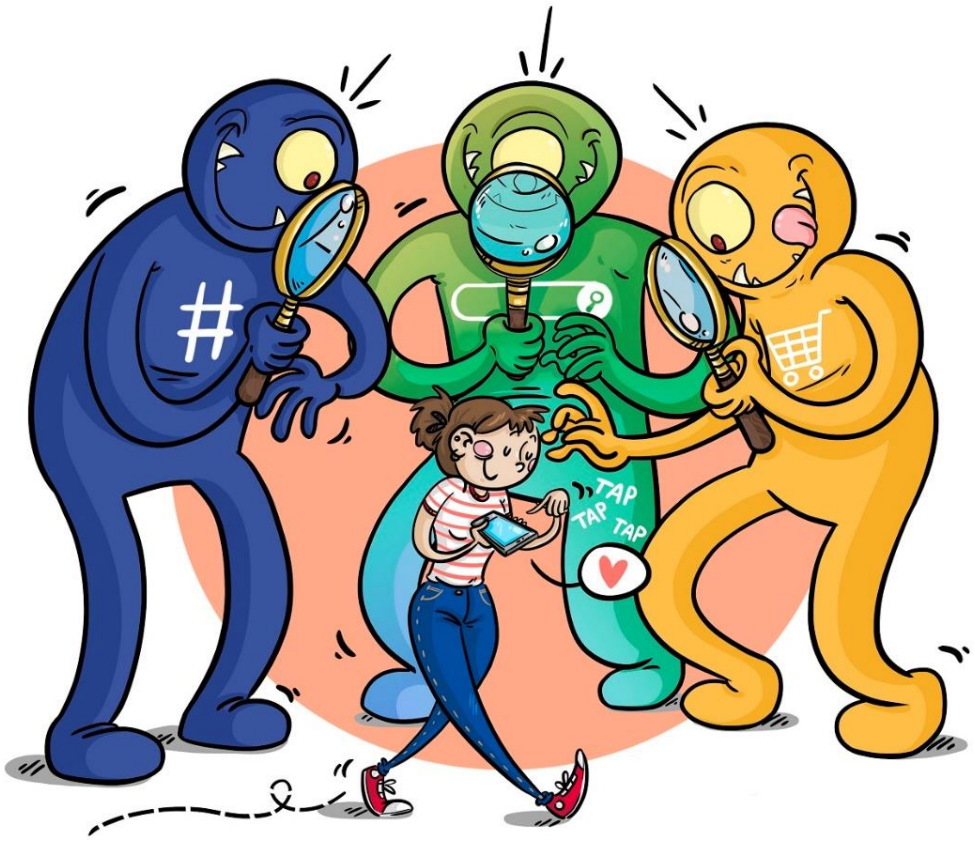
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



CYBERSECURITY RESEARCH DIRECTIONS FOR THE EU'S DIGITAL STRATEGIC AUTONOMY

APRIL 2021

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACTS

For contacting the authors please use fabio.difranco@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Herve Debar (Telecom SudParis), Fabio Di Franco (ENISA), Athanasios Vasileios Grammatopoulos (ENISA), Irene Mantzouranis, Evangelos Markatos (Foundation for Research and Technology – Hellas and University of Crete).

ACKNOWLEDGEMENTS

The authors would like to thank the content reviewers for their insightful comments: Elias Athanasopoulos, Mario Barile, Roberto Cascella, Gabi Dreo, Afonso Ferreira, Thorsten Holz, Yoann Klein, Fabio Martinelli, Philippe Massonet, Svetla Nikova, Bart Preenel, Kai Rannenberg, Matthijs Veenendaal, Erkuden Rios Velasco and Pierre-Jean Verrando.

The authors would also like to thank Sara Jotabe for the illustrations and comics in the document.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-458-9 DOI: 10.2824/43660

EXECUTIVE SUMMARY

The EU has been investing in science, research and innovation. It has been helping the European market to stay competitive, improve the quality and quantity of jobs, and continue to support the European way of life. The impact of our research and innovation depends on the capacity of our economies to become more knowledge-oriented and innovation-driven and invest enough resources in addressing the most important challenges and exploiting the right framework conditions to stimulate innovation.

The European Union Agency for Cybersecurity has identified key research and innovation topics in cybersecurity to address specific strategic objectives: in 2018 the goal was to make the EU more cybersecure ([1]). In this document – the second in the series – the objective is to support the EU's digital strategic autonomy.

The term 'digital strategic autonomy' can have different meanings in different contexts. In this report, it is defined as the ability of Europe ([2]) to source products and services that meet its needs and values, without undue influence from the outside world.

This mission-driven roadmap presents seven prioritised challenges to support research, development and innovation in relation to the EU's digital strategic autonomy. These priorities were derived from a set of 17 topics, which in turn were extracted and synthesised from recent research roadmaps. To finalise these priorities, an open survey took place, which was completed by 94 members of the European cybersecurity research and industrial community. For each of these seven priorities, this document (i) explores the origins of the problem and its importance, (ii) describes the state of the art and the long-term objective of the topic and (iii) recommends the necessary steps to reach this long-term objective.

The open consultation revealed that the highest priority is related to **data security**, with an emphasis on privacy, data protection, trust in algorithms and artificial intelligence. The most important research and innovation challenges also include **software** and **hardware security**, **digital communications security**, **cryptography**, and **detection of and response to cyberattacks**. Finally, **user-centric aspects** related to the overall acceptance of digital services, including understanding the consequences of decisions to enforce or bypass security mechanisms, is a knowledge area that should be included in future research.

Based on our findings, digital strategic autonomy will require an overarching vision of the information and communications technology landscape, driven by ambitious policies that aim to (i) protect European values and (ii) satisfy European needs for advanced and resilient services.

([1]) ENISA, *Analysis of European R&D Priorities in Cybersecurity*, 2018 (https://www.enisa.europa.eu/publications/analysis-of-the-european-r-d-priorities-in-cybersecurity).
([2]) In this document, we use 'EU' and 'Europe' interchangeably, with the understanding that it refers to the current 27 Member States of the EU.

TABLE OF CONTENTS

1. INTRODUCTION

The focus of this work is to identify the necessary research priorities to support the EU's digital strategic autonomy and thus digital sovereignty. In this introductory chapter, we (i) analyse how the terms 'digital strategic autonomy' and 'digital sovereignty' have been used and propose the definition used in this report, (ii) define the scope and target audience, and (iii) outline the structure of the report.

1.1. DEFINITION OF DIGITAL STRATEGIC AUTONOMY AND SOVEREIGNTY

Over the past few years, people have been increasingly using the term 'digital sovereignty'. During the 2018 State of the Union speech, called 'The hour of European sovereignty', President Juncker argued that the time had come for the EU to start working towards 'becoming more autonomous and living up to our global responsibilities' ([3]). The term 'digital sovereignty' may have different meanings in different contexts, ranging from 'nation state sovereignty' to 'personal technological sovereignty ([4]). These contexts extend from individual citizens to social movements and can include entire countries. These ambitions are reflected in the revised EU strategy on cybersecurity, which aims to 'build greater resilience and strategic autonomy' and

([3]) Juncker, J.-C., 'The hour of European sovereignty', State of the Union 2018 (https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en.pdf).
([4]) Couture, S. and Toupin, S., 'What does the concept of "sovereignty" mean in digital, network and technological sovereignty?', paper presented at GigaNet: Global Internet Governance Academic Network, Annual Symposium 2017, 2018 (http://dx.doi.org/10.2139/ssrn.3107272).

which states that it is in the EU's strategic interest to ensure that 'the EU retains and develops the essential capacities to secure its digital economy, society and democracy' ([5]).

According to a recent European Union Agency for Cybersecurity (ENISA) consultation report ([6]), European digital sovereignty can be perceived as encompassing three categories:

European digital sovereignty features three aspects: people, industry and politic

1. data sovereignty over the personal data of EU citizens – the personal aspect,
2. digital sovereignty of the data-driven European industry – the industry aspect,
3. digital sovereignty of the EU and EU Member States – the political aspect.

A recent strategic note of the European Political Strategy Centre (EPSC) addresses strategic autonomy in the digital age ([7]). The note develops concepts related to the capability of Europe to maintain its strategic autonomy in an environment in which digital technologies are pervasive. Strategic autonomy can be defined as 'the ability, in terms of capacity and capabilities, to decide and act upon essential aspects of one's longer-term future in the economy, society and their institutions' ([8]). Strategic autonomy enables nations – and through them the EU – to retain their independence and authority. The note defines three dimensions: industrial, operational and political.

- The industrial dimension requires that Europe is able to fulfil its digital needs. This aspect supports the operational capability of Europe to leverage digital technologies, to operate its critical infrastructure and to ensure that the infrastructure is resilient to cyberattacks. Control of this critical digital infrastructure, in turn, enables political strategic autonomy, namely the ability to make informed decisions freely and independently.
- The operational dimension relates to the resilience of the European communication infrastructure and information and communications technology (ICT) systems. Owing to cascading effects, a vulnerability affecting one service in one Member State can have significant repercussions for others and eventually Europe as a whole.
- The political dimension is associated with digital sovereignty, in a manner well described by Viviane Reding (former Vice-President of the European Commission). She defines digital sovereignty ([9]) as the 'capacity to influence norms and standards of information technology', which is based on the more general definition of sovereignty as the 'capacity to determine one's actions and norms' ([10]).

We can thus define **digital strategic autonomy as the ability of Europe to source products and services that meet its needs and values, without undue influence from the outside world**. Needs may include hardware, software or algorithms, implemented as products and/or services. Values imply a digital ecosystem that is fair and that respects privacy and digital rights. Sourcing denotes that a product or service is either produced in the EU and verified to conform to our needs and values, or acquired from outside and certified to comply with our needs and values. This concept implies that Europe needs to produce some of these products independently and provide such services. However, in cases in which there is a dependence on

([5]) European Commission, Joint Communication to the European Parliament and the Council – Resilience, deterrence and defence: Building strong cybersecurity for the EU, JOIN(2017) 250 final, Brussels, 13.9.2017.
([6]) ENISA, *Consultation paper – EU ICT industrial policy: Breaking the cycle of failure*, 2019 (https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/eu-ict-industry-consultation-paper).
([7]) European Political Strategy Centre, 'Rethinking strategic autonomy in the digital age', EPSC Strategic Notes, No 30, 2019 (https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf).
([8]) Timmers, P., 'Policy in focus – Strategic autonomy and cybersecurity', 2019 (https://eucyberdirect.eu/wp-content/uploads/2019/05/paul-timmers-strategic-autonomy-may-2019-eucyberdirect.pdf).
([9]) Reding, V., 'Digital sovereignty: Europe at a crossroads' (https://institute.eib.org/wp-content/uploads/2016/01/Digital-Sovereignty-Europe-at-a-Crossroads.pdf).
([10]) In 2016, Germany and France promoted European digital sovereignty – ANSSI, 'The European digital sovereignty – A common objective for France and Germany', April 2016 (https://www.ssi.gouv.fr/en/actualite/the-european-digital-sovereignty-a-common-objective-for-france-and-germany/).

sourcing, Europe should still be capable of operating its digital infrastructure without any unjustified influence.

1.2. SCOPE AND TARGET AUDIENCE

The present study provides an analysis of the key research and innovation knowledge areas to support the EU's digital strategic autonomy. Digital strategic autonomy is established by ensuring a solid capacity to develop and maintain a strong ICT industry, which in turn will lead to strategic autonomy for Europe and its citizens. The development of ICT companies, which should be supported by a robust research and development ecosystem, can contribute to creating a pipeline of innovations that are developed in Europe and that are primarily designed to meet the needs and values of European citizens.

EU digital strategic autonomy is the ability of Europe to source products and services, without undue influence from the outside world.

Therefore, the main objective of this report is to identify, analyse and describe the most important knowledge areas necessary for developing products and services that meet the EU's needs and values and that guarantee a resilient ICT infrastructure. Investing in these areas of cybersecurity research and development is of paramount importance for controlling and operating resilient ICT infrastructure without interference. Resilience to technology attacks, such as denial of service or malware, and resilience to data attacks, such as social platform incidents, are key components that Europe should encourage by developing and guiding the appropriate technologies.

This research roadmap could serve policymakers in providing objective-driven strategic guidance for defining future projects and investments in cybersecurity. The prioritised knowledge areas could be of use in defining industrial and research policies, with the ultimate goal of ensuring EU digital autonomy and sovereignty. Moreover, researchers could use the research and development areas presented in this report as a guide to addressing the research and technological challenges and reviewing the state of the art and the long-term objectives of each priority.

