-of-the-art tools.

3.2 Malware analysis and national database of threats

Malware represent one of the primary threats in cybersecurity because they are both means for accessing, controlling and compromising a remote system (Botnet), and tools for the removal or destruction of information on target com-

puter systems. A typical example would include the compromising of the DNC (Democratic National Committee) email accounts [13] during the last US election campaign in 2016. According to the SANS Institute[14], breaches caused by malware account for 69% of reported violations, with an annual increase of 10%. In particular, according to the Symantec Security Threat Report 2017[15], in 2015, there was a 30% increase in new malware not previously reported in 2014, with a total estimate of over 350 million new malware found in 2015 alone and as many in 2016.

These numbers suggest that behind the creation and deployment of new malware there is a wide reuse of code. In fact, detailed analyses have shown that many malware found are nothing more but diversifications or partial reengineering of pre-existing malware. This process of code transformation and diversification means that traditional protection systems based on *signature detection* are not able to detect new malware that, while capable of producing the same effects as the original ones, have a different form.

Malware – Any program used to disrupt the operations of a computer, steal sensitive information, access private computer systems, or display unwanted advertising. The main mode of malware propagation is to generate parasitic software fragments (*code injection*, see box on page 122) that are inserted into an existing executable code.

Botnet – Network composed of devices infected by specialised malware (*malicious bot*, described in the box on page. 60) and controlled by a so-called *botmaster* who can remotely launch *Distributed Denial of Service* (DDoS) attacks against other systems or carry out illegal operations, at times commissioned by criminal organisations.

One of the fundamental problems in cybersecurity rests in the *attribution of responsibilities*, i.e., the determination of the identity or the place from which an attack originates or where intermediate attacks [77] come from. The ability to trace an attack backwards (*traceback*) results in more accurate attributions and therefore more sophisticated forensic analyses.

Various methods exist to circumvent a network level traceback analysis, for example by spoofing UDP and TCP packets, i.e., by disguising an identity by

[13] WikiLeaks' DNC Email Leak Reveals Off The Record Media Correspondence. SanFrancisco.cbslocal.com. July 22, 2016.

[14] SANS Institute: "Incident Response Capabilities in 2016". The 2016 SanFrancisco.cbslocal.com, SanFrancisco.cbslocal.com, June 2016.

[15] Symantec – 2017 Internet Security Threat Report, April 2017.

altering the data that distinguish it, or by using a *laundering host*, i.e., compromised hosts that are not directly attributable to the attacker.

Network evidence is therefore only partially relevant towards the attribution of responsibility for an attack, especially when it is carried out by malware. More evidence can be obtained by evaluating the similarity with other known attacks that recycle the same code. In this analysis it is therefore essential to efficiently determine whether two programs are similar from a computational point of view and whether they share syntactic structures. A classic case is the established correlation between *Stuxnet* and *Duqu* malware [12]. The two malware, despite having completely different payloads, with completely different aims (one targeted at compromising industrial control systems, the other to remotely access systems), share a good part of the code and are in fact considered attributable to the same author.

The fact that a very large part of the malicious code distributed via the web each year comes from already existing malicious code represents the Achilles heel of malware-based attack systems. By analysing the code it is in fact possible to trace and correlate the actors who carry out cyber attacks through malware. In the analysis of the human genome, the possibility to trace different individuals back to similar genomes makes it possible to associate individuals and thus correlate the possibility of them manifesting the same disease. In terms of malware analysis, by analysing the similarity of codes, it is possible to correlate different attacks with similar code, thus providing a powerful tool for both forensic analysis and attack prevention. In addition, as the possibility to trace different genomes to similar phenotypes allows for the classification of genotypes, the possibility of correlating different malware to the same attacks allows for the classification of obfuscation techniques, thus providing a powerful tool to detect and prevent attacks.

3.2.1 State of the art

The engineering of the analysis and prevention process of malware attacks requires, by nature, an interdisciplinary approach involving code analysis techniques and machine learning technologies for its classification. The state of the art in malware analysis mainly consists of signature detection and behavioural analysis techniques with the ultimate aim of classifying and preventing infections due to new malware.

In terms of classification, the most widespread methodologies in use are machine learning (in particular supervised machine learning) and techniques for the static and dynamic analysis of the isolated code in a sandbox. Little is known in terms of early threat detection, i.e., prevention and monitoring of malware market trends through the prediction of new models and attack methods. This is one of the areas in which the state of the art is lacking both in terms of

available technologies and of their effective implementation and experimentation. Existing malware databases only permit a hash-based query of malware (i.e., on the syntactic structure) without providing any semantic or similarity correlations in terms of behaviour and/or code writing. This is one of the fundamental limits for the solutions available on the market (e.g., *Virus Total*[16] by Google. Expanding correlation tools is one of the major challenges. This would make it possible to increase the value of the data available and at the same time to improve the accuracy of malware analysis and understanding.

3.2.2 Challenges

Malware is constantly evolving, and the associated analysis and detection techniques are progressing accordingly, inherently leaving a margin of advantage for the effectiveness of new malicious software. The main research and innovation challenges concern prevention (*early threat detection*) and malicious code classification. This can take place at departmental, corporate, regional or national levels.

In terms of research, considering the continuous evolution of malware, driven by the need to adapt them in order to impede the advancement of analysis and detection techniques that are continuously produced, it is necessary to break this paradigm to avoid ultimately "following" the new variants of malware. This requires flexible and adaptable tools, able to identify hostile behaviours, both for what they do and for the ways in which they are carried out. The latter, in fact, can vary in a way that cannot be determined in advance, without altering the purpose of the code. We are therefore faced with the possibility of creating an unlimited number of variants of the same malware with few common syntactic structures. Knowing how to recognise and isolate similar structures makes it possible to reconstruct the phylogenesis of malware and provides tools to support attribution. Machine learning approaches can be used to semi-automatically extract the main patterns employed to develop new malware, making it harder for attackers to build malware that bypass security countermeasures.

To this end, it is essential to define updated models for the representation of malware capable of accurately capturing aspects of interest for the analysis to be carried out. To date, numerous representations have been proposed in the scientific literature, divided into two large families: representation by means of graphs that illustrate the functioning of malware, and representation by means of quantitative parameters that show the presence or absence of certain contents or their numerical consistency. Each representation captures a different appearance and has a different level of resistance to malware blurring techniques. Comparing the different solutions from a methodological point of view,

[16] `https://www.virustotal.com/it/`

and proposing new representation models and integration modalities for the different types of representation, allows for both a considerable improvement in the capabilities of automatic analysis and an increase of the attackers' difficulty in evading the analysis with obfuscation techniques.

In order to be able to effectively defend oneself from malware, it is also necessary to be able to identify how the inside of the computer or - more generally - a company network, was reached. Perhaps, for example, through the opening of a malicious attachment or by visiting a website containing malware. This requires the monitoring of corporate networks, not only in terms of network traffic, but also of the activity of individual terminals (PCs, tablets, smartphones) to correlate the infection with the actions that have determined its installation and activation.

A second major challenge is scale. The evolution of the malware market is a case of Big Code. We are in fact faced with a huge quantity of code that is put onto the net, with the same characteristics of speed, variety and volume as Big Data. The volume of new malware that appears on a daily basis makes the manual analysis of individual *samples* impossible. In this regard, the most effective solutions commercially available today adopt automatic machine learning-based analysis techniques to group samples into families and restrict manual analysis to cases that do not seem to belong to known families.

In this perspective it is important to create a national database of threats, where one can transfer knowledge acquired over time thanks to the analysis of new malware and from which useful information to effectively support these same analyses can be extracted.

The code, compared to other data, has its own characteristics that pose new challenges to both theoretical and applied research. The code (be it benevolent or malicious) has an *extensional* aspect, which represents its syntactic form, and a *intensional* one, which represents its functionality when it is executed. Both of these characteristics must be taken into account in the classification and analysis of large amounts of malware. Extensional aspects allow us to understand how a given threat occurs in a given malware, while intentional aspects allow us to understand and reconstruct the phylogenesis, useful for assigning responsibilities or early threat detection.

Honeypot – Security mechanism set to detect, deflect or in some way counteract unauthorised attempts to use systems or data. Usually, it appears as part of a website with data or resources of interest to potential attackers, but in fact it is isolated, monitored, and used as "bait" to understand the intentions or strategies of attackers.

It is also necessary to integrate malware analysis into security analysis processes. This involves the development of new organisational and process models, with adequate training and recruitment of technical personnel. To under-

stand the evolution of malware, identifying those that are truly new is functional to the deep understanding of *Advanced Persistent Threats* (APT) (see box on page 53).

3.2.3 Objectives

The main objectives to be pursued can be summarised as follows:

- The creation of a national database built on the basis of an infrastructure that collects and coordinates incidents/responses in the event of a malware attack. There is a need to improve and adapt existing threat representation schemes. See, for example, OpenIOC[17], CybOX[18], and STIX[19]. In our country it is necessary to set up a national database of malicious code where government agencies can compare threats involving national systems and properly report on them. This requires collection tools (*honeypot*) and tools for automatic analysis and code classification, as well as the implementation of consultation and information sharing mechanisms in accordance with appropriate security policies.

- To provide organisations and decision makers with tools for automatic classification and grouping of malware based on: (i) similarity and code sharing, (ii) sharing of remote command and control servers, (iii) target attack platforms, (iv) target attack market, (v) malware objectives, such as data theft and service interruption. These tools should enable those responsible for a network to take short-term action, such as early identification of whom to report the attack to and the implementation of the most appropriate countermeasures to prevent the large-scale spread of infections. They should also make it possible to develop medium-term actions aimed at identifying malware campaigns, attributing origin and setting up stable defence systems.

- To equip organisations and decision makers with tools for identifying: (i) vulnerabilities (process, systems, and software) exploited by malware, in order to allow for the planning of corrective actions and to improve prevention, detection, and defence capabilities; (ii) the malware's aims, in order to develop appropriate defence strategies, which must involve not only the strictly technical areas, but also the organisational and procedural ones as well.

[17] `https://www.fireeye.com/services/freeware.html`
[18] `https://cyboxproject.github.io/`
[19] `https://oasis-open.github.io/cti-documentation/`

- To develop an ecosystem of tools and methodologies for the automatic surveillance of cyberspace through the monitoring and grouping of malware based on the communication channels used (for example, shared Internet domains or domain generation algorithms), both for command and control activities and data exfiltration. These tools should enable the early detection of malware campaigns, potential links between different types of malware, and the development of early warning techniques based on traffic analysis.
- To develop tools and methodologies for infection prevention based on: (i) awareness raising and training of people using IT tools (especially non-IT specialists), (ii) the development of traffic monitoring systems on the corporate network (e.g., web browsing) to identify ways of using the network that increase the probability of malware infection.

3.3 Early response to cyber attacks

The last ten years have been characterised by a substantial increase in the number of very heterogeneous cybersecurity incidents: from identity theft to cyber-espionage, from financial frauds to *ransomware*. This phenomenon is the consequence of a paradigmatic evolution of the world of cybercrime, which today acts according to a model of *crime-as-a-service* in which extremely powerful and complex hacking tools become accessible at affordable prices and can be used without requiring in-depth technical expertise.

Ransomware – Malware that restricts the use of a device, for example by encrypting data or denying access to the device itself.

APT – Advanced Persistent Threat – Threats, represented by a hacker or, more often, by a group of hackers, whose objective is to hit a system through a series of targeted attacks, characterised by advanced solutions, to acquire and maintain control of the system for long periods of time.

At the same time, the complexity of attacks has also increased. Attacks on giant victims such as Target[20] or Yahoo[21] have shown that cyber criminals are

[20] `https://www.reuters.com/article/us-target-breach/target-cyber-breach-hits-40-million-payment-cards-at-holiday-peak-idUSBRE9BH1GX20131219`

[21] `http://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html`

able to infiltrate complex organisations, take full control of large-scale systems, and stay in such systems for years, effectively hiding their presence and actions. This kind of particularly complex and structured attack, typically known as *Advanced Persistent Threat* (APT), is now a fundamental problem for all large organisations (public and private) operating in a global context. The asymmetry between attackers and defenders continues to grow: while the time needed to penetrate a system is reduced thanks to increasingly effective attack tools, the time needed to discover and eradicate the presence of a cyber threat grows, leaving the assets of organisations at risk for long periods. Reducing this asymmetry is a fundamental objective in order to protect systems, and the organisations that manage them, from APT attacks.

Kill chain – Methodology for the characterisation of a cyber attack through its various logical phases: reconnaissance, weaponise, delivery, exploitation, installation, command and control, and act on objective. In an initial phase, the attacker studies his victim (reconnaissance) to define an attack strategy and acquire all the tools necessary to implement it (weaponise). In this phase the attack has not yet become operational and the victim is completely unaware of it. The attacker therefore has all the time he needs to design the attack as effectively as possible.

Recent attacks on big private corporations and public administrations have shown that they often impact society on every level. From the unavailability of essential services to the theft of identity, citizens are increasingly becoming the last link in a long chain through which the victims of an attack are linked.

Each attack, complex or simple, passes through a series of steps that the attacker develops to reach his final goal (the so-called *kill chain*). To anticipate the attack, it is necessary to provide organisations with tools that can help them acquire all the information necessary to trace the attack while it is still in the reconnaissance and weaponise phases. Information must be aggregated, linked and analysed with the aim of foreseeing potential threats. The automation of this process is fundamental to anticipate the response to attacks and to raise awareness within organisations of the threats they face.

Given the increasing complexity of attacks, it is necessary that their prevention exploits heterogeneous and multi-level information. It is no longer sufficient to rely solely on network traffic monitoring and connected devices to find out known vulnerabilities; it is necessary to integrate these approaches with information that can be obtained at other levels. For example, information about user interactions at the application level (their so-called *social graph*[22]) can aid in the understanding of whether certain traffic flows between devices are more or less suspicious.

[22] `https://www.cbsnews.com/news/facebook-one-social-graph-to-rule-them-all/`

Finally, as highlighted in section 5.4, the introduction of IoT scenarios, where a large number of mobile and pervasive devices communicate online, opens up totally new attack scenarios, to be carefully considered for prevention. In this instance as well, it is no longer sufficient to just monitor the traffic generated by such devices: this must, in fact, also be appropriately "interpreted" on the basis of the specific devices involved and their owners/users.

An evolution of defence systems aimed at anticipating the response to attacks in order to cancel or reduce their impact will have both direct and indirect positive effects. Not only will it allow us to reduce the number and, above all, the magnitude of accidents, but it will also increase the confidence of citizens and businesses in the adoption of tools and processes increasingly based on the intensive use of computer systems and interconnected networks. This trust, if expressed in business world, will be fundamental towards fully realising the *Enterprise 4.0* vision and all of the related technological evolution programs.

3.3.1 State of the art

Many of the existing solutions are strongly based on teams of specialists able to extract information useful towards defining potential impairment indicators to be used in automatic defence systems from the data. These teams are extremely expensive and are unlikely to handle an enormous amount of information, which is destined to grow by various orders of magnitude in the near future.

In addition to raw data, the analysis of the texts of message is also an inexhaustible source of information on planned attacks and, more generally, on potential attack victims. However, this source requires a complex elaboration that often involves almost all levels of linguistic analysis, from the morphological to the lexical-semantic and pragmatic ones.

> **Threat Intelligence** – The process to identify the features of an emerging threat, with particular reference to context, indicators, mechanisms, and implications. This process includes the collection and analysis of all information that could be useful for the decision making process regarding how to respond to the threat.

At the commercial level, there are various threat Intelligence services that provide tools and data on emerging threats. Many of these services have a general target group and therefore offer information that is not always contextualised. Contextualisation to the application case is offered as a service to be tailored to the specific framework of the customer, but in fact it represents an aspect that cannot be overlooked by those who want to protect themselves from targeted threats. The integration of natural language processing within threat intelligence processes is recent: a project was recently presented by Crowd-

Strike[23] and other projects are being developed. However, with the exclusion of the extraction of named entities, there is still no software for understanding multilingual natural language at a semantic level.

The threat intelligence solutions available today offer dedicated functionalities and only in rare cases are integrated into suites capable of supporting operators in a complete process that, starting from the selection of information sources, leads to the implementation of countermeasures. The lack of adequate support for the integrated process is often compensated by human operators, with the expected inefficiencies.

Finally, today very few solutions use heterogeneous data sources in an integrated way to identify possible vulnerabilities and evaluate the danger of specific observed phenomena, taking into account the context of the devices involved and their use.

Deep and Dark web – The parts of the web containing data not publicly indexed or whose access is protected through anonymous networks. It is believed that about 80% of the contents present today on the world wide web are hidden in these parts.

3.3.2 Challenges

The development of a process based on threat intelligence that offers the characteristics described above necessarily involves a series of challenges that, to date, prevent its complete realisation. Of these, the most important are:

- *The acquisition of data from protected sources* — Many of the activities currently related to the development of new attacks require a strong collaboration between different criminal actors. Such collaboration often takes place through protected and difficult to penetrate channels, mostly represented by the *deep and dark web* or private chat rooms. The technologies usually adopted for the acquisition of information from the open web collide with the "challenging" techniques designed to check that only real persons get access to specific information. The integration of these sources into automated intelligence processes requires the study of new solutions to overcome these barriers without human operator intervention.
- *The creation and dynamic updating of knowledge bases on cybercriminals and their operations* — These must include linguistic information regarding the different names under which, even in different languages, concepts and entities are expressed, so that these subjects can be linked together with the processed non-linguistic data for an integrated analysis.

[23] `https://www.youtube.com/watch?v=VNuPmxGakw0`

- *Multilingual text analysis* — The meaning of the texts must be unambiguously explained and the semantics extracted from them must be aggregated into topics and themes to obtain an overall picture of the thinking, intentions and objectives of cyber-criminals, thus intersecting the information in a way that is independent of the language, syntax and lexicon they are expressed with.

- *Lexical-semantic profiling* — The profiling of the authors of texts and semantic (not just lexical) analysis allows to identify and group deep and dark web texts on the basis of the writing style, also at the content level.

- *The automated distillation of indicators of compromise and rules for detecting attacks* — The collection of information related to potential attack vectors, per sé, is not sufficient to make the systems safer. Rendering this information usable requires the distillation of clear indicators of potential compromise and related rules for the identification of attacks. The automation of this process is a necessary step to adequately cope with the increasing number of attacks.

- *The contextualisation of intelligence elements* — One of the major limitations of threat intelligence systems available on the market today lies in their inability to automatically contextualise the information collected within the specific context of interest. The definition of appropriate methodologies for contextualisation is fundamental to correctly rank threats according to their priority and, consequently, improve the efficiency of defence systems, thus reducing their management costs.

- *Vulnerability Characterisation and discovery of attacks through heterogeneous complex information* — Many of the attack prevention monitoring systems (e.g., traffic monitoring) do not take into account the type of device usage by their users, and the type of interactions that they typically (or reasonably) perform when using the devices. Thus, to reduce false positives and negatives, it is necessary to integrate multi-level information, including the use of applications, the social network of users, and the profiles of the devices they use. This will guarantee a clearer picture of possible vulnerabilities, and improve the quality of prevention and discovery.

- *Vulnerability and prevention in pervasive environments* — With the spread of IoT technologies, attack scenarios expand enormously, as well as the possible negative effects of attacks on end users, as amply illustrated in section 5.4.

- *The assessment of the quality of the collected information, of the reliability of the sources and of the effectiveness of the countermeasures* — The

amount of information available for intelligence processes makes it necessary to study appropriate methods to evaluate the quality, reliability, and effectiveness of the responses that derive from them. These methods will play a key role in making the overall process less "noisy", increasing its effectiveness and efficiency.

- *Integrated intelligence, monitoring and system protection processes* — Solutions to the challenges outlined above will not provide satisfactory results unless they are framed within integrated processes that, starting from the identification of information sources to the management of accidents, trigger a cycle of continuous security improvement.

3.3.3 Objectives

The main objectives to be pursued are the following:

- *Advanced threat intelligence* — The development of a threat intelligence platform that allows acquisition from hidden and protected sources, with the possibility of automatically overcoming barriers posed by evasive or *challenging* systems, capturing the data reached and enriching them with semantic content identified in an automated way. The ultimate goal is to build a knowledge base for cybercriminal groups and the various actors related to this ecosystem.

- *Vulnerability identification in complex environments* — The development of a framework for monitoring and analysing the behaviour of complex systems for identifying vulnerabilities and possible attack pathways. The framework will have to specifically target interconnected systems, IT infrastructures for the management of *supply chains*, and complex computer ecosystems.

- *Automation of forensic investigations* — The development of a suite of tools for the automated analysis of attacked systems, in order to automatically extract and correlate information related to attacker activities. The objective of these tools is to support the forensic analyst's work by automating the identification processes of the attacker's activities, with particular reference to multi-step attacks.

3.4 Early response to social attacks

Protecting decision-making processes from disinformation and counter-information activities is a vital task for any country. Historically, this is a job

entrusted to intelligence services and has been set up such that the dissemination of information and knowledge occurred top-down, through newspapers, political party authorities or academic hierarchies.

The internet has radically changed the way knowledge is created and accessed [72], overturning all mediation systems in favour of direct access to an unprecedented array of content. The complexity of the phenomena of the reality is apparently accessible to everyone, but not always in an understandable way: our cognitive system struggles to adapt to new concepts such as *uncertainty*, *complexity*, and *probability*, tending to favour simpler (or simplified) and therefore reassuring syntheses and narrations. Against this changed backdrop, the old problem of spreading false information and its consequences must be faced.

The process of disseminating false information passes through a series of cognitive mechanisms that leads us (everybody, no one can be excluded) to acquire information in accordance with our world view and to ignore contrasting arguments. We all tend to form, then, strongly polarised groups on shared narrations [61]. This makes the dissemination of false information fruitful both economically and in terms of special interests and influencing public thought. The problem is serious and very delicate and science in general, and information technology in particular, play a direct and fundamental role in this challenge. It is therefore necessary to put in place a number of initiatives and synergies on several levels to ensure a better understanding of the problem in the current context and to develop effective responses[24].

The advent of social media has radically changed the process of construction and access to knowledge, allowing an unmediated production and consumption of information. In the next few years, given the growing emergence of scientific processes with considerable impacts on society (automation of work, biotech, etc.), it is expected that there will be a significant increase in the problems to be faced to meet the population's information needs in a targeted and timely manner, in order to avoid the proliferation of narratives that are misleading and potentially damaging to the democratic process.

Narrations that are perceived as harmful to an agency, entity or person are often referred to as *Fake News* in the press and have become a topic of central importance, both at political and institutional levels[25].

At the European level, academic and institutional communities recognise the problem of misinformation, fake news and information warfare as a high-priority topic: the World Economic Forum has been reporting, since 2013, on the massive dissemination of misleading and inaccurate information through the internet as one of the most serious global threats, while referring to it as

[24] `https://www.weforum.org/reports/the-global-risks-report-2017`

[25] `https://www.weforum.org/reports/the-global-risks-report-2017`

Digital Wildfire[26].

The former President of the Italian Chamber of Deputies Boldrini, convening experts from all relevant sectors for a survey, stressed the importance of digital education and the central role of information in democratic processes. The Italian National Regulatory Authority itself as guarantor for communications recognises the problem in the articulation and modulation of information in a completely new environment and promotes and sponsors an initiative to set up an observatory on the dynamics of misinformation on social media.

However, given the complexity of the phenomenon, a technological solution alone is not enough. The approach in the construction of solutions must necessarily be strongly interdisciplinary and must aim at creating synergies between the different actors within the IT system. In this scenario, the establishment of an observatory on information flows in social media could represent a bridge between the various stakeholders, who could jointly design targeted solutions and shared strategies.

To not recognise the interdisciplinary nature of the problem would mean excluding Italy from the international debate on the subject, while with the establishment of such an observatory we would play a leading role in a pilot initiative that could then be replicated on a European scale.

3.4.1 State of the art

At present, the contrast strategy advocated by the *debunkers* makes maximal use of online sites where flagrantly false news is reported. While this activity is certainly useful for those who need to quickly check the veracity of a piece of news, it has been shown that in the fight against disinformation, debunking sites can even be counterproductive, leading those who believe in false news to reinforce their own beliefs and to double down on spreading them [82].

Debunker – A person who analyses online news to highlight discrepancies, inaccuracies and groundlessness.

Bot – A software application, also called *web robot*, which performs automated tasks. Examples of the proper use of bots include the transmission of useful information, the automatic generation of contents and automated responses. Examples of misuse include theft of personal data, spamming and spreading of improper messages.

[26] `http://reports.weforum.org/global-risks-2013/risk-case-1/digital-wildfires-in-a-hyperconnected-world/#read`

An alternative approach is algorithmic; it targets automated solutions aimed at neutralising the vast amount of on-line information considered to be false. While such an approach can help to identify bots [32] and false profiles – for example by building "trusted" environments, in which the on-line identities are most likely associated to real identities [19] – it is limited by the impossibility to algorithmically decide if a statement is false, unless the expressive power of the used language is brutally reduced [62]. It is no coincidence that recent attempts to introduce automated filters on social media have highlighted both the problem of false positives (often linked to an ironic or sarcastic use of language) and the problem of false negatives (linked to changes in the use of language by those who wish to hide their communications). But the greatest danger of a purely algorithmic approach, in which the process of classification and response to fake news is completely automated, rests in the risk of unwarranted censorship, thus increasing already present polarisations and exacerbating the conflicts between social groups belonging to different *echo-chambers*.

Echo-chamber – A digital location in which people end up talking only within groups that have homogeneous ideas, with self-powering mechanisms. Communication within such groups tends to reinforce the shared beliefs and to attenuate, if not eliminate, the dissonant ones.

From what has been said, it is clear that the road to a brute algorithmic response to the problem is not practicable. To promise a software that is able to distinguish true and false would belong to the realm of fake news itself. Therefore, in terms of *fact-checking* and source verification, with consequent labelling of the information, at the most it is possible to obtain a statistical classification in which an exemplary set of elements considered truthful and/or reliable is however identified a priori. For this reason, it is not necessary to demonise the "partial" classification tools; they are useful to filter the enormous amounts of data available on the internet before processing them with traditional methods, i.e., by "real" people who decide what has to be done. At present, this is the strategy adopted on some social media platforms. Although the results are not completely satisfactory, this might be in part due to the inadequate specialisation of the employed teams of analysts.

Polarisation –The tendency to break off into distinct echo-chambers based on conflicting and opposite beliefs; such echo-chambers tend to reject a priori external information.

3.4.2 Challenges

Users will continue to choose their sources of information based on the consistency with their worldview. The main challenge consists in avoiding the sce-

nario in which echo-chambers linked to the various world-views become so "polarised" that debate, which is necessary for full democracies, stops. We must therefore create synergies to design and implement ad hoc tools for monitoring and sensing public opinion online that allow to understand current polarising arguments, in order to timely intervene or, even better, to act preventively before the debate degenerates into a clash between two factions without contacts. From this point of view, information technology has a central role to play compared to other disciplines; at the same time, the need to lower disciplinary barriers suggests *complexity science* as a possible interdisciplinary framework for aggregating data and models, while maintaining a strongly quantitative component that avoids excessive speculation.

Complexity science – A discipline developed from the successes of statistical physics in interpreting the collective phenomena of matter; the possibility of analysing large amounts of data has allowed phenomena from the social, economic, biological sciences to be seen under a new light and reinterpreted, up to the point of opening new perspectives on the understanding of the behaviour of complex technological systems such as network infrastructures.

However, scientific activity alone risks not having any effects if synergies are not established between information operators, who must be constantly updated on the observed dynamics, allowing them to better understand the effects of their actions in the *infosphere*. Training courses and meetings should therefore be organised, aimed at the media, to promote reciprocity and the pursuit of common objectives both in general and on specific topics such as public health.

Finally, it is very important to train and update those responsible for protecting and regulating the intersection between the infosphere and the cyberspace, in order to provide insights on the evolution of processes and information in these new spaces. This would help them towards taking effective and timely actions to introduce forms of regulation in these virtual, and no longer geographical, spaces. At the same time, it must be made clear that any intervention must strongly protect the diversity of opinions, because even if not taking into account obvious ethical implications, diminishing the richness of a system means reducing its reaction and adaptation capacities.

For this purpose, the great challenge is not only to produce models consistent with the observations of experimental data, but also to simplify and communicate such models so that they become useful tools in the hands of those who have the task of protecting our society.

3.4.3 Objectives

In order to understand and verify the dynamics of social media information, it is necessary to be able to continuously observe and analyse the large flows of

information exchanged between users. The analysis cannot be purely algorithmic (due to the problems mentioned above) nor purely anthropic, if only for the volumes at stake. Based on the state of the art and the level of knowledge currently present in Italy, we must aim at achieving the following goals in a relatively short time (the first results presumably from six months to one year from the beginning of the project):

- *Monitoring and sensing of the information space on social media* — Continuous monitoring of social media should be carried out to identify topics of interest and trends in order to understand users' information needs. Monitoring will be useful to identify and follow the dynamics (birth-life-death) of the echo-chamber. Based on the data collected, it will be possible to carry out various evaluations based on metrics and/or machine learning algorithms.

- *Polarisation Degree* — Polarisation separates the echo-chamber, decreasing diversity and undermining democratic processes. It is necessary to develop metrics and rankings of proven effectiveness, as has already happened in other fields for the analysis of competitiveness and development potentials of [62, 20] nations. Being able to define a *polarisation rank* would result in a quantitative indication for local, regional, national and European newspapers on their performance on social networks, taking into account the accuracy and polarising effect (or lack thereof) of the presentation of news.

- *Early Warning of potential topics that could transmit fake-misleading-specious information* — The approach must be statistical, in which a classifier based on machine learning will use syntactic and semantic characteristics, as well as the network of information flows, in order to make accurate predictions on possible topics likely to convey or become fake news.

- *Benchmarking* — For analysing and comparing the characteristics of information cascades related to certain news, it is necessary to measure the effectiveness of the penetration of various types of communication regarding specific topics, such as immigration, vaccines, health, food, and geopolitics.

Once these objectives have been achieved, it will be possible to integrate the means and techniques developed in order to aim at a higher objective, namely the protection of the *biodiversity of online information ecosystems*, where biodiversity signifies the coexistence of different animal and plant species in the same ecosystem, achieving a balance thanks to their mutual relationships [54].

The analysis of the echo-chamber and their interactions will allow us to evaluate the robustness and biodiversity of information ecosystems at various levels, from local to global ones.

3.5 Early response to physical attacks

The images and the videos that are posted on the web, or taken from surveillance cameras, are becoming increasingly important to support national and international territorial control agencies in their activities to fight terrorist organisations and organised crime. Moreover, public or private video surveillance tools are increasingly becoming fundamental for law enforcement investigations.

At the national level, however, there is still a lack of coordinated and continuous efforts to monitor the territory through the videos acquired by surveillance cameras scattered throughout the territory, to process and analyse the data collected, and to effectively use this information.

A similar situation is taking place in the context of automatic monitoring of images and videos shared by users via their social profiles. Although the acquisition and analysis of such multimedia content increasingly represents a valuable element for law enforcement agencies, such analysis is typically carried out manually, without the support of automatic collection and analysis tools.

3.5.1 State of the art

The amount of video data produced by video surveillance cameras, especially high-definition cameras, is growing dramatically. Just consider that a single HD camera can generate approximately 0.7 TB of compressed video data per month, and that there are tens of millions of installed ones: a study by IHS[27] reports that there is an average of one camera, not necessarily HD, for every 29 inhabitants of the planet. It can therefore be reasonably argued that video data generated by these cameras are becoming the "biggest" Big Data [45]. It is not just a question of volume: the problems posed by the very high speed of real-time collection and the necessity to quickly analyse and understand video content must also be considered. All this leads to new technological challenges ranging from the compression, storage and transmission of videos, to the automatic analysis of their contents, up to the development of analysis tools and metadata synthesis able to make the results of these analyses available to specialised users.

The international funding agencies have identified these needs and many international projects have been funded, both in Europe under Horizon 2020 and in the USA as part of the activities supported by the DARPA. Although

[27] `https://www.ihs.com/info/0615/video-surveillance-methodology.html`

research in the sector is undergoing a great expansion, with strong interest and economic support from large multinationals such as IBM, nVIDIA, Google, Facebook, and Microsoft as well, Italy still lacks a specific plan of wide-ranging and large-scale investments, able to involve the best and brightest from the Italian academic and industrial spheres to deal convincingly with these problems.

A virtuous circle between universities, business and the government has led to the development of a world-class, competitive, state-of-the-art knowledge in countries such as Germany and Sweden, that is also boosting their economy [65, 53].

3.5.2 Challenges

The main challenges regard:

- *Collaborative visual intelligence at the urban level* — The development of visual intelligence systems designed to support the control of the territory by law enforcement agencies requires integrated systems for the acquisition and processing of videos, first and foremost, which tend to come from: video surveillance cameras, aerial cameras from remote sensing systems (from satellites to drones), mobile cameras on cars and public transport which will increasingly be connected in vehicle-to-vehicle and vehicle-to-infrastructure mode, self-centric cameras (linked to the people who wear them), and smartphones possessed by citizens and/or police forces. This will require the creation of integrated systems and services, based on the collaboration between human competences and Artificial Intelligence, tendentially through state-of-the-art neural architectures, to process visual big data in real time. The objective is to provide: (i) results including visual analysis, (ii) classification and detection of events of interest, (iii) automatic correlation between different views from different sensors, (iv) identification and re-identification of individuals, (v) automatic detection and prediction of behaviours and/or intentions of groups of people.

- *Automatic monitoring of visual content from the web* — The development of systems that can automatically analyse shared images and videos on social media is extremely important in order to counter the threat of terrorism. The great challenge in this area is that of identifying and reporting to law enforcement agencies contents of probable criminal nature. In particular, an open problem is the automatic analysis of images/video to identify cultural and religious symbols to detect content of potential terrorist nature, such as videos used to recruit followers. A more subtle, but equally important, aspect is to automatically understand the impact that these visual contents are intended to have on social media users. The

multimedia content shared in social media for propaganda is typically chosen to attract the interest of the largest number of users (i.e., to become viral) and to evoke strong feelings in the observers. Therefore, a fundamental challenge to understand the strategy of terrorists, and hinder their efforts, is to analyse the relationship between visual content and virality, as well as to provide tools that can infer the emotional content evoked by images and videos.

- *Managing, viewing and analysing visual content on a large scale* — The cardinality and complexity of visual data of interest make it necessary to use solutions based on *visual analytics* that, by combining advanced visualisation techniques with automatic analysis, are able to extract information from the analysed data and to present it in a timely and effective manner to the operators who have to make national security decisions. To this end, it is essential to provide the operators with aggregate and filtered information contextualised to geographical, temporal and social aspects. Automatic analysis allows repetitive or similar behaviours to be highlighted (e.g., to detect suspicious persons who have been physically in the same place in a certain time interval or who have made similar movements). This analysis must be guided by the user who, on the basis of his exploratory activities, provides the algorithm with the necessary parameters for its operation, e.g., the locations on which to carry out the analysis, the time period, the individuals to be observed, and so on. Another challenge, orthogonal to visualisation, consists in the development of techniques to reduce the data analysed, thus minimising its complexity and cardinality while maintaining the richness of information, in order to allow for a more effective visual exploration.

3.5.3 Objectives

The progress made in recent years in the field of artificial intelligence applied to computer vision, with particular reference to the impact related to the use of deep learning techniques, makes it prime time for the implementation of long-term, national projects for:

- the acquisition and automatic analysis of videos from surveillance cameras on the entire national territory, aimed at identifying suspicious behaviours and individuals, even for time frames of many months, independently from changes of light, weather conditions and clothing;

- the automatic analysis of images and videos posted by monitored people on their social profiles, in order to (i) identify the place from which images come, without using metadata that are not always available, (ii)

describe the emotional content of videos and/or photos posted and/or shared with other users;

- the development of advanced visualisation techniques for the effective use of the analysis carried out by algorithms on visual data, to make timely use of such data by operators who have to make decisions related to national security, both for terrorist attacks and natural emergencies.

In particular, projects must pursue the development of:

- automatic reconstruction systems of views integrated by fixed, mobile and wearable cameras;
- systems for the detection of people and targets "in the wild"; their possible (re)-identification on a large temporal and spatial scale;
- predictive tracking systems for moving targets, with social behavioural models for the analysis of crowd behaviour in case of critical events and specific behavioural models for the analysis of relationships between people;
- technologies to identify recurring symbolic elements in images and videos, and analytical methodologies to evaluate the emotional content of visual data in order to recognise images with a strong emotional impact and to automatically predict perceptive attributes such as the "potential" virality and popularity of specific visual data;
- systems for geographic and temporal visualisation of personal data and metadata, catastrophic events and/or social media information, with visual mechanisms to parameterise automatic analysis algorithms;
- architectural models for the realisation of a new generation of video surveillance systems for public safety and security.

3.6 Forensic analysis and evidence preservation

Computer forensics has been enjoying a period of extraordinary attention over the past 20 years, frequently earning prime time attention in TV news and talk shows. This is largely due to the fact that for a long time the main sources of evidence have remained *technologically stable* and therefore have allowed for the development and improvement of methodologies and tools for extraordinarily effective forensic investigation. Digital evidence sources, that cannot be assimilated to operating system artefacts, have long remained limited to (digital) documentary sources such as databases (e.g., for accounting purposes), records of telephone traffic and chronological records with various denominations, for which effective investigation approaches have been developed.

3.6.1 State of the art

However, this situation was destined to change: in as early as 2010 Garfinkel [37] predicted the end of the *golden age* of forensic computing in the face of the exponential increase in storage capacity, the diversification of digital evidence sources and the spread of cloud computing and encryption.

The work of Karie and Venter in 2015 [49] summarises in a taxonomy that includes almost thirty points the main challenges faced by computer forensic science in terms of technological, legal, personnel and operational issues. These include the problems already highlighted by Garfinkel and others related both to the difficult interoperability between different instruments used in investigations and to the lack of personnel adequately trained to carry out digital forensic investigations.

It is worth noting that some of the challenges have in the meantime been exacerbated by a further increase in storage capacity and a marked diversification of evidence sources. All this requires a profound rethinking of traditional computer inspections, essentially based on the execution of an image copy (bitstream) of the media found and the subsequent laboratory analysis.

To date, it is no longer possible to follow such an approach, both due the time needed to acquire copies of the supports (with consequent blockage of the activities of the subject under investigation), and due to the technical impossibility of making image copies of certain types of devices, such as the latest generation of mobile devices, embedded systems and IoT devices, for which it is necessary to resort to the so-called *logical acquisition* or to ignore a likely precious evidence source.

Accordingly, it is therefore of fundamental importance to develop new forensic acquisition and analysis techniques that, combined with an adequate legal consideration, allow to avoid or overcome the current impasse, bringing the discipline back to the glory of *golden age*.

3.6.2 Challenges

The main challenges therefore relate to the following:

- *The exponential increase in data volume* — Reducing the time needed to generate copies can also be addressed by implementing a so-called *forensic triage*. Although different approaches to the preventive selection of sources have been proposed, the problem persists, mainly because each solution has to balance different interests. In addition, the preventive selection of the source:
  - apparently violates the principle of completeness of the evidence, and a hypothetical defender could argue that the investigative and

probative reasoning is flawed by the previously made selection and therefore that the defence would be deprived of the possibility to carry out further defensive investigations);

- is intrinsically exposed to *anti-forensic* actions, as a hypothetical attacker would inevitably be aware of the artefacts under investigation and could alter or destroy them. In fact, some types of cyber attacks have recently appeared to deliberately introduce *fake evidence* in order to deflect investigations.

- *The diversification of test sources* — Upon first reflection it is evident that it is not possible to imagine a generalised model of acquisition without the effective collaboration of device manufacturers. In fact, in the impossibility of directly accessing the stored information, it becomes necessary to trust those voluntarily communicated by the device itself.

  Furthermore, It should be also taken into account that, due to limitations on hardware resources or confidentiality requirements, small devices often do not allow access to information stored internally, except by exceptional means. In the case of mobile devices, it is well known that manufacturers tend to increase security measures towards external accesses that are not authorised by the device owner. The strategy is certainly commendable from the point of view of confidentiality, given that a weakening of the protections would result in a sure advantage for both legitimate investigations and abusive intrusions, but it also represents a serious obstacle for the former.