1.3. STRUCTURE

This report is organised as follows.

- **Chapter 2** contains a number of practical examples illustrating fictional scenarios in which the need for digital strategic autonomy in Europe is highlighted, and what could happen if Europe fails to maintain its digital strategic autonomy.
- **Chapter 3** further analyses the research and innovation knowledge areas that were considered by the cybersecurity community to be the most significant for ensuring European digital strategic autonomy. A comic strip and an independent scenario are included for each prioritised research topic to improve audience engagement and help readers adopt lateral thinking.

  The seven prioritised research areas are:

  1. data security,
  2. trustworthy software platforms,
  3. cyber threat management and response,
  4. trustworthy hardware platforms,
  5. cryptography,
  6. user-centric security practices and tools,
  7. digital communication security.

- **Chapter 4** includes considerations of transversal aspects that cover all research areas and that will reinforce the European impact on cybersecurity.

- **Annex A** introduces the methodology used in the report, the knowledge areas considered in the survey and the list of priorities identified as a result of the open consultation. It concludes with an analysis of respondents by country and by organisation type.

2. STRATEGIC AUTONOMY IN EUROPE: SCENARIOS

Digital technologies have pervaded our everyday lives, to the extent that it is extremely hard to live in their absence. In the following paragraphs, fictional – yet plausible – scenarios that could undermine the EU's strategic autonomy are briefly described.

Interference with navigation services. *'*A cyberattack against a navigation server generated fake traffic causing confusion to drivers and autonomous vehicles.' In this context, autonomy translates to the availability of maps and associated information and obtaining access to positioning and routing algorithms and systems, without fearing that access to these data might be blocked or that the data are fraudulent. However, external interference (e.g. Global Positioning System signal jamming) may affect specific activities such as military exercises ([11]). The areas of Data security and Trustworthy software platforms are analysed in Sections 3.1 and 3.2, respectively.

Untrusted artificial intelligence (AI). 'Hackers found a way to poison the results of an AI cooking app to promote specific products.' Although interference with cooking seems to be limited with respect to autonomy, it is an example of when one's freedom of choice might be altered if the recipes or ingredients received are not of interest to the recipient. Moreover, one's choice to buy the ingredients from a provider might be influenced by an altered e-commerce list presented. The area of Data security is analysed in Section 3.1.

Disruption in the medical care system. 'A hospital became out-of-service following a ransomware attack that rendered its digital systems unusable.' Cyber-securing our medical infrastructures is of great importance, especially during pandemics (such as during the coronavirus disease 2019 (COVID-19) pandemic), so that they are available when we need them the most. All medical devices are seamlessly connected, to support care staff and patients with regard to various procedures of medical care, monitoring, administering medicine, connecting beds and rooms, and using global platforms to exchange information. Medical files have to be available to authorised personnel to enable them to provide efficient care. However, the high level of dependence of the medical infrastructure on ICT, and its vulnerability to malicious code, has already been seen in the impact of ransomware, such as the WannaCry ransomware used to attack the National Health Service in the United Kingdom ([12]), the ransomware attack on the Rouen University Hospital Centre in France ([13]), and more recently the ransomware attack on a hospital in Germany, which was directly linked to a death ([14]). The capability to verify the absence of vulnerabilities and malicious code in the infrastructure, software or services we procure in combination with the ability to defend systems against cyberattacks are also important elements of autonomy. The areas of Trustworthy software platforms and Cyber threat management and response are analysed in Sections 3.2 and 3.3, respectively.

([11]) https://www.defensenews.com/global/europe/2018/11/16/finland-norway-press-russia-on-suspected-gps-jamming-during-nato-drill/
([12]) https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/
([13]) https://www.lemonde.fr/pixels/article/2019/11/18/frappe-par-une-cyberattaque-massive-le-chu-de-rouen-force-de-tourner-sans-ordinateurs_6019650_4408996.html
([14]) https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/

No safety at home. 'A new vulnerability affecting 1 billion smart cameras was discovered.' Smart home security mechanisms (such as electronic locks, cameras, alarms and remote-controlled doors) aim to protect people's personal space and assets while preserving the user's experience. Products sourced from untrusted producers may feature software or hardware vulnerabilities or even contain backdoors that could be triggered/exploited by malicious attackers, and thus may compromise domestic safety and people's privacy. The areas of Trustworthy software platforms and Trustworthy hardware platforms are analysed in Sections 3.2 and 3.4, respectively.

Lack of supply chain availability. 'Lack of supply of many digital components was observed after a manufacturer, located outside the EU, temporary halted exports because of non-compliance with EU regulations.' Many products and services require electronic components and platforms. Supply chain issues may result in a lack of availability of electronic components required by the EU industry. Without such components (e.g. processors and chips), the supply of both personal electronic devices and elements of the digital infrastructure cannot be guaranteed, which potentially endangers Europe's strategic autonomy in industries that rely on the supply of devices, such as the automotive industry. The supply chain problem is linked to the areas of Trustworthy software platforms and Trustworthy hardware platforms, which are analysed in Sections 3.2 and 3.4, respectively.

Absence of control over communication infrastructure. 'Hackers monitored users and their data by exploiting vulnerabilities in the new generation of mobile communications.' The evolution of digital communication infrastructure has been guided by standards. Europe has been a leader in mobile telecommunication standards (e.g. the Global System for Mobile Communications ([15])) and should continue to guide coordinated secure technological advances through leadership of standardisation to ensure its autonomy over communication infrastructure. However, this has become increasingly challenging as the telecommunication industry transforms from an industry based exclusively on hardware to a software- and even cloud-based industry. The areas of Trustworthy software platforms and Digital communication security are analysed in Sections 3.2 and 3.7, respectively.

Need for post-quantum secure communications. 'Encrypted network traffic recorded today could be broken in 10 years through the use of post-quantum computers.' To preserve today's secrets for longer, the EU will have to develop post-quantum cryptography. For this reason, the EU should opt for the adoption of and transition to post-quantum secure communication infrastructure when needed. The area of cryptography is analysed in Section 3.5.

Lack of control over a product or system lifecycle. 'Numerous smartphone devices are vulnerable as they do not receive the latest security updates.' The current best practice for suppressing vulnerabilities in software-based systems and products after production is patching. This process is well accepted by end users. However, the patching processes for hardware devices (e.g. firmware updates and updates to the lower layers of the infrastructure) remain difficult and a research topic, for example in the context of the internet of things (IoT) ([16]). The patching process itself is a strategic autonomy concern. On the one hand, patch availability is critical for protection ([17]) and the absence of reliable and timely patches could have an impact on strategic autonomy. On the other hand, unverified software updates may include malicious code that could insert backdoors ([18]) or introduce new vulnerabilities into the system. Controlling patch availability and authenticity is thus critical for service operation and consequently strategic

([15]) https://en.wikipedia.org/wiki/GSM
([16]) Sönnerup, J. and Karlsson, J., 'Robust security updates for connected devices', Master's Thesis, Lund University, Sweden, 2016 (http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8841016&fileOId=8872290).
([17]) https://www.zdnet.com/article/fortinet-removes-ssh-and-database-backdoors-from-its-siem-product/
([18]) https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

autonomy. A complementary issue is assurance and certification. The areas of Trustworthy software platforms, Trustworthy hardware platforms and user-centric practice and tools are analysed in Sections 3.2, 3.4 and 3.6, respectively.

Critical infrastructure interruptions. 'Hackers infiltrated the power grid system and took it out of order.' The protection of critical infrastructure against cyberattacks is of great importance, as it is needed to preserve the EU's autonomy. A disturbance in the operation of the healthcare system during a pandemic, such as the COVID-19 pandemic, may put human lives in danger. In the transport sector, our heavy reliance on guidance mechanisms could, for example, significantly impair all transport systems, such as autonomous vehicles, trains or flights. As a result, this may affect our safety, as accidental or malicious failures can occur. The same is true for the energy sector. Failures in providing essential services threaten the EU economy and the well-being of its citizens and may also cause loss of human lives. Deploying and operating self-sufficient critical infrastructure and essential services is a key element of Europe's digital strategic autonomy. The areas of Trustworthy software platforms and Trustworthy hardware platforms are analysed in Sections 3.2 and 3.4, respectively.

Loss of algorithmic control leading to loss of understanding of decision support algorithms. 'A false positive alert of an AI-powered cyberdefence system caused problems in the internal network of the ministry.' The United States and China are investing heavily in AI technologies. Global companies based in the United States, such as Google, Amazon, Facebook, Apple and Microsoft (GAFAM), and their Chinese counterparts (Baidu, Alibaba, Tencent and Xiaomi (BATX)) are doing so to be able to fully control the technology for their own benefit. Governing both the data and the algorithms that process it appears to be necessary to ensure that digitalisation is beneficial to European society. However, not understanding where the data are located, how they are protected in transit or at rest (e.g. using encryption, anonymisation and/or access control technologies) and how they are processed raises endless suspicions regarding the soundness of the digital society. Such concerns have been raised by the significant amounts of evidence on social platform incidents, such as the Cambridge Analytica data scandal ([19]). Europe should ensure strategic autonomy by having trustworthy and explainable AI systems. The area of Data security is analysed in Section 3.1.

Lack of data. 'The application of AI systems in Europe may be limited because of data protection regulations.' There is a strong belief that all problems are solvable, as long as vast amounts of data are available and can be processed by powerful algorithms. For example, the application of AI to medical data may significantly improve diagnosis and treatment. However, Europe has strong privacy requirements that require data to be handled according to regulations. Controlling access to and use of data is critical to ensuring that we have enough data available to feed algorithms (and in the end command and control systems). As a side note, access to data (e.g. data for cyber threat intelligence) is becoming critical for cybersecurity operations. The areas of Data security and cyber threat management are analysed in Sections 3.1 and 3.3, respectively.

All of the abovementioned scenarios show how activities – in many cases critical activities – may be disrupted and, when mapping such problems on a larger scale, may affect European citizens as a whole. To preserve Europe's strategic autonomy, which could be affected by such problems, we should leverage our strong research and development workforce and our societal values to develop and provide products and services that cover the EU's needs and meet the EU's values.

([19]) https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/

3. KEY AREAS FOR DEVELOPING THE EU'S DIGITAL STRATEGIC AUTONOMY

In this chapter, the seven most important knowledge areas that were defined through consultation with the cybersecurity community are presented. The priorities are ranked by order of preference by the community, the highest appearing first. A full list of all the knowledge areas is available in Section A.2.

3.1. DATA SECURITY

Every morning, Alice fires up her preferred navigational application on her phone to navigate from home to work. Without thinking about it, she provides information to the system about her location and speed. In turn, the guidance system provides her with information about road conditions and the best itinerary to reach her destination. The application may also assist her in selecting the best time of departure, by estimating her time of arrival. However, does Alice know what kind of personal data she provides and how these data are being processed?

3.1.1. Current and future context of data security

As shown in the abovementioned scenario, every time Alice uses her smartphone she sends information about her current location to the cloud. Alice provides information not only when she travels but also when she shops, when she eats and when she works, since most of the applications and services she uses collect information about her. Unfortunately, if she does not provide these data, she will not be able to use these applications or services. To make matters worse, Alice often has difficulties in understanding how much information she provides, when she provides it, and for what reason this information is being used, beyond her current needs.

As if this was not enough, the deployment of home assistant devices, which listen to and may potentially record every private conversation, may result in constant monitoring even inside our homes. This constant monitoring will continue to feed AI algorithms aimed at taking care of all of our human needs, from the simplest to the most complex.

3.1.2. Definition and criticality of the problem

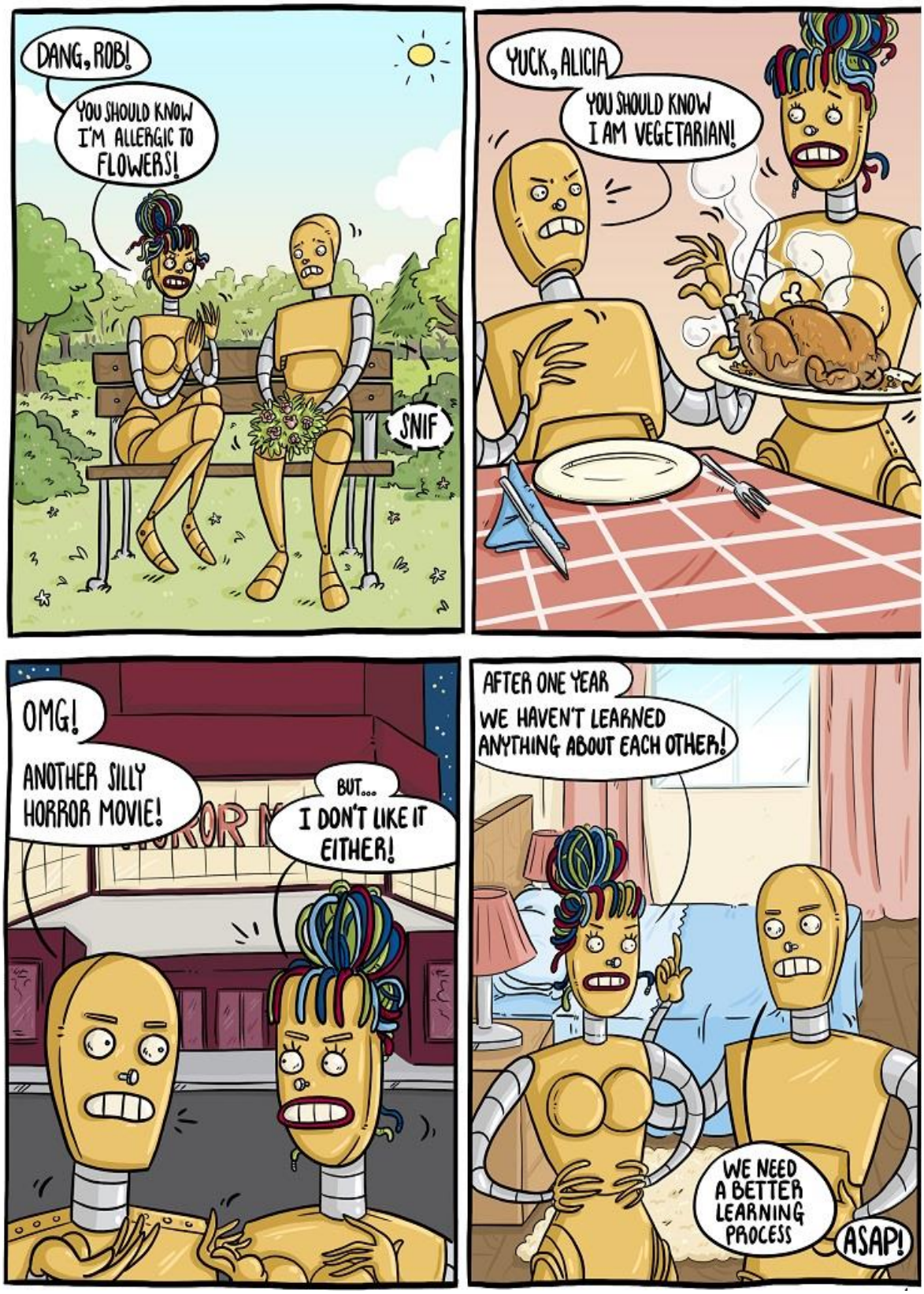
AI is becoming the new driver of daily and critical services, such as powering energy production and distribution, managing multimodal transport and piloting healthcare infrastructure. Without trusting the data and the algorithms that process it, it is hard to imagine a trustworthy future for our digital society. The issue in question is the risk of losing control over both information and the algorithms that process it. Although the EU has taken the initiative to protect EU citizens'

information by enforcing the General Data Protection Regulation (GDPR) ([20]), this loss of control might have already happened to a certain extent, since many people worldwide rely on services provided by GAFAM or BATX for both collecting and processing data.

With respect to data, the top cloud providers (Amazon, Microsoft, Google, SalesForce) are based outside Europe. However, there is an imminent risk in this situation, as there are national regulations, such as the Cloud Act ([21]) in the United States, that may force providers to grant access to European citizens' data. This goes against the provisions of regulations such as the GDPR ([22]), which aims to protect the personal data of EU citizens. European and Member States initiatives exist for launching a sovereign cloud ([23]), but their impact remains limited at this stage, in terms of both market penetration and scope.

With respect to algorithms, we are also becoming used to treating algorithms as a cloud commodity; namely, a lot of machine learning code relies on one or two very popular libraries ([24]). Although this is very efficient for many software developers, providers of the libraries could potentially gain power over information about software related to machine learning (e.g. through information on downloads and requests for support). To make matters worse, our focus on the results of the libraries may deprive us of our capability to understand and develop the basic technology behind such libraries. Moreover, if the suppliers discontinue development or maintenance of the libraries for internal reasons, this may affect countless services that have a direct dependency on the libraries.

([20]) European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, OJ L 119, Brussels, 4.5.2016, p. 1–88 (https://eur-lex.europa.eu/eli/reg/2016/679/oj).
([21]) https://en.wikipedia.org/wiki/CLOUD_Act
([22]) https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf
([23]) https://vpnoverview.com/news/european-cloud-service-gaia-x-in-the-making/
([24]) One of the most used libraries in machine learning is Tensorflow, developed by Google. It uses Apache License 2.0, so it may be hosted by third parties for download and may be further developed by the community. However, most open-source projects are hosted on sites such as GitHub and NPM (both based in the United States).



Although we interact with AI in our everyday lives, we are not always aware of how the learning process works. Explainable and trustworthy AI algorithms that provide us with a clear understanding of how they are processing data are needed.

3.1.3. Efforts towards ensuring data security

Data protection is one of the rights enshrined in Article 8 of the EU Charter of Fundamental Rights ([25]), and the introduction of the GDPR has created an obligation to protect EU personal data. It has had a worldwide impact on countries and businesses, leading to changes in laws and practices even outside Europe.

Several projects are tackling this aspect of the GDPR and tools related to it. For instance, the PDP4E project ([26]) offers software, system engineer methods and software tools that allow engineers to apply data protection principles in a more structured way to the projects they carry out. The DITAS project ([27]) aims to provide content-based solutions to virtual data containers, enabling secure computing at the edge. The Decode project ([28]) increases the digital strategic autonomy of European citizens by enabling them to produce, access and control their data and exchange contextualised information in real time and in a confidential and scalable manner. In this context, ENISA has published a number of studies on the security of personal data ([29]) and, in particular, cryptographic protocols and tools and their possible implementation in real-life applications. Recently, ENISA has published new studies on security and privacy considerations that arise from the use of autonomous agents ([30]) and best practice and techniques for pseudonymisation ([31]). However, data security extends beyond the data protection scheme and includes the security of any type of data in transit, in use and at rest.

Another notable European activity is the deployment of several regulatory frameworks that formalise the needs and requirements of an EU digital economy. The recent ENISA mandate on information technology (IT) certification schemes ([32]) should hopefully provide certain assurance levels regarding digital products and services deployed in the EU, although the exact extent and impact of this regulation remains to be evaluated.

It seems that these activities are supporting the development of privacy-aware regulations. However, tools for managing personal data properly have not been disseminated widely, and the security of algorithms that process data needs to be studied further.

Moreover, Europe has started to support research projects on developing technologies related to AI (under, for example, the Horizon 2020 AI4EU ([33]) initiative) while making data openly available to support the development of algorithms (e.g. through the open data pilot in Horizon 2020 and the Connecting Europe Facility (CEF) Telecom Public Open Data ([34]) call). Although Europe is investing a significant amount of money in fundamental algorithms, this amount seriously lags behind the amounts that other countries are investing.

([25]) European Union, *Charter of Fundamental Rights of the European Union*, C 326/02, Brussels, 26.10.2012, pp. 391–407.
([26]) https://www.pdp4e-project.eu/
([27]) https://www.ditas-project.eu/project-overview/
([28]) https://decodeproject.eu/
([29]) https://www.enisa.europa.eu/topics/data-protection/
([30]) ENISA, *Towards a framework for policy development in cybersecurity – Security and privacy considerations in autonomous agents*, 2019 (https://www.enisa.europa.eu/publications/considerations-in-autonomous-agents).
([31]) https://www.enisa.europa.eu/news/enisa-news/enisa-proposes-best-practices-and-techniques-for-pseudonymisation
([32]) https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act
([33]) https://www.ai4eu.eu/
([34]) https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2019-public-open-data

3.1.4. Recommendations

To sustain and further develop its data-based digital economy, Europe should control key technologies related to the following domains.

Europe should invest in transparent, trustworthy information processing for its citizens and businesses regarding data security.

- **Understanding and mitigating vulnerabilities of AI.** During sensing or processing, machine learning algorithms are vulnerable to attacks ([35]); these are widely known in the community and have also been demonstrated. The EU should invest in technologies to prevent, detect and mitigate the impact of algorithmic vulnerabilities, particularly in the context of control systems used in critical infrastructure.
- **Ensuring the availability of machine learning and big data platforms that are sourced, hosted and sustainable in Europe.** Europe should develop and encourage sustainable AI platforms that (i) are always available, (ii) are easily accessible and (iii) provide alternatives for EU-based services.
- **Developing new technologies for data security and privacy, to support advances in regulations and the emerging needs of the digital society.** As data are becoming an active component of command and control processes, new techniques should be developed to protect active data, regardless of syntax, semantics and location. This includes, for example, computing on encrypted data, including multiparty computation, functional encryption and somewhat homomorphic encryption (see Section 3.5 for further details). The EU should invest, in particular, in technologies favouring local/edge AI treatment to complement the investment that has already been made in cloud-based treatment. This includes an increased focus on local AI agents, namely developing methods and tools to support privacy-friendly global training, deployment to edge and local execution of the AI algorithms – to the extent that this is feasible.
- **Explainable AI.** In many cases, AI algorithms are acting as a black box. For greater social acceptance and technical certification purposes, it will become necessary to trace the processes by which the algorithms reach a decision and explain these processes to the user in an understandable manner. This extends to AI algorithms training, and it may be combined with AI to protect the privacy of training data and user data, as well as the model, although the latter is rather difficult to achieve. In addition, providing open tools so that users can verify AI externally could support trustworthy AI development and deployment. Such tools would be able to evaluate the AI by executing built-in tests, in a similar way to how penetration testing tools work (such as Metasploit).
- **Securing decision support and actuating.** AI algorithms provide decisions based on input data. An effort should be made to ensure secure sensing, in conjunction with secure hardware (Section 3.4), secure actuating, and secure operating systems and middleware (Section 3.2).
- **Social trustworthiness of AI.** Current social networks exhibit many biases, without the user being aware or conscious of them ([36]). Although the modern press has been cross-checking facts to a greater extent, it does not meet the need to validate content for correctness or appropriateness. The EU should support new techniques for developing the trustworthiness of social online interactions, independently of the service or platform.

([35]) Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z. B. and Swami, A., 'Practical black-box attacks against machine learning', in *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, Association for Computing Machinery, New York, 2017, pp. 506–519.
([36]) Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A. and Sadeh, N., 'A field trial of privacy nudges for Facebook', in *Proceedings of the 32nd Annual ACM Conference on Human Factors in Computing Systems*, Association for Computing Machinery, New York, 2014, pp. 2367–2376.

3.1.5. Long-term objectives

Data security needs to go beyond data at rest in the long term, protecting active data in an environment without borders and well-defined lines. Data security also includes algorithms such as AI and machine learning algorithms. Active data protection should cover information and algorithms, from sensing to acting. Transparency provided by clarity of purpose, process and result will increase trust and use. Success will lead to Europe establishing transparent, trustworthy information processing for its citizens and businesses.

3.2. TRUSTWORTHY SOFTWARE PLATFORMS

Bob enters his autonomous vehicle and starts the engine. A new operating system software update is available! The vehicle starts downloading the update and attempts to install it. Unfortunately, the update is not compatible with a third-party application, leading Bob to seek an alternative solution. Will he need to download and install code that has not been validated by the car manufacturer and risk installing an unwanted trapdoor?

3.2.1. Current and future context of trustworthy software platforms

Software is progressively penetrating all aspects of everyday life, from the smallest objects (such as light bulbs) to the most complex ones (for example vehicles). As demonstrated by the abovementioned scenario, essential software, trusted to fulfil daily needs – such as the operating system in Bob's car – may be compromised for various reasons, betraying the user's trust. In this scenario, Bob may no longer be able to operate his car safely if he installs questionable code.