  However, the confidentiality argument does not apply in case of devices (e.g. medical and diagnostic devices, embedded vehicle control units, control systems of industrial plants, "smart" systems), for which it is not just in the interest of the owner, but also of the entire society, to acquire information that prove its correct functioning or - on the other hand - that allow to detect possible abuses (recall of the recent case of the control units of some car manufacturers that were "programmed" to falsify the results of emission tests).

- *The volatility of the sources and extension of the* window of opportunity *for acquisition* — A separate challenge that must be considered is the so-called *window of opportunity* for obtaining the evidence source. Although the information contained in the computer supports is not subject to natural degradation like biological samples, it is subject to storage times that were explicitly or implicitly programmed during their design. In some cases, such as for accounting documents and phone traffic records, the law establishes a *retention time*, i.e., the period within which the information must be stored and beyond which it can, and in some cases must, be destroyed.

However, there are cases of logs whose *retention time* is linked to the reasons that they were collected (i.e., for the diagnosis of device/system malfunctions) and not, therefore, to investigative purposes. The question therefore arises of defining and - possibly - regulating which information must be compulsorily collected and as well as the related acquisition methodology, while respecting the legitimate expectations of privacy and the needs of crime repression (often in the interest of the person who owns the device to be examined).

A particular aspect that falls under this point regards how to correctly generate and conserve logs, an area in which today total anarchy reigns. While it is true that system logs are generally generated and stored correctly by IT infrastructure operators, who are also the main users, for diagnostic or performance optimisation purposes, it is also true that - as anyone with minimal forensic experience can testify - application logs, where available, rarely result in the answer to even the most basic investigative questions and are often not even documented. Moreover, for more traditional evidence sources as well, such as the documentation of telephone traffic, rendering semantically homogeneous the information obtained from the various operators and enriching it with annotations that allow them to be interpreted correctly at a later time are problems that frequently arise, further complicated by continuous technological evolution.

3.6.3 Objectives

The objectives of the project can be identified along three action lines, each correlating to a specific challenge:

- *The exponential increase in data volume* — The development of methodologies and tools for forensic triage that are able to limit the time of acquisition and subsequent analysis without compromising the quality and reliability of the evidence;

- *The diversification of evidence sources* — The analysis of new evidence sources and the development of more flexible, but equally effective, analysis methodologies than bitstream copying;

- *The volatility of the sources and the extension of the* window of opportunity *for acquisitions* — The development of guidelines for the correct mode of generation and preservation of chronological recordings and the definition of minimum retention periods, also taking into account the requirements for the forensic analysis of the generated data.

3.7 Risk management at systemic level

Risk management is a well-established discipline in the areas of financial investments, business, and project management. However, traditional risk management methodologies cannot be applied to the field of cybersecurity. In particular, the dynamic nature of cyber risks (threats, agents, vulnerabilities, accidents, and impacts) is not properly represented in the static and iterative methods of current risk management models and standards.

It is necessary to develop an approach aiming at creating a *dynamic framework for cyber risk management* (Dynamic Cyber Risk Management – DCRM) capable of properly considering evolving ICT vulnerabilities across an entire organisation and mitigating related threats and risks. Such an approach requires a new dimension compared to traditional risk management: the need to be dynamic and the ability to adapt continuously.

3.7.1 State of the art

Many efforts have been undertaken by the research community and industry to develop a solid and coherent discipline applicable to cyberspace. Different reference frameworks and specific standards have been developed in recent years, including ISO/IEC 27005[28], NIST 800 30[29], IT Risk (ISACA) [30], COSO[31], ITIL[32], and OCTAVE[33]. However, all these frameworks rely on a static approach and cannot be applied to the management of dynamic cyber risks. In addition, these models are partially questionable when introducing and assessing risks based on the probability of events. In particular, in large organisations this assessment process can be complicated and time-consuming; due to vulnerabilities and evolving threats, the results of a risk assessment can quickly become obsolete.

Critical infrastructure protection is becoming one of the cornerstones of national security. The European Commission already requires Member States to raise their awareness and improve their mutual cooperation. The NIS Directive (illustrated in section 1.2.1) in particular encourages the development of trust-

[28] https://www.iso.org/standard/56742.html

[29] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[30] https://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/The-Risk-IT-Framework.aspx

[31] https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf

[32] https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[33] https://www.cert.org/resilience/products-services/octave/

worthy relationships between public and private subjects and the enhancement of a shared and cooperative culture of risk management.

3.7.2 Challenges

The tools to develop a global framework of public-private governance for cyber risk need to be defined, introducing innovative intelligence tools and specific methodologies. One of the main challenges is to strengthen reporting and information sharing policies and procedures between national authorities, particularly in the private sector, in order to keep a comprehensive overview of the threat landscape and to improve response capabilities.

It is therefore important to define frameworks that outline methodological approaches, policies, processes, and enabling technologies to be adopted by institutions and companies to address specific cyber risk management requirements and by governmental organisations to share information on key threats, vulnerabilities, and accidents occurring in the cyberspace.

These frameworks will allow all institutions involved in risk management to build a context of higher (*situational awareness*) at a national level, enabling them to:

1. understand the current security position of all relevant critical infrastructure stakeholders;
2. assess and, if applicable, support progress towards proper positioning;
3. notify internal partners of cyber risks;
4. coordinate the public authorities responsible for responding to incidents and taking appropriate mitigation measures;
5. determine the decision-making process of policy makers on strategic priorities.

3.7.3 Objectives

The two main frameworks that are needed are:

Dynamic Cyber Risk Management – DCRM — The components of the DCRM must be designed, developed, implemented, and validated in real-world contexts taking into account the following important principles:

- the clear definition of the cyber risk management policy and related criteria for risk assessment and management (organisational attitude to risk, risk management criteria and tolerance level, articulation of roles and responsibilities);

- a focus on the evaluation of *dynamic risk management*: the key aspects of critical operations and critical services, the vulnerabilities, the presence of dynamic threats, the probability of accidents, the impact of an ongoing accident;

- applicability to the different companies and critical infrastructures;

- flexibility in relating to different and new legislation;

- clear processes and activities to support early detection (risk identification) and rapid response to accidents (risk mitigation), enabling immediate operational initiatives, providing feedback to corporate risk management and governance processes; this includes dynamic detection, assessment, and management of new threats and vulnerabilities;

- the possibility to share information on dynamic cyber risks and accidents within a secure framework to public bodies (see PPIS below);

- the use of clear indicators and metrics to support both the continuous improvement of the DCRM framework and the revision of the security guarantee model, related checks, and reference frameworks.

Public–Private Cyber Risk Information Sharing – PPIS — The components of the PPIS must be designed, developed, implemented, and tested in institutional governmental organisations, taking into account the following fundamental principles:

- the alignment with the EU cybersecurity strategy, the specific national legislation and the sector-specific requirements (e.g., energy, telecommunications, water, etc.);

- the clarity of roles and responsibilities regarding information sharing and collaboration between the public and private organisations involved;

- a focus on the "need to know and share" and on the specific security requirements of all stakeholders and players for sharing information, collaboration and mutual trust;

- the use of clear indicators and metrics to assess and monitor risk trends at the national and sectoral level;

- a focus on early detection and rapid response to accidents.

3.8 Active Defence

The improvement of computer attack techniques often implies that victims realise too late that an attack is taking place. Correcting a vulnerability may prevent a new exploitation, but cannot do anything with respect to the attack that brought it to light. A proactive approach is therefore needed to set up a so-called *active defence*.

Active Defence – The use of hacking and penetration testing techniques (see box on page 44) to detect vulnerabilities of systems before they can be exploited for attacks; the use of counter-attack techniques and malware generation to identify and stop ongoing attacks.

In general, the concept of active defence is intended to play an increasingly central role in the protection of national strategic infrastructures. With advanced technologies and automatic tools for strengthening their own defences, the companies involved will be able to guarantee a greater protection of their strategic assets. Consequently, the delicate management of sensitive data and critical infrastructures will also be strengthened, improving the country's defence against cyber attacks.

It has never been more urgent to launch appropriate training campaigns to increase active defence capabilities. Understanding attack techniques and their practical applications is useful not only for the training of qualified personnel, but also for those who intend to start new careers, e.g, as system programmers.

3.8.1 State of the art

Among the most popular active defence training initiatives there are *Capture-The-Flag* (CTF) style competitions, used by an increasing number of companies and government agencies, following the example of companies like Google, Facebook and the GCHQ.

CTF – Capture-The-Flag – A competition with simulations of realistic scenarios in which participants carry out active defence activities for complex computer systems, application attacks to applications, and development and analysis (*reverse engineering*) of malware.

Bug Bounty – A reward program aimed at detecting vulnerabilities in computer systems or services (*bug hunting* phase) and immediately reporting them confidentially to the owners of the target systems, with clear legal safeguards for all stakeholders.

At the international level, it is worth mentioning the initiatives taken in the USA by the DARPA which, in addition to having launched a specific defence programme, has recently organised the first CTF competition between autonomous systems, called the *Cyber Grand Challenge* (CGC)[34]. The teams' participants combined the most innovative active defence techniques and artificial intelligence to develop systems capable of identifying vulnerabilities in the supplied software, to generate patches and to attack rival systems without any support from analysts.

In Italy, the *CyberChallenge. IT* is worth mentioning. It is a project of the CINI National Laboratory for Cybersecurity, presented in Section 6.2.1.

Other projects involve the Digital Transformation Team, the National CERT and CERT-PA to define national "responsible disclosure" policies in order to facilitate the rapid resolution of PA security issues and to minimise risks for the people. This initiative is connected to European projects such as the *EU Free and Open Source Software Auditing* (EU-FOSSA)[35] that studies the identification of vulnerabilities in critical software, through *Bug Bounty* initiatives as well.

3.8.2 Challenges

In the field of active defence, new methodologies need to be defined for the prevention and mitigation of attacks. They must go beyond the traditional concept of passive defence in order to identify and respond promptly to emerging threats, such as *zero-day* vulnerability. In fact, because of the nature of heterogeneous and highly dynamic modern hybrid systems, it becomes necessary to anticipate hostile actions by putting into practice the same operations of a potential attacker. The main purpose of this activity is to identify possible flaws in the system security, in order to strengthen the defence where this is more necessary or convenient. In addition, actions should be developed in a multidisciplinary framework, taking the specific operational context into account and involving experts from the different application domains.

> **Zero-day** – The software vulnerabilities that are unknown to system operators interested in defending against attacks, but known to attackers. Until the vulnerability is known, attackers can use it to compromise the system itself or other systems. An attack that exploits a zero-day vulnerability is called *exploit zero-day*.

Such methodologies must lead to the development of innovative products for the analysis and protection of services and infrastructures. This process should take place by involving the main national industries active in the field

[34] `https://www.darpa.mil/program/cyber-grand-challenge`

[35] `https://joinup.ec.europa.eu/collection/eu-fossa`

of cybersecurity, and by creating innovative start-ups with strong vertical competences.

In addition, in order to ensure the effectiveness of these initiatives, legislators must define and regulate security protocols for critical infrastructure operators. It will be necessary to define codes of conduct and engagement to allow active defence operations, such as penetration testing (see box on page 44), without putting the security of the infrastructures at risk.

Finally, procedures must be defined for threat prevention, mitigation and reporting. These procedures should refer to appropriate CERTs (see box on page 17) dedicated to the protection of specific infrastructures of interest, such as transport, energy and telecommunications.

3.8.3 Objectives

Among the main objectives, the following should be included:

- *Active Defence Practices* — In this regard, it is appropriate to "institutionalise" initiatives such as the *CyberChallenge. IT* project of the CINI National Cybersecurity Laboratory (presented in section 6.2.1), extending them to all potentially interested students from all age groups.

- *Bug Bounty programs* — With the dual goal of training and improving national information technology security, it is necessary to promote the growth of the *Bug Bounty* programs (see box on page 74. Universities will deal with training, usage, and ethics, while companies have the task of increasing the use of such tools, still looked at with scepticism. Common initiatives may consist in the practice of "bug hunting" by university students as part of exams for cybersecurity laboritories, in close collaboration with partner companies, guaranteeing full the confidentiality of detected weaknesses.

- *Legislation on the subject of "white-hacking"* — The legislator is responsible for considering the legal implications of such practices, providing safeguards for *white-hat hackers* who participate in penetration testing and bug hunting campaigns. An understanding of the phenomenon is necessary, in addition to the introduction of clear legal distinctions between those who exploit vulnerabilities and those who communicate them to the operators of the systems/services analysed in a timely manner. Tools such as *responsible disclosure* should become part of initiatives of law proposals, aiming at protecting on the one hand companies and PAs and their interests and on the other hand those who find the vulnerabilities and are committed to confidentiality. These people should not be targeted by legal actions.

- *Incident Response* — An important step towards defending national interests and strategic infrastructures and industries is the creation of "vertical" CERTs dedicated to a specific aspect (such as energy distribution, transport, financial markets) with state, industrial and academic partners. Another additional responsibility of these consortia should be the definition of the boundaries of the digital counterattacks, (a topic that is becoming increasingly relevant, as highlighted by the proposed US law *Active Cyber Defense Certainty Act*[36]), that is aimed at actively defending against ongoing attacks and identifying the perpetrators.

White Hacking – Activities of IT experts, also called *ethical hackers* or *white hats*, who oppose the criminal use of computer systems. These experts specialise in *penetration testing* and in all methodologies for testing system security, they differ from *black hats* due to their positive and altruistic aims.

[36] `https://www.congress.gov/bill/115th-congress/house-bill/4036/text`

CHAPTER

4 Enabling Technologies

Enabling technologies increase the cybersecurity level of a complex system. In this chapter we consider some of the key ones.

The challenges posed by hardware architectures are analysed first. Unfortunately, they have not been considered nationally for some time, despite the fundamental role they play in terms of the so-called national technology.

Next come vertical systems, such as encryption (in particular post-quantum cryptography), biometric systems, and quantum technologies. They are known as technological cornerstones for which Italy has a great scientific and industrial tradition, which should be transformed into an international competitive advantage.

Afterwards, we consider Artificial Intelligence and discuss the ways intelligent agents can be used maliciously and how they can be exploited to guarantee better defences.

We conclude the chapter by considering an enabling technology in which we think Italy should invest in order to build an additional competitive advantage: the construction of a national blockchain.

It should be noted that in this chapter, technologies such as machine learning, big data and data analytics are not considered to be “enablers” as they are, in fact, transversal to many security systems and widely used by them. In this light, the algorithms underlying data analytics as well as those used for machine learning must be protected and their protection is considered in chapter 5.

4.1 Hardware Architectures

As with software, data and communication infrastructure, the hardware must be designed, built, tested, used, and maintained taking into account possible cyber attacks and their consequences. The main security issues arising from hardware components within the *IoT* and *Industrial Control System* devices will be analysed in sections 5.4 and 5.5 respectively. This section considers hardware systems in their complexity, with particular attention directed to their impact on the so-called *National Technology*.

Design Bug – This error is mainly attributable to the fact that, during the design phase, attention was paid to functional aspects but not security ones, rendering the device vulnerable even though operating correctly.

Hardware Trojan – An additional or modified component with respect to the initial design, aimed at introducing various kinds of vulnerabilities. Modifications can be made either during circuit design, by unreliable suppliers of functional blocks (IP cores) available on the market or by malicious designers, or during the manufacturing process by unreliable manufacturers.

Side-Channel Effect – The possible vulnerability of a circuit or system deriving from the possibility to measure (from the outside) and analyse the values of specific physical aspects of hardware, such as timings, voltages, currents, induced electromagnetic fields, temperatures, energy consumption, etc. These values can be correlated with data retrieved from the software in order to fraudulently exfiltrate secret information.

Counterfeited hardware device – A device that, taken from a decommissioned machine (e.g. by desoldering them from their motherboards), is illegally recycled and fraudulently put back onto the market, possibly after having suitably counterfeited the package. Beyond the economic damage, the use of recycled components can have serious consequences on the safety of the systems in which they are used (due to their high failure rate) and great impact on security.

The hardware runs the software and is, in fact, the last line of defence: if the hardware is corrupted, all the mechanisms introduced to make the software secure (at any level) can prove useless. Unduly protected hardware can be the weak link in the chain, becoming an easy gateway to the system, its functionalities and data.

As with software, *hardware vulnerability* may result from project bugs (*Design Bug*) or intentionally inserted faults (*Hardware Trojans*). In addition, unlike software, hardware can be observed and controlled (and therefore also physically attacked) *from the outside*, through physical quantities and/or its physical interactions with the real world (*Side-Channel effect*). Furthermore, in the case of hardware, in addition to the typical software attacks and those directed towards the misappropriation of data and service interruptions, there are also attacks aimed at the theft of intellectual property intrinsic to the technological solutions used for counterfeits through the fraudulent re-entry of decommissioned and therefore typically worn out devices back onto the market (*Hardware Counterfeiting*).

Physical attack – The physical interaction with a hardware device to access its internal elements (e.g., via *probing*) or to inject faults during the execution of a security algorithm. Injected faults can, for example: (i) force the value of a processor register in order to modify the running flow of a program, forcing it to skip security control functions; (ii) alter the quality of a random number generator; (iii) discover the value of the secret key used in an cryptographic algorithm. Faults can be injected via laser pulses, electromagnetic pulses, abnormal values on supply voltages and/or timing signals, operating temperature variations.

4.1.1 State of the art

Many papers and books can found in the literature that contain detailed analyses of the state of the art on hardware security; the reader could for example consider [68, 63, 48].

The use of *Design for Testability* solutions, such as scan chains (which were introduced to allow device testing at both the end of the production process and in the field), without taking security into proper consideration, entail critical issues that have been known for years. In addition, in early 2018, two attacks, known as *Meltdown*[1] and *Spectre*[2], also found widespread resonance in the mass media, exploiting bugs in the hardware design of advanced processors. These bugs make it possible to take advantage of the side effects of executing *out-of-order* machine instructions (unauthorised loading of cached data) to read the contents of memory locations that should not have been accessed. Exfiltrated data may include, for example, passwords, secret keys, sensitive data, permissions to access other services, and so on.

The Meltdown attack (known as CVE-2017-5754[3]) creates a software exception (trap) that aborts instructions executed in advance and then gets a *privilege*

[1] `https://meltdownattack.com/meltdown.pdf`

[2] `https://spectreattack.com/spectre.pdf`

[3] `https://access.redhat.com/security/cve/cve-2017-5754`

escalation (see box on page 122) specific to Intel processors. The Spectre attack (CVE-2017-5753[4] and CVE-2017-5715[5]) is based on the classical technique of *branch-prediction*. and, thanks to its generality, can be successfully run on Intel, AMD and ARM processors.

In both cases, the design flaws do not affect the operations of the processors involved in any way, but they do introduce security vulnerabilities. Under certain conditions, it is in fact possible for a "normal" user (process) to fraudulently access information that should instead only be accessible to "privileged" users. Although developing attacks such as Spectre or Meltdown is extremely complex (and therefore unlikely to take place in practice), they are a further demonstration of how by corrupting the hardware or exploiting its vulnerabilities, any mechanisms introduced to secure software (at any level) can turn out to be useless. In this respect, the impact of Meltdown and Spectre on the Cloud is analysed in section 5.2.

In conclusion, it is important to stress the need to consider the security aspects and the different vulnerabilities of hardware and software in an integrated way. In some cases, such as that exploited by Meltdown and Spectre, the hardware vulnerability can only be eliminated by modifying the design of the next versions of the processors, thus the only way to remedy ("put a patch") on existing processors, which will remain flawed forever, is to take software-level actions or to modify all the operating systems that use the faulty processors. In other cases, it is the hardware that "comes to the rescue" of software vulnerabilities, carrying out a series of checks and operations directly at the hardware level, rather than at the software level, in a safer and less attackable way.

4.1.2 Challenges

The following are among the main challenges to be addressed in this area:

- *Hardware Security* — In analysing hardware security issues (*Hardware Security*) one has to consider various aspects, such as: (i) the implementation technology used; (ii) the hierarchical abstraction level considered (logic blocks, IP-core, chips, plates, systems, etc.); (iii) the various types of components used (processors, memories, input/output devices, sensors, actuators, interconnect networks, custom devices, devices with reconfiguration capacity, etc.); (iv) the application domain (automotive, industrial, consumer, etc.); (v) the complexity of the system (integrated, mobile, personal, server, cluster, HPC, etc.).
- *Hardware Trust* — Security issues should be considered at all stages of the life cycle of a hardware device (*Hardware Trust*): from design to man-

[4] `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5753`
[5] `https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715`

ufacture, from testing (both at the end of production and field) to decommissioning.

- *Length of life cycle of hardware devices* — Except for very special cases (such as FPGA-based systems, with or without partial dynamic reconfiguration mechanisms), the *operational life* of the hardware is typically much longer than that of the software, which can be periodically updated, even remotely. Hardware can also pose security problems beyond the end of its operational life, as discarded components and devices can be attached to extract stored data or used as counterfeit devices. While in the first case there are obvious data protection problems, in the second case, in addition to the already mentioned safety problems, there may be security problems, as well. For example, security issues may come from the use of a device, assumed to be of last generation, but in reality of a previous generation that was known to contain some vulnerabilities, which have been eliminated in the latest releases of the same family of products.

- *Vulnerability tolerance* — As noted above, hardware vulnerabilities, regardless of their nature, can only be corrected by modifying the design and are therefore bound to remain permanently in the devices. To continue using vulnerable devices safely, it is necessary to develop architectural solutions capable of *tolerating* the vulnerabilities by preventing their exploitation by malicious attackers. Several different solutions can be considered, depending on the type of vulnerability and the level of criticality of the system that uses the devices. By way of example, there may be: (i) solutions based exclusively on software and aimed at preventing malicious attackers from exploiting known vulnerabilities. This is the solution adopted, in the case of Meltdown and Spectre, by many operating systems that are modified to prevent the exploitation of certain functions; (ii) solutions in which, in a way conceptually similar to smart cards, the affected devices are "confined" in *protected* (trusted) zones and are allowed to run only secure code, developed and loaded in protected and guaranteed environments, making it impossible to inject the malicious code that could be used to launch attacks of any kind; (iii) solutions based on the interaction of appropriate combinations of different components, such as processors, FPGAs, Smart Cards, dedicated hardware devices; (iv) solutions aimed at tolerating *byzantine* behaviour [50] in the case of complex systems with many interacting devices.

- *National Technology* — The need to develop a national technology will be discussed in the conclusions of this volume (chapter 9). Here it is important to note that, when setting up a "national" production of hardware devices, the entire production chain must be trusted (and therefore de-

veloped in protected environments): from the design process (the people involved, design support tools, IP core providers) to the production, testing, installation, and maintenance processes. Careful planning and management would ensure the project's viability at a cost that is compatible with Italy's financial resources.

- *Certifications* — In the case of hardware certifications, it should be pointed out that, with respect to the vulnerabilities analysed above, the limitations resulting from the difficulty (or impossibility, in many cases) of measuring the level of resilience of a device towards a certain type of attack should be taken into account. *Design errors*, such as those that make Meltdown and Spectre attacks possible, are extremely difficult to identify and no certification of the processor security level would be able to certify their absence. Identifying a "well-known" *trojan hardware* is theoretically possible, although it is both costly and time-consuming. This type of analysis could not, however, guarantee the absence of any unknown trojans. It is possible to measure a device's resilience to *side channel attacks*, if quantity and quality of the resources used in the attack are defined in advance. For certifying the impossibility of *physical attacks*, it is necessary to define accurate models of the behaviour of the target technology with respect to the means of attack, such as current injection, light, laser, electromagnetic sources, etc. Models will then have to be developed at different hierarchical levels of abstraction (electric, logical, RT, system) in order to integrate them into simulators capable of assessing the resilience of the devices and the effectiveness of any countermeasures against this type of attack.

- *Root causes analysis of a vulnerability* — In case of discovery of a successful attack, understanding whether the vulnerability that made it possible is ultimately attributable to hardware can be very complex and tracing it back to the root cause can be even more complex. The difficulty in identifying design errors that made Meltdown and Spectre possible is emblematic.

4.1.3 Objectives

In order to address the challenges summarised above, it is necessary to implement a set of actions aimed at attaining the following objectives:

- *Awareness and training* — (i) awareness among policy makers and stakeholders of the severity of the threat and of the significance of the issues associated with hardware security, including from an economic point of view; (ii) actively raising the awareness of whomever, at the national level, is involved in various ways in the design, production, and testing

of hardware systems, through the set of actions and projects extensively illustrated in sections 6.2 and 6.3. In this regard, it should be pointed out that it is necessary to act at the university level, within the courses aimed at training hardware designers: the aspects of *Hardware Security and Trust* are nowadays almost completely absent in the Italian university panorama. However, it is also necessary to have refresher courses for designers operating in the *Design Center* throughout the country, and for whoever uses FPGA components in the most diverse architectures and applications.

- *Specialist laboratories within the Competence Centers* — Similarly to what already happens in many other countries, departments focused on *Hardware Security and Trust* should be created within the to-be-instituted Competence Centres in cybersecurity (considered in section 2.3). In particular, actions should be undertaken in order to create specialised laboratories within the *National Centre for Research and Development in Cybersecurity*, focused on research, development, and technology transfer, capable of providing the following to both public and private national stakeholders:
  - Analyses, qualitative and quantitative evaluations, measurements of resilience to physical attacks of hardware systems, at all levels of abstraction, for the various types of components, and for the variegated complexity of systems;
  - Analysis of the impact on security of different technologies, from the so-called "emerging" technologies to established microelectronics and packaging technologies;
  - Support for the *National Evaluation and Certification Centre* in its various phases and for the different types of certifications discussed in section 6.5;
  - Support to policy makers in the drafting of rules relating to security issues arising from the disposal of hardware equipment;
  - Advice on security issues in the management of all phases of the life cycle (definition of requirements, procurement, design, production, testing, analysis, etc.) of hardware infrastructures.
- *Support to the CERT network* — Establishing a close collaboration with the network of national CERTs to support them in all phases of vulnerable *root causes analysis*.
- *Development of "national" vulnerabilities-tolerant architectures* — Developing national architectures capable of guaranteeing pre-defined security levels, even in the presence of hardware devices containing vulnera-

bilities of varying nature, known and/or not yet revealed. The proposed solutions should be adaptable to the criticality of the target systems.

- *Support to "national" productions* — Following the definition, by policy makers, of "national" productions considered strategic for national security and those to be found, instead, on the foreign market, the Laboratories mentioned above must provide the necessary support for the implementation of the relevant security policies.

4.2 Cryptography

In the area of communications security, encryption is the basic technique to ensure secure information exchange by guaranteeing the indecipherability of messages. It is one of the fundamental mechanisms for data protection and identification. It now used pervasively, for example, when we connect to our bank via the web, disable the device to immobilise our car or when we use ATMs, credit cards, smartphones, and even keys for coffee machines. New technologies like the *blockchain* (presented in section 4.6) are also based on encryption techniques to ensure the integrity and security of transactions.

It is well known that, in recent years, the number of vulnerabilities of encryption systems has increased considerably [15, 69, 7]. Encryption-based attacks, once considered possible only by government agencies, are in fact now part of the standard hacker skill set, as demonstrated by the presence of various types of hacker training sessions and technical presentations on cryptographic attacks in latest editions of Black Hat[6,7,8] and DEFCON[9,10].

The security of a cryptographic system is not only dependent on the ways different algorithms are combined and implemented, but it is also strongly linked to the security of the algorithms themselves. Systems which were considered inviolable just a few years ago are now considered insecure. For instance, it has been proven that it is possible to compute collisions for cryptographic hash functions such as MD5 and SHA1 and, consequently, any digital signatures based on these functions can be falsified [69, 70]. The introduction of quantum computers will undermine standard encryption systems such as RSA; it is

[6] https://www.blackhat.com/us-16/training/crypto-uses-and-misuses-how-to-use-cryptography-properly-and-attack-those-that-dont.html

[7] https://www.blackhat.com/us-17/training/schedule/index.html#beyond-the-beast-a-broad-survey-of-crypto-vulnerabilities-57601483747943

[8] https://www.blackhat.com/eu-17/training/crypto-attacks-and-defenses.html

[9] https://www.youtube.com/watch?v=lTngMxmymX4

[10] https://www.defcon.org/html/defcon-25/dc-25-workshops.html

therefore of paramount importance to study *post-quantum* algorithms, capable of withstanding technologies that will likely be available in a few years.

Finally, it is necessary to highlight how the hardware that executes the cryptographic algorithms constitutes, in fact, the last line of defence: if an attacker corrupts the hardware, all the mechanisms introduced to make the software safe (at any level) may prove to be useless. Even in the presence of the best cryptographic algorithms, a hardware that is not adequately protected, regardless of the context in which it operates, can constitute the weak link in the chain, becoming an easy access door to the system, its functions, and its data.

Cryptographic systems must therefore be be set up correctly, in order to ensure their robustness, with regard to both algorithms and to their software and hardware implementation; this section highlights the main challenges and lines of research in this area.

4.2.1 State of the art

In recent years, many companies have adopted an "imaginative" approach to cryptography, by developing proprietary systems that have been regularly violated. One such example is represented by the automotive protection systems (see, for instance, [36, 75]). These failures have brought about a fundamental change, with the increasing adoption of standard cryptographic systems. However, as we have pointed out, in many cases is not easy to choose and configure the cryptographic mechanisms in order to provide the desired guarantees. Research on cryptography has produced excellent results since the 1970s, but the growing pervasiveness of cryptography requires us to face new challenges. New solutions need to be provided to ensure that the theoretical security of cryptographic algorithms is preserved from their implementations and that they remain secure over the years even in the face of revolutionary technologies, such as quantum computing.

Security of cryptographic systems Recommendations on the correct use of cryptographic systems are regularly issued by important bodies such as the *National Institute of Standards and Technology* (NIST)[11], the *European Union Agency for Network and the Information Security* (ENISA)[12], the *PCI Security Standards Council*[13], the *Agence nationale de la sécurité des systemes d'information* (ANSSI)[14], and the *Bundesamt für Sicherheit in der Information-*

[11] `http://csrc.nist.gov/groups/ST/toolkit/key_management.html`

[12] `https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/algorithms-key-size-and-parameters-report-2014/`

[13] `https://www.pcisecuritystandards.org/document_library`

[14] `http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf`

stechnik (BSI)[15]. Nevertheless, translating the recommendations into secure configurations and implementations is not always immediate. Public and private initiatives such as Better Crypto[16] and Cryptosense[17] are trying to fill in the gap between the theoretical recommendations and their practical implementation.

Postquantum encryption The*European Telecommunications Standards Institute* (ETSI) has set up a working group[18] and published a White Paper[19] on the possible impact of the quantum technologies on current IT security solutions. In 2013, the European Commission funded the PQCRYPTO project (*Post-quantum cryptography for long-term for long-term security)*[20] on these issues. NIST has recently issued an international call for tenders[21] for encouraging the design and development of asymmetric cryptographic systems that are resistant to cryptanalytic attacks performed with both quantum and conventional computers and that, at the same time, can interact with existing protocols and communication networks. In Italy research on post-quantum cryptographic systems has focused on solutions that use codes for error correction [52, 8, 55].

4.2.2 Challenges

The exponential increase in attacks made on systems that adopt cryptographic solutions has highlighted the need for a systematic analysis of the applied encryption algorithms, i.e., how a cryptographic system is created and configured. There is extensive literature on cryptographic protocol analysis, at the *logical* level of message exchange (e.g., [5, 17, 30]) and specific protocol implementations have been analysed (see, for instance, [14, 13]), but it is necessary to devise systematic and repeatable solutions to the problem of building and configuring secure cryptographic systems.

- *Security of existing cryptographic libraries* — To understand the level of security of applications it is necessary to analyse the security of the cryptographic libraries and APIs used. In fact, in many cases it is not possible

[15] `https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile`

[16] `https://bettercrypto.org/`

[17] `https://cryptosense.com`

[18] `http://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography`

[19] `http://www.etsi.org/technologies-clusters/technologies/quantum-safe-cryptography`

[20] `http://cordis.europa.eu/project/rcn/194347_en.htm`

[21] `http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents.html`

for a developer to understand whether the use of a certain cryptographic mechanism can provide the security guarantees required by the application. Likewise, it is not possible for the end user to understand the level of cryptographic security of an application. A case in point is represented by home banking apps: The user must trust the developers and has no visibility with respect to the actual level of protection. It is therefore essential to perform a systematic analysis of standard libraries and to develop tools and techniques to assess the cryptographic security level of applications. An accurate monitoring of "typical" cryptographic errors is also required in order to prevent future attacks. This will make it possible to move towards a certification of cryptographic systems based on the recommendations of the international bodies mentioned above.

- *Security of a cryptographic algorithm as part of a hardware/software system* — Cryptographic algorithms are typically built in complex ecosystems that, if poorly configured or implemented, could compromise theoretical security. Recent attacks have shown that it is very important to pay attention to the system as a whole. The KRACK [74] attack on WPA2 shows how a protocol error can completely compromise the security of data parameters in input to cryptographic algorithms. Some vulnerabilities of *Java keystore*[22] that allow one to extract keys and cryptographic certificates used by applications written in Java are illustrated in [33]. An unsafe implementation of the key generation for RSA encryption is described in [58]; for some devices on the market, it allows to determine the prime factors and therefore to completely break the cryptographic scheme. As far as traditional encryption is concerned, it is therefore of fundamental importance to investigate the security of cryptographic systems as a whole, rather than investing in the search of new cryptographic algorithms.

- *Post-quantum encryption systems* — The robustness of the main asymmetric cryptographic systems currently used to digitally encrypt and sign data and communications is based on the difficulty of solving, in a computationally efficient way, the problems of integer factorisation and extracting discrete logarithms. However, these systems are increasingly at risk of decryption due to the growing computing power available. In 1994, P. Shor [66] introduced an algorithm, specifically designed to be run by a quantum computer, that can solve the problems of integer factorisation and extracting discrete logarithms much more efficiently than the equivalent algorithms designed for conventional computers. When the first quantum calculators will be available, as their ability to factor integers

[22] CVE-2017-10345 and CVE-2017-10356 `http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html`

into prime numbers will be much faster than that traditional computers, any encryption system that uses keys of practicable size will become vulnerable, and therefore practically no longer usable [59]. Considering the growing development of quantum technologies for electromechanical and optical systems, it is easy to anticipate the introduction, within a few years, of quantum machines with computing power in line with theoretical forecasts.

A recent report by the Global Risk Institute[23] states that there is a

> One in seven chance that the basic tools of public key encryption will become obsolete by 2026, with a 50% of of this happening by 2031.

It is therefore extremely important to define alternative *post-quantum* schemes that can guarantee an adequate security margin even in the face of quantum processors.

- *Quantum cryptographic systems* — Unlike post-quantum cryptographic systems, quantum cryptographic systems create cryptographic primitives based on the properties of quantum mechanics. Quantum cryptography represents an important area of research developed by S. Wiesner [76]. One of the main the challenges of this discipline is undoubtedly its feasibility in practice. However, interest in this technology is always increasing and there are now several companies that that develop and market systems based on quantum cryptography. Among these we have IDs Quantique (Geneva, Switzerland)[24], MagiQ Technologies Inc. (Boston, MA, USA)[25], and QuintessenceLabs (Canberra, Australia) [26].

- *Homomorphic cryptographic systems* — The most complex challenge is using and analysing encrypted data directly on the cloud: today it is first necessary to decrypt them or move them to local systems, without taking full advantage of the capabilities offered by the cloud. There are new approaches that would solve this problem, such as *homomorphic scratch* by C. Gentry [38], which allows users to work on encrypted data, obtaining the same results as the same operations performed on plain text data. These techniques permit running applications on data stored in the cloud without ever having to decrypt them. Unfortunately, these techniques are computationally very complex and therefore remain of purely

[23] `http://globalriskinstitute.org/download/a-quantum-of-prevention-for-our-cybersecurity-1-pdf/`

[24] `https://www.idquantique.com/`

[25] `http://www.magiqtech.com/`

[26] `https://www.quintessencelabs.com/`

theoretical interest. Experts predict that in the future homomorphic encryption implementations of practical interest will be available for use in concrete scenarios.

4.2.3 Objectives

The main objectives to be pursued are

- to develop tools and techniques to (i) assess the level of cryptographic security of cryptographic applications, libraries and APIs; (ii) monitor typical cryptographic errors in order to prevent future attacks; (iii) investigate "applied written analysis" techniques capable of circumventing the security guarantees of cryptographic algorithms. All this in order to prepare new quality certifications of cryptographic systems.
- To advance the current state of cryptoanalysis of systems based on mathematical problems other than integer factorisation and extracting discrete logarithms. Design new cryptosystems whose security level is accurately quantifiable, in relation to both quantum and classical computers. Investigate the feasibility of post-quantum cryptosystems on general purpose and/or dedicated computing devices.

At the national level, the main objective of this area remains the establishment of a *National Cryptography Laboratory*, as established by the DPCM Gentiloni. This laboratory will have to face the fundamental challenge of understanding where our country will have to invest in cryptography, launching projects of national importance. The important issues to be considered are: (i) the risks and opportunities for the development of *national encryption algorithms* and (ii) how to deal with the emergency related to the arrival of quantum computers.

4.3 Biometry

Digital identity verification is an essential element for the security of IT and non-IT systems. The importance of digital identities is evidenced by the fact that their theft is one of the most widespread digital crimes. In addition, the theft of a legitimate user's digital identity is often the first step used by hackers and criminals to undertake very complex attacks.

Traditional methods for the recognition of individuals are based on keys, tokens, identity documents and passwords. These approaches, although still valid, are about to show all their limitations in terms of safety and security and, above all, usability. In fact, there are more and more common devices with touch-screens or, more generally, with interfaces that do not rely on traditional keyboards.

For this reason, in addition to the authentication tools mentioned above, biometric recognition technologies that assess physical or behavioural traits of the person, such as fingerprints or faces, are rapidly spreading. Through accurate acquisition sensors, biometric systems digitise a user's biometric trait and create a representation, called a *template*, which summarises the unique and constant characteristics of the specific individual.

The template is specially designed to be effective and efficient in subsequent comparisons. In an initial recording phase, called *enrollment*, the template is stored in a document or archive. During the subsequent recognition steps, the template acquired from a person undergoing verification is compared with stored templates. The biometric system decides whether the recognition is successful using a measurement of similarity or difference between the template and the archived one.

Biometric traits cannot be lost, they are difficult to share, are not prone to theft and guarantee excellent results in recognition accuracy. These features are leading to an increasing use of biometric systems in several operational contexts, such as the control of physical and logical access to data, applications and tools (including computers and mobile phones), and the intelligent monitoring of environments.

The performance of a biometric system can vary considerably depending on the biometric trait used and the level of cooperation required from users. The choice of the biometric trait to be used for specific applications is based on an accurate analysis of operational and security requirements, taking into account the laws on the protection of personal data.

4.3.1 State of the art

Biometric technology, by automating the passport screening process through automated kiosks, helps to make the task of law enforcement agencies easier when identifying passengers. In the banking sector, biometric methods such as fingerprints, irises, voice, palm veins pattern, and behaviour, alone or in a combined way, are used to block accounts and repress fraud. Biometric applications are also present in the judiciary system and many important innovations in identity management have arisen in this area. Today, the biometric applications used by police forces are truly multimodal: fingerprints and facial and voice recognition play a fundamental role in improving public security and in finding wanted persons.

Furthermore, on the assumption that "identification provides a basis for other rights and give voice to those who have no voice", the *World Bank Group* has launched projects and initiatives to use biometrics to ensure targeted services and assistance (medical care, education, ...) in developing countries.

Biometrics have already been the subject of many European projects in the various Framework Programmes that have followed one another over the years, up to the current H2020. Some examples are *Tabula Rasa*[27] project, which involved twelve partners. focusing on the vulnerabilities of biometric systems; the BEAT[28] project, aimed at standardising the current experimental protocols in order to ensure the repeatability of experiments on the basis of scientific and technological advancements in all biometrics-related areas; the PROTECT[29,30], project, oriented towards research on possible emerging biometrics; the IDENTITY[31] action oriented towards the exchange of researchers active in this area.