Software is at the heart of digital infrastructure, and nowadays with the DevOps paradigm it is being put into production almost at the same time as it is being written. New software development paradigms such as Agile and SCRUM are entering the critical infrastructure domain ([37]). Vulnerabilities in these environments may have terrible cascading effects. As proof, a recent set of 11 vulnerabilities touching the VxWorks real-time operating system and reaching the maximum severity level has affected many industrial control systems (ICS) vendors ([38]). This is only one example from roughly 15 000 software vulnerabilities published yearly in the Common Vulnerabilities and Exposures (CVE) repository ([39]).

Although quite a number of new operating systems, virtualisation platforms and middleware systems have been developed and introduced in the past few years (such as Android, OpenStack), only very few of them have a European origin. Platforms such as the RIOT operating system ([40]) remain confidential and are for research use only. Although many global European companies develop software and integrate it into their systems, the number of world-class software vendors headquartered in Europe is scarce.

3.2.2. Problem definition and criticality

With the introduction of computing and communication abilities in the majority of items utilised daily, Europe may become vulnerable to supply chain disruptions. For instance, Google has partially suspended business with China; it is no longer providing services for Huawei, except for those publicly available via open licence sourcing ([41]). It is not clear how Europe will respond

([37]) Kasauli, R., Knauss, E., Kanagwa, B., Nilsson, A. and Calikli, G., 'Safety-critical systems and agile development: A mapping study', paper presented at the 44th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), Institute of Electrical and Electronics Engineers, 3 August 2018, pp. 470-477 (https://arxiv.org/pdf/1807.07800.pdf).
([38]) ICS CERT, ICS Advisory ICSA-19-211-01 – Wind River VxWorks (Update A), original release date: 30 July 2019, last revised: 8 August 2019 (https://www.us-cert.gov/ics/advisories/icsa-19-211-01).
([39]) https://cve.mitre.org/
([40]) https://riot-os.org/
([41]) https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUSKCN1SP0NB

if a large software vendor decides not to support the European market any more. Indeed, responding to such an event requires significant effort and might introduce large additional costs. We are at a point where, despite the noteworthy number of software developers and software companies residing in Europe, we cannot ensure that we will be able to replace essential software components should the ones currently deployed become unavailable.

Software is increasingly consumed as a cloud service. However, as previously noted, the major cloud platforms are located outside Europe. This creates several problems. First, such vendors may restrict the availability of their software services to their own clouds only, creating lock-ins for both functionalities and data. Second, they could also prohibit third-party software vendors from creating native software services on their cloud platforms. If Europe were to lose access to these cloud platforms, it would consequently lose access to the software services that are exclusive to them.

Furthermore, systems and services rely on third-party libraries and services that are independent and beyond the control of the software developers. As an example, even a major software vendor such as SAP today controls only a small portion of the source code in its products and relies on open-source software for over 90 % of its products' functionality; it is therefore developing tools for vulnerability management of this external software ([42]).

3.2.3. Efforts towards establishing trustworthy software platforms

Many initiatives have taken place in Europe with the aim of publishing and supporting open-source platforms. However, some of these initiatives have failed; the Mandriva Linux distribution, for example, failed as the company supporting it went bankrupt a few years ago. The most popular Linux distribution providing commercial support is currently the Red Hat Enterprise Linux, whose headquarters are located outside the EU, followed by the SUSE Linux, which is supported by SUSE, a company based in Germany. The mF2C project ([43]) has set the goal of designing an open, secure, decentralised, multi-stakeholder management framework, including novel programming models, privacy and security, data storage techniques, service creation, brokerage solutions, service-level agreement (SLA) policies and resource orchestration methods.

In effect, although Europe has a booming ICT service industry, it hosts only a few of the top commercial software companies and supports relatively few open-source software distributions. This is creating a potential supply chain issue, as Europe may not have a sufficient expert workforce and enough companies to develop software solutions to meet its needs.

3.2.4. Recommendations

Europe must be able to develop its own software platforms and tools to adequately verify software that is sourced from outside its borders. Likewise, Europe should support, promote and host, inside its borders, open-source alternatives to commercial products, to be able to cope in the event of supply chain disruption. Finally, as the demand for cloud services grows, Europe must ensure an open and secure European cloud software services market.

([42]) https://projects.eclipse.org/proposals/eclipse-steady
([43]) https://www.mf2c-project.eu/

More specific action items include the following:

Europe must be able to develop its own software platforms and tools to adequately verify software that is sourced from outside its borders.

- **Trustworthy operating systems.** Europe should ensure that it maintains its expertise on operating systems development, even if the scope is limited to specific environments, such as cyber physical systems and secure components. It should encourage the emergence of open-source alternatives for servers, desktops and mobile devices.
- **Trustworthy middleware.** Nowadays, software systems rely on third-party libraries and services that are independent and beyond the control of software developers. Europe needs to be able to validate these third-party libraries and services to ensure that they do not introduce additional software vulnerabilities into the system ([44]).
- **Detection of malware and botnets.** Particularly for sensitive environments such as governmental systems and critical infrastructure, Europe needs to maintain the capability (in terms of both expertise and tooling) to detect malware and malicious network activity.
- **System and virtualisation security.** As virtual environments gain in popularity and become commodities, Europe must retain the capability to specify and enforce cybersecurity properties in hypervisors. This is linked to cybersecurity aspects of network operating systems and routing equipment, which are described in Section 3.7.
- **Secure software development platforms.** Europe should maintain the capability to develop, assess and certify secure software, possibly built from several third-party sources. This includes (i) the capability to build secure software systems and (ii) the ability to ensure that the systems that are built meet specific security requirements. This depends on 'trustworthy middleware', which can help ensure that third-party libraries and services are also secure.
- **Risk assessment platforms.** To ensure the security of complex ICT systems, there is a need to assess the risks of potential attacks, in order to define the necessary countermeasures during both design time and runtime. Measuring the achieved level of security is a difficult task. This task also includes assessing the dependencies on the system (both software and hardware).
- **Trustworthy sensors.** Software platforms should support secure command and control infrastructure that cooperates with hardware-based sensing and actuating (Section 3.4), as well as AI-based decision support (Section 3.1). This could be a component of secure software and configuration updates.
- **Open-cloud software services.** Europe needs to create an open market for cloud software services and enable the same cloud services to be available across different cloud providers. This would protect Europeans from being locked in to a particular cloud service, enable European software vendors to offer cloud services and protect Europe from losing access to critical software services should certain clouds become unavailable.

([44]) https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A9-Using_Components_with_Known_Vulnerabilities.html

Although most attacks exploit a system's vulnerabilities, social engineering attacks exploit human weaknesses. One of the defence measures against social engineering attacks is raising people's awareness.

3.2.5. Long-term objective

The long-term objective of trustworthy software platforms is to ensure that deployed software is of sufficient quality and is developed following the 'secure-by-design' and 'secure-by-default' principles. The EU should facilitate not only the development of methods and tools for accomplishing this goal but also the development of training programmes for skilled software developers. Of course, the security properties of these trustworthy platforms should be maintained during the whole lifecycle of the products and services into which they are integrated, at a time when the lifetime of embedded systems is increasing significantly. These actions could be supported by enhanced assessment and certification methodologies for specific application scenarios ([45]).

3.3. CYBER THREAT MANAGEMENT AND RESPONSE

Claire arrives at work and logs in to the computer system. She receives an email from her boss, with a document attached. Without realising that the email address subtly mimics the one from her boss, she opens the document. Unknown to her, the document contains malware that infects her computer and starts scanning the network surroundings. By finding shared folders and a vulnerable Active Directory server, the malware gains administrative access to the system and starts encrypting the Active Directory server's hard drive. In the Security Operations Centre (SOC), alarms start flashing as machines and network connectivity go down. What will the operator do to remediate the situation?

3.3.1. Current and future context of cyber threat management and response

In the abovementioned scenario, malware tricked the user and was used to gain access to the internal network of the company. Such malicious actions may cause extensive damage to company assets, such as loss of data due to the encryption of a hard drive, when the assets are not protected and the SOC is not prepared to respond to such a cyber-incident.

The area of operational security, also known as incident management, started in the early 1980s, with the understanding that completely secure systems were not achievable, at least not at a reasonable cost and while allowing ease of use. The concept of an intrusion detection system ([46]) that is able to detect malicious behaviours (such as malicious code or activities) has evolved over the years.

The tools have evolved rapidly since the late 1990s into large platforms that combine a number of technologies. Security information and event management (SIEM) platforms collect events from many sensors and help operators classify alerts and evaluate the associated risk. Security orchestration, automation and response (SOAR) platforms augment the capabilities of SIEM platforms with regard to automation and response.

3.3.2. Problem definition and criticality

During the past 20 years, there has been a significant development of tools for intrusion detection. However, the difficulty of deploying and operating these tools has led to the

([45]) Baseline security recommendations have been developed by ENISA. For example, for IoT devices, see ENISA, *Baseline Security Recommendations for IoT*, 2017 (https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot).
([46]) Denning, D. E., 'An intrusion-detection model', *IEEE Transactions on Software Engineering*, No 2, 1987, pp. 222–232.

emergence of SOCs as managed security services to facilitate deployment and operations for organisations that do not have the skills and funds to deploy such services.

At the same time, legislation such as the Network and Information Security (NIS) Directive ([47]) and its national implementations require that critical infrastructure operators report cybersecurity incidents to the authorities and inform their peers through Information Sharing and Analysis Centres (ISACs). Europe needs to preserve and develop the ability to design and deploy EU-designed detection sensors in its most critical infrastructure. It also needs to preserve its ability to design and deploy SIEM and SOAR platforms, including open-source alternatives when commercial components cannot be sourced in Europe. These tools, and the workforce behind them, have thus become a critical resource that is fragmented by the variety and number of environments in which the tools must be deployed for monitoring.

The need to protect our critical infrastructure was also exposed during the COVID-19 pandemic. This is particularly the case for our medical care infrastructure, which experienced stress as a result of the number of patients needing treatment. The high impact that a cybersecurity incident could have on a medical centre poses a great risk that could put even more stress on medical care systems. Taking out a hospital's cyber systems during a crisis could result in medical staff losing access to patient records, medical cyber equipment being taken out of service, and medical surgeries being halted, consequently putting human lives in danger.

Although the challenge is encountered worldwide, operating SOCs is a strategic autonomy issue, as it depends on people and processes. With respect to people, Europe appears to suffer from a significant shortage of a skilled workforce to operate SOCs and manage cybersecurity incidents. Unfortunately, a delay in diagnosis and response may result in attackers (i) penetrating systems more easily, (ii) residing inside the systems for longer periods of time and (iii) being able to inflict significant damage. With respect to processes, SOCs handle vast amounts of log and trace data, possibly containing very sensitive information on EU companies and citizens. Processing these data locally and sharing information among well-identified circles of trust for mitigating cyber threats, in compliance with the applicable EU regulatory frameworks, is also an asset that needs to be protected.

3.3.3. Efforts towards ensuring cyber threat management and response

Research on cyberattack detection and mitigation has been, and is still, a hot topic because of the mutations of attacks. New tools and new detection and correlation mechanisms are required to respond to the increasing complexity of attacks.

At the same time, the digitalisation of society is introducing digital controls in many new places. As a result, attackers have more possibilities of gaining easy access, as product designers tend to focus more on functionality and less on security. This is demonstrated by, for example, the fact that, from 2017 to 2018, 80 % of the vulnerabilities found in medical devices were exploiting network access and 40 % could be triggered remotely with basic skills and no particular privileges ([48]). Consequently, although there has been significant progress, in terms of both technology and regulations, a significant gap between attackers and defenders remains, especially in certain sectors.

([47]) https://www.enisa.europa.eu/topics/nis-directive
([48]) Debar, H., *Vulnerabilities in the Internet of Medical Things*, FOSAD, 2019.

Several research projects have addressed the issue of SOCs and SIEM platforms. The DiSIEM project ([49]) aims to extend existing SIEM platforms by providing a set of diversity-related components to improve their capacities. The Cyber-Trust project ([50]) aims to develop an innovative cyber threat intelligence gathering, detection and mitigation platform to tackle the grand challenges of securing the ecosystem of IoT devices. The ReAct project ([51]) aims to fight software exploitation and mitigate advanced cybersecurity threats in a timely fashion.

Although the sector of cyber threat management and response has made significant progress, the effectiveness of attack detection and mitigation remains plagued by a large volume of false alerts (reducing SOC effectiveness) and undetected advanced persistent threats. New solutions are needed to support defenders who have to deal with the increasing number and complexity of attacks.