4.3.2 Challenges

The main challenges concern, in particular, the following aspects:

- *Behavioural Biometry* — The so-called *Behavioural biometrics* have always existed, but have been poorly considered for their limited identification capabilities and high implementation costs. The hardware innovations in recent years have made it possible to build very sophisticated, low-cost sensors and install them in the most advanced devices.
- *Improvement of acceptability and usability* — Biometric technologies are often perceived as being excessively invasive, difficult to use, or dangerous for privacy, e.g. due to the risk of template theft.
- *Interoperability* — Current biometric systems use different acquisition sensors and recognition algorithms. Implementation and maintenance of biometric databases and complex information systems therefore require the adoption of interoperability management techniques. This theme becomes particularly important with the development of new forms of authentication.
- *Personal data protection* — We must ensure the protection of templates through the joint use of encryption and biometrics, using erasable biometrics as well.
- *Homomorphous classifiers* — It is necessary to create homomorphous classifiers, able to work therefore directly on encrypted templates, borrowing the necessary technologies from homomorphic encryption.

[27] `https://ec.europa.eu/programmes/horizon2020/en/news/eu-funded-project-take-biometric-security-systems-next-level`

[28] `https://www.beat-eu.org/`

[29] `http://cordis.europa.eu/project/rcn/202685_en.html`

[30] `http://projectprotect.eu/(BES)`

[31] `http://www2.warwick.ac.uk/fac/sci/dcs/research/df/projects/identity/`.

4.3.3 Objectives

The main objectives of the project include:

- Building appropriate datasets for all biometrics deemed "mature" and making them available, scalable, and usable as common references for security validation.
- Developing metrics to validate biometric systems against key criteria such as usability, resistance to sophisticated attacks aimed at replicating biometrics or behaviours of an individual, interoperability, costs, and performance.
- Starting experimentation on the definition of behavioural traits to be used in behavioural biometrics that are at the same time biometric and secure, as they cannot be replicated.
- Developing "usable" technologies in order to increase the commercial implementation of biometric systems with particular reference to acquisition techniques that are non-contact and at a greater distance.
- Developing techniques for accessing multiple databases and exploiting other comparison methods, managing multimodal fusion methods in a flexible way on the basis of the available biometrics.

4.4 Quantum Technologies

The development of *Quantum Technologies*, over the last two decades, has created the foundations for a new scientific and industrial revolution. In particular, the application of quantum technologies will represent a *game-changer* in strategic areas such as secure communications and novel computing paradigms (*quantum computing*).

Fundamental developments to create intrinsically secure communication systems are in progress using quantum cryptography, in particular the quantum distribution of cryptographic keys (*Quantum Key Distribution*, QKD), which, by using the quantum properties of light, allows for the detection of attacks and violations of the communication channel in real time, thus guaranteeing transmission security. The QKD generates secure encryption keys, shared only between the transmitter and receiver and unknown to third parties, through the transmission of single photons via conventional and unprotected communication channels (e.g., fibre optic or in free space). The cryptographic keys, whose security is guaranteed by the laws of physics, can then be used to encrypt mes-

sages between two users, or for other cryptographic protocols, see [39, 64] and ETSI[32].

Quantum technologies are strategic for this country and it is therefore fundamental that Italy strengthens its scientific and technological capacity in this sector in order to limit, if not eliminate, its dependency on foreign countries and companies in such a strategic field. In the short/medium term it is unlikely, due to its high costs, that QKD will be used by private citizens. The expected groups of users of this technology are, rather, government, diplomacy, security, defence, health, financial institutions, banks and multinational companies. Many of these potential users act at a global level and, therefore, their interest in this technology will grow proportionally to the development of QKD systems on a global scale.

It is, therefore, important to perform field trials of the new, intrinsically secure, communication technologies based on the principles of the quantum mechanics, and to connect them with the most advanced cyber-security and data protection techniques. The project is very ambitious and not without risk, but it offers the possibility of carrying out research which might have a significant technological and economic impact in the near future. The objective is to exploit, to the maximum potential, the specific skills and foundational results of Italian research, to promote the transition from *quantum science to quantum engineering*, and to develop the quantum technology required by the country.

4.4.1 State of the art

Experimental QKD networks using optical fibres were built in various areas in different continents, for example in Vienna[33], Tokyo[34], and in China. Of particular relevance is the current Chinese project[35], for the construction of a 2,000 km QKD link from Shanghai to Beijing, supported by a QKD ground-to-satellite link to reach extremely distant areas. QKD links in optical fibre have already been used during the elections in Switzerland[36], for the secure transmission of voter information, during the Football World Cup 2010[37] and in Australia[38] for government communications. The applicability of QKD systems to existing

[32] "Quantum Safe Cryptography and Security: an introduction, benefits, enablers and challenges", ISBN 979-10-92620-03-0 – `https://docbox.etsi.org/workshop/2014/201410_crypto/quantum_safe_whitepaper_1_0_0.pdf`, 2014.

[33] `http://www.secoqc.net/html/technology/network.html`

[34] http://www.uqcc.org/QKDnetwork/index.html

[35] `http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7607012`

[36] `https://www.newscientist.com/article/dn12786`

[37] `https://phys.org/news/2010-06-world-cup-physics-thwart-hackers.html`

[38] `https://www.computerworld.com.au/article/278658/`

optical fibre networks has been demonstrated in [24], and recently QKD *point-to-multipoint* connections have also been established in optical fibre networks. Today commercial products or industrial prototypes are available for the implementation of QKD *point-to-point* systems in optical fibre. These systems are produced by both small-medium enterprises and large companies such as, for example, ID Quantique SA (Switzerland), QuantumTech (China), Toshiba Research Europe (UK) and QuintessenceLabs (Australia).

Many European countries have launched ambitious research programmes to transform laboratory prototypes into commercial products. In the UK[39], the government has invested GBP 270 million in a five-year programme, with the goal of reaching 1 billion in funding in the long term, for the further development of quantum technologies and their transfer to the industry. Research programmes have also been launched in the Netherlands[40] (EUR 135 million for a 10-year programme), in Germany[41] and outside Europe, primarily in China and the United States.

In Italy, the research in this field is prominently recognised on an international level. In particular, recall the collaboration between the INRIM and the CNR for the creation of a quantum communication backbone across the country (project Q-SecGroundSpace, in progress), and the collaboration between the University of Padua and the ASI that led to the first quantum communication via satellite [78, 73].

Thanks to the impetus provided by the European *Quantum Flagship* initiative, a national plan is under development to promote the transition from quantum science to quantum engineering.

4.4.2 Challenges

The main challenges are related to the design, implementation and experimentation of a communication infrastructure, which exploits the QKD technology on a global scale, to support critical services such as financial transactions, telemedicine, industrial control systems, and energy control systems (*smart grids*).

QKD *point-to-point* connections in optical fibres will be limited to maximum connection distances of the order of a few hundred kilometres, despite the planned improvement of single photon devices. For transmissions over longer distances, it will be necessary to develop *quantum repeaters*[42], instruments which are currently only available as laboratory prototypes. In the short-term we envisage that a QKD network on a global scale can be achieved with the

[39] `http://uknqt.epsrc.ac.uk/`

[40] `https://qutech.nl/investmentquantumtechnology/`

[41] `http://www.qutega.de/en/home/`

[42] `http://quantumrepeaters.eu/quantumrepeaters.eu/index/`

exchange of cryptographic keys over relatively small distances (from a few hundred to a few thousand kilometres) using optical fibres and exploiting *trusted nodes* to switch from a *point-to-point* optical link to another, coupled with QKD connections in free space via satellite for exchanging the cryptographic keys over intercontinental distances.

The challenges, therefore, concern the development of QKD platforms on optical fibres, QKD space platforms and their interconnection for ensuring secure intermodal operations on a global scale. In addition, as noted in ETSI's White Paper, it is fundamental the interaction between quantum and classical cybersecurity techniques to guarantee the continuity of the protection levels.

For QKD *point-to-point* connections over optical fibres, significant technological developments have already taken place, and the first commercial solutions are already available. However, for the widespread use of this technique for the protection of the communications, it is necessary to validate the reliability of this technology "in the field" and to develop an accurate and reliable instrumentation which can be used by the operators of telecommunication companies, and not only in research laboratories.

Current commercial QKD systems use single photon devices (sources and detectors) which can be improved in terms of performance and the quantum protocols implemented. For example, single-photon detectors are currently being developed in laboratories, based on semiconductor or superconducting technologies, with high temporal resolution and low background noise, which seem fundamental to ensure a high (effective) *bit rate* over long distances.

Satellite QKD systems are an advanced research topic, and important scientific and technological efforts are still needed to make them commercially usable. It is necessary to verify their experimental feasibility, to develop the measurement technologies and infrastructure needed for the satellite-earth QKD links, and to investigate the satellite-satellite QKD connections. At the same time, an *intermodal trusted node* to connect the QKD *free-space* system with the QKD fibre optic system and to demonstrate the interoperability of the two QKD systems also needs to be developed.

In parallel, in order to respond to a primary requirement of the emerging quantum communications industry, it is also necessary to develop standardisation criteria and control techniques to ensure the traceability of single photon measurements and the security of their protocols.

Finally, for both terrestrial and free-space quantum communications it will be fundamental to identify the best type of information encoding to maximise efficiency and security. In the last few years, in addition to the standards based on single photon and binary coding of quantum information (generally in the polarisation of the photon), new proposals have been developed, based on classic light pulses and continuous variables [47] and on a coding deriving from the spectral and temporal degrees of freedom [60]. These alternative schemes have

great advantages in terms of high efficiency and selectivity of detection (using homodyne type systems). They also offer the possibility of manipulating the information in a deterministic way in advanced protocols such as teleportation, *entanglement swapping* and quantum repeaters [34], of which the project will study possible implementation schemes. It is therefore essential to complement existing sources and detectors with the new ones that make it possible to exploit the best information coding schemes in the various sections of a global quantum communication system.

4.4.3 Objectives

The project aims to achieve the following objectives and sub-goals:

- The development of an Italian QKD experimental platform on a global scale based on optic fibre and free-space QKD systems:
  - Designing, commissioning, and testing a QKD system in optical fibre;
  - Developing a prototype transmitter and receiver for a QKD system via satellite;
  - Studying coding schemes based on discrete and continuous variables with an adaptive configuration, based on channel characteristics;
  - Integration of components in photonic circuit platforms;
  - Designing, developing, and testing a *trusted node* for exchanging secure encryption keys between fibre optic and free space links;
  - Developing a metrological infrastructure for the characterisation of single-photon devices in QKD systems.
- Integration and interaction between legacy cyber-security and QKD techniques.
- The development of new schemes and technologies for the next generation QKD systems:
  - Designing and testing of innovative single photon sources and detectors;
  - Studying and developing information coding schemes for QKD systems that allow maximum efficiency and security;
  - Designing and implementing advanced quantum communication protocols such as *quantum teleporting, quantum repeaters* and *entanglement swapping*.

4.5 Artificial Intelligence

Artificial intelligence and machine learning have been playing a fundamental role in many applications, ranging from medical image analysis to conversational agents. However, less attention has been paid to the ways intelligent agents can be used maliciously and to the new, possibly severe, emerging threats. It is needed to address the issue of the equilibrium that is likely to be established between attackers and defenders, and to look for a systematic approach to services protection that is not simply based on tracking attackers to fix security issues. While it looks hard to come up with a single general recommendation, there are cases in which the appropriate pushing on the establishment of the right battlefield in the never-ending competition between attackers and defenders has a strong consequence on the evolution of security policies. As an example, the development of spam filters in the case of large centralised systems typically benefits from the expertise gained in facing similar attacks, as well as from the large amount of data that can be used for training the spam classifiers. The field of artificial intelligence has flourished by exhibiting the growing capabilities of challenging human intelligence mostly with classic games, like chess and Go, and linguistic games.

To some extent, the field of computer security can be regarded as a rich collection of challenging games, where we must clearly arrange things in such a way as to favour the defender. This is opening new exciting scientific challenges where, from one side, the expertise in more traditional computer security can contribute towards setting up the "game" properly so as to play on a biased battlefield. We need to devise guidelines to bring models of AI containment into the world of cybersecurity with the purpose of developing software and procedures for checking the vulnerabilities

The research and the development of security policies related to the rising impact of artificial intelligence is likely to be reflected in the dynamic establishment of an equilibrium between attackers and defenders. A systematic approach to security, which is increasingly required to protect services, cannot simply track the attackers and patch up security issues, but must be driven by a long-term view on the evolution of the interactions of intelligent agents, where we must place the defender in the more advantageous battlefield.

4.5.1 State of the art

At the end of the eighties, D.E. Dennings published a seminal paper [29] where he framed security as a truly AI problem, mentioning before others the role of expert systems and statistical approaches to learning to deal with security issues. The DARPA IDS challenge and, immediately after, the KDD Cup IDS de-

sign challenge[43] opened the doors to a new field at the crossroad of computer security and artificial intelligence. Years later, at the ACM SIGKDD international workshop on "Privacy, Security, and Trust"[44] an important list of contributions was selected that covered a wide range of AI approaches. Other relevant KDD workshops took place in 2010 and 2012, while more or less at the same time the field of "Adversarial Machine Learning" was definitely established at the ACM Workshop on Artificial Intelligence and Security [44]. A fundamental step towards new foundations on the field of computer security with emphasis in artificial intelligence is the "Manifesto from Dagstuhl Perspectives" on 2013[45] while the field has also quickly spread to traditional AI and ML events like ICML 2014 (workshop on Learning, Security, and Privacy) and AAAI 2016 (1st Artificial Intelligence for Cyber Security workshop).

The presence of the subject in both computer security and artificial intelligence events is clearly indicating that the state of the art of most important approaches relies on the establishment of tight links between the traditional communities of computer security and on artificial intelligence, particularly machine learning. Interestingly, while there are currently visible signs of quick evolutions of symbolic models that are based on formal methods and knowledge representation to machine learning approaches, the field in general is likely to make additional progress in the near future. In particular, there are problems of computer security where one can benefit from the appropriate integration of symbolic and sub-symbolic models of computation (see, for instance, the IJCAI-2018 tutorial on "Neural-symbolic Learning and Reasoning with Constraints" by Luis Lamb et al.[46]

4.5.2 Challenges

As already pointed out, models based on artificial intelligence are, in fact, transversal to most modern security systems. Interestingly, the dramatic growth of network-based services is gradually exposing systems to new threats that very much depend on a new population of algorithms that adopt intelligent techniques. The time has come in which intelligent agents can concretely be designed to fool other agents charged with protecting critical information, and even to deceive humans. The vulnerabilities of AI systems are somewhat different with respect to the traditional software vulnerabilities. As we will see in more detail in section 5.3, the learning algorithms can be deceived to drive learning agents to undesirable states. This poisoning of the learning environment

[43] http://www.kdd.org/kdd-cup/view/kdd-cup-1999

[44] https://www.springer.com/gp/book/9783540784777

[45] http://drops.dagstuhl.de/opus/volltexte/dagman-complete/2013/dagman-v003-i001-complete.pdf

[46] https://www.ijcai-18.org/tutorials/

can take place in different contexts, including computer vision and natural language understanding. Here are some novel challenges connected to different approaches to artificial intelligence, that lead to the birth of truly new security problems:

- *Threats from automatic text generation and fake news* — Machines can autonomously generate and post text on the internet with such quality that it can hardly be distinguished from human-produced content. This can give rise to critical issues, including the spread of fake news and calls for the development of associated agents purposely designed to discover misleading information and capable of identifying the presence of automatic generation; see section 3.4.
- *Poisoning of learning environment and chatbot induction to offensive tweets* — The explosion of conversational agents might gradually increase their impact on the interfacing of nearly any service for personal and business purpose. While the protection of services on the internet already has a solid scientific and technologic tradition, the exposition of novel services based on chatbots opens the doors to a truly new scenario where the construction of security-by-design schemes seems to be very difficult to reach. *Tay*, an artificial intelligence chatbot designed by Microsoft, caused quite the controversy when it began posting racist and sexist tweets, thus forcing the company to shut the service down just a few hours after its launch. This suggests that the release of similar bots requires reasonable levels of security. An open problem with modern chatbots that are driven by machine learning techniques is that humans or other machines can poison the learning environment by strongly biasing the interaction. This is what happened with *Tay*, which was artificially stimulated in the framework of an offensive conversation, from which it learned to reproduce similar behaviour. This is a good example from which we can see the importance of an appropriate integration of knowledge-based reasoning schemes with learning, that can potentially reduce the risk of similar a degeneration.
- *Adversarial Learning* — The explosion of multimedia information also comes with new threats for humans and machines. The emerging watermarking security brings new challenges to the design of watermarking systems. The recent trend regarding the automatic generation of images/videos does not only bring forth issues related to the presence of counterfeits, but it opens the doors to the automatic creation of non-real visual environments. As an example, from a given book of faces one can construct new faces where some features are emphasised and modified, to the point where even the age and sex can be changed. Interestingly, other learning systems can be designed with the purpose of

distinguishing faces that are automatically generated from those coming from a book of real faces. In the last few years, this duality has led to the development of the new field of adversarial learning. As an example, in addition to the more traditional security issues connected with car information systems, the emerging field of autonomous driving leads the way to an impressive range of possible threats. The most noticeable example is the possibility of changing a few bits in images to significantly change the associated category and the corresponding actions.

- *Identity detection* — When enabling AI systems in different facets of ordinary life, we must realise that we are dramatically nearing the scenario that Alain Turing had foreseen at the dawn of computer science. In many cases, the set up of appropriate security policies does require the disclosure of the identity of the agent offering the service. This is interwound with the inherent structure of most models of intelligent behaviours and seems to be a never-ending challenge that must properly be faced.

- *Social engineering attacks* — Phishing attacks are assuming a truly new form with attackers that can fully exploit the trend of interacting by means of social networks. The growing amount of personal information that is spread in different sites makes it possible to gather users' profiles that can be very useful to set up deceiving policies with malicious objectives. Social engineering attacks are now able to employ malicious agents able to impersonate people and acquire critical information. This is becoming a very serious threat, considering the growing capability of intelligent agents able to mimic the human voice, which allows them to issue deceiving calls with malicious purposes. Although in a different field, a somewhat similar scenario is that arising from swarm attacks where autonomous robots cooperate with and monitor large areas, potentially also coordinating actions.

- *Automation of vulnerability discovery* — In the initial phase of computer security studies, scientists and engineers were are mostly concerned with the identification of attacks that were carried out by hackers. As time goes by, AI and ML methods are depicting a new scenario in which we prospect the automation of vulnerability and hacking discovery, that is clearly accelerating the search for fallacies and pitfalls of computer systems, as well as the possibility of automating human-like denials of service.

Web spamming – The action intended to mislead search engines into ranking some pages higher than they deserve.

4.5.3 Objectives

In order to face the above mentioned challenges, in the following passages we list some recommendations and objectives to pursued:

- *Diffusion of ethics principles* — Scientists in the field of artificial intelligence should constantly bear in mind the importance of the ethical side in the development of their ideas and on their concrete implementation. In particular, they should promptly share the risks connected to harmful applications.

- *Biasing the battlefield* — Studies in computer securities can benefit from the progressive set up of conditions that favour the intelligent agent involved in defence with respect to the one which carries out attacks. An important foundational issue is that of studying the conditions and the modalities to push the establishment of a stable bias towards the defender.

- *Development of symbolic / sub-symbolic systems* — While there is no doubt regarding the crucial role of machine learning in the spectacular development of new applications and useful services, the black box nature of many of the underlying models offers at the same time quick methodologies for the construction of systems to prevent security attacks, and new fallacies and pitfalls that can be used by attackers. This calls for the promotion of foundational studies aimed at shedding light on these models with the purpose of better facing the rising threats of learning-based systems.

- *Diffusion of security risks coming from AI* — Policymakers, scientists, and engineers should collaborate to face the malicious uses of AI at different levels and should also be involved in the construction of appropriate policies of diffusion of awareness on the risks connected to these novel threats.

- *Bridge with traditional approaches* — Some mature approaches to computer security should be properly adapted to the novel framework of transactions regulated by intelligent agents.

- *Promotion of Openness* — Scientists are strongly encouraged to promote and explore open models of diffusion of AI and ML culture by emphasising pre-publications and favouring approaches that privilege safety and security. This should be joined with the promotion of a culture of responsibility associated with the nature of scientific discovery.

4.6 Blockchain and Distributed Ledger

Bitcoin and other cryptocurrencies fill the pages of newspapers every day. They are based on *Distributed Ledger Technology* (DLT), also known as *blockchain*, of which cryptocurrencies represent just one of the possible applications.

DLT – Distributed Ledger Technology – Technology based on a distributed database called a *blockchain*, which contains transaction blocks. Thanks to public key cryptography and consensus algorithms, it can guarantee its irreversibility and integrity (over time).
It employs a naturally decentralised approach and does not require intermediaries to validate or authenticate transactions. Each node in the network maintains its own copy of all transactions and the nodes work to verify the validity of a new transaction through a process called *consensus*. Each of these transactions is sent to all nodes within the network to be verified and grouped into transaction blocks marked with a timestamp.
There are two main categories of the DLT: *unpermissioned* (open) and *permissioned* (regulated). The first is maintained by public nodes and is accessible to anyone (Bitcoin is the best known example). The second (for example, the Corda platform) involves only authorised nodes and thus facilitates faster, safer and cheaper transactions.

The aim of this chapter is to analyse opportunities, risks and challenges of adopting a national infrastructure, which provides the Italian system with the technology for an informed and controlled use of DLTs.

4.6.1 State of the art

The future of financial infrastructure report published by the World Economic Economic Forum in 2016[47] forecasted that 80% of banks would start DLT-based projects by 2017. More than 24 countries and more than 90 central banks are investing in, or discussing, the adoption of DLTs. In the last 3 years alone, more than 2,500 patents on DLTs have been registered and more than USD 1.4 billion invested. Multiple countries and both national and international organisations are analysing the opportunity to support the development of DLTs as a basis for public and private sector applications. These include the Singapore Monetary Authority (MAS)[48], the Hong Kong Monetary Authority (HKMA)[49], the Bank of

[47] www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf

[48] http://www.mas.gov.sg/~/media/ProjectUbin/Project%20Ubin%20%20SGD%20on%20Distributed%20Ledger.pdf

[49] http://www.hkma.gov.hk/media/eng/doc/key-functions/finanical-infrastructure/Whitepaper_On_Distributed_Ledger_Technology.pdf

England (UK)[50] [51]. The European Parliament [52], and the European Central Bank [53] have recognised the many regulatory challenges and opportunities offered by DLTs.

In Italy, according to Assinform (the association of Confindustria that brings together ICT companies), in 2017 a growth of +2.3% is expected throughout the entire ICT market, driven by the most important components related to innovative ideas, principally concerning DLTs [54]. Conservative estimates also forecast that investments in DLT-based projects will exceed EUR 2 billion in 2017.

In addition to this, the interest of various scientific and technical communities is evident. (W3C - Blockchain Community Group, OASIS - ISITC Europe, ITU-T, Committee, ITU-T, Committee. ISO/TC 307)[55].

4.6.2 Challenges

A national DLT (open or regulated) opens up challenges related to research, innovation and progress in various fields: from monetary control to digital rights management and patent protection; from possible innovations in e-voting to smart contracts, and to support the tracking of supply chains, as well as the introduction of other scenarios aimed at creating innovative public services. The most important challenges include:

- *Extension of DLT beyond financial applications* — The original and currently predominant use of the blockchain is related to cryptocurrencies. As currency applications dominate the discussions surrounding DLTs, and represent the most mature and well known applications, they are influencing the development of innovative application-based technologies. However, the accessability of DLTs with low management costs compared to transaction value and the availability of a register capable of storing information in a permanent and secure way would extend the possibilities of using this technology beyond the boundaries of financial applications. The challenge in this area is not to create a legal, national digital currency, but rather the management and control of a national DLT (potentially

[50] http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx

[51] http://www.bankofengland.co.uk/research/Documents/onebank/cbdc.pdf

[52] http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

[53] https://www.ecb.europa.eu/paym/initiatives/shared/docs/dlt_task_force_mandate.pdf

[54] https://www.confindustria.ud.it/upload/pagine/Industria%2040/la%20posizione%20del%20sistema%20confindustria/Confindustria%20Digitale%20-%20Assinform%20-%20%20Lug%202016.pdf

[55] https://www.iso.org/committee/6266604.html?view=participation

permissioned) to support non-financial applications and forms of "near money" (e.g., local currency, debt securities) with low costs and with high accessibility and usability. In order for this to be possible, it is important to identify forms of certification that require less computational and storage capacity and therefore allow limiting energy consumption, which in the case of bitcoin is becoming too expensive.

- *Analysis and protection from illegal transactions* — Beyond the new possibilities and challenges that they present, DLTs also introduce new security issues. Transactions are by themselves semi-anonymous (especially within unpermissioned DLTs) and this has introduced wide-ranging illicit markets, which live in the deep/dark web (see box on page 17). In addition, the lack of authentication (both strong and weak) has introduced large-scale financial fraud (in addition to exchange sites, fake lotteries, false online sales and so on, which have been subsequently closed down) The challenge in this field therefore includes the analysis of the traffic (which for all intents and purposes can be classified as Big Data) and the identification of the hidden and illegal areas, both through forensic and machine learning tools, and through a technical-economic study of the financial market based on unpermissioned DLTs.

- *Modelling, analysis and verification of smart contracts* — Smart contracts are programs automatically executed by the network of nodes that controls a cryptocurrency. The consensus mechanism used to ensure the consistency of the blockchain also ensures that the execution of these programs is correct (a crucial property, given that smart contracts are typically used to transfer currency). One of the main research challenges of smart contracts concerns their modelling, analysis and verification. This type of research is particularly innovative and urgent, since the inadequacy of currently available tools (both practical and theoretical) undermines the security of the entire smart contract ecosystem, as evidenced by the many successful attacks[56,57] against Ethereum, the most widespread platform that supports them.

- *Regulatory and process issues* — Another point to consider is the need to ensure that rules are properly enforced. Judiciary and law enforcement agencies should have the means to act in case of abnormal DLT behaviour due to technical problems or misuse due to human error or malice. There are also other challenges related to the integration with other public administration systems, to standardisation and design of the procedures by which individuals and companies can access the DLT, and

[56] `http://blockchain.unica.it/projects/ethereum-survey/attacks.html`
[57] `https://www.coindesk.com/understanding-dao-hack-journalists/`

the building and governance of the DLT physical infrastructure, which should be considered a critical infrastructure for our country.

- *Advent of quantum computers* — A final challenge is to carefully study the impact that quantum computers will have on DLTs. This technology is based on conventional cryptography and the advent of quantum computers could corrupt the information contained in the ledger or violate its confidentiality.

4.6.3 Objectives

The activities related to the development of a national DLT pursue five objectives, different in both scope and impact.

- *DLT as an infrastructure to provide public services* — The creation of a permissioned Italian DLT that supports smart contracts, where all those public services that need regulatory control and high guarantees in terms of data/functions protection can be migrated, e.g. all administrative applications that require the legal registration of documents, such as notarial deed, business, cadastre, and protocol registers. The expected spill-over effects include the improvement of these services in terms of reliability, security, transparency, and accessibility, and a reduction in costs compared to traditional methods of storing and processing information.

- *Electronic voting* — Experimental organisation of internal elections through blockchains, in compliance with the rules set by the GDPR (Section 6.1.1). European legislation does not specify detailed arrangements for general elections in the Member States, but there is an interest in using electronic voting in accordance with the constitutional principles of electoral law (universal, equal, free, secret and direct suffrage). The objective is to test electronic voting systems based on blockchain and smart contract technologies, characterised by relatively low costs and high transparency and security levels, in order to evaluate the possibility of their use in real-world environments.

- *Digital Right Management* — The blockchain can be used to record sales, loans, donations and other transfers. All transactions are witnessed and agreed upon by all users without the need for a trusted third party. In addition, manufactured articles cannot be transferred unless they are legitimately owned. Identifying copyrighted or patent-protected works and resolving related disputes is an extremely important legal activity. The development of the blockchain in this area can allow for multi-territorial licensing policies and further guarantee the rights of creators and purchasers by providing effective dispute resolution mechanisms, such as

tariffs, licensing conditions, and concession/withdrawal of management rights. Buyers could therefore, for example, check to see if they are buying legitimate copies of music or videos.

- *Supply Chain* — The supply chain is the basis of today's production and distribution processes on a global scale and comprise various activities, including: contract management, payments and invoice issuance, labelling and packaging, logistics and transport. In this regard, solutions must be developed that allow for the use of DLTs for efficient, reliable and transparent tracking of interactions taking place in a supply chain, with the aim of significantly reducing costs due to poor performance and errors of current management processes, often partially entrusted to human operators. The proposed solutions will also represent an important deterrent for illegal activities, as the transactions reported in the ledger will be relatively easy to use for anti-fraud and anti-counterfeiting checks. As a result, the entire supply chain will become more efficient and safe, with important impacts on management costs, authentication guarantees of end products and the possibility to reliably reconstruct the entire history of any product, from its origin to its retail distribution.
- *Crypto-exchange analysis for control of illegal activities* — The monitoring and analysis of transactions in existing unpermissioned DLTs can help in detecting fraud and illegal behaviour. Specifically, the objective is to provide the governmental authority with tools capable of detecting illegal activities such as money laundering, tax evasion, illicit trafficking (for example, drugs, weapons, human beings), and ransomware payments. In addition, the reliability level of *miner nodes* should be checked in order to estimate the possibility of dangerous situations for DLT integrity.

CHAPTER

5 Technologies to protect

This chapter analyses *technologies to protect*, such as wireless communications, Cloud, IoT, industrial Control Systems (ICSs), and robots, which are playing a key role in the digital transformation process in the PA and in industrial sectors, becoming increasingly pervasive.

Their protection and increased resilience to cyber attacks is therefore a priority and should be pursued along two directions: on the one hand by inserting appropriate security measures into legacy systems which employ outdated technologies, and, on the other hand, pursuing the concept of *Security by design* in the next generations of technologies. Designing and developing these technologies with the concept of cybersecurity at the heart of their development can become a competitive advantage for Italian companies.

In the end, the chapter deals with the protection of algorithms, which are the actual driving engines of all digital technologies: the poisoning of *ground truth* of machine learning algorithms or the alteration of algorithm code for managing data replicated on different servers are examples of threats that must be managed in a resilient cyberspace.

5.1 Wireless communications and 5G

The wireless and mobile nature of communications in cellular systems has historically implied the need to protect data in transit. This activity has been duly tackled over the course of previous generations of cellular systems, with solutions that, though gradually and through various evolutions, have now reached a level of protection considered satisfactory (it is not a coincidence that over the last ten years there have been no significant developments in this field).

However, the 5G network includes not just the mobile network, but also landlines, supplying services arranged end-to-end and with performance parameters that are by far better than the actual solutions. Moreover, it has a wider ecosystem that involves many players and more complex relationships and business opportunities; it sets new requirements (e.g., relative to the IoT environment and to highly reliable and low-latency applications); it is characterised by increased heterogeneity and dynamism, radically new technical solutions, among which the "softwarisation" of network functions and the splitting of the network into "slices".

Such functions are today at least partially implemented in hardware, also by virtualising current physical devices. A network implemented in a software can be split into slices, each of which supplies, end-to-end, a virtual autonomous network to a subgroup of users, able to meet specific needs of a specific scenario/case of use, in a comprehensive framework, in which different organisations coexist within a network (multi-tenancy).

This set of features deeply changes network security issues.

5.1.1 State of the art

The first generation systems did not specify any solution for the protection of communications, but the GSM (second generation) already explicitly introduced solutions for user authentication and encryption at the radio interface level. GSM security solutions proved to be extremely preliminary and insufficient for a number of reasons, starting from the total inadequacy of the cryptographic techniques adopted. The COMP128 algorithm, although not initially made known to the scientific community, following a nefarious *security by obscurity* model, was in fact "broken" in 1998 in a very short time after its (presumably involuntary) disclosure. In addition, the GSM did not provide any mutual authentication, i.e., it was not limited only to authentication of the user terminal against the network, but it also allowed the user to verify the authentication of the base station which led to attacks based on *rogue base station*, i.e., fictitious base stations, controlled by attackers able to intercept communications. Finally, no security solution in the core network part of the GSM had been standardised.

The following third generation, UMTS, was probably the generation in which the greatest progress was made in terms of security, both in terms of quality of the solutions adopted and in terms of interventions in the many subsystems involved. First of all, 3G systems adopted cryptographic algorithms from the AES (Advanced Encryption Standard) family, which are much more secure and still state-of-the-art. The application of cryptographic techniques has also been significantly improved, both through the explicit differentiation of encryption keys (and techniques) from those of data integrity, and through the introduction of privacy features and protection for users from attacks to recognise

and trace location (location privacy). 3G systems have also solved the problem of rogue base stations by providing a highly effective mutual authentication technique. Finally, they have also defined security solutions at the network core and related reporting.

In line with the progress made in 3G systems, the fourth generation, 4G, made a number of improvements and, above all, explicitly adopted the theme of *security by design*, i.e., has considered security aspects since the outset of the architectural specification phase, organising the overall architecture into five explicit domains (and proposing, where necessary, specific algorithms to provide the relevant protection services):

- *Network access security* — Radio Interface Protection;
- *Network domain security* — Protection at the level of information exchange and signalling between network components;
- *User domain security* — Mobile terminal security and interface between USIM and device;
- *Application domain security* — Application service-level protection;
- *Visibility and configuration of security*: — Techniques to check if (and which) security aspects are active.

5.1.2 Challenges

In view of the considerable progress made in recent generations, with regard to the security of cellular networks and briefly summarised above, it is legitimate to wonder if security should also play an important role in 5G networks, or if the bulk of the work has already been done. The answer is that, despite the significant improvements made to cellular networks over previous generations, the new emerging requirements in 5G systems and, above all, the radical change of perspective that characterises the 5G network (which includes not only the cellular network but also the fixed network), bring about new problems that must be faced. While the previous 2/3/4G systems were well defined a priori and their requirements clearly listed, homogeneous and relatively stable, as well as the related security and data protection solutions, the emerging 5G systems are strongly focused on the integration between heterogeneous technologies, partitioning (slicing) and virtualisation of network infrastructures, and on the support of extremely diversified services. They are also no longer exclusively dedicated to human users.

We therefore believe that the security architecture of 5G systems should be extended to cover (at least) the following aspects:

- *IoT and heterogeneous Terminals* — One of the most significant differences between traditional cellular systems and the new generation 5G consists in the availability of services no longer necessarily reserved for terminals managed by humans, but extended also to *Machine-Type-Communication* (MTC). This will lead to the spread of terminals with extremely disparate characteristics (in terms of cost, energy consumption and complexity of implementation) so that a "one-size-fits-all" security model, which had characterised security solutions in previous generations, may no longer be adequate. For example, security mechanisms designed for mission-critical services may not be applicable at all in a context of IoT devices, where network sensors have very few computational and energy resources and where data transmission is sporadic. 5G systems will therefore not only be called upon to support cryptographic techniques (for authentication or encryption of data) that are extremely variable in terms of robustness and level of protection, but, above all, it will be necessary to develop both new models for the management of such heterogeneous security solutions and new trust models.

- *Signalling Traffic* — In addition to the need to identify differentiated security solutions for the services offered, that are also more flexible than the 'unique" solution currently offered by 4G systems, another important aspect related to MTC services is that signalling traffic could even be more dominant than data traffic. This is followed, for example, by the need to develop solutions capable of recognising (and defending oneself from) attacks aimed at saturating the network resources dedicated to signalling traffic; a well-known bottleneck in the case of MTC services is the access to the RACH (Random Access Channel) which could become critical in case of simultaneous and malicious activation by a botnet (see box on page 48) IoT.

- *Virtualisation and softwarising of network functions* — A fundamental feature of the 5G network is the migration to virtualised systems, in which network functions are no longer provided by specific physical devices, but made of software and run on virtual machines or containers, in Cloud environments. These functions are routinely routed or dynamically shifted where necessary and also relocated to the edge of the network to meet the low latency requirements of critical 5G applications. This new paradigm of network function virtualisation brings with it numerous new security challenges. On the one hand, the physical separation of these functions into separate devices is no longer applicable as a security measure and it is necessary to identify separation and isolation solutions for functions in a virtualised environment. It is in fact necessary to think about solutions for the security of the environment in which

the network functions will be performed, that are independent for each "slice" into which the network will be divided. On the other hand, the ability to perform network functions on virtual machines leads to the need to identify (and possibly adapt them from the IT world) solutions for authorisation, management and secure migration of software images that implement these virtualised network functions. Finally, of course, virtualisation does not only bring "problems", but also offers new opportunities, for example to develop virtual network functions dedicated to security itself, i.e., it offers the possibility of rethinking security functions in a perspective of *Security-as-a-Service* (SEaaS) and automation of network protection functions.

- *"Flexible" security* — The 5G network will be characterised by the need to have extremely flexible security solutions and to be adaptable to the specific (different) scenarios considered. For example, services with very low latency characteristics will require security solutions which in turn require very low latency and therefore (ultimately) flexibility in the ability of the network to activate the most suitable security solutions for a given scenario. In addition, the problem of flexibility in security management must go hand in hand with tools to simplify the management of network security, allowing rapid adaptation to new services and needs, not only regarding network operation, but also the security solutions proposed.

5.1.3 Objectives

The following objectives should be pursued in relation to the contexts described above:

- *Secure implementation and management of virtualised and logically segmented networks* — This objective includes specific tasks, such as:
  - secure techniques of virtualisation and, above all, of isolation for the network "slices" and for the functions in charge of such segmentation, including hardening of the network functions, their authentication and integrity management, and so on;
  - the need to "secure" the emerging platforms, architectures, technical solutions and languages (e.g., P4) for the software programming of network functions. Research has so far focused mainly on the identification and development of highly flexible solutions, with unfortunately limited attention paid to the significant security issues involved in these new approaches;
  - integration of security in the management and orchestration services of the network functions, with particular attention to the

programmability of heterogeneous security solutions for heterogeneous services and the assessment of the security status of the network through special visualisation techniques;

  - development and control of virtualised modules to implement network security features such as firewalls, deep packet inspection and traffic flow analysis, threat mitigation and isolation techniques based on the *software-defined networking* paradigm, programmable and relocatable network probes for the detection of modern sophisticated intrusions, such as advanced persistent threats - APT (see box on page 53), which use lateral movements, etc;

- *Security of 5G network scenarios dedicated to IoT services* — The security of 5G network scenarios to support IoT must be guaranteed by developing and experimenting:

  - lightweight cryptographic solutions, designed for sensors and actuators with very low cost and very low energy consumption, and their integration in the IoT communication protocols emerging in mobile environments (NB-IoT, LTE-M), in Low Power WAN unlicensed contexts (for example LoRaWan) and in short range contexts (RFID, NFC, BLE, etc);
  - access control solutions for large-scale IoT scenarios, based on flexible management of authorisation attributes and capable of operating in multi-tenant environments;
  - algorithms for the scalable analysis of data generated by sensors, also able to identify anomalies and traffic patterns that can be traced back to coordinated large-scale attacks, for example, driven by Mirai botnets.

- *Data protection in new technologies and new communication environments and "wireless sensing"* — Research must be focused on data security and data protection related to emerging communication technologies and contexts and *wireless sensing*, including:

  - the analysis of security aspects (including protection from Jamming and Denial of Service attacks) in dense network contexts, and for beamforming technologies, massive MIMO, mmWave, and integration or improvement of security solutions in 3GPP and IEEE 802 protocols and technologies – in the latter case, as it is certainly an integral part of the future 5G networks (e.g.,802.11ax/ay, etc);

– the study of new physical cryptography techniques (including quantum techniques), able to exploit the unique characteristics of the radio channel, their integration in the 5G architecture and experimentation in real systems;

– the use of wireless technologies (and waveforms) not only for communication, but also for personal and environmental security, through the development and testing of radio signal-based solutions for pattern recognition and protection of environments from physical intrusions.

5.2 Cloud

The Cloud paradigm undoubtedly offers great economic benefits and significant flexibility in the use of resources; however, the problem of security in Cloud environments is one of the major concerns for companies and public organisations that want to move their services, applications, and sensitive data to the Cloud, as evidenced by numerous analyses such as, for example, the Gartner reports[1,2] and IDC[3].

An IT system is considered to be secure based on the correctness of its *security policy*, i.e., the set of rules to ensure an appropriate level of protection, and its ability to apply this policy correctly. The Cloud paradigm is based on the principle of delegation to a third party of every type of service (infrastructure, maintenance of data, and applications). From the point of view of a security expert, this delegation makes part of the system inaccessible and therefore impossible not only to verify the correct application of the policies envisaged, but, in some cases, simply specify with due precision the policy to be adopted.

Cloud Service Providers (CSPs) can adopt advanced security procedures and mechanisms. However, from the user's point of view (*Cloud Service Customer* – CSC), it is normally not possible to know the details of the policies implemented in these systems. Basically, the *security policies* of the CSPs are inaccessible for users and, above all, they cannot be monitored. In this context, ensuring that local regulatory constraints are respected can also become an insurmountable problem.

[1] `https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/`

[2] `https://www.gartner.com/doc/3328818/survey-analysis-cloud-adoption-trends`

[3] `http://www.oracle.com/assets/cloud-inhibitors-3257526.pdf`

5.2.1 State of the art

At the European level, the ENISA has played an important role in recent years, providing Cloud stakeholders with a detailed overview of the benefits and security risks associated with migrating their applications and data to the Cloud[4].

At the Community level, references to *Cloud security* are increasing in strategic documents and in the major 2016 and 2020 research framework programmes [5]). In this respect, the *Data Protection, Security and Privacy (DPSP) European cluster* has as its objective to maximise the results of European research projects in the area of *Cloud security*[6]. Added to this is the specific European Commission action aimed at making the best use of the potential of Cloud Computing: *Pre-commercial Procurement Cloud for Europe*[7].

At the Italian level, this action translates into the *Three-year Plan for Information Technology in the Public Administration 2017–2019* by AgID[8], whose objective is a coordinated rationalisation of the whole PA and in which the development of an evolutionary strategic model of the Cloud of the PA[9] is envisaged. In particular, this plan provides for the following: (i) the identification of a set of physical infrastructures of the PA that should become *National strategic Hubs* (PSN); (ii) the definition of a public service pathway to the Cloud, also with resources provided by the PSNs and by the *Public Connectivity System* (SPC); (iii) the definition of a qualification process of PSNs and other CSPs. This strategic plan must be accompanied by appropriate strategies for the provision of professional and security services[10].

In this direction, the SPC project *Security Cloud*[11] has as its objective the provision of *Security-as-a-Service* (SEaaS) services according to the Cloud Computing paradigm. These include the management of digital identities, remote digital signatures, services to support administrations in the prevention and

[4] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

[5] http://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-179-EN-F1-1.PDF

[6] https://eucloudclusters.wordpress.com/data-protection-security-and-privacy-in-the-cloud/

[7] http://www.agid.gov.it/agenda-digitale/innovazione-del-mercato/gara-pre-commerciale

[8] https://pianotriennale-ict.italia.it/

[9] https://www.agendadigitale.eu/infrastrutture/come-cambia-il-cloud-della-pa-dopo-il-piano-nazionale-e-delle-regioni/

[10] http://www.agid.gov.it/notizie/2017/04/05/workshop-agid-csa-italy-spc-cloud-sicurezza-del-sistema-cloud-computing-nazionale

[11] https://www.ictsecuritymagazine.com/articoli/spc-cloud-le-best-practice-cloud-security-sistema-cloud-computing-italiano/

management of cyber incidents and in the analysis of vulnerabilities of information systems. Currently, only a limited number of CSPs offer SEaaS[12].

Another fundamental aspect is how to let different Clouds communicate in a secure way, in order to allow the integration of services offered by different subjects, thus creating *Cloud federations* able to provide new and richer functions. The *SUNFISH*[13] project addresses this issue by proposing an architecture and related enabling technologies to create Cloud federations that are *secure by design* and democratically administered. One of the main instances in which SUNFISH has shown its effectiveness concerns the safe integration of the private Cloud of the Ministry of Economy and Finance and the Ministry of Interior for the reliable and confidential management of payrolls of Armed Forces personnel.

Finally, at an international level, the *Cloud Security Alliance* (CSA) is an organisation dedicated to defending and disseminating *best practices* that can enhance the security of Cloud environments[14]. Since 2010, the CSA has promoted the first professional certification program for the acquisition of Cloud security expertise.

5.2.2 Challenges

The main challenge for the correct adoption of the Cloud lies in the construction of methodologies and techniques that allow to define and verify the level of security of an IT system that uses and integrates Cloud services.

It is important to highlight how through the information provided by CSPs (collected in public repositories, such as cloud28[15] and CSA STAR[16]) you can obtain useful data to build a security policy for Cloud, as shown by the results of recent European research projects dedicated to the topic, such as SPECS[17], MUSA[18], SLA-Ready[19] and SLALOM[20].

It is essential that CSCs should be able to choose between the services offered by the different CSPs in an unequivocal and well-informed manner where sensitive data are physically stored, in order to ensure compliance with the relevant laws. By way of example, it is necessary to allow those who manage sen-

[12] `http://www.crn.com/slide-shows/security/300083542/the-20-coolest-cloud-security-vendors-of-the-2017-cloud-100.ht`

[13] `http://www.sunfishproject.eu/`

[14] urlhttps://cloudsecurityalliance.org/

[15] `https://www.cloud28plus.com/`

[16] `https://cloudsecurityalliance.org/star/`

[17] `http://www.specs-project.eu`

[18] `http://www.musa-project.eu`

[19] `http://www.sla-ready.eu/`

[20] `http://slalom-project.eu/`

sitive data or take part in public procurement to choose between different offers, through a clear and quantitative evaluation of the services and guarantees of security and protection of the personal data offered. To be able to compare the security procedures and policies implemented by CSPs, or even more, the services offered by a third party that in turn uses Cloud services, the adoption of the Cloud paradigm becomes a key enabling factor. Therefore, the development of *security metrics* that allow to quantitatively evaluate a Cloud service offering, possibly enriched by *security benchmarking* procedures, that allow to evaluate the overall security status of a Cloud service by CSCs, represents one of the most important challenges from the user's point of view.

Similarly, there is a growing demand from the CSP for the need to take out insurance against cyber attacks. This is a demand that is difficult to meet, because of a *cyber insurance market* that is still immature due to difficulties in assessing both the *residual risk*, i.e., that which cannot be mitigated with appropriate security measures, and the damage suffered in the face of an attack[21].

The focus on the possibility of cyber attacks against CSPs has recently increased following the discovery of two serious vulnerabilities of modern processors brought to light by the *Meltdown* and *Spectre* attacks (analysed in section 4.1. These attacks allow a process to read the private memory of another process. In fact, within the infrastructure managed by a CSP, the sensitive data of a CSC could be read by another process, managed by a different CSC, with consequent loss of confidentiality of such data. Given the frequency of discovery of new vulnerabilities of this kind, it is necessary to work on solutions that can guarantee confidentiality even after the compromise of the Cloud infrastructure. An example of these solutions has been investigated under the SUNFISH project[22], where the *Secure Multi-party Computation* [23, 40] is used to distribute sensitive data over different Clouds in a Cloud federation, so that attacking a single Cloud is not enough to filter data.

MPC – Secure Multi-Party Computation – A class of protocols to manage message exchange between n processes, each of which provides data, unknown to others, to calculate a function $F(i_1, i_2 \dots i_n)$. Some of the processes can be malicious and work together to filter out data from others. An MCP protocol has the objective of correctly calculating F by ensuring that malicious processes do not become aware of the data provided by the correct processes. Many cryptographic distributed protocols (*voting, on-line auction*, etc.) can be considered special cases of MPC.

[21] `https://www.dimt.it/index.php/it/mercatoconcorrenzaregolazione/10466-9la-responsabilita-contrattuale-nella-gestione-dei-dati-nel-cloud-computing`

[22] `http://www.sunfishproject.eu/`

At the national level, the main challenge is to develop a *community Cloud* model, which allows interoperability between services developed for the PA at a national level (such as SPID, e-invoicing, etc.) and those already present at the local level in regional Cloud structures, properly supported by appropriate security services provided according to an SEaaS model. Such a community requires an infrastructure to securely integrate services offered by different Cloud services. A related challenge is therefore the further development of Cloud federation solutions along the lines of the objectives pursued by the SUNFISH project.

A further point to develop is a structured relationship with private subjects in order to ensure that their solutions (timely tested and certified) can also be integrated into the national Cloud. Therefore, there must be collaboration between the national and regional *service brokering* activities, and the different suppliers, with a structured process of validation and integration of services and security solutions with respect to the national Cloud.

Ultimately, the challenge that the adoption of the Cloud paradigm poses in terms of security, especially taking into account the Italian context, is to provide CSCs, both public and private, with tools that allow, on the one hand, to gain awareness of the risks that the Cloud introduces and, on the other, to have guarantees, security services and countermeasures commensurate with the effect produced by the threats introduced by this paradigm.

5.2.3 Objectives

With reference to the challenges to be addressed and summarised above, the main objectives to be pursued are set out below.

- To design and develop tools that allow CSCs to evaluate and compare the security services and policies implemented by CSPs, with respect to their own security requirements and current regulations on data protection and location, through the use of appropriate security metrics and *security benchmarking*.
- To define models and tools for the drafting of insurance policies for CSPs, capable of estimating the *residual risk* and evaluating the damage suffered in the event of a cyber attack, taking into account the different impacts that failure to comply with a regulatory constraint or a specific security requirement have on the PA compared to a private organisation.
- To define safe Cloud federation models and tools that can reliably integrate services offered by different Cloud services.
- To develop solutions to guarantee the confidentiality of data on the Cloud even in case of compromise of part of the Cloud infrastructure.

- To develop an open-source *security service* that can be, through reuse, adopted and specialised by public bodies, and above all by Italian SMEs, allowing them to comply with regulatory constraints, such as those present in the GDPR (see section 6.1), which can have exorbitant costs when applied in small amounts to the use of services in the Cloud.

- Based on specific cases of use applicable to the PA, to develop demonstrators of the solutions identified to overcome the above mentioned challenges and, in particular, demonstrate how these can improve the competitiveness of the Italian Cloud, thus facilitating the development of innovative business.

5.3 Algorithms

An algorithm is a procedure defined by a finite series of elementary steps for solving a problem. The concept of the algorithm is fundamental with respect to software development: given a problem that you want to automate, programming essentially represents the translation or encoding of an algorithm in a program (which represents the logic of processing) through a language that can be interpreted and executed by a computer. It can therefore be deduced that algorithms are the basis on which automation and the ease of use in our daily lives are based.

A direct consequence of the central role of algorithms is the fact that they are also a high value asset that must be protected from cybernetic attacks, just like computing infrastructure and data. The problem is even more obvious when one considers the impact that automatic learning algorithms are having on everyday life.

Contrary to what one might think, algorithms are not immune to threats. An algorithm is nothing more than a function that receives a set of values (data) in input and generates others in output (called a *solution*) through the execution of a finite number of intermediate steps. An attacker may then attempt to compromise an algorithm by altering the input data and/or sequence of operations to be performed on such data. Below are some examples of application scenarios for which an algorithm attack can have serious consequences.

Most of the web applications that we all commonly use (e.g., current account management, household management, etc.) are implemented in a distributed and replicated way. The replication is, in fact, the technique mainly used to guarantee the availability of a service in the face of load variations (due to changing demands) and the possible presence of faults that would otherwise lead to a degradation of service quality and consequently of the level of user satisfaction.

In the paradigm of replication, the service is offered by multiple copies of the same service and the basic requirement is that this distribution be completely transparent to the end user. To this end, a customer interacts with a reply by means of reading operations (e.g. access to the balance of a current account) and/or writing operations that update the status of the reply (e.g. deposits or withdrawals from a current account).

In this case, an attacker may have an interest in compromising the availability of the service (he may want to make the service inaccessible) or the integrity of the managed information (he may, for example, alter the results of reading and writing operations). All this can be achieved through the compromise, by the attacker, of one or more instructions contained in the fragment of code that manages the operations, causing the behaviour of the service to deviate from the specifications and expectations. This type of attack is easily possible once the attacker has taken control of a replica. In the literature there are some solutions for the definition of replication algorithms tolerant to the presence of attackers who take control of some replicas (so-called algorithms tolerant to Byzantine or mischievous [50] agents).

Another application context in which algorithms represent a weak point is that in which they are based on *machine learning*; these kind of algorithms are at the basis of many applications that we all use daily and in which we often place considerable trust. For example, Facebook uses algorithms for machine learning for the recognition of faces in images; Amazon and Netflix analyse the tastes of customers (last things seen or purchased) to suggest products with them; Google uses machine learning algorithms in the field of translations and travel, suggesting a less busy route according to our habits and the places where we usually go on a given day of the week; Apple and Microsoft use machine learning to provide us with a voice assistant that can help us use a phone or a tablet with only our voice, perhaps when we are driving. Other companies are currently perfecting automatic driving by artificial intelligence methods. Recently, machine learning algorithms have also been widely used in healthcare for the study of patient data and patient records, to identify, for example, the people most likely at risk of contracting certain diseases, such as diabetes, or of facing heart problems.

In all these examples, the algorithm learns a certain behaviour that must be repeated based on the input data provided to it. It is therefore clear that the correctness of all these applications depends heavily on the correctness of the data on which the algorithm is trained. An attacker could therefore aim at compromising the data from which the application learns to induce incorrect behaviour; for example, improper driving in the case of self-driving or a deliberately incorrect diagnosis in the predictions applied to the health context.

5.3.1 Challenges

Ground truth – A set of data used to train machine learning algorithms, which are today the basis of multiple applications such as, for example, the recognition and classification of e-mail as spam or the recognition of a user's habits to pre-calculate and suggest optimised routes or targeted purchases.

Code injection – A technique that takes advantage of a vulnerability of a code based on giving a different data input to a program from that expected to induce it to execute specific code provided ("injected") by an attacker to modify the behaviour.

Privilege escalation – A technique that exploits the vulnerabilities of the code based on the exploitation of programming and/or configuration errors that allow an attacker to gain administrator privileges starting from a normal user account. With administrator access privileges, an attacker can take control of the entire system, such as altering stored data, changing procedures and rules for accessing parts of the system, stopping or changing parameters of running applications.

Among the main challenges to be solved from the point of view of algorithm protection, we can certainly mention:

- *Poisoning of ground truth* — Ground truth data is collected either automatically (e.g. by storing information about a user's paths in a completely transparent way) or manually (e.g. by asking the user to indicate which emails are considered spam). In both cases, these data are stored and an attacker may try to compromise the integrity of the data during the storage process. In addition, in the case of automatic data collection, these can be altered by compromising the sensor technology.
- *Exploiting vulnerability* — Each algorithm must be encoded in a programming language in order to be interpreted and executed by a processing system. The coding process of an algorithm is not error-free and often leads to the introduction of vulnerabilities (see box on page 10) which can become a gateway for an attacker. From the point of view of algorithm protection, two types of vulnerability exploitation are particularly relevant and must be taken into account: (i) code injection and (ii) the scaling of privileges.
- *Viruses and Malware* — Malware (see box on page 48), by entering existing executable code, act by modifying an already running algorithm or the information used by the algorithm, taking care to not modify the algorithm to hide the evidence of compromise and avoid creating suspicion.

5.3.2 Objectives

Below is a list of possible projects involving both a research component and an innovation component.

- *New approaches to code injection detection* — Discovering the presence of unwanted software is a very difficult task because intrusion techniques and programs themselves are constantly evolving and, to date, there is no valid general methodology. New approaches must therefore be investigated in such a way as to merge the results from different contexts such as anomaly detection, secure coding or static or dynamic code analysis into a single framework that guarantees flexibility and accuracy in the detection.

- *New approaches to make learning algorithms more robust* — Most machine learning algorithms currently used as automation support are not designed to be attack resistant. It is therefore necessary to think of an evolution of their design that makes them safer while preserving their attributes. This can be carried out both in the definition of new logics on which they are based and in the structural modification of the algorithms themselves.

- *New approaches to vulnerability assessment* — The objective of this project line is to develop new approaches also through the integration of existing technologies that take into account that threats to informatic security can come not only from intrusions into the company perimeter but also through the manipulation of the functional logic of expert systems by compromising algorithms representing the "core" of the applications.

5.4 IoT

IoT devices are now used in a wide variety of situations, including mobile devices (smartphones and tablets), home automation applications, industrial sensors and actuators (Industrial IoT – IIoT), transport (from automotive to rail, from shipbuilding to aeronautics and drones), critical infrastructure and Cyber Physical System (monitoring and control systems). The most recent investigations estimated up to 6 billion devices connected to the internet at the end of 2017, with a forecasted growth to 21 billion in 2020.

In general, the use of IoT devices makes it possible both to improve the quality of the services offered by the equipment they are inserted in, and to create additional, completely new ones.

IoT – Internet of Things – An expression that refers to the multitude of "things", or "objects" that, connected to the network and uniquely identified, are able to communicate with each other, or with other systems, without requiring any human intervention. Objects includes devices, equipment, plants and systems, and machinery in the most diverse fields of our daily lives.

IIoT – Industrial IoT – An IoT device used in the industrial field which has become particularly important following digitisation initiatives facilitated by the various development plans within *Enterprise 4.0*.

Like all networked systems, IoT devices face the problem of cybersecurity, which however, in this case, must tackle the new issues introduced by the peculiarities of the involved devices and by their typical usages. IoT devices have, in fact, a set of "physical" characteristics that make them peculiar both in the ICT panorama and among the hardware architectures analysed in section 4.1. These features include: low costs, low operating margins, reduced energy consumption, limited processing capacity in terms of both computing power and storage capacity, limited connectivity in terms of protocols and bandwidth. In addition, the devices used for the connection of remote sensors and actuators, as they are installed in the field and left for long periods of time, are more likely to be subject to physical attacks exploiting Side-Channel Effects (see boxes on page 81).

The spread of IoT devices and the new services they made available have significantly increased the so-called *surface of attack*, by actually introducing new vulnerabilities. Many applications, in fact, enabled by the IoT scenarios, open the door to totally new and largely unexplored vulnerabilities, which can expose users to particularly serious effects, if not prevented and treated in a specific way, as it was recently shown by the successful attacks that exploited, for example, IoT devices present in toys, vending machines, and in smart switches for home automation [79, 81]. This phenomenon is also particularly felt today in the industrial field where, thanks to the incentives made available by the various development plans of *Enterprise 4.0*, the diffusion of IIoT devices has reached very significant levels, as shown in section 5.5.

It is then necessary to highlight that discovering and disclosing a vulnerability in a *single* IoT device immediately translates into a vulnerability for *all* the equipment and *all* systems using that device.

In addition, when multiple IoT devices of the same type are used within a given system, a successful attack on that type of IoT device can result in the *byzantine* behaviour [50] of the system, with potentially dire consequences when the system is used in safety-critical applications.

Another critical issue is posed by IoT-based systems used in critical infrastructures: they in fact require high degrees of safety and security, and mostly have not been designed paying proper attention to the vulnerabilities introduced by the adopted IoT devices. Unfortunately, there is still today a lack of appropriate design methodologies for systems that use IoT devices and that, at the same time, must guarantee the levels of security required for the target systems and for their adoption within critical infrastructures.

It is also worth noting the growing interaction of insurance services with IoT mobile devices and sensors, which has two fundamental aspects: (i) the development of specific insurance products aimed at those who use IoT devices with respect to damage potentially done to third parties (examples include drones and self-driving vehicles equipped with IoT devices); (ii) the provision of traditional insurance policies with a "consumption" rate clause, with premiums and a modality related to quantities that can be measured in the field by IoT devices (for example, mileage actually travelled by car, or other aspects related to individual lifestyles). In Italy, the current integration of insurance services with IoT technology will enable insurance companies to meet the growing demand for highly personalised insurance products; however, this integration poses obvious problems in terms of protection of personal data.

5.4.1 State of the art

The analysis of the state of the art will be addressed by first considering the main aspects of the actions undertaken in the governmental sphere and then the main on-going research projects.

In the United States, the NIST has defined the programme for cybersecurity in the IoT (*NIST Cybersecurity for IoT Program*)[23], supporting the development and application of standards, guidelines and related standards tools to improve cybersecurity of connected devices and of the environments in which they are used.

In addition, the Department of Homeland Security published, in November 2016, the *Strategic Principles for Securing the Internet of the Internet of Things*[24] guide, which outlines a set of principles to improve the security in the design, production, and installation of IoT devices.

Finally, the Department of Technology and Innovation of New York City coordinated a research project in cooperation with public and private organisations, universities, and standardisation institutes for the production of guide-

[23] urlhttps://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

[24] `https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf`

lines on the implementation of IoT systems, whose use can have a potential impact on public spaces and goods[25].

In Europe, ENISA activated a programme for the development of guidelines on security of critical infrastructures based on IoT technologies in smart cars, homes, and cities.

The UK government launched the IoTUK[26] programme aimed at promoting the adoption of technologies and high quality IoT services in the field of health services, smart industries, and smart cities. The programme pays special attention to the security of services and systems, to their dependability and to data interoperability. In addition, it aims to promote cooperation initiatives between universities, companies, research centres, and start-ups.

In Asia, Singapore's government launched the *Smart Nation*[27] initiative, with the objective of improving the quality of life in urban contexts by way of IoT technologies. Concurrently, they started the *Singapore Cybersecurity Strategy*[28] programme, acknowledging that security plays a key role in ensuring a broad and effective implementation of the Smart Nation project.

In terms of research projects, among those funded by the European Commission, particularly significant are the USEIT[29] project, aimed at developing new encryption algorithms, policy languages, and tool security measures to ensure that users of IoT devices are guaranteed secure and confidential access, and the ANASTACIA[30] project that aims to create a trustworthy-by-design development framework to support all the phases of design and implementation of an intelligent and dynamic security monitoring.

5.4.2 Challenges

The main challenges to be addressed in this area include:

- *Modelling*— In the well established domains of system dependability and safety, accurate models of the main possible faults, errors, and failures have been developed and widely used worldwide. In addition, in several domains these internationally recognised and accepted models have found adequate acceptance in terms of de jure and de facto standards. Unfortunately, in the case of IoT devices, consolidated and accepted models of possible types of attacks and of their potential consequences are still lacking.

[25] `https://www.diffchecker.com/diff`

[26] `https://iotuk.org.uk/`

[27] `https://www.smartnation.sg`

[28] `https://www.csa.gov.sg/news/publications/singapore-cybersecurity-strategy`

[29] `http://www.chistera.eu/projects/useit`

[30] `http://www.anastacia-h2020.eu`

- *Correctness of physical quantities*— When IoT devices are used in the field, it is crucial to be able to measure a wide range of their "physical" characteristics, such as power consumption, temperature, supply voltage, workload, geographic location, etc. Plenty of architectural solutions based on a proper mix of hardware and trusted software exist and are widely adopted in complex IT systems. Unfortunately, they are not applicable to IoT devices, mainly due to their costs and complexity. In general, in fact, the drive to reduce the cost of the final devices implies that the protections at the device level are usually rather poor.

- *Abnormal behaviour* — In the case of architectures and IoT-based systems for industrial applications, "abnormal" behaviours induced by malicious attacks mostly do not manifest themselves as physical "faults". As a consequence, they may not be detected by the normal solutions adopted to monitor the system. More generally, it is necessary to study approaches and solutions to correctly interpret the interactions of IoT devices with their users and with other networked devices, based on heterogeneous and complex data, in order to develop efficient solutions for monitoring and anticipating attacks.

- *Holistic solutions*— Unfortunately, holistic cybersecurity architectural solutions compatible with the nature of IoT devices and with the critical level of the systems in which they are used are not yet available.

- *Software Updates*— Typically, when a software vulnerability is revealed, updates are made available within a short time, containing the changes (*patches*) made to overcome that vulnerability. Not installing these updates puts the system at serious risk, since its latent vulnerability, until then only known to experts, is now in the public domain and can be maliciously exploited by anyone. It is therefore clear that, if the involved software application is an integral part of an infrastructure, failure to update it could have catastrophic consequences on the infrastructure itself in the event of cyber attacks.

- *Hardware and Software Integrity* — In the case of systems using IoT devices with remote software upgrade capability and/or partial or total hardware reconfiguration capability (e.g., through the established use of FPGA-based devices) it is mandatory to be able to guarantee the integrity of software updates, of the reconfigured hardware portions, and their reconfiguration files.

- *Personal data protection and confidentiality* — Many of the IoT solutions available today or in the near future include sharing of information between users. This implies an exchange of data that may be detrimental to

the protection of personal data when implemented without proper protections and without an adeguate awareness of the users with respect to the data exchanged and their relevance.

- *Integration and trade-off between safety and security*— The use of IoT devices in industrial control systems and, more generally, in *safety critical systems* poses new challenges arising from the need to ensure, in parallel, adequate levels of safety and security, as highlighted in section 5.5.
- *IoT and 5G* — 5G networks will make it so available services are no longer necessarily reserved for terminals managed by human beings. They will also be extended to terminals with IoT devices, where the network sensors will be equipped with very few computational and energy resources and where data transmission will typically be sporadic. As analysed in detail in section 5.1, 5G systems, in order to safely manage IoT devices, will therefore need to support not only extremely variable cryptographic techniques in terms of robustness and level of protection, but also implement new models for the management of heterogeneous security solutions and new trust models.
- *Insurance risk assessment* — When dealing with insurance services, an important risk element is the difficulty of ensuring the security of IoT devices used to provide new services. Calculation of insurance risk models is made difficult not only by possible errors in real time probability estimations, for which reliable data are needed to translate estimates into consistent policies and premiums, but also for the assessment of the severity of events covered by cyber insurance policies. For example, it is difficult to quantify the economic losses or personal injury that new devices such as drones or self-driving vehicles could cause as a consequence of physical attacks to involved IoT devices.

5.4.3 Objectives

With reference to the challenges to be faced and summarised above, it is necessary to activate a set of projects that, in their globality, aim to provide adequate and sustainable responses to each of the challenges and, in particular, to achieve the objectives indicated below.

- *Modelling* — To develop appropriate models of possible attacks on systems using IoT devices. The consequences of the attacks should be analysed and described both at the *physical* (or *structural*) level, where the consequences are typically incorrect values of physical quantities detected from sensors and transmitted to the control system, and at the *functional* (or *application*) level, where abnormal system functionalities occur as a result of the above incorrect values.

- *Correctness of physical quantities* — To develop efficient solutions in terms of usability and costs for the verification of the correctness of the measured entities and of physical characteristics of IoT devices. In particular, the developed architectural solutions must support a hierarchical distribution of the trust chain, for instance by entrusting a "certified" (and therefore assumed "secure") PC or smartphone with the control of the security of the whole set of IoT devices connected to it.
- *Abnormal behaviours* — To develop platforms and monitoring systems to identify abnormal behaviour in IoT devices used to manage sensors and actuators. In particular, the proposed solutions must be able to:
  - extend the performance of current SIEM systems (Security Information & Event Management), widely used for the defence of IT systems, by developing at the IoT level (true end-point, in this case) hardware architectures charged with performing locally intelligent analyses of events that occurred to data, communications, commands, controls, etc. The results of such analysis should then be sent to the SIEM system;
  - execute locally, on the end-point, part of SIEM itself. This will practically require, on the one hand, considering the actual values of the signals exchanged with the sensors and actuators as events and, on the other hand, adopting effective and efficient machine learning techniques for the timely detection of anomalous behaviours;
  - perform monitoring, attack tracking, and attack anticipation for IoT systems, resorting to integrated approaches exploiting network traffic monitoring, device utilisation by end-users, interactions between end-user and devices, social network activities between users and devices;
  - perform analyses of data generated by sensors to identify traffic anomalies and patterns that can be traced back to large-scale attacks, such as the ones driven by Mirai-type botnets.
- *Holistic Solutions* — To define methodologies and tools for the design and development of IoT-based secure, distributed, and heterogeneous applications. In addition, to develop platforms for the secure and usable deployment of heterogeneous and dynamic IoT-based systems. The proposed solutions must be able:
  - to guarantee the fulfilment of confidentiality, authentication, protection and security requirements and to enable secure human-to-machine and machine-to-machine interactions; to ensure, when

needed, the requirements of usability, efficiency, scalability, dependability, and user-awareness;

  - to ensure measurable levels of data and information protection "at rest", "in motion", and "at use", in order to ensure both confidentiality and authenticity of end-to-end data transfer and the integrity and availability of the interconnection infrastructures;
  - to ensure the development, on the IoT side, of suitable hardware architectures compatible with today's most widely adopted standards on communication and storage capabilities;
  - to provide facilities and services to properly manage encryption keys; they should support the whole life-cycle of each key, as well as all the professionals involved in the implementation and usage of the management system;
  - to be usable by non-expert cybersecurity technicians, too;
  - to be applicable, after the necessary customisations, to any application and system using IoT devices.

- *Hardware and software integrity* — To properly adapt the solutions already widely adopted in other IT fields to the peculiar characteristics of remote IoT devices.
- *Certification and periodic review* — Adequate national procedures should be defined for certification and periodic review of IoT devices, according to their criticality inside the systems in which they are used.
- *Personal data protection and confidentiality* — We need to define architectures that fulfil the requirements in terms of the protection of the user's personal data from malicious access via IoT devices. In addition, the IoT devices used must ensure compliance with the requirements of the GDPR, introduced in section 6.1.1.

In addition, it is considered strategic for the country to achieve, over the next 3 years, the development of a holistic solution applicable to at least two "vertical" solutions whose security levels can be predefined and subsequently validated through the most advanced state-of-the-art approaches.

5.5 Industrial Control System

In the recent past, critical infrastructure operators have strongly supported the thesis that *Industrial Control Systems* (ICS), which include *Supervisory Control and Data Acquisition* (SCADA) systems, *Distributed Control Systems* (DCS) and

other systems, such as *Programmable Logic Controllers* (PLC), were intrinsically safe, since they were disconnected from public networks and therefore protected by the *air gap* between the control systems themselves and the corporate network. Consequently, they considered that there was no need to put any security mechanisms in place.

Nowadays the scenario has changed radically due to the high level of integration reached between *Information Technology* (IT) and *Operational Technology* (OT), so the myth of intrinsic security has been partly, if not completely, shattered. In fact, the introduction of information technologies in physical control systems, motivated by the reduction of costs and the improvement of their performance, has undoubtedly favoured the birth of a series of intelligent technologies, from smart grids to smart transportation and smart manufacturing. This evolutionary process, which brings new functionalities and services, has, however, at the same time, highlighted the need to increase the security and resilience of industrial control systems.

Among the aspects to be taken into account in the design and development of security solutions for industrial control systems, particular attention should be paid to the difference between the lifetime of an ICS and that of an IT system stem. Typically, in fact, while the life time of an ICS, based on technologies designed and developed for a specific domain, is in the order of 10-15 years, that of an IT component is much shorter, typically in the order of 3-5 years. This difference is an extremely critical factor when planning upgrades and maintenance for industrial control systems, due to the stringent availability and reliability requirements posed by these systems. The scenario presented shows, therefore, the need to address the security and reliability issues of industrial control systems combining *cross-functional* expertise, allowing to fully understand the possible implications of the installation and use of IT technologies on the operation of industrial control systems.

5.5.1 State of the art

Among the initiatives concerning the security of ICS systems, it is worth mentioning the publication by NIST of document 800-82 *Guide to Industrial Control Systems (ICS) Security*[31], which provides an accurate analysis of the typical topologies of such systems, and identifies possible security threats and presents countermeasures to be taken to mitigate the risks involved.

Another important initiative was the creation by the American government of a dedicated CERT: the ICS-CERT[32], whose task is to coordinate the efforts and initiatives of government and industry institutions to improve the level of secu-

[31] `https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final`

[32] `https://ics-cert.us-cert.gov/`

rity of the industrial control systems used for the monitoring and management of critical infrastructures.

In Europe, ENISA has published several studies on the security of industrial control systems, addressing issues such as: analysis of vulnerabilities and the exposure window of SCADA systems to attacks[33]; testing of the security level of industrial control systems[34]; certification of the security skills of professional figures working in the field of ICS/SCADA[35]; analysis of the level of maturity, from the security point of view, of ICS/SCADA systems used in critical infrastructure[36]; the identification of lessons to be learned from the assessment of security incidents involving SCADA[37]. The most recent document produced by ENISA on the security of industrial control systems was published in February 2017 and is a report on the analysis of dependencies of ICS/SCADA systems from communication networks[38].

Another initiative in the European panorama was the creation of a specific working group on Industry 4.0 and industrial control systems by ECSO[39].

5.5.2 Challenges

The following are among the main challenges to be addressed in the area of ICS:

- *Securing Legacy Systems* — As mentioned above, in current industrial control systems, technologies that have an extremely long lifespan (some installed before OT networks interconnected with IT networks) and technologies that are subject to rapid obsolescence coexist with each other. The integration of the two technological domains has generated new vulnerabilities and introduced new exploitable pathways to implement attack strategies: it is therefore necessary to develop specific security measures.

- *Security and Availability of Industrial Processes* — An important requirement of ICS systems is to ensure the widest possible availability of industrial processes. Fulfilment of this requirement complicates the pro-

[33] https://www.enisa.europa.eu/publications/window-of-exposure-a-real-problem-for-scada-systems

[34] https://www.enisa.europa.eu/publications/good-practices-for-an-eu-ics-testing-coordination-capability

[35] https://www.enisa.europa.eu/publications/certification-of-cyber-security-skills-of-ics-scada-professionals

[36] https://www.enisa.europa.eu/publications/maturity-levels

[37] https://www.enisa.europa.eu/publications/can-we-learn-from-scada-security-incidents

[38] https://www.enisa.europa.eu/publications/ics-scada-dependencies

[39] https://www.ecs-org.eu/

cedures for the management and updating of IT-based tools and mechanisms for the security of components of industrial control systems. Consequently, it is necessary to develop techniques and methods to ensure the security of the system without undermining its continuity of availability.

- *Analysis of the relations between safety and security in industrial control systems* — Given the peculiar features of industrial control systems, the analysis and modelling of dependencies between the properties related to safety and those related to security are of great importance, in order to correctly and effectively manage the system throughout its entire life cycle.

- *Impact of the IIoT on industrial control systems* — Growth of the IIoT implies a potential increase in the number of attack sources, introducing a wide variety of distributed sensors and other devices that have not always been designed in accordance with industrial safety standards. In this respect, standardisation bodies should define standards and requirements to reduce the security impact of the use of IIoT devices on industrial control systems. Particular attention should also be paid to the development of tools for the definition, organisation and implementation of appropriate *assurance case* aimed at jointly demonstrating the adequacy of the system with respect to both safety and security standards.

5.5.3 Objectives

In relation to the challenges posed by the security of ICS systems, it is necessary to activate project initiatives aimed at achieving the following objectives:

- *Analysis of vulnerabilities of ICS/SCADA systems* — Definition of specific techniques for the analysis of vulnerabilities of ICS/SCADA systems, motivated by the peculiarities of these systems, also derived from the coexistence and integration of IT and OT technologies. In this regard, there is a need: (i) to propose a taxonomy of systems; (ii) to develop methodologies for identifying vulnerabilities and threat analysis; (iii) to identify countermeasures and best practices for the treatment of risk.

- *Framework for the analysis of the safety and security properties of ICS/SCADA* — Define a framework for the analysis of the safety and security properties of these systems, identification and modelling of their interdependencies and requirements (which can also be conflicting) and automatic assessment of the impact of security issues on safety aspects. In particular, there is a need to: (i) implement tools and processes for simulation and monitoring of cascading effects caused by cyber attacks; (ii)

design solutions to mitigate such effects, increasing the resilience of the systems involved; (iii) develop tools for the definition, organisation and implementation of appropriate *assurance cases* aimed at jointly demonstrating the adequacy of the system with respect to safety and security standards.

- *Training programs* — To be defined and implemented are targeted training programs for professional profiles in the field of industrial control systems, as illustrated in section 6.2.

5.6 Robot

In this section we analyse, with reference to the aspects of cybersecurity, the scenarios in which a device (*robot*), able to perform directly mechanical actions in the physical world, can operate completely (or partially) autonomously and without a direct and continuous control by a human operator. With this characterisation, a refrigerator, for example, does not fall within the scope considered because it typically does not move in the environment (even if it could open its door automatically), while a vacuum cleaner is included if it can move independently inside an apartment.

Robotics is now breaking its classical boundaries and, as an automatic system used mainly in the industrial and automation world, it is hybridising with technologies such as Cloud Computing, Artificial Intelligence and IoT. It also plays a central role in the context of *Enterprise 4.0*, in which some significant trend lines can be identified:

- *Informatisation of industrial sectors* — Cloud Computing and Artificial Intelligence enter industrial manufacturing processes (and automatic assembly lines) and significantly change their canons. From series production we are moving on to custom production in which the same assembly line, thanks to the use of increasingly sophisticated robots, is able to produce different objects on the basis of specific requests supplied directly by the end customer. This is already the case in a number of contexts, such as, for example, the custom painting of certain types of cars.

- *The robotisation of the consumer world* — Robotics enters and transforms everyday life and work, with a view to maximise the efficiency and security of services, not only in the industrial production sectors, but also pervasively in many other areas of society. In this context, we are witnessing a strong transformation of the objects of our daily life, which, from simple instruments under the control of the human being, are becoming autonomous and able to make decisions. Typical examples range from vacuum cleaners to cars.

- *Intelligence distribution* — While in the 1980s the *intelligence* of robots was located within the robots themselves, today there is a tendency to relocate part of this intelligence to the Cloud (technology identified as *Cloud Robotics*) in order to have cheaper, lighter, and smarter robots. While this approach has considerable advantages in the development of increasingly autonomous and connected robots, connecting a robot to the internet and delocalising its intelligence (and thus its ability to make decisions) opens the door to cyber attacks on these devices.

As far as cybersecurity aspects are concerned, in addition to the security problems deriving from the physical actions of the robot, a further aspect to consider is the fact that the "autonomous" motion capability can also be instrumental to the acquisition of data and information through mobile sensors, with potential risks for the protection of information and personal data.

Without wishing to be exhaustive, we list below a series of devices whose security is critical in relation to actions that they can carry out in the physical world. The car is an already well studied case in which a cybernetic attack can cause significant consequences. Criticism in this area has already emerged from the academic context and there have been demonstrations that have required the intervention of the car manufacturers: for example, in 2015, Chrysler carried out or recalled various models of cars[40] following the demonstration of serious vulnerabilities that can be used to obtain remote control of the vehicle. In general, the growth of driving aids, up to self-driving vehicles, increases the number and criticality of decisions made by interconnected IT and electronic systems (i.e., ECUs) rather than by the driver. While this increases security in everyday use of the vehicle, critical signals with a significant effect in the physical world (e.g., brakes) are controlled by systems that could be compromised by a cybernetic attack.

Autonomous driving capabilities also extend to other classes of *unmanned* vehicles, able to operate without the direct control of the operator, whose use is spreading rapidly in the military field, in emergency scenarios, in agriculture, in mines, and in numerous other "outdoor" contexts. In these contexts, the use of drones and micro-drones is increasingly widespread, through which it is possible not only to acquire data for monitoring, but also to perform operations such as the release of plant protection products. It is not difficult to imagine the consequences of intrusions into such systems.

Even in the home, robots are already a widespread reality, not only with regard to the vacuum cleaner that builds the map of the house in order to clean it systematically, but also with regard, for example, to telepresence devices that, although mostly guided, allow you to see what children do at home or interact

[40] `https://www.theguardian.com/business/2015/jul/24/fiat-chrysler-recall-jeep-hacking`

with the faraway grandparents. By way of example, devices capable of interacting in natural language with the operator (e.g., Siri[41], Alexa[42]) have been attacked through the audio channel. The use of voice commands is a feature that quickly spreads even on mobile robotic devices. It is evident that the presence of mobile systems inside a house is an important critical factor from the point of view of security. Their presence offers, in fact, a mobile observation point, which poses not only questions of protection of personal data but also the possibility of improper acquisition of information for improper use.

The category of so-called robotic service systems extends to environments such as the office, restaurant, shopping centre, hospital, where the introduction of autonomous systems for transport or interaction with the user, although not yet very widespread, is expected to expand strongly in the next few years. Also in these contexts, cybernetic attack on the device can have very significant consequences.

One of the most interesting applications in the medical field is *robotic surgery*, which makes it possible to perform surgical operations by manoeuvring, through a console, a robot that is not completely autonomous but capable of performing controlled manoeuvres. The technology now makes it possible to operate the robot remotely (*tele-operated deep-freezing robots*) also using "normal" telecommunication networks. This obviously paves the way for cyber attacks that can alter robot behaviour, with consequences on patient vehicles. Recently, a surgical robot (Raven II), which uses the standard *Interoperable Telesurgery Protocol* on the internet for communication between console and robot, has been successfully subjected to various types of cyber attacks, for the purpose of analysing possible risks to the patient (even a simple "denial of service" attack, if it occurs at particular times of the procedure, can lead to the death of the patient) [18]. These robots must be designed to be resilient to possible cyber attacks before they can be used in practice.