([49]) https://cyberwatching.eu/projects/1040/disiem
([50]) https://cyberwatching.eu/projects/1269/cyber-trust
([51]) https://react-h2020.eu/

Monitoring systems and being prepared to quickly respond to cyberattacks is an important part of cybersecurity.

3.3.4. Recommendations

Europe should develop its own tools and methods for attack detection and incident response.

Europe must be able to develop its own tools and methods for attack detection and response to incidents in order to be able to resist and mitigate cyberattacks. The development of new devices and new services is creating new vulnerabilities and attack paths, for which we may not have the right detection mechanisms. Industrial control systems are going online and creating new attack scenarios that have not been considered before. This capability is increasingly important when facing nation state actors or handling systemic threats. Specific action items include the following.

- **Cyber threat intelligence.** Europe has invested a significant amount of effort in cyber threat intelligence, for example the Malware Information Sharing Platform ([52]) and the OpenCTI ([53]) open-source software. These efforts should be sustained to ensure that Europe is able to influence standards currently under development at the Internet Engineering Task Force (IETF) or the European Telecommunications Standards Institute (ETSI).
- **Cybersecurity analytics.** The wealth of information acquired in SOCs remains enormous, posing a significant challenge to operators. New cybersecurity analytic tools leveraging machine learning, AI and visualisation should support operators in assessing and triaging alerts quickly and efficiently, thus improving the response.
- **Situational awareness.** Given the complexity and diversity of current IT systems, SIEM and SOAR platforms should be extended to offer operators a complete view of the situation. This aspect also includes developing methods to raise the awareness and improve the training of operators, to enable them to keep up with the threats. New data streams, coming from, for example, ISACs, will also assist operators to become acquainted with the application sector view.
- **Attack detection, mitigation and response.** Current sensors may suffer from false positives and false negatives and therefore may not detect multiple cyberattacks effectively. Furthermore, many new platforms do not include endpoint protection (such as smartphones), and thus are missing detection and mitigation capabilities. The impact of and response to cyberattacks, from a technical, legal, business and human standpoint, requires further study. Automated response procedures should be further examined regarding technical feasibility and possible legal implications. Moreover, strategies regarding incident response that require the cooperation of several stakeholders with different levels of administrative control should be developed. These strategies could take into account several utility functions.
- **Deception.** Although use of the word 'honeypot' has decreased in recent years, new deception techniques could be developed and prove to be effective at triggering alerts related to malicious activity and protecting legitimate systems from exposure. This area could include exploring adversarial machine learning techniques to learn more about attackers leveraging AI tools to deploy advanced attack schemes.
- **Cyber defence.** It has already been demonstrated that critical infrastructure could suffer greatly from heavy attacks; therefore, it is necessary to think ahead and plan protection mechanisms and operating modes that enable the infrastructure to 'fail gracefully' and operate in the best possible manner in a degraded or even manual mode.
- **Post-design and post-perimeter defence and response strategies.** The perimeter of many of our organisations is becoming increasingly vague as practices such as

([52]) Malware Information Sharing Platform (https://www.misp-project.org/).
([53]) OpenCTI – open cyber threat intelligence platform (https://www.opencti.io/en/).

smart working gain in popularity. As a result, strategies for protection, mitigation and response must be adapted to these trends.

- **Trusted information sharing.** Beyond technology, there is a need to establish and foster trusted forums for cyber threat information exchange, whereby data on incidents can be shared to a limited community in a detailed manner. The ISACs already mentioned are key actors in developing these community forums and improving Europe's cybersecurity readiness.

3.3.5. Long-term objectives

Europe should try to remain autonomous in the long term, as far as cyber threat management and response are concerned. Autonomy refers to capabilities and capacity related to SOCs, including skills and training programmes, SIEM platforms, managed security services and cyber threat intelligence information acquisition. This is a prerequisite condition, to ensure that digitalisation of society conforms to our needs and values and does not induce unacceptable cyber threats. The priorities should be balanced between prevention, for instance hardening current systems and building trustworthy software and hardware components (Sections 3.2 and 3.4, respectively), and efficient responses to incidents, which requires people who are well trained and who are able to react in the event of an attack (cyber response and capacity building). This balance is fundamental to preserving the practical use of IT and cyberphysical systems. Success will enable Europe to retain sufficient autonomy to fight against major cyberattacks and actors that pose a threat.

3.4. TRUSTWORTHY HARDWARE PLATFORMS

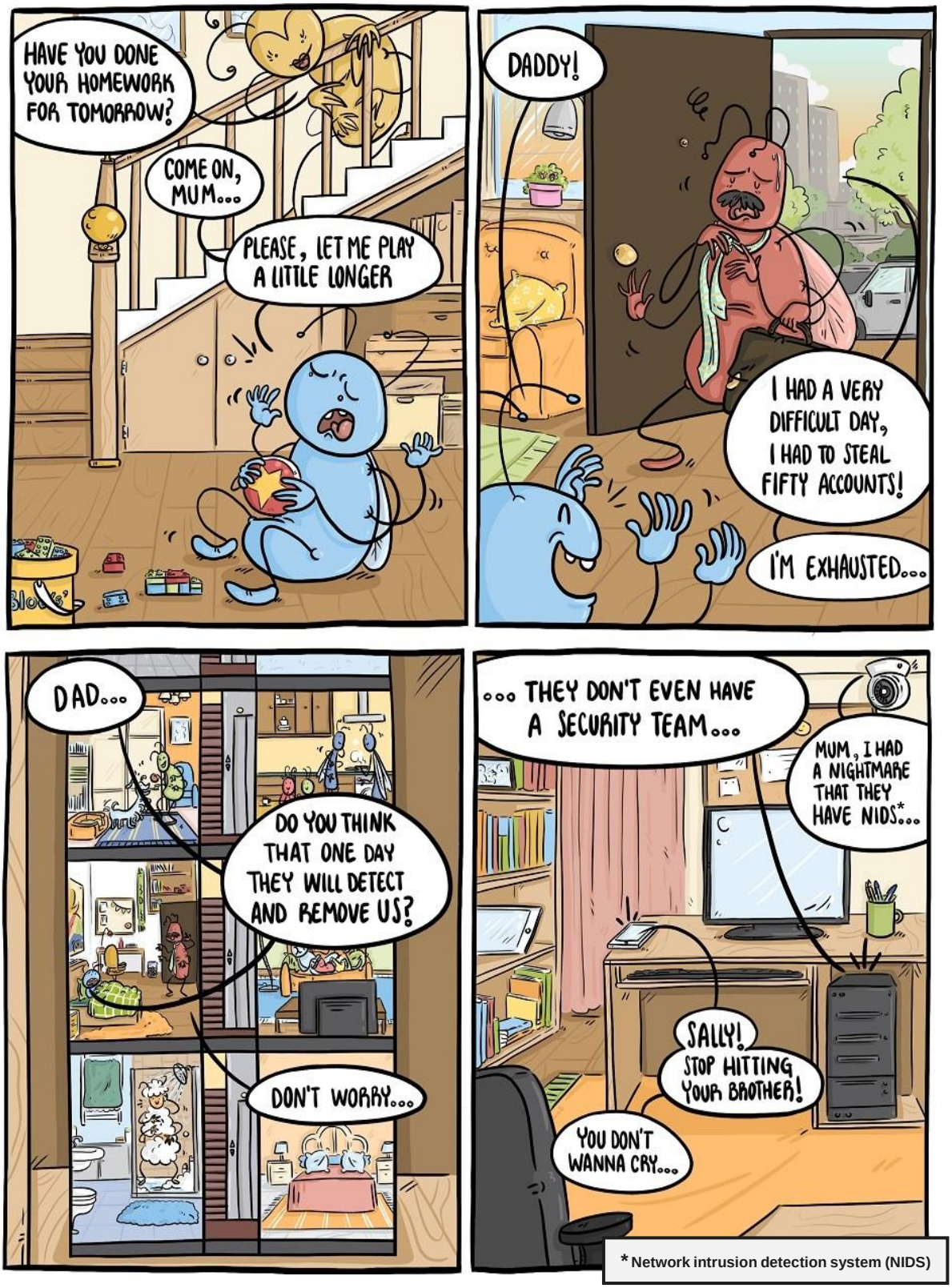
Daniel has just acquired a brand-new smartphone with an advanced security feature enabling him to store his private data and prevent applications from accessing it. Unfortunately, this functionality has a significant flaw. If the smartphone is dropped in water, it triggers a hardware bug that attackers can exploit to gain access to his personal data.

3.4.1. Current and future context of trustworthy hardware platforms

Suppliers, many of them located outside Europe, are increasingly introducing new features such as secure boot, image signing and unique device identity in their hardware platforms. Although they were introduced to increase the security of devices, these features might undermine usability, making it difficult for the end user to understand the added value in terms of benefits and drawbacks. Moreover, as demonstrated by the abovementioned scenario, such features may not be trustworthy, since additional testing may be needed to validate the absence of bugs and exploits.

At the same time, complex attacks involving hardware implementation or hardware/software interactions (such as Spectre ([54]), Meltdown ([55]) and Rowhammer ([56])) are becoming a threat to extremely popular hardware platforms. Although fixes are available for a few of them, an extensive fix without significant performance loss remains out of reach at the time of writing this report.

([54]) Kocher, P., Horn, J., Fogh, A., Genkin, D., Gruss, D., Haas, W., Hamburg, M., Lipp, M., Mangard, S., Prescher, T., Schwarz, M and Yarom, Y., 'Spectre attacks: Exploiting speculative execution', in *Proceedings of 2019 IEEE Symposium on Security and Privacy*, Institute of Electrical and Electronic Engineers, New York, 2019, pp. 1–19.
([55]) Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y. and Hamburg, M., 'Meltdown', arXiv preprint, 2018, arXiv:1801.01207.
([56]) Mutlu, O., 'The RowHammer problem and other issues we may face as memory becomes denser', in *Proceedings of the Conference on Design, Automation and Test in Europe*, European Design and Automation Association, 2017, pp. 1116–1121.



Any system may feature hardware or software side bugs or vulnerabilities. To minimise security incidents, software should be kept up to date, and trustworthy hardware platforms should be used. In addition, an appropriate configuration is needed to increase security.

3.4.2. Problem definition and criticality

Sourcing hardware components manufactured in Europe is a rarity nowadays, as manufacturers have moved their production to Asia. European countries have failed to provide incentives to suppliers of chipsets to persuade them not to relocate production to Asia, even though there is a risk of intellectual property (IP) rights violation ([57]) and tampering ([58]) ([59]). Vendors and suppliers outsource various aspects of design, fabrication, testing and packaging of integrated circuits (ICs). This widens the threat scenarios, which now include malicious insertion of Trojan circuits, designed to act as silicon time bombs, IC piracy, untrustworthy third-party IPs and malicious system disruption and diversion ([60]). As a result, there is an increasing risk that hardware components including backdoors or undesired functionality might be exploited by an attacker, while the verification of the vulnerabilities in hardware is expensive and time-consuming, and unfeasible for the majority of chips.

Moreover, the EU supply chain for the ICT industry might be disrupted or lose its competitive edge if component suppliers from other continents decide to follow aggressive selling methods, such as using different price strategies for the European market or, even worse, restricting the possibility of buying certain components.

In the near future, operating fleets of drones or vehicles with remote secure management will be challenging without a local 'trust anchor'. A trust anchor is a hardware anchor that bridges communication between an operating system and hardware, integrating a highly secure system on a chip for holistic system defence. The anchor helps an operating system kernel to actively monitor its extensions and can also track bus traffic within the system-on-a-chip platform to prevent untrusted third-party IP modules from performing malicious operations ([61]) and thus causing security challenges. As an example, the SecureIoT project ([62]) aims to provide security services in the areas of Industry 4.0, socially assistive robots and connected autonomous cars.

Sharing hardware platforms in virtualised environments, as envisaged for the future 5G networks (see Section 3.7), enables attackers to leverage hardware vulnerabilities. Maintaining hardware expertise is crucial to ensuring that Europe develops its own IoT infrastructure, sourced from locally designed components.

Consequently, it is of paramount importance that Europe sources its own trustworthy hardware, not only to secure its supply chain and competitive edge but also to possess the capacity to control secure infrastructure of the future, from autonomous drones and vehicles to 5G networks and power grids.

([57]) US Government, *2005 report to Congress of the U.S.–China Economic and Security Review Commission*, US Government Printing Office, Washington, DC, 2005.
([58]) Kömmerling, O. and Markus, G., 'Design principles for tamper-resistant smartcard processors', in *WOST'99: Proceedings of the USENIX Workshop on Smartcard Technology*, USENIX Association, Berkeley, California, 1999, pp. 9–20.
([59]) Hu, W., Mao, B., Oberg, J. and Kastner, R., 'Detecting hardware trojans with gate-level information-flow tracking', *Computer*, Vol. 49, No 8, 2016, pp. 44–52.
([60]) Karri, R. and Koushanfar, F., 'Trustworthy hardware (scanning the issue),' in *Proceedings of the IEEE*, Vol. 102, No 8, 2014, pp. 1123–1125.
([61]) Jin, Y. and Oliveira, D., 'Trustworthy SoC architecture with on-demand security policies and HW-SW cooperation', paper presented at the 5th Workshop on SoCs, Heterogeneous Architectures and Workloads (SHAW-5), 2014.
([62]) https://secureiot.eu/

3.4.3. Efforts towards establishing trustworthy hardware platforms

Europe is a global leader in security relating to embedded systems, from smart card security to other embedded platforms. There is also a strong level of expertise in micro-architecture attacks among European research teams. For example, the FutureTPM project ([63]) aims to design and develop a quantum-resistant trusted platform module (TPM). However, investment in hardware, and particularly secure hardware, seems to have been limited since the development (and widespread commercialisation) of smart cards and SIM cards. It is relevant to come back to hardware and examine if, given these new threats, Europe can maintain its edge with regard to the development of secure hardware components. Acquisitions and merging of European companies by non-European players might affect our autonomy in procuring critical components. In fact, in 2017, 30 % of the acquired European small and medium-sized enterprises (SMEs) – market leaders in specialised high-tech areas – were acquired by non-EU companies ([64]). In such cases, (i) the EU loses know-how, (ii) the IP moves outside Europe and (iii) the European industry becomes dependent on imported components.

The EU should possess the capability and capacity to guarantee access to and control over trustworthy hardware.

3.4.4. Recommendations

There are many ways in which hardware tools could support and improve cybersecurity as a whole. Specific action items include the following.

- **Bootstrap security.** Research and design new methods to ensure the continuous integrity of hardware/software platforms, ensuring smooth operation and secure transition from hardware to firmware to software, during the whole lifecycle of a product (design, manufacturing, maintenance).
- **Hardware-induced vulnerabilities.** Design and develop methods for detecting and remediating hardware-induced vulnerabilities, as well as hardware trojans, to ensure strong platform integrity. Black/white box testing technologies for hardware should be studied extensively.
- **Side channel attacks.** Detect and protect platforms that may leak information because of radiation or power consumption, and certify those that are less prone to leakage. This topic has been studied in either very small (smart card) or very specific (military) contexts and lacks wider applicability.
- **Hardware-anchored cybersecurity tools.** Hardware remains one of the best trust anchors available, but it has significant costs. Efficient (cost, energy) hardware support for cybersecurity is a difficult challenge, but one that also holds significant promises for more secure platforms. This may form the basis required for strong authentication (which has remained elusive so far) and global identity management (including not only people but also businesses, objects and services). Research into new approaches beyond public key infrastructure should also allow massive deployment of secure hardware with reduced complexity.
- **Open hardware architecture.** The example of the RISC-V foundation ([65]) demonstrates that it is possible to develop and share hardware architecture openly. This model should support Europe in developing alternative hardware supply chains in the event of difficulties with the current supply.

([63]) https://futuretpm.eu/index.php/home/mission-and-motivation#
([64]) European Commission, *Innovation kitchen – Horizon 2020 SME instrument impact report: 2018 edition*, Publications Office of the European Union, Luxembourg, 2018.
([65]) http://www.riscv.org/

- **Safe sensing.** Post-treatments, typically AI, require that sensors provide reliable information further up the chain. However, attacks are targeting sensors more and more, for example computer vision ([66]). Europe should explore the development of reliable and secure sensing technologies.

3.4.5. Long-term objective

The long-term objective of trustworthy hardware platforms is to ensure that the EU possesses the capability and capacity to guarantee access and control over high-quality hardware components, in order to meet its industrial development needs as such components become key in almost all products and services that are being developed and commercialised. Moreover, the Cybersecurity Act ([67]) enables ENISA to establish a European cybersecurity certification framework for ICT products, services and processes that provides different levels of assurance.

3.5. CRYPTOGRAPHY

> *One of the most singular characteristics of the art of deciphering is the strong conviction possessed by every person, even moderately acquainted with it, that he is able to construct a cipher which nobody else can decipher. I have also observed that the cleverer the person, the more intimate is his conviction.*
>
> — Charles Babbage, originator of the digital programmable computer

3.5.1. Current and future context of cryptography

Cryptography is one of the leading areas of research in Europe and one of the most advanced theoretical areas of cybersecurity, relying on models and formal proofs for verification and validation.

In the cryptographic community, competitions are being organised to develop new algorithms. Since 2017, the National Institute of Standards and Technology (NIST) has been running a competition for quantum-safe cryptographic algorithms, with the process expected to be completed in accordance with NIST standards during the period 2022–2024 ([68]). The selected algorithms will guarantee that the confidentiality and integrity of the data are protected from attacks by conventional and quantum computers. It is critical during the standardisation process that all weaknesses are properly analysed and reviewed through peer review in a transparent manner, which has not always been the case ([69]).

Mastering cryptography is a key element for nation states, and acquisition of technology from third parties is a significant weakness, as shown by the story of the Crypto AG company ([70]). Given the importance of strong cryptographic algorithms and protocols to national security, many EU Member States have created national crypto strategies to ensure long-term access to state-of-the-art crypto tools. Unfortunately, this has limited the possibility of publishing lists of recommended cryptographic algorithms and protocols that are valid in all Member States, and has thus created fragmentations in the single market.

([66]) Madry, A., Makelov, A., Schmidt, L., Tsipras, D. and Vladu, A., 'Towards deep learning models resistant to adversarial attacks', arXiv preprint, 2017, arXiv:1706.06083.
([67]) European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, Brussels, 7.6.2019, p. 15–69 (https://eur-lex.europa.eu/eli/reg/2019/881/oj).
([68]) See https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Workshops-and-Timeline for the status of the standardisation of post-quantum cryptography.
([69]) NIST's process of standardisation has been opaque on at least one occasion (https://en.wikipedia.org/wiki/Dual_EC_DRBG) and ETSI has been accused of weakening a critical protocol to provide easier data centre monitoring for a small handful of organisations (https://www.eff.org/deeplinks/2019/02/ets-isnt-tls-and-you-shouldnt-use-it).
([70]) https://www.cryptomuseum.com/manuf/crypto/index.htm

3.5.2. Problem definition and criticality

Cryptographic algorithms are one of the fundamental pillars of cybersecurity, providing basic properties such as integrity, confidentiality and authentication of origin. Although cryptography is increasingly being used in classic IT, its use in industrial controls, which are often used in critical infrastructure, has been limited. Issues are related to the difficulty of upgrading legacy equipment, whose lifespan is counted in decades, and using cryptographic tools in power-constrained devices. For example, encrypting or signing data requires additional computing power, which is sometimes not available in resource- or power-limited devices. In addition, all cryptographic material needs to be maintained, for example by regularly renewing keys, and the overheads of management procedures are often difficult to manage. These challenges remain difficult to solve at the extreme ends of the usage spectrum, for example for hardware-constrained tiny devices relying on the environment to obtain energy and for high-speed environments requiring encryption at the speed of memory or cache.

Despite their advantages and formal validation, cryptographic algorithms and protocols sometimes fail. In this respect, the example of the key reinstallation attacks (KRACKs) vulnerability ([71]) shows that even seemingly insignificant deviations from the proven process lead to serious vulnerabilities; this core protocol issue had significant additional effects on the features of newer protocols as they leveraged the older functionality ([72]).

Recent announcements of quantum computers and testbeds by companies such as Intel, Google, IBM and ATOS indicate that it will become necessary to prepare quantum-resistant cryptographic algorithms and protocols. Europe is contributing to the trend in the quantum flagship ([73]). Since legacy cryptographic algorithms, protocols and suites require a significant amount of time to become deprecated, and their replacements also require a significant amount of time to be deployed, maintaining Europe's capabilities in cryptography necessitates forward-thinking and planning.

Beyond cryptographic algorithms and protocols, the EU should also invest in supporting infrastructure, such as public key certificate authorities. Today, the top free and commercial certificate authorities (Let's Encrypt ([74]), Comodo, Symantec, Digicert, GeoTrust ([75])) represent a cumulative 97 % of the market share and are located outside the EU. Controlling the keys and the infrastructure is required to ensure the confidentiality and availability of our communications.

([71]) Vanhoef, M., 'Key reinstallation attacks', 2017 (https://www.krackattacks.com/).
([72]) Vanhoef, M. and Piessens, F., 'Release the Kraken: New KRACKs in the 802.11 Standard', in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, Association for Computing Machinery, New York, 2018, pp. 299–314.
([73]) https://qt.eu/
([74]) https://letsencrypt.org/
([75]) Durumeric, Z., Kasten, J., Bailey, M. and Halderman, J. A., 'Analysis of the HTTPS certificate ecosystem', in *Proceedings of the 2013 Conference on Internet Measurement Conference*, 2013, pp. 291–304.

Key management is essential for cybersecurity. Not having control of the encryption or signature keys puts a system's security at risk and affects the trust it has established with other systems.

3.5.3. Efforts towards establishing strong cryptography

A number of European projects, such as the Networks of Excellence, have worked towards fortifying Europe in the area of cryptography. The EU-funded Ecrypt I and Ecrypt II Networks of Excellence ([76]) organised a competition to create a new stream cipher; the Fentec project ([77]) is developing new solutions for functional encryption, providing new cryptographic building blocks for privacy-sensitive applications.

Cryptographic functions and protocols have become mainstream for information systems. Today, most web traffic is secured by the Hypertext Transfer Protocol Secure (HTTPS), although the underlying protocol has changed over the past 25 years from Secure Sockets Layer (SSL) to Transport Layer Security version 1.3 (TLSv1.3). Issues related to other fundamental protocols such as the Domain Name System (DNS) and the Border Gateway Protocol (BGP) need to be addressed, but the process of introducing secure alternatives to existing fundamental infrastructure is very slow ([78]). For example, despite the fact that the current version of the DNS security extensions protocol was standardised between 2005 and 2013, the validation rate of domain names worldwide was less than 30 % ([79]) in April 2020.

Although significant progress has been made with regard to algorithms and protocols, the overall infrastructure required to operate them remains insufficient. For example, public key infrastructure and certificate distribution remain mostly in the private sector, and the level of trust that can be associated with certificates remains difficult to evaluate, as shown by the example of the DigiNotar failure ([80]).

3.5.4. Recommendations

As computing power, memory and mathematical tools progress, it is clear that cryptographic algorithms and protocols are aging and thus becoming weaker. Research and standardisation in cryptography should, therefore, continue to ensure that the available tools are efficient when faced with emerging computing paradigms. Specific action items include the following.

- **Post-quantum cryptography.** Although they are probably still far away from commercial (or even practical) use, quantum computers are starting to appear in specific settings. This new paradigm implies a complete rethinking of cryptographic structures, and this can be considered an opportunity for a global refresh of our cryptographic tools, enabling their use in environments in which they cannot currently be deployed.
- **Basic cryptographic building blocks.** Cryptographic tools need to be adapted to the new environments, applications and domains in which we want to use them. For example, fully homomorphic encryption (FHE) remains extremely expensive and beyond reach, despite its promise to secure cloud environments. Research is necessary to either develop alternative and more efficient homomorphic encryption schemes, such as somewhat homomorphic encryption, or adapt algorithms to new applications.
- **Standards-based maintenance of cryptographic suites.** Standards frequently specify cryptographic suites, enabling authentication and confidentiality in a homogeneous and coherent way. As time passes, certain cryptographic suites weaken and must be updated, to remove compromised algorithms or to increase key lengths.

The EU must invest in the ability to establish, control and verify standards for processes and products and develop its own crypto policy and infrastructure for the public good.