In general, there are three types of possible attacks that can alter the functioning of a robotic system, compromising its physical interaction:

- The first, most trivial and catastrophic, is a direct attack on the robot, in which the attacker manages to take direct control of the locomotion systems of the robot itself, being in a position to control it directly, in order to cause physical damage.
- The second type is a direct attack on the robot's decision-making system, which in *Cloud Robotics* runs on a Cloud system. In this case, the robot behaves as it should, but control and handling data can be altered or unduly extruded. In this case, local safety systems (such as obstacle avoidance) should still be able to avoid direct physical damage.

[41] `https://www.apple.com/it/ios/siri/`

[42] `www.amazon.it/alexa?`

- The third type of attack falls within the context of *spoofing* attacks. In this case, the intelligence is not directly attacked, but the data on the basis of which the intelligence itself processes its own decisions is altered, so that the robot performs the operations required by the attacker. An interesting example of such an application is the so-called *GPS spoofing*[43],thanks to which it was possible to divert a military ship by altering the GPS data received from it.

5.6.1 State of the art

In October 2016, the EU Department of Policy for Citizens' Rights and Constitutional Affairs approved a study paper on European civil legal rules in the field of robotics, commissioned by the Legal Affairs Committee of the European Parliament to analyse the prospect of a future regulatory framework of civil rules for robotics[44]. The result has produced a general framework of ethical principles aimed at protecting humankind from robots, by declaring: (i) the duty of robots not to cause harm to humans; (ii) the obligation to respect the rules of caution and attention to man; (iii) the principle of objective civil liability for damage caused by robots, in accordance with the model of "vicarious" liability (responsibility) for damage caused by robots: the machine, in fact, lacks its psycho-physical autonomy on which to base a legal "individual" responsibility.

The document concludes that the creation of an ad hoc legal category for IA products is inappropriate.

The ethical, social and juridical conviction is thus made one's own, so that only a natural person can be held responsible through diversified imputation mechanisms.

The problem of cybersecurity in medical robotic devices has been addressed by regulatory bodies such as the US Food & Drug Administration (FDA) which has promoted various initiatives to protect public health from vulnerabilities related to cybersecurity. In particular, in 2016 it issued guidelines recommending manufacturers to address cybersecurity during the design and development of medical devices, which may lead to more effective mitigation of patient risks[45,46]. In addition, data protection is required in robotic systems that store [67] patient medical information.

[43] https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/

[44] http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf

[45] https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

[46] https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

Among the scenarios outlined in the previous section, that of the car has not only aroused the interest of government agencies to various nations, including the USA[47], but has already requested the intervention of legislators. The approval of a law on this subject in the USA is recent, where road testing is already common practice; other countries will follow soon.

5.6.2 Challenges

Without wanting to repeat the challenges arising from the technologies that intersect with robotics, such as Cloud and IoT, already analysed in the previous sections, we want to analyse those interdisciplinary challenges that are arising with the evolution of robotics and that involve, in addition to the scientific and technological spheres, sociological and legal ones as well.

- As far as sociological and legal matters are concerned, Italy (and many other countries) still have no rules governing the use of robots and autonomous devices within the company. For example, the flight of autonomous drones in an unsupervised way is currently illegal. In general, there is still a lack of in-depth understanding of critical profiles introduced by possible cyber attacks in different areas, such as:
  - the management/manipulation of the individual's personal data acquired by the robot in social contacts;
  - the possible manipulation of the human emotions of weak subjects in daily contact with artificial social machines (robot in domestic or paradomestic environments, especially those close to the elderly, children, sick);
  - the physical vulnerability of those who use mechanical medical devices to integrate/substitute their own organic dysfunctionality, even as prostheses;
  - the circulation of automated or autonomous vehicles and means of transport.
- From a strictly scientific and technological point of view, the problems of interest can essentially be clustered into two categories:
  - Studying how, from an architectural point of view, attack and, consequently, defence strategies are defined in the field of robotic systems on which there are typically embedded systems as well as con-

[47] United States Government Accountability Office: VEHICLE CYBERSECURITY - DOT and industry have efforts under way, but DOT needs to define its role in response to a real world attack, 2016 – `http://www.gao.gov/assets/680/676064.pdf`

ventional processing systems, such as PCs, tablets, mobile phones etc. [25].

– Monitoring and safety. In fact, in the case of devices considered in this field, the study of anomalies in behaviour has a specific connotation that focuses on interaction with the environment, and in particular with human beings. Characterisation of abnormal behaviour of autonomous devices poses a research challenge in the near future.

5.6.3 Objectives

The main objective of the project is to identify and consolidate the methodological bases for the development of research and innovation in the field of cybersecurity for the categories of autonomous systems considered here.

From a strictly technical point of view, the following lines of action have been identified:

- the specialisation of cybersecurity technologies for autonomous robotic systems, developing protocols and security solutions that guarantee not only the information but also the physical security of these systems and are therefore able to suitably combine safety and security;
- the regulation, from a legal point of view, of the aspects related to the introduction of autonomous systems in society and the system of imputation of liability for damages;
- the definition of long-term social and educational objectives in order to prepare citizens adequately for the spread of robots in everyday life, so that they become not only passive users, but active participants in the ongoing change and sensitive to risks in terms of protection of personal data, safety and security.

CHAPTER

6 Horizontal Actions

This chapter presents a number of horizontal *actions*, transversal to the enabling technologies and to those to be protected, which were analysed in the previous two chapters.

First of all, the aspects related to the defence of personal data protection are analysed, also in connection with the forthcoming entry into force of the GDPR regulation.

Necessary actions in the fields of education, training and awareness-raising are then presented. It is now strategic to train every sector of society to understand the historical change that occurred with the development of the internet, which has added a new dimension to our way of life. In order to respond to the problems posed by the growing use of cyberspace and criticisms in terms of the protection of information systems, it is necessary to promote the culture of security and to make citizens and workers aware that the lack of attention to these aspects can put an entire community at risk. In order to achieve this objective, it is necessary to strengthen specialist education sectors, to increase security to the level of a strategic objective, and to further consider basic education, university education, and vocational training.

6.1 Protection of personal data and GDPR

In a world where state security agencies and the global giants of the internet economy collect and record data on our behaviour, the protection of such data has a direct impact on citizens' rights. This impact is mainly due to the handling of personal and sensitive data having become commonplace, increasingly restricting the right to protection of personal data and freedom of expression.

This sometimes generates fear in those who are less aware of the actual scope of this phenomenon, and conformism in those who are acquainted with its dynamics.

Cybersecurity is not only the protection of national assets, but is also a fundamental citizen right. An overall reflection is therefore needed on what digital security means in a context where state surveillance powers are expanded, anonymity and technologies for personal data protection are limited, outlawed, or even their users monitored, while guarantee systems are weakened and *backdoors* are installed in the most popular software with the complacency of unscrupulous companies.

> **Backdoor** – A method of bypassing normal authentication in a computer system and accessing it remotely to take full or partial control. Backdoors can be hidden within system programs, software applications or hardware components and can be introduced by programmers, designers or compilers. There can be mathematical backdoors hidden in cryptographic systems, aimed at decrypting data streams. Typically, whoever discovers a backdoor can exploit it, while a mathematical backdoor can only be used by those who have introduced it.

Failing to secure data and information endangers our privacy, which is the precondition for exercising the rights of opinion and association, free speech, press and movement, freedom to conduct business, and property rights as well. For this reason, protecting our personal data and the information that qualifies us and our actions becomes a fundamental requirement: the knowledge of our most intimate beliefs and conduct can allow others to manipulate us, intimidate us, or even blackmail us.

Large organisations are aware that the first line of defence is provided by adequate risk management and observation of security procedures, but often companies and institutions do not have a recovery plan in case of cyber attacks and public managers and decision-makers have little awareness of the real risk that occurs when a single link in the security chain is broken.

The following section addresses the main issues related to the protection of personal data arising from the *General Data Protection Regulation* (GDPR) introduced by EU Regulation 2016/679[1] of 27 April 2016, which repeals the previous Directive 95/46/EC.

6.1.1 The legislation

The main purpose of the GDPR regulation, applicable from 25 May 2018, is to reform, update and standardise the legislation on the protection and free move-

[1] `http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4964718`

ment of personal data, so as to make it more solid and consistent across the various EU countries.

Directive 95/46/EC and the GDPR regulation are profoundly different: while the former sets out a series of requirements, similar to a checklist, the latter defines the objectives to be achieved, leaving the choices of the most appropriate instruments to the implementer in relation to the context, at the same time obligating the documentation of the reasons that motivated these choices.

Given that *personal data* refers to all information relating to an individual and his/her professional and public persona[2], the concept of data protection that characterises the GDPR also includes the obligations related to their management, which concern both security and other areas such as storage, confidentiality, anonymisation, and cancellation at the request of the interested party.

The GDPR distinguishes between the *processor*, the *controller*, and the *subject*, i.e., the person to whom the data are related.

The GDPR requires companies to review data management systems within their organisational structures to prevent data loss or mis-sharing. The new Regulation revises the concept of *accountability*[3]: the responsibility for processing lies with the controller and with the processor. Companies must also appoint a *Data Protection Officer* (DPO) who is responsible for overseeing internal organisational processes and is an expert in data protection law and techniques[4].

To protect the entire supply chain of services for the company, data processing issues are not limited to the company perimeter, but involve subcontractors, distributors, agents, outsourcers, industrial and commercial partners, cloud providers, etc. All business partners are involved in the process and must implement shared and efficient strategies.

The GDPR also requires the application of the *data protection by design* principle, which requires data protection to be considered from the conception and design phase of a system for the processing or management of personal data, involving those involved in the development of services, products, and applications that use personal data.

In closing, we highlight some basic principles of treatment that affect security. Since no database is secure on the internet, some of the basic principles of the GDPR are precisely aimed at limiting the scope of exposure to risks:

- *Data minimisation* — I collect only the necessary data and not others;

[2] `http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016R0679&from=IT`

[3] `http://194.242.234.211/documents/10160/5184810/Guida+al+nuovo+Regolamento+europeo+in+materia+di+protezione+dati`

[4] `http://www.garanteprivacy.it/titolare-responsabile-incaricato-del-trattamento`

- *Aims limitation* — I cannot decide to do what I want with data, but only pursue the purpose for which I have collected it;
- *Storage limitation* — I am required to delete data as soon as the purpose for which I collected it ends.

6.1.2 Impact of legislation

The GDPR will have a direct impact on each Member State, which in turn will be obliged to comply with the rules uniformly applied across the EU. For this reason, its implementation will, on the one hand, require companies and public bodies to carry out a thorough review of their data management systems and, on the other hand, will increase public awareness of data protection issues.

Companies that do not comply with GDPR provisions by the due date are subject to fines up to EUR 20 million, or 4% of the global turnover recorded in the previous year. Furthermore, anyone who suffers material or non-material damage as a result of an infringement of the regulation is entitled to request compensation for damages.

The protection of personal data is already a priority for many players, but the transition period prior to the date of application of this regulation is crucial for many individuals, organisations, companies, and services operating in the EU. All these parties will have to analyse their approach to data protection in order to identify any discrepancies between the methods applied and the requirements imposed by the GDPR. To this end, companies must place the protection of personal data at the heart of their internal processes and strengthen corporate communication through specific training programmes that ensure adequate training for those who have access to users' personal data[5].

Data breach – An event that puts an individual's personal data at risk by making them accessible or publicly available. Personal data include health or financial information, copies of identity documents, credit card data, etc. The main causes of a data breach are typically cyber attacks, system vulnerabilities, and/or human errors.

The severity of the penalties makes it clear that it is important to raise awareness of the need for compliance with the GDPR. In addition to the pecuniary consequences, compromising data security and violating the regulation on the handling of confidential data can result in consequences that are not only monetary; harm can be done to business reputation, trademarks can depreciate and the goodwill towards a company can diminish.

[5] `http://www.garanteprivacy.it/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili`

Finally, organisations should not underestimate the risk that, through the collective actions for damages allowed by art. 82 for anyone who suffers material or non-material damage as a result of an infringement on the regulation, they are sentenced to pay large amounts, even when individual damages are small. The number of victims of data breaches might be very high, often in the order of tens of thousands or tens of millions.

The implementation of the new regulation is therefore a key step for data processing legislation and will allow greater control over the use of personal data. There is a real risk that the regulatory instruments provided by the GDPR are not fully used by citizens because of a lack of awareness of the risks of protection of personal data to which they are subject every time they take any action mediated by the internet: from access to web-based or mobile services (email, e-banking, e-commerce, etc.) to the use of devices that are increasingly smart (smartwatches, fitness trackers, etc.). These risks further increase if we consider the amount of personal and sensitive data that every day are uploaded to social platforms such as Facebook and Twitter. It is therefore necessary, on the one hand, as illustrated in detail in section 6.3, to increase awareness of the need of protecting personal data on social media and, on the other hand, to provide adequate regulations on how service providers should inform users about their rights.

6.1.3 Implementation of legislation

On 13 December 2016, the EU Article 29 Working Party (WP 29) issued three documents with indications and recommendations related to the forthcoming implementation by Member States of the GDPR. The final version of the Guidelines[6] was approved on 5 April 2017.

For Italy, there is therefore a need to proceed rapidly with the adoption of the GDPR regulation regarding both regulatory aspects and company awareness.

As far as the regulatory aspects are concerned, at the time of writing, the Personal Data Protection Authority has not disclosed information regarding codes of conduct designed to supplement the GDPR with specific and detailed provisions. These provisions will play a key role, as compliance with the detailed requirements will determine the presumption of conformity in the case of infringement proceedings.

With regard to the preparation of codes of conduct and technological tools aimed at providing support to companies for the implementation of GDPR standards, there are some initiatives worth mentioning in the European landscape,

[6] `http://garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3815707`

which may represent a useful reference basis. In particular, the code adopted by CISPE.cloud[7] provides a good example for operators who offer cloud computing services; the Danish Confindustria has also approved guidelines[8] for the implementation of the GDPR at the business level, aiming to provide guidance to Danish companies on controls that support the implementation of the regulatory requirements.

Finally, it should be pointed out that the joint adoption of the two GDPR and NIS regulations (see section 1.2.1) introduces security incident reporting obligations, on the one hand to protect data subjects under attack (GDPR) and, on the other hand, for the "systemic protection" of national and European critical infrastructures (NIS). The development or transformation of these functions, therefore, cannot be further postponed, in order to meet the May 2018 deadline. In particular, an evolution towards the so-called *Next Generation SOCs* is emerging, in which a decisive role is played by *soft law* tools and sources of self-regulation of specific categories, through correlation rules that include methods and techniques of business-oriented data analysis and that, above all, can be integrated with monitoring tools designed for Big Data.

Security Operations Center (SOC) – The centre for the provision of services aimed at the security of information systems internal to a company or at external customer sites. Provided services typically include: (i) management of security features related to the IT infrastructure (network, systems, and applications); (ii) monitoring of IT infrastructure for early detection of intrusion attempts or improper use of systems; (iii) control to improve the level of protection through *security assessment* and *early warning*. While having different roles and purposes, in some cases SOCs also act as CERTs (see box on page 17).

6.1.4 Objectives

In a company context, compliance to the procedures for the processing of personal data and sensitive information with GDPR regulations can actually be carried out in two ways: customising existing technologies that have already been developed as a part of business logic or implementing innovative algorithms from scratch. The implementation objectives to be pursued are as follows:

- Identify tools and technologies of *data discovery* that can recognise, on the basis of heuristic rules, the databases within the entire information system in which information subject to the requirements of the GDPR is present.

[7] `https://cispe.cloud/code-of-conduct/`

[8] `https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Persondataforordningen_engelsk.pdf`

- Develop tools and technologies that, by analysing data and information life-cycle processes, are able to report and track down procedures that lower the levels of security or open the door to breaches of personal data protection policies. This tool must therefore be able to assess how much the implementation of a data processing procedure exposes the company to a risk of a GDPR violation.

- Develop methodologies and tools integrated with best practices in cybersecurity. In particular, integrate cyber risk management frameworks, such as the *National Framework of Cybersecurity* [10], with the methodologies imposed by the GDPR. Many of the Framework's best practices correspond to GDPR implementation practices. A unified vision of cybersecurity and personal data protection policies provides an integrated view both in the risk assessment process and in adaptation and remediation initiatives, helping to develop project synergies and improve investment efficiency.

- Deliver a regulation (*recommender*) with simple rules to support companies in designing procedures for accessing and managing information which meet the GDPR requirements. The recommender must have the ability to abstract itself from the specific technologies and procedures used and should guide the user in defining an adequate data processing workflow in relation to both the data sources and the applications that shall access data or manage its life cycle.

6.2 Education

One of the main reasons for the success of cyber attacks in various areas, now reported daily even by the non-specialist press, is the lack of a suitably qualified workforce in the cybersecurity sector. The scarcity of professionals with adequate skills makes companies, public bodies, and entire countries vulnerable, and exacerbates the difficulties of managing accidents. A number of specialised studies foresee a shortage of more than one and a half million units of labour by 2020[9], highlighting a steadily growing demand[10].

Italy also suffers from the shortage of professionals in the area of cybersecurity, that is exacerbated by the migration of young people, trained in our

[9] `http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html`

[10] `https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf`.

universities, but attracted abroad by more attractive salaries. In the absence of appropriate professional skills, the *Enterprise 4.0* programme can become a boomerang for key sectors of our economy: extending the principle of "everything connected, always" to the manufacturing world will lead to a significant increase in the risk of cyber attacks that succeed in stealing sensitive information from companies and compromising their operations.

To mitigate these risks, significant investments are needed to train security experts with strong technical expertise capable of (i) defining protection and control policies, strategies, and programmes, to protect data, networks, and systems; (ii) managing situations, events and people in the presence of cyber attacks; (iii) contributing to a culture of cybersecurity in companies and society at large.

Given the pervasiveness of the aspects of cybersecurity in the professional, educational, and academic spheres, as well as in the wider social context, training in this field should be addressed along six complementary lines:

1. *Advanced Training* — Aimed at providing the fundamental cybersecurity technical and methodological tools through degree courses, university Master's courses, and Doctoral programmes offered by universities;

2. *Basic Education* — Aimed at providing the basics of cybersecurity from at least the secondary schools, regardless of the specific school type, with the objective of laying the foundations for a better understanding of the topic and of promoting cybersecurity among the possible choices of university courses;

3. *Vocational training* — Aimed at continuing training for all professions that are increasingly confronted with cybersecurity issues;

4. *Talent scouting* — Aimed at finding young talents to be directed towards a career in cybersecurity, attracting their interest through IT challenges, simulations in protected virtual environments and, in general, through initiatives that allow participants to experience possible operational contexts and to evaluate opportunities for professional growth;

5. *Training* — Aimed at strengthening, improving, and evaluating the practical capabilities of operators and procedures for countering and managing cyber incidents within organisations;

6. *Citizens' awareness raising* — Aimed at providing citizens with the basic notions of cybersecurity and the basic concepts of what is now commonly called *cyber-hygiene*.

Of the six guidelines, the first five are analysed in this section, while the sixth will be dealt with in the following section.

6.2.1 State of the art

Advanced Training Many prestigious foreign universities, including MIT, Harvard, Cambridge, Carnegie Mellon, Georgia Institute of Technology, Imperial College, Eindhoven, ETH Zurich, etc.[11] offer advanced training programs in cybersecurity.

In Italy we are not in year zero. At the University of Milan, a Master's degree and a three-year degree in Computer Security have been offered for years. For some years now, the University of Trento has been part of a consortium within the European Institute of Innovation and Technology (EIT) which offers a Master's Degree in Security and Privacy. Since the 2017-2018 academic year, Sapienza Università di Roma has also offered a Master's Degree in Computer Security. Study plans in cybersecurity are planned or in progress within various Master's Degree courses in Computer Science or Computer Engineering. These initiatives are accompanied by many first and second level Master's courses, accessible respectively after a three-year *laurea* or a subsequent *laurea magistrale*. Also, other Master's training courses such as that of the Cyber Academy[12] of the University of Modena and Reggio Emilia are offered. For a complete picture, please refer to the study[13] carried out jointly by CINI's *National Laboratory of Digital Competences, Training and Certification* and the *National Laboratory of Cybersecurity*. This second laboratory is also leading various training and awareness-raising initiatives[14], bringing to Italy what had been done by the Association for Computing Machinery (ACM), which set up a commission to draw up curricular guidelines based on a complete vision of cybersecurity, which take into account the specific disciplinary needs for open and critical training and the relationship between curriculum and type of workforce required[15].

Basic Education Many countries pay particular attention to these aspects; for example, in Great Britain more than EUR 20 million have been invested in the *Cyber Schools Programme*[16] for young people between 14 and 18 years of age, to encourage them to approach these issues and develop skills that will be increasingly important in defending the backbone of the economy.

[11] https://digitalguardian.com/blog/cybersecurity-higher-education-top-cybersecurity-colleges-and-degrees

[12] http://cyber.unimore.it/

[13] https://www.consorzio-cini.it/index.php/it/lab-cfc/59-italiano/laboratori/lab-cfc/notizie-in-evidenza/1183-il-laboratorio-cfc-e-l-osservatorio-delle-competenze-digitali-2017

[14] https://www.consorzio-cini.it/index.php/it/labcs-home/formazione-in-cyber-security-in-italia

[15] https://www.csec2017.org

[16] https://www.gov.uk/guidance/cyber-schools-programme

In Italian high schools, at the moment, little attention is given to cybersecurity issues and none among the 34 actions considered in the National Plan for *La Buona Scuola Digitale*[17] is dedicated to cybersecurity.

Talent scouting Numerous international initiatives have been set up to promote the spread of the cybersecurity culture by leveraging competition as a stimulus to attract young talent. For example, in Great Britain, under the brand name *CyberFirst*[18], the government supports the growth of the next generation of cybersecurity experts through a scheme of courses, apprenticeships and competitions for young people aged 11-17.

One of the most popular training initiatives is certainly the *Capture-The-Flag* (CTF) competition (see box on page 74). Countries such as Australia, the UK, Austria, Germany, Switzerland, Spain, Romania and the USA have been organising competitions for some years, which select the best candidates to build national teams.

Annually, the ENISA organises the *European Cybersecurity Challenge* (ECSC), a competition dedicated to European national teams in which, since 2017, Italy has also participated under the aegis of CINI and MISE.

CyberChallenge.IT [19] is the first Italian programme of talent scouting in cybersecurity promoted by the CINI National Cybersecurity Laboratory. The project aims at identifying excellences in cybersecurity among high school or early university students. The 2017 edition saw 700 applications from all over Italy, while the 2018 event will offer training courses at 8 Italian universities and will culminate in the first Italian cybersecurity championship. At the same time, the initiative aims to train young people for the Italian team participating in ECSC 2018.

Training *Cyber Ranges* (see box on page 35) can play an important role in training at all levels and various states are using them for training in both civilian and military cybersecurity. EDURange[20] is a platform for the construction of scenarios and individual training paths. Arizona's Cyber Warfare Range[21] offers paths of increasing complexity for individual training. The Michigan Cyber Range[22] is not limited to reproducing the ICT infrastructure of a single organi-

[17] `http://www.istruzione.it/scuola_digitale/allegati/Materiali/pnsd-layout-30.10-WEB.pdf`

[18] `https://www.ncsc.gov.uk/new-talent`

[19] `https://www.cyberchallenge.it`

[20] `http://blogs.evergreen.edu/edurange`

[21] `http://azcwr.org`

[22] `http://www.merit.edu/cyberrange`

sation, but includes an entire virtual city (Alphaville). Locked Shields exercises, performed using NATO's Cyber Range in Estonia, support very sophisticated training activities where an attack team, *red team*, contrasts with multiple *blue teams*, which have the task of defending the scenario assigned to them from attacks launched by the red team.

6.2.2 Challenges

The existing training initiatives in our country are unfortunately still insufficient and suffer two major shortcomings: the limited number of experienced researchers who can teaching the needed skills, and an inadequate national coordination between academia, high schools, and the public and private sectors to define the necessary professional profiles. Moreover, at the university level, even though the activation of new training courses is a particularly important requirement, compliance with the fulfilment of the minimum requirements in terms of teaching staff imposed by current legislation means that, in various establishments, the activation of new cybersecurity degree courses would imply the closure of some of the existing courses.

From the point of view of training programmes for young talents, the main challenge is to intercept them at an early stage of their studies when they have not yet decided on a definite direction to invest their skills, and to show them career opportunities and the stimulating aspects of activities in cybersecurity. This can be pursued through the involvement of high school students and the promotion of female participation, undermining the principle that cybersecurity is a domain for men only.

As far as vocational training is concerned, provisions should be made for continuing training programmes. Training employees on the field through courses and practical exercises is just as important as acquiring new technology. This training should be aimed not only at IT professionals but also at managers, technical operators, and executive staff.

In private business organisations this issue is dealt with at different levels of maturity: much can still be done in small and medium sized companies that often have less investment capacity but represent the backbone of the Italian economy. But, even more importantly, it is necessary to devote efforts to this issue in the public context, where the working age of employees, the stratification of the roles held over the years or the lack of funds for training often do not contribute to the development of awareness of security issues: the challenge becomes even greater in those public areas that represent critical infrastructures for the country, such as, for example, health care.

In particular, the preparation of operators who are directly confronted with critical situations (e.g., cyber attacks, security incidents, *data breaches*, etc.) is crucial not only for an effective and efficient management of the event when it

has already occurred, but also from the prevention and *lesson learned* points of view. Reference examples and best practices can be taken from highly critical sectors (e.g., in the nuclear, aerospace, oil and gas fields, etc.) where a continuous training based on drills has always been implemented, suitably designed for the specific context aimed at guaranteeing the highest level of *resilience*.

For this reason, developing techniques and tools capable of automating activities to support confrontation of possible attacks is a major challenge. The next-generation Cyber Ranges can perform this task by adapting the complexity of the considered scenarios to the tasks of the professional figures involved in the drill.

6.2.3 Objectives

The following should certainly be included among the most significant objectives of training:

- *Plan for advanced training in cybersecurity* — A specific plan should be drawn, in concert with the public sector, private companies, and universities, in order to define professional profiles trained through degree courses, university Master's courses, and Doctoral programmes. These courses, taking the current Bachelor's and Master's degrees in computer science and computer engineering as their starting point, should provide basic cybersecurity technical and methodological tools. In particular:
  - The universities shall:
    * redesign the *curriculum of basic computer science or computer engineering courses*, introducing security concepts from the very beginning of the studies;
    * offer *new university courses* on cybersecurity topics to be included in existing curricula;
    * set up *graduate courses*, especially *lauree magistrali*, to train professionals able to understand complex systems and to monitor heterogeneous and constantly changing environments, taking all levels of risk into account;
    * set up *Doctoral courses* to train experts and researchers able to understand international developments in cybersecurity research, anticipate attack dynamics, and create new passive and active defence tools;
    * collaborate in the implementation of the *National Training Cyber Range* presented later in this section;
    * offer *Master's courses* aimed at training immediately operational experts, attracting not only recent graduates, but also

employees of public bodies and private companies, to be involved and retrained on cybersecurity issues;

* apply to participate as local nodes in national research and training programmes for young talent, such as the CyberChallenge. IT.

– The Ministry of Education, Universities and Research will have to define a special plan which, starting from the current emergency situation, provides for the allocation of specific resources (teachers, researchers, funding) for the development of higher education and research in cybersecurity. This plan, as detailed in section 9.5, is essential both to avoid that our researchers go to countries where their professional skills are better recognised and remunerated and to encourage the return or the arrival of highly qualified researchers from abroad.

- *Plan for basic cybersecurity education* — The long-term strategy must include enriching programs at schools of all levels, from the moment pupils start using smartphones and networked devices independently. The provision of adequate security knowledge must have the dual purpose of introducing the basic concepts of cybersecurity and making children aware of the risks associated with a careless use of the network and of the applications used on their devices. To this aim, it is important to:

  – promote public-private partnerships to provide students with economic incentives (e.g., through scholarships) to reduce the costs of cybersecurity training;

  – sponsor training programmes for the research of young talents, promoting Italian participation in international competitions such as the European Cybersecurity Challenge (ECSC);

  – introduce compulsory notions of IT security in school curricula, starting from the concepts of digital identity, threats and risks, tools and behaviours for the safe use of the network, etc.;

  – prepare ad hoc training for teachers identified as potential trainers on the topic, while stimulating the development of new professional skills within the teaching staff;

  – encourage and strengthen opportunities for training experiences in dual-training systems (learning and working)[23] which, by exploiting the combination of knowledge and know-how, offer participants the opportunity to get closer to the problems of cybersecurity;

[23] `http://www.istruzione.it/alternanza/`

  - highlight how digital transformation has eliminated some types of work but has created others, and that there are many job and career opportunities in the cybersecurity field.

- *Plan for professional training in cybersecurity* — The problem of vocational training is wide and complex because, as it happens with security on the workplace, it affects not only the specialists but all employees of any company, both in the private sector and in the public administration. Vocational training and refresher courses through *continuous training* therefore play a crucial role. Each individual must understand that misbehaviour in terms of security can be the weak link in the defence chain and facilitate malicious access to the IT systems and relevant data of their organisation. In this respect, in particular, companies and public authorities shall specifically:

  - implement periodic cybersecurity training and refresher programs for non-technical personnel such as executives, managers and board members;
  - implement training programs to fill the cybersecurity gaps of middle and senior technical staff;
  - sponsor training initiatives of young talents, with the aim of getting in touch with potential candidates to be recruited;
  - define and implement specific training programs on cyber security and risk management for professional profiles operating in the field of industrial control systems, to meet the complex challenges that arise when the aim is to protect such systems from cyber attacks;
  - develop platforms for sharing up-to-date information on identified vulnerabilities and threats, both within the individual organisation and across the entire supply chain. These platforms should improve the quality of training and raise awareness of possible security risks.

- *National National Plan for Awareness-raising* — Finalised to provide the population with the basic notions of cybersecurity and the basic concepts of cyber-hygiene; this plan is analysed in detail in the following section.

- *Talent scouting* — In order to identify young talents, it is important not only to involve students at an early stage of their careers, but also to promote the construction of a community of experts that provides a platform for recruiting the profiles best suited to the various professional roles in cybersecurity. This can be done by following the career development of

young people after leaving initial training programmes such as the CyberChallenge.IT[24]. A first objective to consider is their involvement in the training activities of subsequent classes (according to a model of *peer education*), in order to train new generations of trainees. A second objective is the promotion of degrees, Master's and Doctorates in cybersecurity. An important and concrete aspect in this context is the creation of a database of young experts and their skills, to enable effective matching between demand and supply in the professional labour market. The CyberChallenge.IT programme is the starting point for creating this platform for the development of the future Italian cybersecurity community.

- *National Cyber range for training* — It is important to aim at the creation of a national Cyber Range dedicated to training. This will enable a set of activities of great importance for the country. Sharing the Cyber Range between researchers, PAs and industries will allow:
  - academia to strengthen cybersecurity training programs with practical sessions, for students to experiment and acquire skills that can be immediately spent in workplaces;
  - researchers to experiment and evaluate the effectiveness of innovative cybersecurity techniques in a controlled environment;
  - public and private sectors to train the staff in charge of cyber defence and also to be able to experimentally evaluate the effectiveness of the defence instruments to be acquired.

6.3 Awareness and cyber-hygiene

The use of the internet is increasingly pervasive, engaging and, as time goes by, the number of devices connected to the net is constantly increasing, just as the activities that can be carried out with the help of the network. The net is today, in fact, the element that unites different contexts, representing the privileged communication tool in both the personal and business environment: for all of us, it is now the infrastructure on which our personal data travel, the data of the companies for which we work, our ideas and our interests. Without the internet we cannot navigate the web, use Facebook, search for information with Google, send and receive electronic mail, send messages with WhatsApp, make purchases and bookings online, and access many PA services.

The offer of online services has reached extraordinary levels of variety and diffusion, thanks to the ease of access to mobile technologies and the flourishing of new applications that can also respond to the needs of niche users.

[24] `https://www.cyberchallenge.it`

Home banking, e-government, electronic healthcare and e-commerce services are now an integral part of the lives of citizens who use the digital channel to interact with public and private organisations.

The extensive use of social media is also favoured by the ease of data and information sharing that these platforms support: in this context of openness, the "natural" defences of a user tend to decrease due, on the one hand, to the fact that communication is mediated by technology, and, on the other, to the expectations of carrying out fun or interesting activities.

Dangers In such a tool-rich, opportunity-packed, and open scenario, the network often becomes a source of danger if its limitations and threats are not properly understood and security aspects are not taken into account. Citizens are potential targets of attack both as consumers of digital products and services, and as members of organisations.

We are therefore faced with a systemic risk that is difficult to manage, especially in the absence of the control mechanisms typical of organisations. In addition, the limitations brought about by the adoption of security mechanisms may conflict with other needs, such as improving the user experience of products and services. An example of this is provided by the federated identity management systems, in which the urgency of reaching a critical mass of users by offering useful and immediate services clashes with the need to prevent and detect identity theft through complex procedures for identification and authentication. It is also difficult to counteract unwanted behaviour in inter-organisational contexts, regulated by commercial agreements, where digital platforms provide the infrastructure for real service ecosystems. Just consider the phenomenon of fraud on mobile payment systems, whereby small amounts are subtracted from millions of users through unaware online subscriptions, triggered by advanced forms of *phishing* (see box on page 28).

Company Digital Divide Paraphrasing the concept of the *digital generational divide*, in the working context there is a clear separation between the companies where the use of technology is predominant (where, therefore, part of the staff has good or excellent IT and security tools) and the companies where instead the use of technological tools plays a marginal role in the employees' daily tasks.

Citizens and their workplace The best-known cyber attacks are carried out on a large scale and affect both citizens and organisations. However, it is not correct to consider these two groups as distinct. In fact, very often, citizens are also workers working in digitised environments where personal and professional spheres intersect, thus creating dangerous short circuits in which cyber threats

can spread and endanger economic resources, the protection of personal data, and the profitability and security of critical infrastructures and democratic systems. Exposure to risk increases when business tools are also used for personal activities: in these cases, attacks can result not only in the violation of personal data protection but also in new vulnerabilities for the company where the victims work.

Social Engineering – A set of techniques designed to mislead a person in order to obtain confidential information. These can then be used fraudulently to carry out an attack, using different tools and technologies.

Work environments, therefore, play an important role in raising employee awareness on security issues, not only for the corporate purpose of protecting the information assets of the organisations in which they operate, but also as a contribution to the basic training that employees transfer to their personal lives as private citizens. Knowledge of threats deriving not only from digital tools and the network through malware, but also from *social engineering* techniques, which are acquired in the workplace, contributes more widely to the strengthening of the country's social awareness on cybersecurity issues.

6.3.1 State of the art

At the European level, the lines of action defined in the field of basic digital skills are based on pillar 6 of the European Digital Agenda for Europe (DAE) *Enhancing digital literacy, skills and inclusion*[25] and have two primary objectives:

- *building digital citizenship*: access to and participation in the knowledge society, with full digital awareness;
- *achieving digital inclusion*: equality of opportunities in the use of the network and development of a culture of innovation and creativity.

In line with these objectives, in Italy several bodies, in various ways, operate for the promotion of training initiatives aimed at cybersecurity. For example, the *Department of Security Information Department* (DIS) has promoted a series of initiatives aimed at Italian high school and university students to spread the culture of cybersecurity through dialogue with the new generations. The *Be aware Be digital*[26] campaign that was recently launched is particularly relevant in this respect.

[25] `http://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/enhancing-digital-literacy-e-skills-and-e-inclusion`

[26] `https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/be-aware-be-digital.html`

6.3.2 Challenges

In such a complex scenario, structured action is needed towards end users that takes the differences due to different age groups - teenagers, young adults, and adults - into account.

Teenagers navigate online with ease, but often do not know the mechanisms and limitations of the internet, and above all do not understand the close link between actions carried out on the internet and in real life; the sometimes tragic situations in which they find themselves involved because of cyberbullying phenomena in social media bear witness to this. Families feel unprepared to tackle the issue competently and parents are often unable to respond to the alarms raised by teenagers. Schools rely on the various external initiatives available, promoted by companies, non-profit organisations, or public institutions: all these initiatives, however, despite their great usefulness, suffer from a lack of continuity and limited scalability on the national territory.

Young adults who enter working life have developed behaviours and habits over time, such as the tendency to easily share information or acquire information on the web, without applying the necessary filter of critical thought. Such behaviours can pose a risk both to them personally and the companies that employ them. Structured initiatives are needed to adequately train young people to become real *networkers citizens*: even those who have not followed curricula with a technological focus must be able to benefit from digital training in security, suitable for a mature use of technological tools, based on risk- and responsibility-conscious behaviours online. In order to achieve this goal, voluntary initiatives are not enough: it is necessary to provide a real civic education on the net, through an educational programme of national scope, at all levels, which includes training and awareness raising on the subject of internet security.

Adults generally lack a broader perception of cyber risk. As a result, they do not adopt what are considered to be the basic rules and behaviours of so-called *cyber-hygiene*. Even when these rules are known, they tend to be circumvented in favour of easier access to services and information. People are therefore exposed to the danger of large-scale attacks, which exploit naive behaviours such as, for example, the vulnerabilities resulting from the systematic failure to update system software, from PCs to tablets and smartphones. In this regard, it is important to point out that the relationship between system vulnerability and security countermeasures is not static, but dynamic: the evolution of technologies and the continuous adaptation of tools to user needs make it necessary to systematically update the software, which in many cases, due to various wide-ranging reasons, is not possible to carry out automatically. Finally, it is necessary to stress the importance of individual *behaviours*: the most sophisticated and perfectly updated technological protections are in fact completely useless if each of us does not adopt safe behaviours. By way of example, one may exclu-

sively use devices with the most up-to-date antivirus, but if one cannot recognise a phishing email and provides his credentials to malicious organisations by accessing a "fake" site, he is actually distributing all of his home keys.

6.3.3 Objectives

The *Italian Digital Agenda*[27] clearly states that our country needs effective measures to promote the digital literacy of the population. In this context, it is necessary to carry out campaigns for the safe use of the network and its communication tools, in order to guarantee the security of individuals and, consequently, of the whole country. For this reason, action should be taken towards increasing citizens' awareness of security issues and to significantly influence their behaviour in the use of digital communication tools.

It is therefore necessary to set up a set of actions for training on the safe use of the network, aiming at increasing technological knowledge and social security for our country, by pursuing the following objectives:

- *A national framework for awareness raising and permanent training* — Develop a structured path at the national level for the definition of a Framework as a reference model for implementing permanent refresher training actions on the themes of network security and conscious use of digital tools. The Framework should define a set of coherent "contexts" and identify for each of them, with the contribution of multidisciplinary specialist teams: (i) the objectives to be achieved, defining, where applicable, the relevant bodies of knowledge and syllabuses; (ii) the sequence of actions to be implemented to achieve them; (iii) detailed operational plans, in terms both of timing and resources.
- *Minimal checks for citizens and cyber-hygiene* — (i) Define a set of minimal controls for citizens and a set of basic cyber-hygiene rules that must be systematically followed; (ii) Identify and activate the most suitable mechanisms for the maximum diffusion of these minimal controls and the basic rules of cyber-hygiene through advertising and mass information campaigns, both in traditional media (newspapers, radio, TV) and in social media.
- *Public, private, third-sector cooperation* — Promote and encourage a virtuous model of cooperation between public, private, and third sector organisations for the enhancement and implementation of today's initiatives that are already implemented, in various forms, on the national territory. In fact, many companies, organisations, professionals, and voluntary associations are already including training initiatives within their

[27] `http://www.agid.gov.it/agenda-digitale/agenda-digitale-italiana`

corporate or social missions. Cooperation would require both the sharing of best practices and the great deal of material already available today, following however a verification with respect to the above-mentioned Framework directives.

6.4 Managing cyber risks of companies

Cyber risk management plays an increasingly important role over time: the more cyber risk is perceived at the company level, the more managers strive to understand its impact even in the absence of specific technical knowledge on the subject.

The CINI National Cybersecurity Laboratory has been working over the last several years to design risk management tools that can be used by both private companies, regardless of their size, and by the PA to evaluate their exposure, as well as by consulting companies that can use them in the delivery of their advisory services.

These instruments take the form of (i) the *National Framework for Cybersecurity*[10], published in 2016 in collaboration with different industrial and governmental actors and suitable for companies that, regardless of their size, already have some degree of security preparation; (ii) the *Essential Controls of Cybersecurity*[11], published in 2017.

These actions were aimed at standardising the cyber language in different contexts, for an immediate understanding and a smoother adoption process.

6.4.1 Objectives

In the light of the experience gained, two project proposals based on these two documents are presented here and a third one is proposed, with the aim of bridging the gap for individual citizens, who are still lacking in tools from the point of view of cyber risk management.

- *National Framework Contextualisations for large organisations* — The National Cybersecurity Framework [10] can be adapted to the different heterogeneous contexts present in the national panorama through the creation of appropriate *contextualisations*. Companies from different industries present different and specific requirements and critical issues in the cyber domain. This means that, depending on a set of factors (such as product sector, type of services or products, size, risk exposure, etc.), the set of security practices to be implemented and the necessary implementation processes can also be very different from each other.

  The contextualisations of the Framework are extremely valuable tools, as they allow for the structuring of the cyber risk management of the target

organisations. The creation of a contextualisation is however a complex operation that requires both a high knowledge of the application domain and a significant mastery of the National Framework.

The project aims to draw up contextualisations of the Framework for:

- large enterprises (depending on the product sector, e.g., energy, construction, telecommunications);
- large hospitals;
- large central governments (e. g. ministries);

by setting up private-academy partnerships for the first case, and public-private-academy for the other two.

The effects of the project will be manifold: (i) raising the general security level of the Italian business structure and the PA, (ii) establishing cross-sectoral consistency in risk management and a common cyber language shared between private and public sectors, as well as between private and private ones, which will facilitate cooperation and sharing of requirements.

- *Dissemination, promotion, and updating of Essential Controls for SMEs* — The definition, update, and promotion of essential cybersecurity checks for small and medium-sized enterprises represent a fundamental element to foster the widespread diffusion of cybersecurity culture within the national entrepreneurial reality and to reduce the exposure of the productive world to the risk of cyber attacks. Essential controls are in fact an instrument for defining a minimum level of protection against cyber attacks and for helping companies to reach this level, thus reducing the attack surface area and providing a basis for the consolidation of the national productive infrastructure against cybernetic risks.

  This is a step in the direction of increasing the security of the cybernetic space for small and medium-sized enterprises, on the one hand by reducing the risk of loss due to accidents and attacks and, on the other hand, by increasing the level of confidence of national and international customers and investors in Italian industries. The net effect is twofold: companies will benefit from a competitive advantage, and an ecosystem of cybersecurity will be established, to be used as a foundation for more advanced initiatives.

  At the national level, essential cybersecurity controls were first defined in the *2016 Italian Cybersecurity Report*[28] published by the CINI National

[28] `http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf`

Cybersecurity Laboratory and CIS Sapienza[29]. These controls focus attention on: (i) the identification of hardware and software systems and services in use and their need or criticality levels, (ii) the compliance with current regulations and management of responsibilities, (iii) the use of appropriate technical solutions for data protection, training, and management of personnel, (iv) incident management and related recovery. Following their publication, compliance with the essential controls of cybersecurity was subjected to a statistical survey by the University Politecnica delle Marche in collaboration with CIS Sapienza. This investigation has shown that some requirements (such as compliance with current regulations, adequate training of personnel and rapid replacement or decommissioning of obsolete software) are more difficult to satisfy than others.

Given this background, further efforts should be made to disseminate and promote essential cybersecurity controls. In addition, it is necessary that these controls are periodically reviewed and updated in order to take into account the evolution of both the threats and the level of cybersecurity of small and medium-sized enterprises. This action must be carried out by considering the estimated levels of satisfaction of the individual essential controls and by introducing appropriate corrective actions in relation to the most critical controls.

After an initial phase of voluntary adherence to such essential controls, a *national certification* based on such controls should be defined, similar to what has been done in the UK for controls known as *Cyber Essentials*[30]. A first step in this direction has been taken with the enactment by AgID of the official list of minimum ICT security measures that are mandatory for all PAs[31]. Similarly, it is desirable that the fulfilment of a minimum number of essential controls and their certification gradually becomes a mandatory requirement for the provision of products and/or services to the public sector by private entities, to start with.

The project regarding the definition, updating and certification of essential controls for SMEs has the following practical objectives:

– The activation of a technical panel responsible for defining and updating essential controls. In this context, universities and research institutions can contribute to the formation of the panel and to the definition and updating phases of the essential controls, as well as

[29] `https://www.cis.uniroma1.it/`

[30] `http://www.cyberessentials.org/`

[31] `http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni`

to the publication of the controls themselves and their accompanying documents. The government can act as guarantor of the certifying body and can issue the related certifications. The companies, on the other hand, will undergo self-assessments of compliance with the essential controls and request the relevant certification in order to be included in the public list of certified subjects.

- The regular update and review of the list of essential checks and accompanying documents.
- The creation and maintenance of a portal for the dissemination of essential controls and self-assessments of compliance with the controls.
- The definition of a certifying body which, at the request of the interested party, carries out procedures to verify compliance with essential controls and certifies the outcome.
- The maintenance of a public database of companies that have obtained certification of compliance with the essential controls.

The spill-over effects on society and industries will result in a general increase in the level of resilience, as well as in the increase of visibility and attractiveness to those subjects who have obtained and maintained certification of compliance with essential controls.

From the point of view of researchers, creating and updating a benchmark based on the essential controls will provide insights into the definition of the controls themselves and of their relationship with other industry standards, both nationally and internationally.

6.5 Affordable Certifications

In modern societies, which continue to rely on ICT technologies for increasing amounts of valuable and critical information and services, ICT security certification is taking on a very important role. Information and service providers' statements about their level of security increasingly need to be supplemented by third-party verifications, preferably carried out in accordance with widely recognised international standards. Also at an institutional level, both Italian and European, the certification of ICT security is a subject of attention, as demonstrated by the recent initiatives of the Presidency of the Council of Ministers and the European Commission. The former, with the DPCM Gentiloni (illustrated in section 1.3.1) and the *National Plan for cyber protection and cyber security* of March 2017 (illustrated in section 1.3.2), envisaged, among other things, the creation of a new assessment and certification centre for components to be used in critical and strategic infrastructures. The latter, in the Joint

Communication to the European Parliament and the European Council of 13 September 2017 that outlines the European cybersecurity strategy (*Cybersecurity Package*[32]), has expressed its intention to propose a *European cybersecurity certification framework*[33].This framework will be applicable to products, services and/or systems and will allow a modulation of the certification level that is appropriate to the application context. The Commission's objective is twofold: to avoid customs barriers within the EU due to national certifications and to pursue the vision of the European *Digital Single Market*.

6.5.1 State of the art

The various types of certification currently available are mainly used on a voluntary basis and only rarely, especially in Italy, as a result of obligations or preferential requirements for the acquisition of goods and services. Below, the three main forms of security certifications that currently exist will be considered: (i) the certification of ICT security management systems used in an organisation or part of it; (ii) the certification of ICT devices, also called *product certification*; (iii) the certification of competences in the field of ICT security.

Certification of ICT security management systems The Information Security Management System[34] - ISMS] has traditionally been certified by ISO, which inherited the old BS 7799 and ISO 17799 standards. The verification methods are defined by the ISO/IEC 27001 standard, which is used as a basis to verify compliance with the security control requirements contained in the connected standard ISO/IEC 27002. The latter reports the requirements, expressed in natural language, in the form of a catalogue from which they can be extracted on the basis of the results of the risk analysis. The catalogue also contains information on how the requirements can be met (*implementation guidance*). A single level of verification, and therefore certification, is foreseen.

The ISO 27001 standard is certainly the most internationally recognised and the most widely accepted and probably effective, but it is also a standard that begins to need updating (the latest release is dated 2013) and often requires very high application and maintenance costs, especially for small companies and in the case of complex ISMSs.

The evolution appears to be"light" certifications, i.e. economic and effective, based on the model of "quick win" security practices. This path has has

[32] `https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en`

[33] `https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework`

[34] `https://www.iso.org/?-27001-information-security.html`

already been followed by the UK with the *Cyber Essentials*[35], which proved to be extremely cost-effective and attracted worldwide interest. These certifications are at different levels: from self-certification for the minimum level, to certifications made by third parties through an on-site inspection for the highest level of certification.

Documents have been developed that provide suitable guidance for the application of ISO 27001 in specific contexts. This is the case for the ISO/IEC Technical Report TR 27019 developed on the basis of ISO/IEC 27002 and containing guidelines to define ISMSs that are suitable for a critical infrastructure. In fact, the report can be used in the energy sector where process control systems are used.

Certification of ICT products The best-known standard used to certify ICT products, intended as components and systems, continues to be ISO/IEC 15408, better known as *Common Criteria*[36]. There are also specific standards for cryptographic modules, i.e. FIPS 140-2[37] and ISO/IEC 19790[38], 24759 and 17825 standards, which are mainly used in the United States.

The Common Criteria provide for seven levels of certification (EAL1–EAL7), which correspond to stricter checks on the object to be certified. They are used both in the context of national security, in which case product suppliers are often obliged to obtain this type of certification, and in what the *National Plan for cyber protection and IT security* (set out in section 1.3.2) defines as the context represented by the national productive infrastructure and the citizens. In both cases, there is only one national institutional certification body in each country. In Italy, specific decrees issued by the Presidency of the Council of Ministers have appointed the National Authority for Security (ANS) and the ISCTI of the Ministry of Economic Development as certification bodies, respectively, for national security and business security. Each certification body accredits a number of assessment laboratories (called Ce.Va. in the first case, LVS in the second) which are responsible for verifying, under the technical supervision of the certification body, whether the requirements contained in the standard are met by the subject of the certification.

Although a considerable number of products have been certified according to the ISO/IEC 15408 standard, its use in the commercial context cannot be considered wide-ranging, due to various factors that have hampered its diffusion. In fact, apart from a few cases in which it has been made compulsory, outside the context of national security, Common Criteria certification is requested

[35] `http://www.cyberessentials.org/`

[36] `https://www.commoncriteriaportal.org/`

[37] `https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards`

[38] `https://www.iso.org/standard/52906.html`

by suppliers who decide independently to use the certification to improve the image of their products. It is clear that such use is not possible with low certification levels that would risk being even counterproductive in terms of product advertisement. As a result, the majority of Common Criteria certifications are carried out at least at average levels (from EAL3 upwards) with correspondingly long times (a few months) and high certification costs (hundreds of thousands euro). Equally high is the cost of the important process of maintaining the certification, which, consequently, is not often carried out, possibly because it is not indispensable for the advertising purposes mentioned above.

Common Criteria certification enjoys a fairly wide recognition in the commercial context, both worldwide, through the mutual recognition agreement CCRA[39], and in Europe, through the SOG-IS[40] agreement. However, the recognition is foreseen only at the low levels of certification (EAL1 and EAL2) in the CCRA, through the medium ones (EAL3 and EAL4), ordinarily, in the SOG-IS and, following specific procedures defined for specific types of products, up to the maximum levels of certification in special cases.

The high certification costs have led to the creation, in some European countries, of lighter product certifications that require considerably less time and costs and are comparable with those of Common Criteria certifications at the first level of certification (EAL1). By way of example, France, through ANSSI, issues a first level security certificate called CSPN[41], which may be extended to the upper levels of Common Criteria and easily obtainable within a guaranteed period of less than 8 weeks; CSPN certification is required in some public tenders.

Similarly, the UK introduced the Commercial Product Assurance (CPA)[42], a certification for off-the-shelf commercial security products, where the government itself acted as a driver. Eleven security functions, which are updated regularly, are checked by authorised laboratories at a cost of about GBP 4 500. The CPA is also required in a number of cases as part of public procurement. Other countries that are about to activate light national certifications are Germany and the Netherlands, which are already testing them on an experimental level.

Certification of competences The additional aspect of the certification problem is the certification of the competences of those who operate in the sector, at various levels of responsibility. The theme has been the subject of study and, subsequently, of attempts at "standardisation" and then of "regulation" for

[39] `https://www.commoncriteriaportal.org/ccra/`

[40] `https://www.sogis.org/`

[41] `https://www.ssi.gouv.fr/administration/produits-certifies/cspn/`

[42] `https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa`

some years. In fact, the market has seen a proliferation of certifications issued by various bodies, very often of a private nature, which have endeavoured to meet the needs of companies and organisations in the best possible way.

The certification of competences requires: (i) defining the knowledge domain, (ii) defining how knowledge translates into operational skills, (iii) verifying the degree of maturity (proficiency) of this translation, which defines the degree of autonomy and responsibility. It is a complex scenario, which entails broad discretionary areas. However, there are established systems at the international, European, and national level, which provide guidelines and which, in some cases, are operational and binding. ISO has produced the ISO/IEC NP 27021 (Information technology – security techniques – competence requirements for security management systems professionals[43]), which defines a framework for professionals and a scheme dedicated to more operational figures (ISO/IEC NP 19896-1/2/2/3 "tester" and "evaluator"[44]).

The European standards body[45] (CEN/TC 428) recently issued a wide-ranging framework standard on ICT professionals, EN 16234-1, which is the outcome of several years of activity by the "Consortium Workshop Agreement" CWA 16458, in which Italy has often carried out a leadership role. The European context has produced a "rule"' which, as such, is in force and applies to all the countries of the Union, replacing those by any national standards bodies (for Italy, UNI[46]).

The European general standard defines ICT competences using the eCF scheme 3.0[47], which describes 42 competences and declines a set of 6 professional "profile" families articulated in 22 "second level profiles", which include the *ICT Security Manager* and the *ICT Security Specialist*. The definition of the competences of the eCF scheme is based on a set of notions, i.e., on a domain specification which deliberately provides little details and is unstructured. As a consequence, professional profiles are only broadly defined. Italy has implemented the European standard by issuing the standard UNI 11506:2016[48], which is a framework standard in four parts (called 11621-1/4). Specifically, part 4 (Information security professional profiles) defines 9 "third level profiles"', which are therefore part of the two second level profiles of the European standard. In Italy, AICA has also proposed different levels of certification: at an intermediate level, the *IT Security* certification[49] and at an advanced level, the

[43] `https://www.iso.org/standard/61003.html`
[44] `http://www.uni.com/`
[45] `https://standards.cen.eu/`
[46] `http://www.uni.com/`
[47] `http://www.ecompetences.eu/it/`
[48] `http://www.ithum.it/uni11506`
[49] `http://www.aicanet.it/it-security`

ICT Security Specialist certification[50], which has a matching profile in the eCF framework.

This is the regulatory framework in which the market players operate: anyone who wants to offer a certification service to individuals must necessarily build its offer in compliance with this legislation, as well as in compliance with the other rules that allow a body to propose itself as a "certifying body".

6.5.2 Objectives

The main objective of this action is the activation of the *National Evaluation and Certification Centre (CVCN)* for the verification of the reliability of ICT components for critical and strategic infrastructures envisaged by the DPCM Gentiloni[51] of 2017. The DPCM correctly entrusts this centre to the Ministry of Economic Development (MiSE), which has already gained, as described in the previous sections, significant experience in product certification, through the Ce.Va. of the Istituto Superiore delle Comunicazioni e delle Tecnologie dell' Informazione (ISCTI), then in the commercial sector, starting from 2003 when the *Computer Security Certification Body* (OCSI) was established at the ISCTI. This centre will have to develop the national certification strategy, taking into account the following boundary conditions:

- *The difficulty in separating the consumer market from the national security market* — The digital transformation process, and in particular the spread of IoT, have paved the way for an invasion of commercial software and hardware products in all market sectors, from the consumer sector to critical infrastructures (which obey to market rules as well as public service rules), to national security. Therefore, establishing which products/services to certify for reasons of national security becomes an absolutely vital exercise.

- *The coexistence of Italian and European certification* — The European certification tends to work towards the creation of a digital single market and therefore to break down the barriers that can be placed on a commercial level for the sale of products within the European market and increasing consumer confidence in online services. National certifications focus on national security. Finding a balance between these certifications will not be easy. A European certification system will guarantee a system of mutual recognition between Member States, as this is the basis of every

[50] `http://www.aicanet.it/per-i-professionisti-ict/servizio-di-certificazione`

[51] `https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/04/DPCM-17-02-2017.pdf`

Treaty of the Union. However, mutual recognition shall take into account the fulfilment of specific requirements dictated by national interest for the critical and strategic infrastructures of individual countries.

- *National Product Certification* — Following the example of the French and British national certifications, as well as the German and Dutch experimental ones, Italy itself could adopt a sustainable national certification for cybersecurity. Geared towards national security and critical infrastructure protection, this certification should be compatible with the European one, beyond having predictable costs and time frames for each certification (*affordable certification*). Another important step will be defining a clear boundary for certifiable products, to make certification valuable to companies using those products, by relieving those companies from the burden of compliance checks. Finally, it is important that certification procedures can also be updated to respond to changing needs that may be required to confront new types of attacks. Certification should be seen by companies not as a financial burden, but as an important step to secure the objects that will populate the national cyberspace. In addition, the development of a national security certificate could lead to the creation of local jobs, considering the certification laboratories that will have to be established throughout the territory.

Other important design objectives may be:

- *National certification of companies* — For the security of national supply chains it would be important to introduce a national certification with sustainable costs for medium, small and very small enterprises, which would never have the financial resources to obtain ISO certification. In fact, in the vast majority of cases, attacks on multinationals occur through the tampering with the information systems of some suppliers, usually small or very small companies, whose security levels are certainly much lower and heterogeneous than those of multinationals. It is therefore necessary to develop a system of sustainable certifications, also to be used in the tenders of large private companies, in order to put them in a position to entrust services to companies that have a guaranteed minimum level of security.

- *Extension of safety standards to security* — For medical devices[52] it is necessary to go beyond *safety* certification[53] and to consider security aspects

[52] `http://www.salute.gov.it/portale/temi/p2_4.jsp?area=dispositivi-medici`

[53] `http://www.salute.gov.it/portale/temi/p2_6.jsp?lingua=italiano&id=8&area=dispositivi-medici&menu=conformita`

as well. Security guarantees would also improve the usability and maintainability of these devices (which are often disconnected from the network due to the risks associated with the presence of vulnerabilities), as these guarantees would allow updates or reconfigurations to be made without running the risk of certification cancellation.

CHAPTER

7 Impact on key aspects of digital transformation

Digital transformation is affecting all sectors of our economy and will profoundly change society, our relationships, and our industries. It brings us all within the cyberspace dimension, which creates a spatio-temporal collapse in which citizens, organisations, and cyber criminals alike, from every geographical area, are only 100 milliseconds apart. In this context, cybersecurity is everywhere: in hardware, software, interconnection systems, business or public service processes, contracts, policies, human factors, and cyber-social interactions. Cybersecurity therefore becomes the essential element of this new dimension in order to guarantee, over time, an adequate level of security for our relations, our businesses and our democracies.

This chapter deals with the impact of digital transformation on some of the most important sectors of society, by analysing how, due to digital transformation, the threat is changing in these sectors and how cybersecurity can play a key role in reducing the risk associated with this threat.

7.1 Democracy

In actual digital society, and even more so in the future, "Cyber is the World of Everything". This implies that citizens are not only interested in the protection of sensitive data; digital technologies are spreading like wildfire penetrating the physical world and involving various aspects of daily life, from transport to health services, from the environment to banks, to the educational system, the electoral system and other essential services provided by the PA.

For a democratic state, it is therefore essential to guarantee a good level of cybersecurity both to protect national security (including the protection of free

elections and election campaigns from external interference) and to ensure economic welfare and growth of the country. This requires a serious commitment to developing national cybersecurity strategies that align national security needs with those of economic growth, promoting a more proactive security right from the design of all digital policies and increasing the ability to prevent, deter and detect cyber attacks and respond to them in a coordinated manner with the various institutions involved in the cybersecurity architecture.

Raising the citizens' awareness about the many risks linked to the digital revolution (from computer intrusions to digital addiction, from data theft to ransoms, from sabotage to scams, from fake news to incitement to online hatred) is another important aspect.

The cyber challenge is very demanding because the threats connected to the digital revolution evolve faster than public policies; for this reason it is particularly important to increasingly involve the government, universities, research centres, and companies. The virtuous triangle between institutions, universities, and the business world is the precondition for facing such technological challenges and providing an effective response in any democracy[1].

It is essential to strengthen cooperation instruments in the European and international dimension and it is necessary that democratic countries find a minimum common denominator starting from the full awareness that digital societies are in fact much more fragile and vulnerable than generally thought. Citizens may easily be victims of intrusions, disinformation campaigns, manipulations of all kinds and their fundamental rights can be eroded: in this context democracy itself, with tragic results, may become the victim of *cyber insecurity*.

Cybersecurity and awareness of the risks to which the pervasiveness of the internet and its applications exposes us, therefore, become essential elements for democracy. We would like to consider here two aspects: on the one hand the possibility of using the network to spread fake news in any part of the world and, on the other hand, the possibility of reducing the distance between the State and its citizens by using the internet for political and opinion consultations, with the related risks of fraud that this entails.

Fake news There have always been information campaigns aimed at polarising public opinion in specific directions in the event of both elections and conflicts. The ease with which news of any kind can now be disseminated from anywhere in the world has transformed the net into a powerful tool for the control of opinions. As mentioned in section 3.4, it is essential to develop tools for detecting abnormal diffusion dynamics, *warning* tools for network users, but above all campaigns to raise awareness of the phenomenon and critical use of

[1] `http://www.ispionline.it/en/pubblicazione/italy-building-cyber-resilient-society-18229`

the net based on a scientific research approach of sources and on the risks of being trapped in so-called *echo chambers* (see box on page 61).

E-Voting systems In many countries, methods and technologies for electronic voting are being tested; recently, various proposals to use *Distributed Ledger Technology* have been put forward (illustrated in section 4.6) as the basis of electronic voting systems in which it is not necessary to have an authority that has control over the underlying information systems and that offers voters the opportunity to count and control the votes autonomously, without the risk of addition of illegitimate votes. We have experienced, also in Italy, how these electronic voting systems or platforms can be prone to attacks, see the case of the hacking of the Rousseau platform of the 5 Star Movement of August 2017[2]. These instruments must therefore be used with caution, especially for general elections. In fact, as already seen in the previous chapters, there are no 100% secure computer systems and the chances of a successful attack depend on how much an attacker is willing to invest and, therefore, on how much one can potentially earn from the attack. In the case of parliamentary elections, there can be many who want invest a great deal in order to govern, control or destabilise a nation.

7.2 Essential Services: Energy

Electricity is of fundamental importance for the economy and society in general, as they are dependent on its availability. A power failure can have a direct impact on the provision of other services (transport, finance, communications, water supply, etc.) for which the backup power is not available or the service restoration time exceeds the backup autonomy. The increasing use of renewable resources and polygeneration lead the electricity grid (hereafter EPES - *Electric Power and Energy System*) to become increasingly decentralised. The presence of subjects (prosumers) that produce energy on a small scale and feed it into the network makes the energy flow bidirectional.

The stakeholders involved in the process are growing, as well as the smart IoT devices connected to the grid. The interconnected devices - from smart home devices to electric vehicles - are constantly increasing, and are equipped with advanced functions, requiring the increasingly articulated management of smart grids. The impact of digital transformation in the energy sector affects the entire energy supply chain: from supplies to aggregators, distribution and transport, up to sales and communications with end customers. The separation

[2] `http://www.repubblica.it/politica/2017/08/02/news/hacker_online_dimostra_la_vulnerabilita_di_rousseau_ho_bucato_il_sito_dati_a_rischio_-172221493/`

between IT (Information Technology) and OT (Operation Technology), which is traditional in the electricity grid, disappears and the two levels are intertwined.

ICT thus becomes the mainstay of future smart grid management and, at the same time, its potential weakness. The security approach of ICS/SCADA legacy systems (shown in section 5.5) is based on the unconquerable castle assumption. The limits of this approach are well known and technological solutions for the protection of existing infrastructures (without affecting their functioning and avoiding invasive interventions) have reached an advanced development stage. The discourse is different for new generation networks that, in order to provide services to various users/stakeholders and improve the QoS/reliability of the electricity system (grid balancing, stream optimisation, etc.), will require a more stringent use of ICT and will therefore potentially be more exposed to cyber threats. The design of new power grids will have to rely on the best practices developed at an international level for the cyber protection of distributed ICT systems, adapting them to the specificity of the application domain. Unlike current power grids, cybersecurity will have to guide the design and development of next-generation electricity grids.

Critical Infrastructures in the electric field are very varied; among others we can mention: (i) large traditional thermal and hydroelectric generation plants; (ii) distributed hydroelectric generation systems; (iii) distributed renewable generation (wind power, solar, etc.); (iv) energy transmission and distribution systems, consisting in hundreds of primary stations and tens of thousands of secondary stations.

Remote controlled and distributed systems are exposed to all risks related to this environment. Even large plants cannot be operated in isolation: the security of systems, networks, and protocols is therefore an essential element. Possible threats may sneakily be posed through non-connected means, such as removable media or devices used for maintenance. The remote control of the distribution networks represents a very complex framework for the large number of systems involved, and the infrastructure of digital meters is even more granular. The different needs of the various area involved need to be taken into account and, for each of these areas, an appropriate "by design" protection strategy should be developed, both at ICT and operational logic levels.

When getting closer to the "leaves" of the system, the order of magnitude of the number of objects grows and with it the need to identify a specific security strategy. Without appropriate IT protection measures, access rules to systems could be violated, power failures and cascade effects to interconnected systems and power services may occur and ultimately, irreparable damages to objects and people may take place. Therefore, EPES will face an increasing number of challenges, requiring the development of IT solutions that balance security requirements with high communication speed and guarantee easy scalability to the number of devices involved.

7.3 Finance

Since the financial crisis of 2008, the Italian bank market has undergone a reorganisation that has led to a reduction in the number of credit institutes and their presence on the territory. The digital transformation was also the occasion for a radical change of the business models. The spread of banking services provided via mobile devices has led to the entry of global operators such as Amazon and Google into the payment business. Since the European Directive EU 2015/2366 (Payment services - PSD2) came into force, the monopoly of banks on payment services has ceased. Expansion of the ecosystem to non-bank operators poses various regulatory and operational security problems.

The digitisation of insurance services has a specific element: the interaction with mobile IoT devices, which concerns insurance relying on autonomous devices such as self-driving cars and the provision of *consumer insurance* with premiums linked to measurable quantities on-field, including individual lifestyles. Digitisation involves an increasing use of context data associated with transactions and collected by IoT devices to carry out online analyses. They are aimed at enabling customised proposals and at dynamically pricing products, based on quantitative non-actuarial models of risk calculation. The on-line analytics leads to an increase in the size of the data associated with individual transactions. Such de-normalisation of financial data increased their unit value on the illegal market, making them a more attractive target for attackers.

In recent years, the financial sector has fallen victim to an unprecedented number of attacks, characterised by distributed and coordinated attack vectors. Analyses of the attacks reveal three key threats:

- *Temporary impairment of banking and insurance services* — The corresponding risk is increased by the high level of interconnection of the banking system and has worsened in recent years, also due to the rapid advances in attack technology. Today, attack vectors that can damage the banking system are automated and distributed bot systems. These carriers are difficult to track and deactivate, in part because they use heterogeneous and unsuspected devices such as mobile phones, printers and even toys.

- *Organised large-scale theft of financial data* — Typically, they are carried out through episodic theft (*Data breach*, introduced into the box on page 144) or through the creation of permanent failures (*leaks*) in banking and insurance processes. The growing competence of the attackers has increased their ability to inject attack vectors targeted not only at users of online services, but also at the internal organisational structure of individual banking and insurance operators, through *spear phishing* attacks (introduced in the box at page 29). Injected vectors also exploit errors

and weaknesses in the configuration and management of cryptographic security controls.

- *Violation of the integration of data present within the banking system* — Other than stealing data from the banking system, attackers may alter it, using different attack vectors, ranging from ransomware to IoT devices and false installations (*fake install*) that use mobile device emulators in the cloud to provide false information. With the increasing spread of financial services on mobile terminals, such carriers are amenable to sophisticated cyber attacks aimed at introducing false or misleading data into the system, thus polluting the data underlying the non-actuarial risk models mentioned above. Attacks can damage the quality of the analytics without being detected, causing permanent damage to the system.

A first specific cyber risk factor is the growing number of unregulated companies operating in the financial sector. These operators are very different in size and product offerings, as well as in terms of security processes and controls, making it more difficult to estimate the probabilities in cyber risk assessment models.

A second risk factor is the role of the financial system in the national economic context. Cyber threats to critical banking services, in addition to damaging individual operators, can create a systemic risk to financial stability. For example, coordinated attacks on the banking system can lead to an impairment of the system's ability (in technological and non-financial terms) to inject capital and liquid assets into the corporate system at particular times of the business cycle. The mitigation of this systemic risk is fully part of cyber-warfare scenarios.

A third risk factor is the predominantly defensive nature of the security controls currently in place by banks and other financial sector companies. Without cyber-intelligence action to identify the most critical attack vectors, the attackers' increasing technical abilities may make the defence unsustainable in the long term.

For the insurance industry, an additional risk factor stems from the difficulty of guaranteeing the security of IoT devices integrated into the new insurance services, as illustrated in section 5.4.

7.4 Transportations

Addressing the impact of cybersecurity in the transport sector requires the analysis of three closely related and interdependent areas: vehicles, enabling infrastructures, and services.

In the field of intelligent road transport vehicles, under the following headings fall all initiatives related to *infotainment* and assisted driving, with the ul-

timate goal of self-driving vehicles. Added value services includes initiatives linked to telemetry (road assistance, preventive maintenance), vehicle security (customised insurance policies, smart anti-theft systems), *shared-mobility* and, more generally, platforms for the collection and analysis of data related to vehicles. Finally, intelligent infrastructures now include all initiatives related to optimisation of consumption and flows, and road signs capable of autonomously adapting to the context conditions. In the future, this field will also include infrastructure enabling the management of fully autonomic traffic of self-driving vehicles.

As far as vehicles and services are concerned, the increasingly widespread use of IoT devices, while on the one hand increases passenger comfort and offers innovative services, on the other hand introduces obvious challenges related to the processing of the bulk of data generated (Big Data Analytics) and, above all, new problems of cybersecurity, both in terms of a disproportionate increase of the attack surface and of the capillarity and pervasiveness of possible attacks, as widely analysed in section 5.4.

It has also been pointed out how the newly introduced services, due to the high personalisation, offer new opportunities and pose new challenges at all levels, from pricing to the measurement of the provided services actually, to the on-line dynamic assessment of insurance risk.

The world of transport is governed by a wide range of international standards and, traditionally, the systems used in this context are designed with specific approaches and solutions to address problems of safety, service quality assurance, and fault tolerance. In this regard, it is urgent to define new standards for integrating the existing ones, considering security issues introduced by new technologies and, in particular, by the IoT.

In closing, it is important to point out the radical paradigm shift in the new enabling infrastructures that the country will be necessarily need to equip itself with, in the medium/long term, to allow both the use of fully self-driven road vehicles and the use of drones in urban areas.

Beyond the necessary legislative adjustments, it is necessary to provide, from the outset, rules linking the project and the subsequent construction of these new infrastructures to the concept and practice of *security by design*, as it is not conceivable nor tolerable to repeat, for these cyber-physical infrastructures, the same mistakes made for computer systems, which were initially designed without considering security aspects at all.

7.5 Industry

Digital transformation will profoundly change the way industry does business in the future. The new industry in fact completely loses the concept of a phys-

ical perimeter, typical of the 80s, finding itself in this way immersed in the cyberspace, with suppliers and customers in one big blob. IoT, artificial intelligence, cloud and blockchain technologies are completely eliminating the perimeter by moving data and services outside of it. For example, artificial intelligence algorithms will require increasing data from the company's business network, suppliers and customers, in order to optimise all business processes, from facility management to sales and production. In this context, cybersecurity is everywhere: in the hardware and software used by the company, in contracts with customers, in the supply chain, and in the human factor, thus becoming an essential element of the company itself.

Unfortunately, security is still considered a burden for the company in too many work contexts. The typical condition of security management at the company level is that it is completely misaligned from other activities. The problem is then aggravated by the fact that, faced with the greater complexity of the products, services and systems involved, costs and management problems are constantly growing.

At the company level, there are numerous risks linked to security, such as: loss of critical information (employees, suppliers, users, application data, etc.), interruption of business processes (damage to corporate web systems, mobile systems and devices supplied to company employees, etc.), damage to the corporate image and reputation.

Unfortunately, given these risks, it is still often the case that security and even possible critical situations are dealt with at the individual level, without any standard reference protocol.

It is therefore important, first and foremost, that a process of awareness is initiated within the company which must necessarily involve *everybody*: from the CEO to the CTO, from the Board of Directors to all employees. Awareness that cyber risk is a primary risk to the company's survival is needed, and it is therefore necessary to initiate proper staff training and cyber risk management process based on internationally recognised and approved best practices.

From the point of view of the supply chain, particular attention must be paid to what comes within the company's perimeter in terms of hardware and software. From here stems the primary need for a sustainable certification system that can help a company understand the various products that it can acquire and/or install internally, with the guarantee of an adequate level of security. Enabling technologies and actions should be considered when looking at the corporate cyber profile, physical assets, and data to be protected.

Certainly, in a national context, the sectors of shipbuilding, mechanics, machine tools, agri-food products and other made-in-Italy goods are the most "at risk" as they represent the beating heart of our economy and therefore those most attractive aspects to competitors or state actors. Appropriate countermeasures based on enabling sector infrastructures, such as ISAOs and Regional

Centres of Competence (illustrated in section 2.3), interconnected and closely linked to the national CSIRT, must be put in place to adequately address the threat.

7.6 Tourism and culture

The digital transformation currently underway in many sectors cannot but also affect tourism and its connected educational-recreational activities related to cultural heritage, to museums, and in general to artistic-cultural interests. *Smart tourism* [41]) is the new password to describe the increasing dependency of tourist destinations, their industries, value chain and tourists, by exploiting ICT technologies able to transform huge quantities of data into added value. The use of IoT devices, smartphones and other mobile devices such as cameras and smartwatches, cloud computing, artificial intelligence and machine learning techniques applied to the analysis of tourist visiting habits and social networks, are creating a new ecosystem. Tourists are then at the centre of this ecosystem and are pro-actively directed, guided and advised towards the experiences that best suite their preferences and are most rewarding in terms of learning and exploration of the territory, even in the case of minor cultural assets [26].

Particularly relevant is also the considerable improvement that these technologies have brought to the usability of museums and cultural assets in general by visitors with disabilities. It should not be forgotten that the same technologies also allow for a more detailed and in-depth monitoring of the health of the assets, permitting a more effective preservation, at the same time allowing for a detailed vision of them that was all but unimaginable until just a few years ago.

By analogy with other sectors, this transformation creates new cyber risks, both for tourists and for the assets themselves. The protection of tourists' personal data can be violated: smart applications can, for example, be tampered to direct flows of people from one place to another, causing huge economic damage and/or critical situations of confusion and panic. The asset monitoring networks can be compromised, again by issuing false alarms – with consequent economic damage – or by not issuing alarms in due time, thus leading to irreparable damage to the asset itself.

Therefore, cybersecurity also plays a crucial role in this sector, however presenting some peculiarities of its own. On the one hand, there is the need to have strong domain skills (on the materials of the goods, on the state of preservation, etc.) when assessing the possible tampering of the monitoring networks. On the other hand there is the need to guarantee, in a context with a strong human component in a recreational/recreational attitude, the overall security of people, while at the same time preserving the confidentiality of personal data and

controlling the possible onset of psychosocial mechanisms that could generate panic.

7.7 Press and communication

Communicating information security is a difficult task. The complexity of the issues, the actors involved and the characteristics of its contents have so far favoured the idea that cybersecurity is a matter for specialists. And yet we know that this is not the case for a reason that is before everyone's eyes: the alarm that arises in citizens for the repeated violations of the cybersecurity of banks, companies and ministries that the press is now reporting with a certain frequency. Certainly, this information is sometimes reported using a language for experts in a country like Italy where the basic computer culture is still limited. Other times such information is reported in a hyper-simplified way, with alarmist tones and, sometimes with an incorrect wordings, unsuitable to explain the nature, the extent, and depth of the phenomenon.

To that we must add the journalism crisis and the absence of a shared narrative of facts due to vested interests, standing above the collective ones. This is the case, for example, when the press refrains from revealing names and figures of data breaches, in which the breach of security concerns the banks that guarantee their debts, advertisers, organised political interests and careers, which would be shaken, instead, by a clear disclosure of facts.

Last, but not less important, is the scarce preparation of the ones charged with explaining cybersecurity topics in non-specialist contexts, who instead prefer to retreat into their comfort zone, where only already publicly known topics, able to attract the audience attention with sensational formulas and to arouse ancient fears, are discussed. Such situations prevent journalism from playing their double role as democracy watchdog and civic maintainers of the society's fundamental values.

Alas, there has never been such an urgent need of good information on cybersecurity topics before. There is a need to educate people, to find a common language, to build a culture of information security starting from the dissemination of its most important topics: personal data protection, freedom, security, health.

For all these reasons, informing and educating on cybersecurity themes is a challenge that concerns everyone: citizens, company, institutions, and universities. And, for this reason, it is of fundamental importance to determine a precise common language, which is appropriate for the correct communication of cybersecurity topics.

In addition to national security, cybersecurity should be identified with the protection of personal data that anticipate and define our behaviour. We need it

because our lives are defined by our digital identities, which interact daily with reality, whose core business is the extraction and collection of data about us in order to resell them to the highest bidder. Risks are evident when digital welfare agencies manage everything that makes us citizens with rights (health, pension, unemployment) and by the fact that the IoT "stuff" is not governed because of an insufficient and outdated legislation.

In this scenario, it is even more evident that linguistic confusion related to the world of cybersecurity does not benefit from words referring to deforming concepts. But words are important: he who speaks poorly, thinks poorly. An example is given by the terms *hacker* and *hacking*. The erroneous association between a hacker and a cybercriminal does not only arouse irrational fears, but it also deprives us of the theory and practice, in which, instead, hackers may be the best allies of cybersecurity.

Clarifying the terms at the origin of hacking may favour the mythopoiesis of the *"good" hacker*, *ethical hacker* that summarises in itself the best qualities of modern societies: autonomy, independence, freedom. In fact, the genesis of the word hacker had a positive adjectivation: the first hackers were the pranksters of university dormitories, soon becoming the most talented in the field, just by playing with their software. However, bad literature and the emerging industry of personal computers have over time transformed hackers into secret officiants of esoteric practices. The bogeymen represented by hackers started to embody personal and social frustrations, fears, uncertainties. Yet hackers established the biggest IT industry brands, from Bill Gates to Steve Wozniack, up to Page and Brin.

Luckily, people are often leaps and bounds ahead of those who pretend to represent and guide them, so they have started to challenge the negative stigmata associated to hackers for so long and have become aware that being a hacker, a virtuoso of programming, expert in networks and computers, is the necessary but not sufficient condition to enter illegally into a protected computer system, which inevitably qualifies them. However, these hackers may be extraordinary defenders of our cyberspace, as many indeed are. Therefore, it is important to realise that, today, there are many types of hackers. The ones committing an offence are qualified by the adjective "criminal". The others have to be found, intercepted and trained in a technological and ethical framework to become the spearhead of our cyberspace policies. As we mentioned in section 3.8, it is important that the legislator understands this basic difference and appropriately qualifies it.

7.8 Cyber social security

The cyberspace is not a mere space of interchange, but a cyber-social ecosystem that takes the form of human experience in an increasingly concrete way through the progressive evanescence of the material/immaterial boundary. Reality is compressed in the aggregation of the digital imagery, where the mobile device becomes the augmented mirror of oneself, the extension of the subject, whose individual space-time is determined by the compulsive-narcissist fruition. The private sphere disintegrates in favour of its shared transmutation, while the frantic need for presence in social media platforms, as narcissistic media, colonises the daily routine of *homo digitalis*, de facto de-socialising it, distancing it from the others to leave it hyper-connected in the cyber-social solitude of selfism. In this context, the violent polarisation of audiences, favoured by the processes of communication and interaction within the cyber-social ecosystem, highlights the centralised dynamics of demarginalisation, the reduction of inhibitory brakes, gamification, positive reinforcement, identity recognition by the peer group, as key elements of deviant and/or criminal behavioural structure.