([76]) https://www.ecrypt.eu.org/
([77]) http://fentec.eu/
([78]) ENISA, *7 steps to shore up the Border Gateway Protocol (BGP)*, 2019 (https://www.enisa.europa.eu/publications/7-steps-to-shore-up-bgp).
([79]) https://stats.labs.apnic.net/dnssec
([80]) van der Meulen, N., 'DigiNotar: Dissecting the first Dutch digital disaster', *Journal of Strategic Security*, Vol. 6, No 2, 2013, pp. 46–58.

This maintenance process should be performed well in advance of any risk of compromise, to ensure that users have sufficient time to upgrade their cryptosystems. Europe should lead crypto- standardisation activities by proposing scientifically sound algorithms and fostering consensus among European solutions.

- **Cryptographic protocols.** As new services and uses emerge, new protocols such as multiparty computation (MPC) and zero-knowledge proofs (ZKPs) are required to ensure that these new services are sufficiently secure by design and that they maintain user trust by avoiding a single point of failure and reducing the risk of leaks. This entails also developing new dedicated symmetric building blocks to increase efficiency.
- **Tools to support security validation of cryptographic implementations.** Tools are needed to ensure that the progress made through stronger cryptography actually translates into secure implementations.
- **Strong EU certification authority.** The EU and its Member States should reflect on the implementation of an EU-based public key infrastructure.

3.5.5. Long-term objectives

To ensure that the EU retains access to state-of-the-art cryptographic protection, we must invest in the ability to establish, control and verify standards for processes and products that are vital to Europe. This may include establishing European-based cryptographic suites to ensure control over IP and limit the risk of hidden issues, such as cryptographic backdoors.

In the long term, as cryptographic algorithms and protocols and the supporting certificates are so fundamental to cybersecurity, Europe should develop its own crypto policy and infrastructure for public good.

3.6. USER-CENTRIC SECURITY PRACTICES AND TOOLS

Never give an order that cannot be obeyed.
— General Douglas MacArthur

It takes 20 years to build a reputation and few minutes of cyber-incident to ruin it.
— Stéphane Nappo, Chief Information Security Officer, BNP

3.6.1. Current and future context of user-centric security practices and tools

It is a well-known issue that users are, in many cases, the weak point of organisations. Phishing attacks continuously result in (i) organisations being infected with malware and (ii) private user accounts being hijacked ([81]).

Security seems to be a very complicated and annoying topic for the standard IT user. The problem of security has existed for a long time, as exemplified by studies led in the late 1990s on email encryption ([82]) that received the test-of-time award 20 years after. We need to acknowledge that, at present, a significant number of users, if not most of them, do not use a secure email system that provides guarantees about the senders of messages and the integrity of the content. Further to this discrepancy, which leads to spam and phishing, email use is widespread for both personal and professional use.

([81]) Caputo, D. D., Pfleeger, S. L., Freeman, J. D. and Johnson, M. E., 'Going spear phishing: Exploring embedded training and awareness', *IEEE Security & Privacy*, Vol. 12, No 1, 2013, pp. 28–38.
([82]) Whitten, A. and Tygar, J. D., 'Why Johnny can't encrypt: A usability evaluation of PGP 5.0', in *USENIX Security Symposium,* Vol. 348, 1999, pp. 169–184.

It appears that productivity and personal interest are considered a higher priority than cybersecurity and that users may reach their goals in creative ways, circumventing any security system.

3.6.2. Problem definition and criticality

Many studies show that phishing and ransomware attacks have a significant economic impact ([83]). In recent years, the WannaCry ransomware has shut down factories in France and hospitals in the United Kingdom ([84]), resulting in serious economic losses and potentially having a negative impact on human lives.

Cybersecurity tools are perceived as a burden to end users. Users tend to believe that such tools reduce productivity, without bringing useful benefits. A recent study shows that even cybersecurity experts cannot agree on what simple advice can be given to users to improve their safety online ([85]).

We are at a point where people trust IT systems because they work, most of the time, and because their dysfunctions are a notable nuisance without being an unbearable burden. Trust, however, is difficult to obtain and easy to degrade. Cyber physical systems must improve their usability so that users do not see themselves as being constrained by the systems and continue using them for Europe to obtain the benefits of the digital society.

3.6.3. Efforts towards establishing user-centric security practices and tools

Several projects have already started in this area. For example, the Encase project ([86]) aims to design and implement browser-based architecture for the protection of minors from malicious actors in online social networks. The Privacy & Us project ([87]) aims to train early-stage researchers to be able to analyse, design and develop innovative solutions to questions related to the protection of citizens' privacy, considering the multidisciplinary and intersectoral aspects of the issue. The Dogana project ([88]) aims to reduce the risk created by modern Social Engineering 2.0 attack techniques. Such projects may have outcomes that will benefit standard users' everyday interactions with IT systems by reducing the risk of attacks.

An enormous number of cybersecurity systems have been developed over the years, and many of them have failed when it comes to deployment. There are many well-known examples, such as the 20 years it took to develop usable standards to secure the internet-routing protocol BGP, which are still not widely used. There are many such standards awaiting deployment, and many security systems, which do more to burden the users than to solve their problems. The example of completely automated public Turing test to tell computers and humans apart (CAPTCHA) is particularly interesting, as we have known for a long time that tests of this kind are more easily broken by algorithms than solved by users ([89]), which has led to them being used more in the creation of ground truth for image processing systems than as access control mechanisms.

([83]) Caputo, D. D., Pfleeger, S. L., Freeman, J. D. and Johnson, M. E., Going spear phishing: Exploring embedded training and awareness', *IEEE Security & Privacy*, Vol. 12, No 1, 2013, pp. 28–38.
([84]) Pascariu, C., Barbu, I. D. and Bacivarov, I. C., 'Investigative analysis and technical overview of ransomware based attacks. Case study: WannaCry', *International Journal of Information Security and Cybercrime*, Vol. 6, No 1, 2017, p. 57.
([85]) Reeder, R. W., Ion, I. and Consolvo, S., '152 simple steps to stay safe online: Security advice for non-tech-savvy users', *IEEE Security & Privacy*, Vol. 15, No 5, 2017, pp. 55–64.
([86]) https://cyberwatching.eu/projects/1304/enhancing-security-and-privacy-social-web
([87]) https://cyberwatching.eu/projects/1272/privacy-us
([88]) https://cyberwatching.eu/projects/1042/dogana
([89]) Yan, J. and El Ahmad, A. S., 'Captcha security: A case study', *IEEE Security & Privacy*, Vol. 7, No 4, 2009, pp. 22–28.

Cyber systems should respect users' privacy. Consequently, it is important that systems let users maintain their privacy and request consent before sharing private information.

3.6.4. Recommendations

Actions should be taken to transform cybersecurity from a burden to an asset and a benefit for end users.

Many actions need to be taken to change the playing field and transform cybersecurity from a burden to an asset that helps systems function better, deliver better digital services and provide a clear benefit to end users. Europe should ensure that services that are useful for European citizens either are available in Europe according to European values or favour the emergence of alternatives that respect these values. Specific action items include research to develop the following.

- **Privacy-enhancing technologies (PET).** Develop practices and tools that support users in preserving online privacy. Research should ensure that users can easily enforce regulations such as the GDPR.
- **Usable security.** Develop cybersecurity methods and tools that actually meet users' needs and that support their activities instead of acting as barriers to productivity.
- **Human-centred security and privacy.** Ensure that the end user is indeed the subject who needs to be protected.
- **Security visibility.** Design user interfaces and interactions that are actually perceived by the end users and that help them adopt actual behaviours.
- **Social engineering and human errors in cybersecurity.** Build examples and methods that can effectively provide new insights into the manner in which humans interact with each other on social media and other online mechanisms, to avoid common mistakes that lead to system compromise.
- **Verifiable computing.** Using tools described in the previous sections, Europe could support the development of methods and tools for verifiable computing, ensuring that end users have the means to verify independently the proper behaviour of ICT systems, further developing and enhancing trust.

3.6.5. Long-term objectives

Developing user-centric security practices and tools will help weave cybersecurity into our digital lives in the longer term. This should enable EU citizens to develop trust in digital technologies for both personal and professional activities. Such practices and tools should become invisible when everything goes well, and should be visible and explicit when there is a need for protection. The success of cybersecurity implies long-term sustainable growth of the European digital society.

3.7. DIGITAL COMMUNICATION SECURITY

The enemy knows the system.
— Claude Shannon

3.7.1. Current and future context of digital communication security

The overall networking environment is moving from ownership-based infrastructure towards on-demand, pay-per-use networking and computing. Software-defined networking ([90]) and large-scale virtualisation ([91]) are already deployed in data centres and IT services, rapidly penetrating cyber physical systems and pushing towards large-scale deployment of sensors and actuators in the IoT. This flexibility, however, blurs the notion of ownership and localisation of communication systems and platforms as they move across infrastructure at will.

Moving towards virtual communication environments (such as cloud computing infrastructure, software-defined networks and slicing) is a trend that companies and governments alike are rapidly adopting. We are currently relying on platforms widely operated outside Europe for services that are in many respects critical. The fundamental promise of the cloud relies on the fact that infrastructure is scalable and that communication is available.

The global picture leads us to an environment in which data centres may be hosted outside Europe and the supporting digital communication infrastructure relies on non-European sourced technologies.

3.7.2. Problem definition and criticality

Owing to the digitisation of services, all major sectors have an increasing level of dependency on digital infrastructure. For example, many services are now offered by cloud providers, and any unavailability, loss of integrity or violation of confidentiality may have serious consequences for businesses or governments that use their services. The use of multitenant cloud storage also poses security risks. Moreover, the unavailability of financial operations – because of, for instance, a denial of service attack – has the potential to affect the operations and economy of most countries and businesses. Although the new connectivity provides numerous opportunities to improve the services offered to customers, it also enlarges the attack surface by exposing the connected industries (Industry 4.0) and critical services (e.g. connected vehicles, smart cities). Moreover, 5G architecture based on network function virtualisation, network slicing and software-defined networking will expand the threat landscape by combining traditional IP-based threats with all-5G network (core, access and edge) threats, insecure legacy 2G/3G/4G generations and threats introduced by virtualisation technology ([92]).

Europe should promote investment in creating resilient secure-by-design solutions for seamless innovative communication infrastructure.

This trend in generic on-demand virtual infrastructure is, at present, one of the possible advantages and drawbacks of cybersecurity. Knowing where a system or service resides is one of the elements that enables the definition of a perimeter, thus allowing filtering and access control. Realising which resources are available permits risk evaluation and the selection of mitigation methods.

Another trend that has an impact on communication is the need for connectivity, which is exhibited by almost every object that we acquire today. From home assistants to connected vehicles, from medical devices to smart meters, many industries and services are heavily

([90]) Kreutz, D., Ramos, F., Verissimo, P., Rothenberg, C. E., Azodolmolky, S. and Uhlig, S., 'Software-defined networking: A comprehensive survey', arXiv preprint, 2014, arXiv:1406.0440.
([91]) Jain, R. and Paul, S., 'Network virtualization and software defined networking for cloud computing: A survey', *IEEE Communications Magazine*, Vol. 51, No 11, 2013, pp. 24–31.
([92]) ENISA, *ENISA Threat Landscape for 5G Networks*, 2019 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks).

transforming themselves, relying on 4G/5G/Wi-Fi/Bluetooth/Ethernet communication capabilities for optimal performance. A lack of connectivity, for example because of a cyberattack, will significantly impair the proper function of essential services.

The current state of the art is that Europe is heavily dependent on outside suppliers for both technology (e.g. communication hardware) and services (e.g. cloud services), whereas other regions that have heavily invested in the development of virtual communication infrastructure are also influencing standards ([93]). This dependency leaves Europe open to difficulties in sourcing and deploying these new technologies and services to support its continuous development.