The transition from the hierarchical analogue world to the global digital system, identified in the transition from the twentieth to the twenty-first century, favoured a process that deeply changed the very identity essence of terrorism. The internet and social media platforms do not represent a territory of conquest of contemporary terrorism, but the cyber-social ecosystem within which it has developed, evolving into completely new expressions with respect to the ideologised terrorism of the last century.

In the last twenty years, the presence of information of a terrorist nature online has increased from about ten to ten thousand sites, highlighting the growing centralisation of the internet Jihadism or on-line jihadism, as a complex evolutionary phenomenon characterised by multidimensional, multifactorial and pervasiveness. The propaganda, traditionally aimed at merging the individual into the mass, turns out to be different from the jihadist cyber-propaganda that is articulated through a strategy of *individualised globalisation*, cyber-experiential, mobile, able to overcome the need for direct affiliation, in favour of the cyber-socio-cultural propagation of the jihadist *modus vivendi*, as well as to redesign the reality and colonise the sphere of perceptions in the most vulnerable subjects [3]. After more than a decade of Qaedist culture, the Islamic State was able to create the first truly globalised imaginary, exploiting social media, viralising and stimulating the sadistic-violent and reactionary impulses of the most vulnerable subjects, in order to motivate, inspire and trigger them into indiscriminate terrorist actions in increasingly spontaneous, asymmetrical and low-cost ways, as sadly has happened more than once in Europe in the last two years. *Terrorist avatarism* [2] spreads day by day through file sharing sites and

social media platforms. The Millennials are both prosumers, followers and influencers constantly immersed in the cyber-social ecosystem, characterised by generational vulnerabilities - mainly due to the absence of a digital literacy and a digital awareness pathway - that together with the vulnerabilities of the single individual may favour the violent cyber-radicalisation of younger and younger and increasingly vulnerable people throughout the superficial complexity characterising the disintermediated experience of the jihadisphere, giving rise to two distinct dynamics of violent cyber-radicalisation [4]:

- *cyber-ecosystemic* — cyber-social radicalisation through the social media platforms;
- *cyber-egosistemic* — mobile radicalisation in terms of cyber-social self-isolation and self-radicalisation.

Today, in the post-truth era, the alarming redefinition of the concept of truth, increasingly in line with that of experience sharing in additive and emotional terms, increases the asymmetric capacity of terrorist entities. Fake news, chatbots and cyber-trolling are emerging as the new weapons of the progressive convergence of mobile cyber-social extremism, hate speech and terrorism. The jihadist hybrid warfare imposes, from the point of view of research, analysis, prevention, anticipation and contrast, and the alliance between public-private convergence on the cybersecurity front, which takes into account both the rapid non-linear evolution of the threat and the specific implications in terms of generational and individual vulnerabilities of the cyber-social ecosystem. In order to achieve this, the intervention strategy must be guided by the following essential principles:

- develop knowledge, training and competence based on cross-disciplinary approaches that integrate social sciences with ICT disciplines;
- promote digital literacy, education and awareness at any level, from the earliest ages, as well as within the family;
- prepare strategies and institutional tactics for reputational protection in a cyber-social environment;
- structure resilience and mitigation models based on specific cyber-social dynamics, with particular attention to space-time elements;
- promote the establishment of a location where experts, coming from the public and private sectors, cooperate in the development of evolutionary scenarios about vulnerability and threats, from the cyber-social perspective.

It is, therefore, evident that cybersecurity cannot be considered as such in the absence of its cyber-social dimension, that, among other things, is increasingly relevant in terms of deviance and crime.

CHAPTER

8 International scenario

This chapter considers the international scenario described by Italian colleagues who have been working in foreign universities or research institutions for some time. The scenario shows how different nations are equipping themselves with adequate staff in cybersecurity competence centres, developing national research programmes and, in the case of training, making plans to reach the necessary workforce level for their sovereign state needs as soon as possible. The chapter also highlights the size of the resources allocated by the various countries in this policy area.

8.1 Canada

Established in 2010, "Canada's Cyber Security Strategy"[1] is based on three fundamental pillars: securing government systems, fostering the security of the country's non-governmental vital infrastructure, and ensuring the protection of Canadian citizens. A summary of the practical measures put in place for the implementation of the strategy is included in the corresponding Action Plan for the years 2010-2015[2]. In summary, the government has: (i) divided the responsibilities of the agencies involved in managing security incidents, (ii) announced the

[1] Public Safety Canada: Canada's Cyber Security Strategy – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf, ISBN: 978-1-100-16934-7, 2010.

[2] Public Safety Canada. Action Plan 2010-2015 for Canada's Cyber Security Strategy – https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/ctn-pln-cbr-scrt-eng.pdf, ISBN: 978-1-100-21895-3. 2013

allocation of specific funds for cybersecurity, (iii) strengthened collaboration with the US Department of Homeland Security[3] and with private companies, (iv) launched campaigns to spread a culture of security throughout the public domain.

8.1.1 Cyber Management: actors, roles, and funding

The roles and identities of government actors involved in the management of accidents are defined in the Government of Canada Cyber Security Event Management Plan (GC-CSEMP)[4], which details how events (accidents and reports of vulnerabilities and possible attacks) involving (or which may involve) government structures are to be managed. The main actors of the GC-CSEMP form the core of the Cyber Security Event Management Team, a group dedicated to the management of events. The following other structures have been created to deal with specific issues.

Public Safety Canada Public Safety Canada has, as one of its tasks, the protection of critical infrastructures and the cyber space, and coordinates the implementation of the security strategy. Public Safety Canada handles initiatives to gather feedback from and raise awareness amongst citizens, academics, businesses, and public administrations. It manages the Get Cyber Safe portal[5], which contains news and reports on recent attacks carried out in Canada. Public Safety Canada incorporates the *Canadian Cyber Incident Response Centre*, which coordinates the national response to cybersecurity threats. This centre collects reports from critical infrastructures, government structures and businesses about new threats that can impact vital infrastructures in the country and circulates alerts, reports and periodic bulletins on cyber threats, vulnerabilities and incidents to its partners. It works closely with CERTs in the UK, USA, Australia, and New Zealand.

Communications Security Establishment The Communications Security Establishment belongs to the Department of National Defence and deals with signal intelligence and information security. This includes the Cyber Threat Evaluation Centre, which deals with the detection and technical analysis of cyber threats operating in network infrastructures of national interest. Not

[3] `https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cybrscrt-ctn-plan/index-en.aspx`

[4] `https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html`

[5] `https://www.getcybersafe.gc.ca/index-en.aspx`

only does the centre play the role of technical advisor, it develops and supplies accident management tools.

Shared Service Canada Shared Service Canada is responsible for providing data processing centres and networks to various government organisations. Essentially, it centralises government IT management. The Security Operation Centre incorporates the Government of Canada Computer Incident Response Team, which is the interface for government agencies involved in an accident, and acts as coordinator at all stages of incident management. It should be noted that it is the Canadian Cyber Incident Response Center that acts as technical and coordination consultant for critical infrastructures.

Treasury Board of Canada Secretariat The Treasury Board of Canada Secretariat provides strategic direction to the Incident Management Mechanism to minimise the impact of losses that may affect the government.

The GC-CSEMP also defines the role of secondary actors. These are not involved in the management of all events, but only in those of particular gravity or those which, by their very nature, fall within the competence of a particular actor (Royal Canadian Mounted Police, Canadian Security Intelligence Service, Department of National Defence / Canadian Armed Forces).

Funding Given the number and the heterogeneity of the government structures involved, it is difficult to accurately quantify the funds that the government allocates specifically for cybersecurity. For the period 2001-11, the 2012 Fall Report of the Auditor General of Canada[6] notes that 13 agencies, involved in various ways in cyber activities, received CAD 780 million in emergency management and national security funds. In addition, a further EUR 200 million has been allocated to projects dealing with protecting critical infrastructures from cyber threats. It is not clear how many of these funds have actually been used for cyber-related issues.

8.1.2 Towards a new Canadian national strategy

The government has recently published the results of the national consultation conducted by PSC[7]. The report highlights four key areas of action: spreading the culture of security and basic awareness; improving the preparation of law enforcement and cyber professionals; developing and promoting standards, best

[6] `http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html#hd5b`.

[7] `https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-cybr-rvw-cnslttns-rprt/2017-cybr-rvw-cnslttns-rprt-en.pdf`.

practices, and certifications; increasing funds and resources for all cyber-related areas. In addition, the need for collaboration between government, academia and businesses emerges as very important.

For the years 2012 to 2019, the Reports on Plan and Priorities list cyber-related funding of about CAD 80.6 million allocated to Public Safety Canada. For cyber and IT Security for the 2014-2020 period, a budget of approximately CAD 760.9 million is given to Shared Service Canada[8].

Fundings for Academia

The funds available for academia are divided between those used to create research centres and networks of excellence and those used for basic research.

Networks of excellence and research centres To facilitate the transfer of know-how to the production sector, a network of excellence was created in 2014. SERENE-RISC includes 24 different academic institutions and more than 24 non-academic public and private-sector partners. In 2017, the Canadian Institute for Cybersecurity was opened at the University of New Brunswick. One of the main partners of the centre is IBM. The centre is led by Canada Research Chair in Cybersecurity, Ali Ghorbani.

Basic research In 2017, a specific NSERC call was launched in collaboration with the Department of National Defence. Cyber-related themes were among the areas of interest of the call, the total funding of which was CAD 2.4 million. Other research funds are the Discovery Grants, which are provided annually by the NSERC. For the period 2014-17, the total funding for projects on cybersecurity themes was about CAD 10 million only for computer science and electrical and computer engineering. In addition to the funding mentioned above, the Canada Research Chair is specific for cybersecurity, which is endowed with substantial seven-year grants.

8.2 China

China's cybersecurity strategy is deeply rooted in the government's attention to information management. Throughout the millennia of Chinese history, the role of information in both civilian and military affairs has been of primary importance. The current Chinese cybersecurity strategy and the new law and regulations on cybersecurity are both firmly grounded in this tradition.

[8]Shared Services Canada, 2017-2018 Departmental Plan – `https://www.canada.ca/en/shared-services/corporate/publications/2017-18-departmental-plan.html`, ISSN 2371-7912. 2017

The *Cyberspace Administration of China* (CAC) is the central internet regulator. The CAC is responsible for policy formulation and implementation, domain name registration and content supervision.

The CAC white paper guidelines that are at the core of the Chinese government's cyber governance strategy revolve around four main objectives: (i) Guarantee cyberspace sovereignty and national security; (ii) Protect critical information infrastructures; (iii) Act against cyber terror and cyber crimes; (iv) Expand international cooperation.

On November 1st, 2016, the Standing Committee of the National People's Congress promulgated the first comprehensive Cyber Security Law (CSL). More than 700 million people in China use the internet. The CSL, which came in to effect on June 1st, 2017, is intended to protect the critical information infrastructure, to regulate Chinese user data, to augment internet security, and to monitor and certify foreign technologies that enter the Chinese market.

Under the new CSL, the mainland network operators (a notion that includes a wide array of actors) must adopt stringent internal and operational procedures as well as strong and updated technical protocols in order to prevent computer viruses and cyber attacks. In addition, telecommunication hardware and software, which is under intense scrutiny, requires proper certifications before it can be used in the domestic market. The law applies to both Chinese companies as well as to international companies that operate in China.

The Chinese cybersecurity information architecture also includes many other actors, including the following:

Ministry of Industry and Information Technology (MIIT). The MIIT closely monitors the cybersecurity aspects related to the development of the information highway and cooperation in the communication technology sector in China and abroad.

Ministry of State Security (MSS). The MSS, which is in charge of the security services, also closely monitors the cyber aspect of information and communication technologies (ICT).

Ministry of Public Security (MPS). The MPS is focused on the cyber crimes committed at the national level as well as cyber terrorist attacks. The Ministry is responsible for the oversight and enforcement of the CSL.

China Information Technology Security Certification Center (CNITSEC) The CNITSEC is responsible for security reviews and approvals of network products, services and the related supply chain in accordance with the CSL.

China National Vulnerability Database of Information Security (CNNVD) The CNNVD provides a public database of confirmed software vulnerabilities. CNNVD's early warning capabilities support efforts in both the public and private sectors to address any cyber vulnerabilities.

8.3 France

An initial cybersecurity strategy was developed in early 2010 in France, shortly after the discovery of a cyber attack to spy on the Ministry of Economy and Finance. Subsequently, in October 2015, the then French Prime Minister Manuel Valls announced the French national digital security strategy in order to support the digital transition of the French society. This strategy is the result of a coordinated interdepartmental effort to address emerging issues on digital security. The definition of this strategy confirms that cybersecurity is regarded by France as a national priority and now also concerns individual citizens. The strategy is characterised by five objectives that describe the role of the State in cyberspace:

1. Ensure freedom of expression and action for France and the security of its critical infrastructure in the event of a major cyber attack. This objective will be pursued by strengthening the scientific, technical and industrial capacities necessary to protect national information, ensure network security, and develop a reliable digital economy.

2. Protect the digital life of citizens and businesses and combat computer crime. France will increase its fight against computer crime and its assistance to victims of cyber violence.

3. Ensure the education and training necessary for digital security. France will increase children's awareness of digital security and responsible behaviour in cyberspace, starting at the school age. Higher education and lifelong learning will also include a section on digital security.

4. Contribute to the development of an environment that fosters trust in digital technology and that can make digital security a factor of competitiveness. France will support the development of the economy and the international promotion of its digital products and services, and will ensure the availability of digital products and services with ergonomic, trust and security levels appropriate to the uses and threats of information technology.

5. Promote cooperation between Member States of the European Union (EU) so as to promote strategic digital autonomy in Europe, the long-term guarantee of a cyberspace that is more secure and respectful of the European core values.

From a practical point of view, the five objectives will be achieved through the federation of effort of many actors. In particular: the ANSSI [9] (*Agence Nationale de la Sécurité des Systèmes d'Information*) is the primary actor in charge of measuring and assessing the risks and effects of cyber attacks, addressed

[9] `https://www.ssi.gouv.fr/`

to both public and private institutions; the CNIL[10] (*Commission Nationale de l'Informatique et des Libertés*, i.e., the National Commission for Information Technology and Freedoms) supports professionals to ensure that they comply with current regulations, and helps private individuals to control their personal data and exercise their rights; public research agencies (CNRS, CEA, INRIA) have increasingly invested in research activities on digital security; regional clusters (such as the SCS polo –*Solutions Communicantes Sécurisées* – in the Provence-Alpes-Côte d' Azur region, and the PEC –*Pôle d'Excellence Cyber* – in Brittany) support local industries by funding research projects and sharing infrastructure and development platforms between local companies; finally, funding agencies (NRAs, FUIs, DGAs) have financed several projects on issues related to digital security.

8.3.1 Agence Nationale de la Sécurité des Systèmes d'Information

The role of ANSSI is to promote a coordinated, ambitious and proactive response to cybersecurity problems in France. A law passed in 2013 establishes that "the Prime Minister defines the policies and coordinates the government's action in the field of cybersecurity and cyber defence; and for this purpose the Prime Minister has at the ANSSI at his/her disposal."

In addition to ensuring the proper functioning of daily life and availability of the IT services that have become intrinsically linked to our lives, there is also an economic aspect at stake. In fact, it is essential that companies protect themselves against cyber attacks in order to safeguard their skills, know-how and competitiveness.

The ANSII coordinates the Centre for the Evaluation of Information Security (Centre d'Évaluation de la Sécurité des Technologies de l'Information, CESTI), which is a service provider that certifies product security. In order to be certified, a product must comply with the rules of the French certification scheme, which allows two types of assessment: compliance with Common Criteria and certification of the first level security (Certification de Sécurité de Premier Niveau, CSPN) of IT products. The CSPN was established in 2008 and provides evidence of the security of products such as software, operating systems and hardware devices. The ANSII also has an adequate CERT network (see box on page 17).

8.3.2 Commission Nationale de l'Informatique et des Libertés

The *Commission Nationale de l'Informatique et des Libertés* (CNIL) is an independent administrative authority which is responsible for ensuring that infor-

[10] `https://www.cnil.fr`

mation technology is at the service of the citizen and does not violate identity and human rights, privacy, individual freedom, and public freedom. The CNIL analyses the impact of emerging technological innovations on privacy and freedom and works with its European and international counterparts to develop harmonised regulation. Its main missions are:

- *Informing and protecting* — The CNIL informs individuals and professionals and responds to their requests. It provides practical and pedagogical tools, and regularly intervenes to foster training and awareness-raising actions, particularly in the context of digital education. Anyone can contact the CNIL in case of difficulties in exercising their rights.
- *Accompanying and advising* — The regulation on the use of personal data is implemented through various tools that have the verification of compliance with organisations as their main objective. Citizens are offered the opportunity to comment on draft laws and decrees, giving recommendations to simplify legal procedures and make requests for advice.
- *Controlling and sanctioning* — The CNIL verifies concrete compliance with the law by on-site inspections or upon queries. A control programme is drawn up on the basis of current issues, the main problems identified, and the complaints made. The CNIL is responsible for the control of video protection systems authorised by the prefectures.
- *Anticipating* — The CNIL detects and analyses technologies that can have a significant impact on privacy. It has a laboratory that allows one to experiment with innovative products and applications. It contributes to the development of technological solutions that protect privacy, advising companies at all levels, in the spirit of a privacy-by-design implementation. To enhance its effectiveness, the CNIL has set up a committee of external consultants who contribute to the establishment of an annual study and research programme.

8.3.3 Public research institutions

In France, many efforts have been devoted to digital security over the past years. In particular, the CNRS (Centre National de la Recherche Scientifique) dedicated the year 2016 to security, and recently created a research group (Groupement De Recherche, GDR) for digital security. The GDR for cybersecurity serves as a stimulus for scientific research. Topics covered by the GDR include encryption, privacy protection, multimedia data security, network and infrastructure security, software and hardware system security, and formal security methods.

The GDR organises various events annually: a summer school in cybersecurity; a week of meetings between companies and PhD students (REDOCS),

where doctoral candidates work in groups with the best companies in the sector in order to address real problems; the "national day" (similar to a conference) at CNRS headquarters in Paris; and the l'Atelier sur la Protection de la Vie Privée (workshop on the protection of privacy), whose objective is to bring together researchers from the French-speaking community whose work focuses on the protection of privacy and personal data, offering them a privileged forum to present and exchange their ideas on this issue. The workshop is multidisciplinary and aims to bring together researchers in information technology, law, economics, sociology, and statistics.

8.3.4 Public funding

The Public Research Agency (Agence Nationale de la Recherche, ANR) has funded 35 cybersecurity projects since 2012. Funding for these projects was EUR 6 million in 2012, EUR 3 million in 2013, EUR 6 million in 2014, EUR 1.5 million in 2015, and EUR 3.8 million in 2016.

8.4 Germany

Since the 1980s, the German government has been aggressive in developing ICT technologies, developing broadband technologies and combating digital divide in rural areas. This attitude has allowed Germany to become a European leader in the ICT sector and fourth in the world[11]. Progress in this area has made it possible for Germany to face the challenges of information security and telecommunications ahead of other European countries.

For example, one of the first steps taken by the German Federal Government was the establishment of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) whose objectives, described in the Act of the same name, include protection of federal government IT networks, verification and certification of software and services, advice for the federal administration, and, more recently, alerts of malware infections.

The national strategy on cybersecurity is part of a broader innovation context that covers all strategic high-tech sectors. This strategy, called "High-Tech Strategie 2020", is described in a series of documents that have been drawn up since 2006 and updated every four years. This plan is implementing the recommendations of a panel of experts that from 2006 to 2013 consisted only in members from research and industrial spheres[12]; starting from 2014, members from civil society have also joined the panel.

[11] `http://www.make-it-in-germany.com/en/for-qualified-professionals/working/industry-profiles/it-and-telecommunications`

[12] `http://www.forschungsunion.de/`

Cyber and IT security are addressed within the "Innovation for a mobile and interconnected life" priority in the strategic plan. In particular, the German government recognises that securing the telecommunications and information infrastructure is one of the main priorities. The solutions sought must offer integrity, confidentiality, and availability in ICT in general, particularly for critical infrastructures of industrial production, airplane navigation, the automotive industry, and traffic management. In addition, the government prioritises research on procedures and techniques for defending against malicious software[13].

The 2010 strategic plan renews the interest in security issues and introduces a new priority on digital identities. In this context, the German government intends to create secure processes for authentication and management of electronic identities and a reliable, secure, and flexible infrastructure based on new identity cards. Security projects were refinanced for the next four years[14].

The 2014 strategic plan expands and further details the priorities in the field of cyber and IT security. The new plan introduces the term "Civil Security", which encompasses all priorities in the field of cybersecurity, identifying them as key areas:

- Cybersecurity: The challenges identified in the plan concern all criminal actions that may violate privacy or trade secrets, targeting unauthorised access and interception of data. The government intends to give priority to research on digital forensics and computational criminology. The implementation of the program is described in the "Cyber Security Strategy for Germany";
- IT security: the challenges in this area concern computer and network security in the classic sense of reliability and security. In this respect, the government intends to further develop expertise in the development and protection of ITs. The federal government supports IT security research with two funding programmes: "Self-Determined and Secure in the Digital World" for academic research, and "IT Security in Industry" for small and medium-sized enterprises to improve their security levels;
- Secure identity: the security of identities is of particular interest to the German government because identities form the basis of privacy, commerce and business on the internet. The government continues to support research on the creation of new interdisciplinary approaches with a "Privacy — Self-Determined Living in the Digital World" forum.

[13] `https://www.fona.de/pdf/publikationen/die_hightech_strategie_fuer_deutschland.pdf`

[14] `http://www.ibbnetzwerk-gmbh.com/fileadmin/Content/Foerderprogramme%20und%20pdfs/BMBF%20%20Ideen.Innovation.Wachstum%20Hightec2020%202010.pdf`

The strategic plan on cybersecurity is implemented on different levels. The first is purely for research and is implemented in "Self-Determined and Secure in the Digital World 2015-2020" and partly in "Research for Civil Security 2012-2017". This programme is implemented by the Ministry of Education and Research. The second, "Cyber Security Strategy in Germany", focuses on cybersecurity and is implemented by the Ministry of Interior[15].

8.4.1 Implementation of the Strategic Plan

The Federal Ministry of Research and Education (Bundesministerium für Bildung und Forschung, BMBF) supports the development of solutions to cybersecurity problems by providing funds for research and innovation (academic and industrial) and by funding cybersecurity-oriented competence centres.

ICT 2020 and Research for Civil Security To address the challenges of the strategic plan, the Federal Government created in 2007 a research funding programme for information and telecommunications technologies research called ICT 2020 (IKT 2020 - Forschung für Innovation) managed by the BMBF, which provides research funding in almost all ICT areas.

The new Strategic Plan 2015-2020, *Self-determined and secure in the digital world*, has considerably expanded research topics in the field of cybersecurity and covers 17 research areas organised in four main areas:

- High technology for IT security: hardware-based trusted platform modules, digital identity management, efficient and secure long-term encryption, quantum communication, new security technologies;
- Secure, open, and reliable information systems: transparency and ease of use, protection from internet attacks, demonstrable security of information systems, IT security in heterogeneous system structures, protection of knowledge and products;
- Fields of IT security application: IT security for *Enterprise 4.0*, cybersecurity for critical infrastructure, applications of information and communication technologies in medicine, cybersecurity in transport and logistics;
- Privacy and data protection: privacy and self-determination in the digital world, internet culture and shift of values in the internet age, privacy and big data.

[15] `https://www.bmbf.de/pub/HTS_Broschuere_eng.pdf`

8.4.2 Centres of Competence and Special Actions

The German Federal Government has also funded the creation of three research centres whose mission is to become national and international points of reference for all competences on cybersecurity issues:

- CISPA, Centre for IT Security, Privacy and Accountability in Saarbrücken[16];
- EC SPRIDE, European Centre for Security and Privacy by Design in Darmstadt[17];
- KASTEL, Centre of Competence for Applied Security Technology in Karlsruhe[18,19].

The centres were financed in two phases: 2011-2015 and 2016-2020. The total amount of 2011 funding for the three centres was EUR 17 million over four years. In 2015, the Federal Government renewed its financing by raising the total amount to EUR 41 million over four years.

Helmholtz Center on IT Security: CISPA In 2017, the German Federal Government and the federal state of Saarland, in collaboration with the Helmholtz Association, decided to set up a research centre on cybersecurity in Saarbruecken. The new centre will absorb the current CISPA competence centre and its 200 researchers with the objective, in the medium term, of hosting more than 500 researchers in all areas of cybersecurity. The centre is currently under construction and will be operational from 2018[20].

Financing for small and medium-sized enterprises Germany is one of the few countries that does not offer incentives for research and development in the form of a tax credit. However, the BMBF has provided funding since 2007 to support research in the field of cybersecurity within SMEs. The areas where the

[16] https://www.bmbf.de/de/geballte-kompetenz-fuer-it-sicherheit-1723.html

[17] https://www.bmbf.de/de/groesstes-europaeisches-forschungszentrum-fuer-it-sicherheit-gegruendet-2023.html

[18] https://www.forschung-it-sicherheit-kommunikationssysteme.de/service/aktuelles/kompetenzzentrum-fuer-it-sicherheitsforschung-kastel-startet-durch,

[19] https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/kastel

[20] https://www.saarland.de/dokumente/thema_innovation/2017-03-14_41_Forschungszentrum_fuer_IT-Sicherheit_EN.pdf

government intends to support SMEs are: privacy and data protection, IT security in networked systems and applications, secure and trustworthy ICT systems and technologies, and procedures and tools for handling IT security incidents. So far, the BMBF has approved over EUR 1 billion in funding for more than 1,500 individual or collaborative projects involving some 2,500 SMEs[21].

8.5 United Kingdom

The development of cybersecurity in Great Britain was led very carefully by the government and in particular by the Cabinet Office (equivalent to the Presidency of the Council of Ministers) and by the security services (equivalent to the NSA in the USA). The thrust has focused on universities, research and training, as well as on companies and, of course, their relations. The main features of these initiatives are outlined below.

8.5.1 Academic centres of excellence in cybersecurity

In 2011, the government launched an exercise to identify existing university research capabilities on cybersecurity in the country. Eight universities (Belfast, Bristol, Imperial College, Lancaster, Newcastle, Oxford, Southampton, and University College London) were initially recognised as centres of excellence, with the aim of helping them to develop their capabilities, channel resources and information. In 2017, the number of centres of excellence has risen to fourteen, with the addition of Birmingham, Cambridge, Edinburgh, Royal Holloway, Surrey, and Warwick. The cooperation between the various centres is strongly supported by the government with the aim of fostering a shared agenda at the national level, both in the academic field and in the industrial and governmental world[22].

8.5.2 Cybersecurity Research Institutes

As a complement to the creation of centres of excellence for research, the government has created, in successive stages, four research institutes in cybersecurity:

- *Research Institute on Science of Cyber Security* – RISCS,
- *Research Institute on Verified Trustworthy Software Systems* – RIVeTSS

[21] `https://www.bmbf.de/de/kmu-innovativ-561.html`

[22] `https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496340/ACE-CSR_Brochure_accessible_2015.pdf`

- *Research Institute on Trustworthy Industrial Control Systems* – RITICS
- *Research Institute on Hardware Security.*

Each institute is led by a director who has the responsibility to select specific research projects, promote collaboration with industries, and facilitate the emergence of research communities around the institutes.

The RISCS[23] is dedicated to understanding the overall security of organisations, including technological, human and process components. Its main objective is to support organisations in their decision-making process in cybersecurity, favouring the correct analysis of present risks, their effects and the cost/benefits of applicable countermeasures. The ultimate goal is to provide organisations with the most appropriate tools to make informed decisions about cybersecurity policies.

The RIVeTSS[24] is dedicated to the valorisation and financing of academic and industrial research activities in cybersecurity, focusing in particular on the verification of programs. The Institute brings together all the avant-garde activities in the field of analysis and verification of programs, favouring the development of industrial theories and tools for the verification of real applications. The ultimate goal is to offer verification tools that are always up-to-date and able to keep up with the rapid evolution of cyber-space systems.

The RITICS[25] is dedicated to the study of industrial control systems and national critical infrastructures in cybersecurity. The Institute involves the most representative academic research projects in the sector that are strongly linked to industry. These projects aim to identify three key issues: the real dangers and threats, the business risks to be considered, the most effective and efficient state-of-the-art defence techniques.

The RIHS[26] devotes itself to the study of security techniques for hardware components. The Institute brings together virtually all the academic activities in the sector, encouraging the creation of collaborations and technology transfer in the world of industry. In this context, the Institute promotes the dissemination and learning of the correct use of the latest hardware technologies in the cyber space.

8.5.3 National Cyber Security Center

The National Cyber Security Center (NCSC) supports and finances a number of initiatives at the national level.

[23] `https://www.riscs.org.uk`

[24] `http://gow.epsrc.ac.uk/NGBOViewGrant.aspx?GrantRef=EP/P021921/1`

[25] `https://ritics.org`

[26] `https://www.ncsc.gov.uk/information/research-institute-hardware-security`

Certification of courses of study in cybersecurity The government offers a certification mechanism for cybersecurity courses, with the aim of guaranteeing quality and usability. This creates a virtuous cycle since this certification attracts the best students from all over the world, providing the industry sector with a continuous recruitment of qualified personnel and professional training of cybersecurity-related skills to existing staff. The certifications guarantee that the students make a conscious choice of their course of study, so that they obtain the qualification of expert in cybersecurity that is highly usable in the industrial field.

Financing of doctoral fellowships in cybersecurity The government sustains an annual doctoral programme for students from centres of excellence. The government assists students annually by offering summer internships at the NCSC or the GCHQ on cutting-edge topics in cybersecurity. Cooperation between the government and the centres of excellence promotes the development of a common cybersecurity agenda between government, industry and academia.

Financing of higher education centres in cybersecurity The government currently finances two Cybersecurity PhD schools in Oxford[27] and Royal Holloway[28].These centres offer over 25 fully sponsored cybersecurity PhD posts, and provide a backbone for the entire country to train new cybersecurity experts for industry and academia. The centres offer multidisciplinary training and research programmes that educate experts capable of responding to cybersecurity needs in known or emerging areas of the cyber space. The diversity of skills and abilities favours the creation of innovative techniques to defend against cyber attacks and their continuous adaptation over time.

8.5.4 Other initiatives

Global Cyber Security Capacity Centre The Global Cyber Security Capacity Centre (GCSCC) is a state-of-the-art centre for the development and creation of cybersecurity training programmes adapted and updated to the needs of the real world. The role of the GCSCC is to develop an integrated programme between all areas of cybersecurity that guarantees effective policies and investments in cybersecurity for public administration and industry. The activities are at the forefront of international research and involve leading industry and government players.

[27] `https://www.cybersecurity.ox.ac.uk/education/cdt`

[28] `https://www.royalholloway.ac.uk/isg/cybersecuritycdt/home.aspx`

Cyber Invest Cyber Invest[29] is a government scheme to stimulate private investment in research activities at top university centres of excellence. The investments are managed through government research funding programmes, and foster the creation of new relationships between universities, industry and government with the ultimate aim of confirming the UK's global role in cybersecurity.

Cyber First Cyber First[30] is a government scheme to encourage high school students to undertake cybersecurity careers. It consists of a programme of orientation-focused summer schools, to be undertaken before choosing a university course. This scheme also offers scholarships to cover the cost of university courses in cybersecurity. The ultimate aim of this scheme is to improve the basic cybersecurity skills of future professionals for the industry.

Cyber Security Academy A special national initiative is the Cyber Security Academy of the University of Southampton (CSA)[31]. CSA is a collaborative program between Universities and leading cybersecurity industries, currently the Defence Science Technology Laboratory, Northop-Grumman and Roke Manor. The objective of the CSA is to foster collaboration between academia and industry through a structured approach based on four basic elements: research, innovation, training, and dissemination. Thanks to the close relationship between the University's research teams, the CSA offers a broad portfolio of research projects of industrial interest, an annual industrial doctoral programme, consulting, and professional training programmes on cutting-edge cybersecurity topics. At the moment, the CSA offers training programmes both for managers, with particular emphasis on cyber risks and the new European regulations in the area of privacy and the GDPR, and for technicians in the sector, with particular emphasis on penetration testing and blockchain systems.

8.6 Singapore

Singapore addresses cybersecurity issues with an approach based on joint actions between government, private sector and academia.

[29] `https://www.ncsc.gov.uk/articles/cyberinvest-securing-our-future-through-research`

[30] `https://www.gov.uk/government/news/cyber-first-improving-cyber-skills-in-the-uk?`

[31] `https://www.southampton.ac.uk/research/centres/cyber-security-academy.page`

The National Cyber Security Agency (CSA) is the national body that oversees strategies, operations, education, and development of the cybersecurity ecosystem. The CSA is a department of the Prime Minister's Office (PMO), which deals with all the most important issues for the government, and is managed by the Minister of Communication and Information (MCI).

With a predominantly top-down approach, the government of Singapore creates a series of directives that typically materialise in a bill and are implemented with the help of the private sector and academia. In particular, the bill for national cybersecurity, presented in the second half of 2017 and approved in 2018, provides for substantial public and private investments aimed at the creation of a national cybersecurity ecosystem.

The government's main objectives include the construction of a national network of cybersecurity experts. To this end, the CSA, in collaboration with leading local and international companies, is creating a national academy of training for cybersecurity professionals that will be used both in government infrastructure and critical infrastructures (CII) such as energy, health, and transport with the aim of providing more security and resilience capacity to the digital community of Singapore. The SCA also contributed to the drafting of guidelines for industrial control systems used in the country's critical infrastructure.

To encourage companies, professionals, and students to make a significant contribution to the cybersecurity ecosystem, the government of Singapore organises the Cybersecurity Awards, which recognise and reward the professional talent present in the country.

Internationally, Singapore works closely with national CERTs. For example, at the time of the ransomware WannaCry attack, the SCA exchanged information and strategies with the UK and shared the analysis with the CERT Asia Pacific community. Another area of international cooperation is represented by critical infrastructures that have an impact beyond the country. In this case, the CSA carries out coordinated actions and recurrent exercises to validate the ability to react to potential attacks on critical international infrastructures such as, for example, global payment systems, air traffic control systems, etc.

In recent years, the CSA has signed a Memorandum of Understanding (MoU) on cybersecurity cooperation with national security agencies in several countries including, in chronological order, France, the UK, India, the Netherlands, the United States, Australia, Germany, and Japan.

From the point of view of the implementation of cybersecurity systems and infrastructures, Singapore operates according to a precise methodology that starts from the awareness of the problem to arrive at the solution by analysing (through installation and testing) all the most advanced technology available on the market and deciding whether one or more systems deserve to be integrated and adopted. Following the analysis phase, which consists in an extremely accurate technical evaluation — sometimes accompanied by a strong acquisition

of know-how — it is decided whether to proceed with the adoption of the solutions *as-is* or to create locally a product that fully meets the needs of the country. This modus operandi requires a considerable investment both in economic terms and in terms of effort; however, it has the advantage of providing a global overview of strategies on the market, through interaction with the major players in the sector, with considerable benefits in terms of know-how growth.

In terms of investments and financing, the government of Singapore has allocated approximately EUR 10 million through the National Research Foundation (NRF), a department of the PMO that defines national research and development trends, to activate cybersecurity projects with high marketing potential or skills development that meet the security needs of the country. Each project is a collaboration between a private sector company and a research or academic institution. Among the most interesting projects are those based on machine learning and artificial intelligence, especially in critical infrastructures, which drastically reduce reaction times in detecting anomalous behaviour that could indicate ongoing attacks.

The National Research Foundation (NRF), in collaboration with the Singapore State University of Singapore (NSU), has also created the Singapore Cybersecurity Consortium (SCC), with the aim of maximising synergies between government agencies, the private sector and academia by encouraging joint research activities, the transfer of know-how, training, and technology awareness.

8.7 USA

In the United States, cybersecurity involves different government departments and agencies that often focus on the most specific aspects of cybersecurity in their sector. The most active actors are:

1. *Department of Homeland Security* (DHS) — The Department's interest in national protection is focused on critical infrastructure protection, including energy and transport infrastructure and border and immigration control tools, such as biometric techniques for identification and authentication.

2. *Department of Defence* (DoD) — The Department of Defence's interest[32] is focused on various basic security issues such as defence techniques from cyber attacks as well as applications.

3. *Department of Energy* (DoE) — The interest of the Department of Energy is focused on protecting energy infrastructure and developing security

[32] `https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf`

management tools (such as public key management) in these infrastructures.

4. *National Institute of Standards and Technology* (NIST) — This Institute has been active for about 20 years in all aspects of cybersecurity for government applications and in the development of security standards, such as the Role-Based Access Control (RBAC) standard.

5. *Department of Justice* (DoJ) — The interest of the Department of Justice is focused on digital forensics issues and the use of digital techniques for investigative and forensic activities.

6. *National Security Agency* (NSA) — The interest of the National Security Agency is focused on a number of topics, including Cybersecurity Science.

7. *Federal Bureau of Investigation* (FBI) — FBI is the main federal agency for the investigation of cyber attacks by criminals, terrorists, and enemies from other nations. In particular, the FBI has a division specialising in cybersecurity and actively cooperates with other government departments, including the DoD and the DHS, in various cybersecurity activities. FBI coordinates various initiatives addressing different aspects of cybersecurity, including the Internet Crime Complaint Centre, the Cyber Action Team, the National Cyber Forensics and Training Alliance.

At the governmental level, the various administrations have often appointed a national cybersecurity officer (*cybersecurity czar*) and the past administration launched a national cybersecurity plan[33].

8.7.1 University and other research and development institutions

Universities in the United States are very active on research topics and teaching related to cybersecurity. Many universities have centres and institutes that deal with cybersecurity, often with specific specialisations. A recent ranking has listed the 20 best universities for cybersecurity teaching and research; the top 3 universities in this ranking are Purdue University, Georgia Institute of Technology, and University of Washington, Seattle campus:

- *Purdue University* — in addition to an MS and PhD in cybersecurity, Purdue offers an MS and PhD in Computer and Information Technology with a specialisation in cyber forensics. In addition, MS and PhD courses in

[33] `https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan`

computer science have several cybersecurity lessons (including encryption, network security, data security and privacy, system security, techniques for secure software development, analytical techniques for security). The Centre for Education in Research in Information Assurance and Security (CERIAS) is also home to professors and students from six different faculties and more than 20 departments, who carry out research on all aspects of cybersecurity, with a strong multidisciplinary emphasis.

- *Georgia Institute of Technology* — offers a Master's programme in cybersecurity divided into three specialisations (information security, security of energy systems, security policies). GeorgiaTech is home to the Institute for Information Security & Privacy (IISP).

- *University of Washington, Seattle campus* — offers a Bachelor's degree (BS) with a specialisation in Information Assurance and Cybersecurity (IAC) with professors from various university campuses. The UW also offers an online certificate in cybersecurity, directed to professionals and technicians already in the field of work. The research is mainly carried out at the Security and Privacy Research Lab, which is part of the School of Computer Science and Engineering. Therefore, the research is mainly focused on the more traditional aspects of cybersecurity. Multidisciplinary research is carried out as part of the Cybersecurity Initiative[34] at the l'International Policy Institute (IPI).

What emerges from an analysis of research and didactic initiatives is that, in many cases, in addition to traditional research themes, there are innovative and interesting multidisciplinary initiatives. The education sector is also very active, with specialist courses within the area of Computer Science and Computer Engineering, and Master's programmes dedicated to cybersecurity and other initiatives aimed at professionals already working in the field. It should be noted that in US there is a strong demand for students with skills in cybersecurity and companies are therefore very active in supporting educational initiatives at universities.

In addition to universities, other research and development activities are carried out by numerous ICT companies (from IBM to Google to Facebook). In addition to these, there are companies specialised in cybersecurity (including the well-known Symantec and RSA) and other organisations and laboratories, such as the MITRE Corporation, a non-profit organisation that operates federally funded research and development centres, and MIT Lincoln Lab, founded in 1951 for activities related to national defence.

[34] `https://jsis.washington.edu/research/ipi/ipi-cybersecurity/`

8.7.2 Financing

There are numerous funding programmes to support cybersecurity research. The main programme is the NSF's SaTC (Security and Trustworthy Cyberspace) programme, whose research themes are alined with the federal government's priorities. The programme, which for 2018 has a total funding of USD 68 million, in addition to basic research projects, also funds projects aimed at teaching cybersecurity. In addition to the SaTC programme, cybersecurity issues are also featured in a number of other NSF programmes, such as the CPS (Cyberphysical Systems) programme and the CICI (Cybersecurity Innovation for Cyber infrastructure) programme. In addition to the NSF, several government departments (the DHS, the DoD, the DoE, and the DoJ in particular) have programmes to support academic research and joint industry-university research projects.

Added to this are the numerous research programmes funded by the DARPA, which have covered various topics related to cybersecurity, including formal models for the cybersecurity of military vehicles, and techniques for protection against advanced persistent threats. For example, the Brandeis programme (financed by the DARPA) has recently funded projects dealing with various aspects of privacy, from the development of efficient encryption techniques in order to operate on encrypted data to the development of specific metrics for privacy. In addition to these sources of financing, there is also funding from companies, in particular companies involved in applications for the US government and in the aerospace sector.

CHAPTER

9 Conclusions

The digitisation of our life brings both opportunities and threats. We must be ready to seize the infinite opportunities for development and manage the complexity that this transformation introduces. If not properly managed, complexity will become a difficult threat to contain, with significant consequences for the independence and development of Italy. For this reason, the security of the national cyberspace is a strategic goal to pursue over time.

The spatio-temporal collapse generated by cyberspace, and practically guaranteed anonymity, change the scale factor and the lower operational costs that have always existed, such as propaganda, espionage, and theft. In the past these were highly risky, lengthy, and difficult to manage. Fake news represents, for example, the evolution of disinformation and propaganda (soft power and информатион) aimed at destabilising and confusing the citizens of a country.

Ransomware campaigns, such as *wannacry* and *notpetya*, phishing and fake news are the tip of an iceberg that includes all the threats brought by digital transformation. The submerged part of the iceberg is characterised by thousands of daily targeted or broad spectrum attack campaigns carried out by sovereign states, cyber-criminals and political activists, aimed at critical national infrastructures, companies, government infrastructures, and citizens in order to steal data, monitor behaviours, monitor operations, control operations, and cheat.

As we have seen in the previous chapters, a national policy must be multidimensional and operate in different directions, with a well-defined core, centred on digital technology and information security. It must take into account that Italy, like as many other European countries, does not produce a considerable quantity of hardware (usually it is of Chinese or US origin), software is

very often imported, and industrial control systems are, for the most part, from Germany.

A proper national cybersecurity policy must manage the threats from digital transformation and keep it within an acceptable risk level over time. Combining Italy's economic competitiveness at the international level with national security and interests is the real challenge when setting up a national cyber policy.

Recent recent attacks *Meltdown* and *Spectre* (considered in section 4.1) have shown that there are no secure parts in a processing system and that there is no *silver bullet* that can solve all problems. We need to find articulated solutions to develop secure computations through a distributed system that is intrinsically insecure and, for example, contains our sensitive information. This will be the main technical challenge of the future.

An appropriate policy should favour the creation of a set of infrastructures enabling national cybersecurity (such as those described in chapter 2) for the public, the private and the public-private partnerships. This development must be seen in the context of a national strategy to coordinate the action of vertical competence centres, and then connect similar regional competence centres in a network. Public and private organisations should deploy, either alone or through partnerships, the actions and the technologies described respectively in the chapters 3, 4 e 6. Finally, organisations should protect the technologies that are driving, or will drive, the digital transformation on which they rely (chapter 5). The national cybersecurity policy should be supported by adequate public funding, as everything we have described directly concerns national security. However, private organisations will also have to play their part, by devoting adequate resources to strengthening their defences, as this will benefit the maintenance of their reputation and their ability to continue to produce goods and/or provide services.

An appropriate cybersecurity policy must unite and coordinate governmental departments, industry and research centres to build a country resilient to the new attacks that can directly impact our values and democracy, as well as Italy's prosperity. It is a continuous process, based not only on technology, but also on digital awareness, education, and culture.

In conclusion, in the rest of this chapter we make some recommendations which, if followed, will allow us to respond adequately to the challenge of digital transformation. The recommendations are not intended to be exhaustive, but touch upon points that we consider essential for a correct implementation of a cybersecurity policy at a national level. A policy that, by nature, must necessarily be dynamic and constantly evolving considering technological, regulatory, social, and geopolitical changes.

9.1 Implementation of the Strategic Plan

The speed with which attacks unfold requires strong coordination between threat detection and response and therefore a full implementation of the *National Strategic Cyber Security Plan*. The DPCM Gentiloni (see section 1.3.2) can claim the merits of both having reduced the chain of command and of clarifying roles and responsibilities. There is, however, a need to ensure the rapid establishment of the new structures indicated by the DPCM itself (the *Comando Interforze per le Operazioni Cibernetiche* and the *Centro di Valutazione e Certificazione Nazionale*), the strengthening of those that already exist (the *Nucleo Sicurezza Cibernetica* and the *CNAIPIC*), and the unification and strengthening of the *CERT-Nzionale* and the *CERT-PA* to achieve the *National CSIRT* as required by the European NIS Directive (see section 1.2.1).

We also hope to see a change of pace in the realisation of a *Foundation* which, having as its sole mission the interest of the public good and national security, can support important actions in the private and public sectors, such as those already reported in the DPCM: a *Centre of Research and Development in Cybersecurity* (see section 2.3) and a *Laboratory of Encryption* see section. 4.2). Other nations have developed similar organisations, in forms appropriate to their own regulations. In the United States, for example, the *Federally Funded Research and Development Centres*, such as the MITRE[1], are heading in this direction. Although these centres are private organisations, they have no commercial purpose and assist the federal government in scientific analysis and research, in technological scouting, and in system engineering. In addition, in Italy, the Foundation could carry out other important actions for training, awareness-raising and technology transfer, through

- the creation of an *Cybersecurity Academy* that, along the lines of the music conservatory model, could track over time the growth of talent discovered through programs such as the *CyberChallenge. IT*;
- the provision of an *ethical venture capital fund*, envisaged by the DPCM Gentiloni, for the creation and strengthening of start-ups that develop technology of national interest (see section 9.6). The fund would play a key role in the activation of a cyber ecosystem between universities and business and would allow the many prototypes, *proof of concepts* and innovative algorithms developed by Italian researchers (and often unfortunately left in a drawer) to be transformed into business opportunities [9].

[1] `http://www.mitre.org`

Following the example of other European countries (see chapter 8), it is important to identify and finance research centres of excellence, distributed throughout the country, whose star point is the National Centre for Research and Development in Cybersecurity. These centres should focus on basic technologies essential for cybersecurity (machine learning, data analytics, operating systems, compilers, software engineering, networks and distributed systems, hardware architectures, etc.) and on other subjects relevant to cybersecurity, such as law, economics, psychology, and sociology.

Finally, certification systems for hardware/software/firmware must be developed at the national level, in a context of coexistence and integration with the actions being carried out at the European level. Introducing affordable well-designed certified systems within sectors such as our critical infrastructure can provide greater guarantees of proper functioning and, at the same time, concrete bases for the threat anticipation actions and the risk analysis systems described in chapter 3.

9.2 National digital politics

Strategies for cyber security should be considered an integral part of the *national digital policy*; involving the government as a whole, they should all come under the direct political responsibility of the Prime Minister.

We hope that the Prime Minister will initially be able to set up a group of advisers, as is often the case in the Anglo-Saxon democracies, able interpret digital transformation in the various fields: economic, legal, social, technological, and industrial. This group should be formed of highly qualified scientists, high level business people, and governmental figures, creating a *Committee of Experts*. The Committee should study the impact of specific *disruptive* technologies on the Italian system, such as the IoT, artificial intelligence, pervasive robotics, cryptocurrencies, etc., and define national strategic plans within the framework of these transformations. It is also important for the Committee to ensure that specific measures taken by the government in each sector are alined with the possible changes required by digital transformation, in order to prevent the promulgation of rules that are outdated from the outset or are destined to become outdated shortly.

At an operational level, it would be desirable for the Prime Minister to set up a new unit dedicated to digital policy, with clear competences and effective powers on services, production, and the public administration. The new unit must be organised in such a way that it does not represent, as has unfortunately often happened in Italy, an additional bureaucratic level aimed at verifying procedural requirements in legalistic-judicial terms. On the contrary, it must be able to plan and guide strategic programmes that enable a continuous and con-

trolled transformation of Italy over time, in order to keep it effectively competitive at an international level. Such a unit would, among other things, be in line with what has already happened in other industrialised countries (not only the leading powers, but also the United Kingdom, Germany and France, not to mention smaller countries such as Israel and Estonia), where digitisation has been a significant factor in the economic growth[2]. In this perspective, such unit should also pursue the fundamental objective of setting the foundations for the creation of a *national cyber ecosystem* [9].

9.3 Security as a competitive factor

Many studies by major institutions and third parties, such as the national central banks [16], have shown that *security in cybernetic domain can no longer be considered a certain cost in the face of an uncertain damage*. The exponential increase in attacks, which will become increasingly smart and complex, will be a constant in the near future. Organisations that do not take appropriate countermeasures by developing a solid internal culture of security are destined to become inevitable targets of fatal attacks that will turn damage from uncertain to uncertain. An organisation that is hit will suffer, in addition to the economic damage due to the subtraction of data, reputational damage that could become lethal to its very survival.

Funding research and the industry in this area wisely, but appropriately and within a strategic programme, is a priority. Achieving the highest possible degree of independence in preventing and managing risks related to data, transactions, and critical infrastructures has to be an important objective.

The above considerations on private and public organisations also apply perfectly to the concept of state organisation. The implementation of a multidimensional national programme for the security of Italy is undoubtedly a necessary condition to ensure economic prosperity and, considering the growing integration within the cyberspace of cyber-physical systems, will also ensure the physical security of its inhabitants.

Although security naturally has a financial cost, it should be considered a competitive factor for companies and, at the national level, a fundamental precondition to guarantee the competitiveness of Italy's entire production system.

[2] `http://www.tau.ac.il/~liort/Cybersecurity%20in%20Israel.html`

9.4 Reducing professional migration

Professional profiles in the field of security are sought after around the world. In Italy, we often find ourselves competing with companies that, across borders, offer far better wages. The number of professional profiles related to cybersecurity that have graduated from our universities is still too low, which is also due to the low number of professors in this specific area available in Italy. This is one of the reasons that the activation of new Bachelor's and Master's degree courses in many Italian universities is hindered; there is only just a handful of university degrees currently offered in the field.

The combination of the brain drain of professionals, who leave Italy to take advantage of better salary opportunities, and the training of a limited number of professionals able to meet the existing needs, makes it necessary and urgent to develop brain retention strategies, so that working in Italy on IT security issues is made more attractive. Israel, for example, managed to halt the drain through the creation of an industrial-university-government ecosystem based on technology parks and incentive policies for spin-offs, thus successfully transforming an endemic weakness into a growth factor.

In addition to these programmes, we must pave the way for our best brains in science and entrepreneurship in the field of security to return to Italy. The mobility of the labour market in this sector is an endemic problem that affects other countries as well as Italy. Some large countries are working both on the formation of the future workforce and on strategies for retaining their professionals within the country confines. Among the strategies implemented there are student loans, which have already been pursued in France and Germany, which could also be considered in our country, to keep new graduates in our government structures, in the public service, and in the national industrial system.

Unless adequate policies are implemented, the situation will significantly deteriorate in the coming years. In this respect, it should be noted that countries such as Germany are implementing very aggressive policies to attract not only scientists and entrepreneurs, but also simple foreign students to degree courses within their universities.

9.5 Special plan for Universities

The implementation of the projects and actions proposed in the previous chapters requires an extensive workforce (technicians, engineers, experts, researchers) all over the national territory. In order to achieve this objective, we need a special plan for the recruitment of university researchers and professors in this field.

We have seen in chapter 8 and in section 9.4 that several countries are taking steps to achieve, as soon as possible, a workforce level that meets their needs in the cybersecurity sector. All this, of course, depends on having top-level researchers and trainers in the sector. We hope that, as has happened in the past for other areas (e.g. chemistry in the 1960s), a wide-ranging plan (*piano straordinario*) is launched in Italy for the recruitment of researchers and university professors dealing with cybersecurity and, in general, digital transformation in all its components: legal, economic and, above all, technological. Only significant special actions can accelerate the creation of the necessary workforce.

Currently, the number of professors and researchers in cybersecurity is so small and scattered throughout the country that universities and research institutions cannot independently activate research or teaching programmes. The reason is that security has always been considered as a secondary element, or at most a supporting element, in the development of educational experiences in the computer science and information engineering sectors. However, at this moment in time, the creation of new degree courses in Italy is an essential element towards increasing the workforce. But this can only be done with an adequate number of expert professors in this field at the individual universities.

Apart from the component related to the development of research projects, investing in cybersecurity training provides a unique response to multiple problems of the country system and is indispensable in the context of the progressive digitisation promoted by the *Enterprise 4.0* plan. Training the new generations will trigger a virtuous process in which the managers and technicians of the future will have the skills, cultural background, and operational capabilities necessary to face the technological and scientific challenges that will change our lives in the coming decades. They will thus be able to implement the initiatives enabling us to adapt to the continuous changes and risks we will face in the future. It should be noted that similar considerations can be found in the document of the U.S. Commission established to improve cybersecurity in the U.S.[3].

9.6 National technology

When defining the national cyberspace, it is also necessary to address the problem of the *architectures* of the systems used. The abstract concept of the *architecture* of a complex processing system has been gradually expanded and now includes hardware, software, algorithms, communication infrastructures, platforms, data, processes, methodologies, contracts, human factors, etc.

[3] `https://www.dropbox.com/s/lgw7bq05bstk2m7/cybersecurity-commission-report-final-post.pdf?dl=0`

Italy undoubtedly has interesting players, although not giants, in software integration, communication infrastructures and specific niche markets that can be useful for the development of pieces of a national architecture. There are areas such as hardware that we have long since abandoned. Given the trends in the top-of-the-range semiconductor market, with investments in the order of a few billion euros to set up a production line for latest-generation integrated circuits, building a national production able to compete with the *over-the-top* is unfeasible. On the other hand, it might certainly be reasonable to think of "national" productions for niche applications and/or sectors considered strategic for national security, such as the *vulnerability-tolerant* architectures presented in section 4.1.

Since Italy lacks industrial leaders in various digital transformation sectors, we must find a national approach to integrating foreign technology with national technology within a domestic architecture over which we must have complete control. A national strategy should be defined in order to decide, for each category (or subcategory) of components and technologies, which are to be developed at national level and which ones can be sourced from the foreign market. We should define clear limits for the latter and, for strategic technologies, we should design tools for enabling systematic checks on software and hardware and, above all, for allowing full and unconditional control over such technologies, if necessary. In this respect, the creation and development of a *National Assessment and Certification Centre* is of primary importance.

Bibliography

[1] R. Baldoni, R. De Nicola (curatori): “Il futuro della Cybersecurity in Italia”. CINI - Consorzio Interuniversitario Nazionale Informatica, 2015 – https://www.consorzio-cini.it/index.php/it/component/attachments/download/416

[2] A. Antinori: “Generation-t: terrorist infosphere and evolution of lone wolf terrorism”. In “Lone actors - an emerging security threat”, NATO Science for peace and security series, (Richman A. et Sharan Y., NATO IOS Press), 2015.

[3] A. Antinori: “From the islamic state to the ‘Islamic state of mind’. The evolution of the jihadisphere and the rise of the lone jihad”. In “European Police Science and Research Bulletin - Summer 2017” (CEPOL, European Union Agency for Law Enforcement Training), 2017.

[4] A. Antinori: “Jihadi wolf threat. The evolution of terror narratives between the (cyber-)social ecosystem and self-radicalization”. in Proc. 1st European Counter Terrorism Centre (ECTC) conference on online terrorist propaganda, at Europol Headquarters, The Hague, 2017.

[5] A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. Hankes Drielsma, P. C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, L. Vigneron: “The Avispa Tool for the automated validation of internet security protocols and applications”. In Proc. Computer Aided Verification (CAV 2005), LNCS 3576, pp. 281-285, 2005.

[6] A. Armando, R. Carbone, L. Compagna, J. Cuellar, L. Tobarra: “Formal Analysis of a SAML Web Browser Single Sign-On Protocol: breaking the SAML-based Single Sign-on for Google Apps”. In Proc. 6th ACM Workshop on Formal Methods in Security Engineering. 2008.

[7] N. Aviram, S. Schinzel, J. Somorovsky, N. Heninger, M. Dankel, J. Steube, L. Valenta, D. Adrian, J. A. Halderman, V. Dukhovni, E. Käsper, S. Cohney, S. Engels, C. Paar, Y.l Shavitt: “DROWN: Breaking TLS Using SSLv2”. in Proc. USENIX Security Symposium 2016, pp. 689-706, 2016.

[8] M. Baldi, M. Bianchi, F. Chiaraluce: “Security and complexity of the McEliece cryptosystem based on QC-LDPC codes”, IET Inf. Secur. 7(3), pp. 212–220, 2013.

[9] R. Baldoni: “L’urgenza di un ecosistema cyber nazionale”; Il Sole24ore, pp. 10, 22 Jan. 2017 – https://www.consorzio-cini.it/index.php/it/component/attachments/download/619.

[10] R. Baldoni, L. Montanari Editors: “Italian Cyber Security Report 2015 - Un Framework Nazionale per la Cyber Security” – http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf, ISBN: 9788894137316, 2016.

[11] R. Baldoni, L. Montanari, L. Querzoni (curatori): “Italian Cyber Security Report 2016 - Controlli Essenziali di Cybersecurity” – http://www.cybersecurityframework.it/sites/default/files/csr2016web.pdf ISBN: 978-88-941-3732-3, 2017.

[12] B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi: “Duqu: A Stuxnet-like malware found in the wild”. Budapest University of Technology and Economics, 2011.

[13] K. Bhargavan, B. Blanchet, N. Kobeissi: “Verified Models and Reference Implementations for the TLS 1.3 Standard Candidate”. In Proc. IEEE Symposium on Security and Privacy, pp. 483-502, 2017.

[14] K. Bhargavan, C. Fournet, M. Kohlweiss: “miTLS: Verifying Protocol Implementations against Real-World Attacks”. In IEEE Security & Privacy Magazine, volume 14, pp. 18-25, 2016.

[15] K. Bhargavan, G. Leurent: “On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN”. In Proc. 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS ’16), pp. 456-467, 2016.

[16] C. Biancotti: “The price of cyber (in)security: evidence from the Italian private sector”. Questioni di Economia e Finanza 407, Banca d’Italia, Dicembre 2017.

[17] B. Blanchet: “An Efficient Cryptographic Protocol Verifier Based on Prolog Rules”. In Proc. 14th IEEE Computer Security Foundations Workshop (CSFW-14), pp. 82-96. 2001.

[18] T. Bonaci, J. Herron, T. Yusuf, J. Yan, T. Kohno, H. J. Chizeck: “To Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics” – `https://arxiv.org/abs/1504.04339`, 2015.

[19] F. Buccafurri, G. Lax, D. Migdal, S. Nicolazzo, A. Nocera, C. Rosemberger: “Contrasting False Identities in Social Networks by Trust Chains and Biometric Reinforcement”. In Proc. International Conference on Cyberworlds (CYBERWORLDS 2017), pp. 17–24, IEEE Computer Society, 2017.

[20] G. Caldarelli, M. Cristelli, A. Gabrielli, L. Pietronero, A. Scala, A. Tacchella: “A network analysis of countries? export flows: firm grounds for the building blocks of the economy”. PloS one 7 (10), e47278, 2012.

[21] T. Catarci, F. Leotta, A. Marrella, M. Mecella, D. Sora, P. Cottone, G. Lo Re, M. Morana, M. Ortolani, V. Agate, G. R. Meschino, G. Pecoraro, G. Pergola: “Your Friends Mention It. What About Visiting It?: A Mobile Social-Based Sightseeing Application”. In Proc. International Working Conference on Advanced Visual Interfaces (AVI), pp. 300-301, 2016.

[22] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno: “USENIX Security”, August 10 -12, 2011.

[23] A. Chi-Chih Yao: “How to Generate and Exchange Secrets” (Extended Abstract) In Proc. FOCS, pp. 162-167, 1986.

[24] I. Choi et al.: “Field trial of a quantum secured 10 Gb/s DWDM transmission system over a single installed fiber”, Opt. Express 22, 23121, 2014.

[25] G. W. Clark Jr., M. V. Doran, T. R. Andel: “Cybersecurity Issues in Robotics”. In Proc. IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA), 2017.

[26] T. Collerton, A. Marrella, M. Mecella, T. Catarci: “Route Recommendations to Business Travelers Exploiting Crowd-Sourced Data”. In Proc. 14th International Conference on Mobile Web and Intelligent Information Systems, pp. 3-17, 2017.

[27] D. Coyle: “Best Practices in Data Center and Server Consolidation,” White paper. Gartner, Inc., 2011.

[28] A. Das, J. Da Rolt, G. Di Natale, M.-L. Flottes, B. Rouzeyre, I. Verbauwhede: “Test versus Security: Past and Present”. IEEE Transactions on Emerging Topics in Computing, 2 (1), pp. 50-627, 2014.

[29] D.E. Dennings, “An intrusion-detection model” IEEE Transactions on software engineering, 1987.

[30] A. Durante, R. Focardi, R. Gorrieri: “A compiler for analyzing cryptographic protocols using noninterference”. ACM Trans. Softw. Eng. Methodol. 9(4): pp. 488-528, 2000.

[31] P. Ferrara, E. Burato, F. Spoto: “Security Analysis of the OWASP Benchmark with Julia”. In Proc. 1st Italian Conference on Cybersecurity (ITASEC’17), CEUR Workshop Proceedings 1816, pp. 242-247, 2017.

[32] E. Ferrara, O. Varol, C. Davis, F. Menczer, A. Flammini: “The rise of social bots”. Commun. ACM 59, 7, pp. 96-104, 2016.

[33] R. Focardi, F. Palmarini, M. Squarcina, G. Steel, M. Tempesta: “Mind Your Keys? A Security Evaluation of Java Keystores”. In Proc. NDSS Symposium 2018, to appear.

[34] A. Furusawa, J. L. Sorensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik: “Unconditional Quantum Teleportation”, Science 282, pp. 706-709, 1998.

[35] J. Gantz & D. Reisel: “The Digital Universe in 2020: Big Data, bigger digital shadows, and biggest growth in the far east”. ICD iView: IDC Analyze the future, 2012.

[36] F. D. Garcia, G. Koning Gans, R. Muijrers, P. Rossum, R. Verdult, R. Wichers Schreur, B. Jacobs: “Dismantling MIFARE Classic”. In Proc. 13th European Symposium on Research in Computer Security: Computer Security (ESORICS ’08), pp. 97-114, 2008.

[37] S. Garfinkel: “Digital forensics research: The next 10 years”. Digital Investigation, 7(Suppl. 1), pp. 64-73, 2010.

[38] C. Gentry: “A Fully Homomorphic Encryption Scheme”. Ph.D. Dissertation. Stanford University, CA, USA, 2009.

[39] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden: “Quantum cryptography”, Rev. Mod. Phys. 74, 145, 2002.

[40] O. Goldreich, S. Micali, A. Wigderson: “How to Play any Mental Game or A Completeness Theorem for Protocols with Honest Majority”. In Proc. STOC, pp. 218-229, 1987.

[41] U. Gretzel, M. Sigala, Z. Xiang, C. Koo: “Smart tourism: foundations and developments”. Electron Markets, 25, pp. 179-188, 2015.

[42] P. H. Gum: “System/370 extended architecture: Facilities for virtual machines,” in *IBM Journal of Research and Development* 27(6), pp. 530-544, 1983.

[43] T. Heer, O. Garcia-Morchon, R. Hummen, S. Keoh, S. Kumar, K. Wehrle: “Security challenges in the ip-based internet of things”. Wireless Personal Communications, 61(3), pp. 527-542, 2011.

[44] L. Huang et al, “Adversarial Machine Learning” in Proceedings of 4th ACM Workshop on Artificial Intelligence and Security, October 2011, pp. 43-58

[45] T. Huang: “Surveillance video: the biggest big data". Computing Now, vol. 7, n. 2, 2014.

[46] Y. Hwang: “IoT security and privacy: Threats and challenges”. In Proc. 1st ACM Workshop on IoT Privacy, Trust, and Security (IoTPTS ’15), pp. 1-1, 2015.

[47] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti: “Experimental demonstration of long-distance continuous-variable quantum key distribution”, Nature Photonics 7, pp. 378-381, 2013.

[48] Y. Jin: “Introduction to Hardware Security”. Electronics vol. 4, pp. 763-784. – `http://jin.ece.ufl.edu/papers/Electronics15.pdf`, 2015.

[49] N. M. Karie, H. S. Venter: “Taxonomy of Challenges for Digital Forensics”. Journal of Forensic Sciences, 60(4), pp. 885-893, 2015.

[50] L. Lamport, R. E. Shostak, M. C. Pease: “The Byzantine Generals Problem”. ACM Trans. Program. Lang. Syst., vol. 4 (3), pp. 382-401,1982.

[51] K. Lee: “The internet of things (IoT): Applications, investments, and challenges for enterprises”. Business Horizons 58(4), pp. 431-440, 2015.

[52] R. J. McEliece: “A public-key cryptosystem based on algebraic coding theory”. DNS Progress Report, Jet Propulsion Laboratory, CA, Pasadena, pp. 114-116, 1978.

[53] P. McGee: “Amazon to open AI centre in Germany’s Cyber Valley". Financial Times, October 23, 2017.

[54] J. Memmott, D. Alonso, E. Berlow, A. Dobson, J. Dunne, R. Sole, J. Weitz: “Biodiversity loss and ecological network structure”. in Ecological Networks: Linking Structure to Dynamics in Food Webs, Oxford University Press, 2006.

[55] R. Misoczki, J.-P. Tillich, N. Sendrier, P. S. L. M. Barreto: “MDPC-McEliece: New McEliece variants from moderate density parity-check codes” – http://eprint.iacr.org/2012/409.

[56] M. Mori: “Controinformazione: la protezione dei processi decisionali del Sistema-Paese. Istituto Gino Germani di Scienze Sociali e Studi Strategici - Research Paper, 2016 – `http://fondazionegermani.org/`.

[57] S. Nag, C. Eschinger, F. Ng: “Forecast Analysis: Public Cloud Services, Worldwide, 4Q16 Update,” White paper. Gartner, Inc. 2017.

[58] M. Nemec, M. Sýs, P. Svenda, D. Klinec, V. Matyas: “The Return of Coppersmith’s Attack: Practical Factorization of Widely Used RSA Moduli”. In Proc. ACM CCS 2017, pp. 1631-1648, 2017.

[59] M.A. Nielsen, I.L. Chuang: “Quantum Computation and Quantum Information”, Cambridge University Press, 2010.

[60] C. Polycarpou, K. N. Cassemiro, G. Venturi, A. Zavatta, M. Bellini: “Adaptive detection of arbitrarily-shaped ultrashort quantum light states”. Physical Review Letters, 109, 053602, 2012.

[61] W. Quattrociocchi, A. Scala, C. R. Sunstein: “Echo chambers on facebook”, 2016 – `https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2795110`.

[62] H. Rogers: “Theory of recursive functions and effective computability”, MIT Press, 1987.

[63] M. Rostami, F. Koushanfar, R. Karri: “A Primer on Hardware Security: Models, Methods, and Metrics”. Proceedings of the IEEE, Vol. 102, No. 8, 2014.

[64] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev: “The security of practical quantum key distribution”, Rev. Mod. Phys. 81, 1301, 2009.

[65] A. Semuels: “Why Does Sweden Have So Many Start-Ups?”, The Atlantic, September 28, 2017.

[66] P. W. Shor: “Algorithms for quantum computation: discrete logarithms and factoring”. In Proc. 35th Annual Symposium on Foundations of Computer Science (SFCS ’94), pp. 124-134, 1994.

[67] D. Simshaw, N. Terry, K. Hauser, M. Cummings: “Regulating Healthcare Robots: Maximizing Opportunities While Minimizing Risks”. Richmond Journal of Law and Technology, Vol. 22, No. 3, 2016.

[68] N. Sklavos, R. Chaves, G. Di Natale, F. Regazzoni (Eds.): “Hardware Security and Trust: Design and Deployment of Integrated Circuits in a Threatened Environment”, Springer, 2017.

[69] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov: “The First Collision for Full SHA-1”. In Proc. CRYPTO 2017: pp. 570-596, 2017.

[70] M. Stevens, A. K. Lenstra, B. de Weger: “Chosen-prefix collisions for MD5 and applications”. International Journal of Applied Cryptography (IJACT) volume 2(4), pp. 322-359, 2012.

[71] A. Sudhodanan, A. Armando, R. Carbone, L. Compagna: “Attack Patterns for Black-Box Security Testing of Multi-Party Web Applications”. In Proc. Network and Distributed System Security Symposium 2016 (NDSS 2016), 2016.

[72] C. R. Sunstein: “Republic: Divided Democracy in the Age of Social Media”. Princeton University Press, 2017.

[73] G. Vallone, D. Dequal, M. Tomasin, F. Vedovato, M. Schiavon, V. Luceri, G. Bianco, P. Villoresi: “Interference at the Single Photon Level Along Satellite-Ground Channels”, Phys. Rev. Lett., vol. 116, no. 25:253601, Jun. 2016.

[74] M. Vanhoef, F. Piessens: “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”. In Proc. ACM CCS 2017, pp. 1313-1328, 2017.

[75] R. Verdult, F. D. Garcia, B. Ege: “Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer”. In Proc. USENIX Security Symposium 2013, pp. 703-718, 2013.

[76] S. Wiesner: “Conjugate coding", Sigact News 15(1), pp. 78-88, 1983.

[77] D. A. Wheeler, G. N. Larsen: “Techniques for Cyber Attack Attribution”. Institute for defence analysis. IDA Paper P-3792, 2007.

[78] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, C. Barbieri: “Experimental verification of the feasibility of a quantum channel between space and Earth”, New J. Phys., vol. 10, no. 3, pp. 33-38, 2008.

[79] T. Xu, J. B. Wendt, M. Potkonjak: “Security of IoT systems: Design challenges and opportunities”. In Proc. 2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD ’14), pp. 417-423, 2014.

[80] F. Zappa: “La criminalità informatica e i rischi per l’economia e le imprese a livello italiano ed europeo”. United Nations Interregional Crime and Justice Research Institute - UNICRI, 2014.

[81] Z. Zhang, M. Cheng Yi Cho, C. Wang, C. Hsu, C.Kuan Chen, S. Shieh: “IoT security: Ongoing challenges and research opportunities”. in Proc. 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, pp. 230-234, 2014.

[82] F. Zollo, A. Bessi, M. Del Vicario, A. Scala, L. Shekhtman, S. Havlin, W. Quattrociocchi: “Debunking in a world of tribes”. PloS one 12 (7), e0181821, 2017.

Authors and affiliations

Cosimo Anglano	Università del Piemonte Orientale “A. Avogadro”
Leonardo Aniello	Sapienza Università di Roma
Arije Antinori	Sapienza Università di Roma
Alessandro Arduino	Shanghai Academy of Social Sciences and Università di Torino
Alessandro Armando	Università degli Studi di Genova
Rocco Aversa	Università della Campania *Luigi Vanvitelli*, Caserta
Marco Baldi	Università Politecnica delle Marche, Ancona
Roberto Baldoni	Sapienza Università di Roma
Antonio Barili	Università degli Studi di Pavia
Massimo Bartoletti	Università degli Studi di Cagliari
Cataldo Basile	Politecnico di Torino
Marco Bellini	Consiglio Nazionale delle Ricerche
Francesco Bergadano	Università degli Studi di Torino
Cinzia Bernardeschi	Università degli Studi di Pisa
Elisa Bertino	Purdue University, West Lafayette, USA
Giuseppe Bianchi	Università degli Studi di Roma “Tor Vergata”
Claudia Biancotti	Centro Studi Banca d’Italia
Stefano Bistarelli	Università degli Studi di Perugia
Nicola Blefari Melazzi	Consorzio Nazionale Interuniversitario Telecomunicazioni
Milena Boetti	Università degli Studi di Torino
Andrea Bondavalli	Università degli Studi di Firenze

Silvia Bonomi	Sapienza Università di Roma
Francesco Buccafurri	Università degli Studi Mediterranea di Reggio Calabria
Enrico Cambiaso	Consiglio Nazionale delle Ricerche
Barbara Caputo	Istituto Italiano di Tecnologia
Barbara Carminati	Università degli Studi dell'Insubria
Francesco Saverio Cataliotti	Università degli Studi di Firenze
Tiziana Catarci	Sapienza Università di Roma
Andrea Ceccarelli	Università degli Studi di Firenze
Nicolò Cesa Bianchi	Università degli Studi di Milano
Franco Chiaraluce	Università Politecnica delle Marche, Ancona
Michele Colajanni	Università degli Studi di Modena e Reggio Emilia
Marco Conti	Consiglio Nazionale delle Ricerche
Mauro Conti	Università degli Studi di Padova
Luigi Coppolino	Università degli Studi di Napoli Parthenope
Gabriele Costa	IMT School for Advanced Studies Lucca
Valerio Costamagna	Università degli Studi di Torino
Domenico Cotroneo	Università degli Studi di Napoli Federico II
Bruno Crispo	Università degli Studi di Trento
Rita Cucchiara	Università degli Studi di Modena e Reggio Emilia
Salvatore D'Antonio	Università degli Studi di Napoli Parthenope
Ernesto Damiani	Università degli Studi di Milano
Rocco De Nicola	IMT School for Advanced Studies, Lucca
Alfredo De Santis	Università degli Studi di Salerno
Giuseppe Di Battista	Università degli Studi Roma Tre
Beniamino Di Martino	Università della Campania *Luigi Vanvitelli*, Caserta
Ivo Pietro Degiovanni	Istituto Nazionale di Ricerca Metrologica
Camil Demetrescu	Sapienza Università di Roma
Arturo Di Corinto	Consorzio Interuniversitario Nazionale Informatica
Giuseppe Antonio Di Luna	University of Ottawa, Canada
Giorgio Di Natale	Centre National de la Recherche Scientifique, Francia
Gianluca Dini	Università degli Studi di Pisa
Marco Evangelisti	Università degli Studi di Torino
Daniela Falcinelli	Università degli Studi di Perugia
Gianna Figà Talamanca	Università degli Studi di Perugia

Marco Ferretti	Università degli Studi di Pavia
Massimo Ficco	Università della Campania *Luigi Vanvitelli*, Caserta
Paola Flocchini	University of Ottawa, Canada
Marie-Lise Flottes	Centre National de la Recherche Scientifique, Francia
Riccardo Focardi	Università Ca' Foscari, Venezia
Luisa Franchina	Associazione Italiana Infrastrutture Critiche
Angelo Furfaro	Università degli Studi della Calabria
Giorgio Giacinto	Università degli Studi di Cagliari
Roberto Giacobazzi	Università degli Studi di Verona
Paola Girdinio	Università degli Studi di Genova
Marco Gori	Università degli Studi di Siena
Franco Guida	Fondazione Ugo Bordoni
Giuseppe F. Italiano	Università degli Studi di Roma "Tor Vergata"
Daniele Lain	Università degli Studi di Padova
Nicola Laurenti	Università degli Studi di Padova
Antonio Lioy	Politecnico di Torino
Michele Loreti	Università degli Studi di Firenze
Donato Malerba	Università degli Studi di Bari
Luigi Vincenzo Mancini	Sapienza Università di Roma
Alberto Marchetti Spaccamela	Sapienza Università di Roma
Gianluca Marcialis	Università degli Studi di Cagliari
Andrea Margheri	University of Southampton, GB
Andrea Marrella	Sapienza Università di Roma
Fabio Martinelli	Consiglio Nazionale delle Ricerche
Maurizio Martinelli	Consiglio Nazionale delle Ricerche
Luigi Martino	Università degli Studi di Firenze
Fabio Massacci	Università degli Studi di Trento
Marco Mayer	Università degli Studi Link Campus, Roma
Massimo Mecella	Sapienza Università di Roma
Maurizio Mensi	Scuola Nazionale dell'Amministrazione
Alessio Merlo	Università degli Studi di Genova
Marino Miculan	Università degli Studi di Udine
Luca Montanari	Sapienza Università di Roma
Marco Morana	Università degli Studi di Palermo

Gian Domenico Mosco	Università LUISS “Guido Carli”
Leonardo Mostarda	Università degli Studi di Camerino
Vittorio Murino	Istituto Italiano di Tecnologia
Daniele Nardi	Sapienza Università di Roma
Roberto Navigli	Sapienza Università di Roma
Andrea Palazzi	Università degli Studi di Modena e Reggio Emilia
Francesco Palmieri	Università degli Studi di Salerno
Ida Panetta	Sapienza Università di Roma
Andrea Passarella	Consiglio Nazionale delle Ricerche
Alessandro Pellegrini	Sapienza Università di Roma
Gerardo Pelosi	Politecnico di Milano
Giancarlo Pellegrino	Universität des Saarlandes, Saarbrüken, Germania
Giuseppe Pirlo	Università degli Studi di Bari
Vincenzo Piuri	Università degli Studi di Milano
Maurizio Pizzonia	Università degli Studi Roma Tre
Marcello Pogliani	Politecnico di Milano
Mario Polino	Politecnico di Milano
Massimiliano Pontil	Istituto Italiano di Tecnologia
Paolo Prinetto	Politecnico di Torino
Francesco Quaglia	Università degli Studi di Roma “Tor Vergata”
Walter Quattrociocchi	Università Ca’ Foscari, Venezia
Leonardo Querzoni	Sapienza Università di Roma
Massimiliano Rak	Università della Campania *Luigi Vanvitelli*, Caserta
Silvio Ranise	Fondazione Bruno Kessler, Trento
Elisa Ricci	Fondazione Bruno Kessler, Trento
Lorenzo Rossi	Consiglio Nazionale delle Ricerche
Paolo Rota	Istituto Italiano di Tecnologia
Ludovico Orlando Russo	Politecnico di Torino
Pierangela Samarati	Università degli Studi di Milano
Nicola Santoro	Carleton University, Ottawa, Canada
Beppe Santucci	Sapienza Università di Roma
Vladimiro Sassone	University of Southampton, GB
Antonio Scala	Consiglio Nazionale delle Ricerche
Fabio Scotti	Università degli Studi di Milano

Andrea Servida	Commissione Europea
Paolo Spagnoletti	Università LUISS “Guido Carli”, Roma
Luca Spalazzi	Università Politecnica delle Marche, Ancona
Francesca Spidalieri	Salve Regina University, Newport, USA
Fausto Spoto	Università degli Studi di Perugia
Marco Squarcina	Università Ca’ Foscari, Venezia
Stefania Stefanelli	Università degli Studi di Perugia
Alessio Vecchio	Università degli Studi di Pisa
Salvatore Venticinque	Università della Campania *Luigi Vanvitelli*, Caserta
Paolo Villoresi	Università degli Studi di Padova
Aaron Visaggio	Università degli Studi del Sannio, Benevento
Andrea Vitaletti	Sapienza Università di Roma
Stefano Zanero	Politecnico di Milano

Projects and Actions to better defend our country from cyber attacks

At the end of 2015, the CINI Cybersecurity National Laboratory produced a White Book to describe the main cybersecurity challenges to be faced by Italy over the following five years. The book focused mainly on the risks of cyber attacks and outlined some recommendations, including organisational ones.

This volume has been created as a continuation of the previous one, with the aim of outlining a set of focus areas and actions that the Italian national research community considers essential.

The book touches upon many aspects of cybersecurity, ranging from the definition of the infrastructures and centres needed to organize cyberdefence to the actions and technologies to be developed to be better protected, from the identification of the main technologies to be defended to the proposal of a set of horizontal actions for training, awareness raising, and risk management.

Reading the volume does not require any particular technical skills; the text is accessible to anybody who knows how to use a computer or surf the internet.

Laboratorio Nazionale di Cybersecurity
CINI - Consorzio Interuniversitario Nazionale per l'Informatica

WWW.CONSORZIO-CINI.IT

9 788894 137347