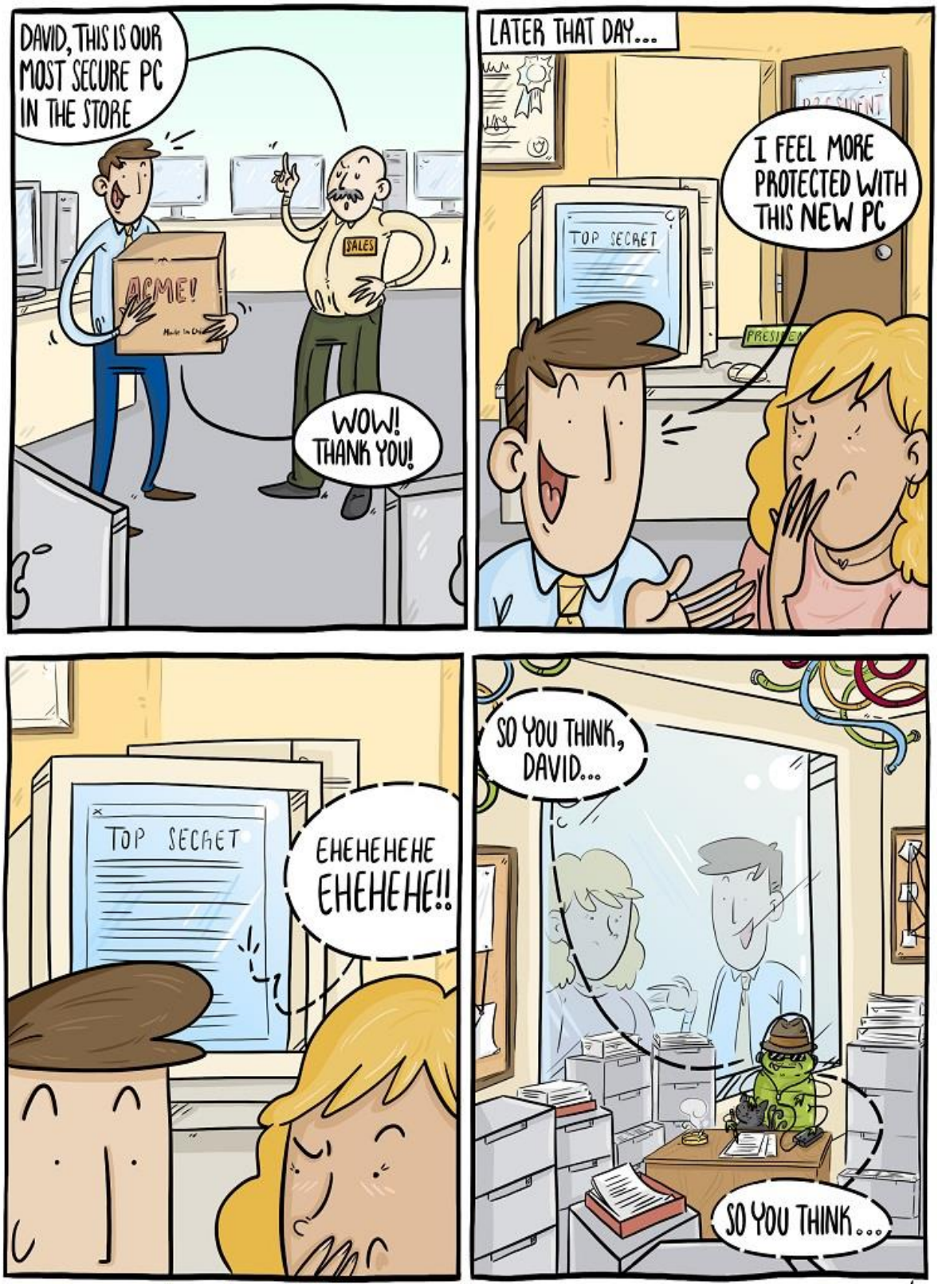
3.7.3. Efforts towards ensuring digital communication security

Europe is already embracing technological advancements in communications, an example being the 5G infrastructure public–private partnership (PPP) ([94]). However, in recent years there has been a marked absence of cybersecurity projects within the 5G umbrella. As a result, although services have been deployed and demonstrated over 5G technologies, the security and safety of 5G infrastructure remains an open question. Although 5G infrastructure technologies are developing rapidly, network operating systems remain behind in terms of security.

Europe has developed activities under the umbrella of the 5G PPP to address this issue; an example of this is the 5G-Ensure project ([95]), which developed security architecture and a roadmap for security enablers in 5G. Another example is ENISA's efforts to develop a detailed threat assessment of 5G infrastructure components ([96]).

In the context of quantum communications, Europe launched the Open European Quantum Key Distribution Testbed (OpenQKD) ([97]) pilot programme. The purpose of the programme is to create and test experimental quantum communication infrastructure, using quantum key distribution ([98]), featuring high-level and quantum-safe security. This programme is expected to advance the technology involved in quantum communications and reinforce the EU's strategic digital capacities.

([93]) Tsiatsis, V., Karnouskos, S., Höller, J., Boyle, D. and Mulligan, C. 'Chapter 3 – IoT – A business perspective', in *Internet of Things – Second edition*, Elsevier, Amsterdam, 2019.
([94]) 5G infrastructure PPP (5G PPP) (https://5g-ppp.eu/).
([95]) https://www.5gensure.eu/
([96]) ENISA, *ENISA Threat Landscape for 5G Networks*, 2019 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks).
([97]) OPENQKD project (https://cordis.europa.eu/project/id/857156).
([98]) Quantum key distribution (https://ec.europa.eu/digital-single-market/en/glossary/quantum-key-distribution-qkd).



Even the most secure system may use insecure communication services. For this reason, it is important to use secure channels and trusted communication providers.

3.7.4. Recommendations

Communication infrastructure is necessary for every service we use. Given this, Europe should consider the fact that maintaining trust and efficiency in communication services is essential for the development of a digital Europe. Specific action items include research to develop the following.

- **Network services as critical infrastructure.** It should be taken into consideration that cyberattacks on network services have a systemic and potentially very significant effect on all services, including the operation of all critical ICT infrastructure. Therefore, network services should be considered a major building block of all critical infrastructure and secured similarly. Secure network management and operating systems of network appliances, either virtual or physical, are major building blocks required to secure the networking infrastructure.
- **Network security.** Develop new methods to detect cyberattacks and mitigate their effects, and then include them in the design of new service protocols. Such research will ensure that network security is achieved from the beginning and not retrofitted as an afterthought. It should also tackle the ability to manage threats over wide-area networks to mitigate their effects and provide by-design practices and tools to ensure that carrying out attacks has too high a cost for attackers compared with the gains they expect.
- **IoT security.** New cybersecurity methods and tools must take into account IoT constraints, such as energy, storage and bandwidth limitations, to provide authenticated and resilient communication channels. In relation to this concept, ENISA has published a report on IoT security ([99]), listing threats and good practices and providing recommendations.
- **Virtual networks.** Develop specific cybersecurity methods and tools that can demonstrably secure virtual environments in which boundaries and borders have disappeared to such an extent that they cannot be used to define security policies and assess risk, and that end users may have less knowledge about the system they uses than the service providers and attackers.

3.7.5. Long-term objective

The long-term objective of digital communication security is to be able to deploy and operate seamless infrastructure that ensures end-to-end secure communication regardless of whether it relies on virtual means or physical means. Developing a secure-by-design network operating system could support Europe's autonomy in managing its digital communication infrastructure and could provide a path towards better control and autonomy over this infrastructure.

Security by design for communication infrastructure beyond 5G is also a significant concern. Even if we do not know what the future of communication infrastructure will be, we need to take into account cybersecurity aspects as early as possible in the design process for these new network paradigms. Therefore, Europe should promote investment in creating resilient secure-by-design solutions for seamless innovative communication infrastructure.

([99]) ENISA, *Guidelines for Securing the Internet of Things*, 2020 (https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things).

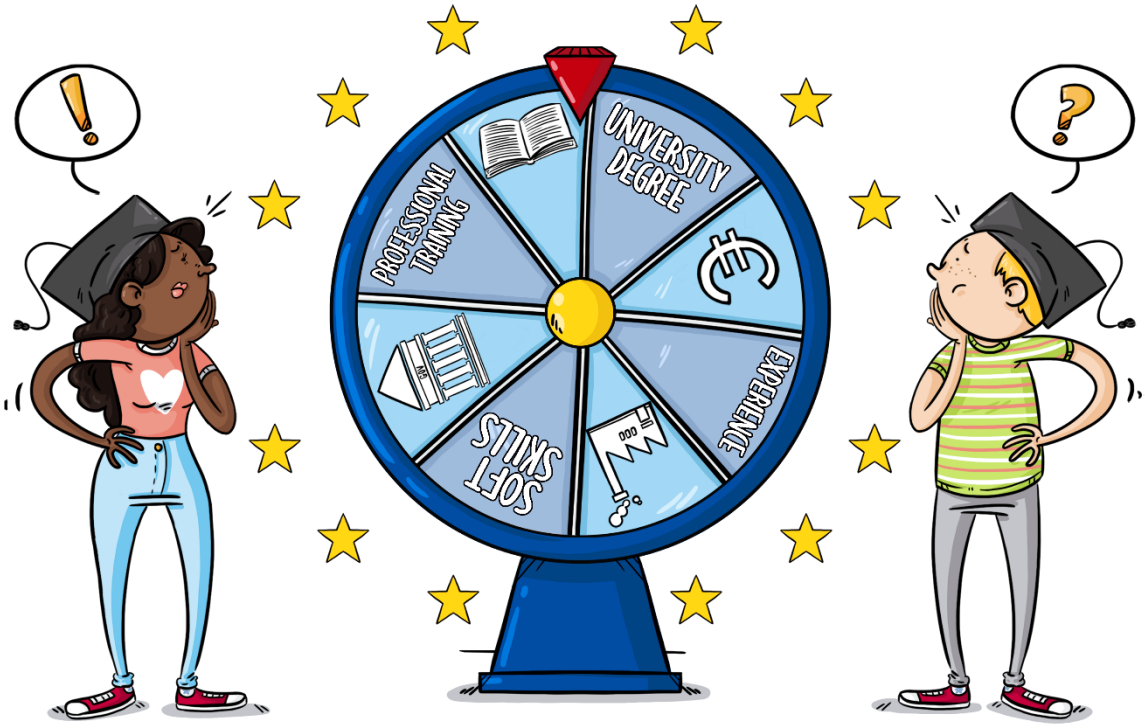
4. SOCIAL SCIENCE DIMENSIONS OF STRATEGIC AUTONOMY

Although digital autonomy and sovereignty rely on technological leadership, and most notably on significant research and development, technical leadership alone is insufficient to ensure sustainable strategic autonomy in the long term. The EU must also count on a skilled workforce and a strong and actionable legal and regulatory framework for research and development.

4.1. HUMAN CAPACITY BUILDING

> *This next president is going to inherit the most sophisticated and persistent cyber espionage culture the world has ever seen. He needs to surround himself with experts that can expedite the allocation of potent layers of next generation defence around our targeted critical infrastructure silos.*
>
> — James Scott, Senior Fellow, Institute for Critical Infrastructure Technology

Europe must ensure (i) that its businesses and governments have access to a sufficient number of skilled people who can design, deploy, operate and audit critical infrastructure services, and (ii) that it retains these skilled people in the context of a global shortage of cybersecurity professionals.



4.1.1. Students and cybersecurity

Although the shortage of trained professionals is widely recognised, it should also be made clear that one (if not the major) reason for this shortage is that there is not a sufficient number of students entering dedicated educational programmes. Some efforts have been made to increase the visibility of cybersecurity curricula, including the publication of training needs related to the deployment of the NIS Directive ([100]). Other initiatives include the EHR4Cyber ([101]) and the Women4Cyber ([102]) initiatives. However, the level of interest in cybersecurity remains significantly below the level of interest in other IT fields, such as AI and game development. Higher salaries elsewhere may well result in professionals or companies moving away from Europe and this skills shortage consequently increasing.

Europe should thus look at additional ways to enrol students in cybersecurity curricula. Several alternative approaches could be adopted, including the Industrial Cyber Security Center of Excellence ([103]). This encourages IT professionals in companies (car manufacturers, critical infrastructure operators, etc.) to follow a 1-year training programme on cybersecurity. Upon return to their companies, the combination of their domain knowledge and cybersecurity skills enables them to act as ambassadors for cybersecurity in their professional environment. Another potential action could be to make the job market more visible and understandable to prospective students.

4.1.2. Skills development

The job market relies heavily on professional certifications. For cybersecurity, most – if not all – of the widely recognised certifications are based in the United States. Take, for example, the Global Information Assurance Certification (GIAC) and the Certified Information Systems Security Professional certification (CISSP), which are widely accepted by many companies and considered useful by professionals. Unfortunately, although Europe has a wealth of professional educational companies, these companies rely on frameworks that originate in the United States to assess skills and deliver certifications. Europe should develop its own cybersecurity skills framework, with the aim of creating a common skills language for individuals, employers and training providers. This will help to facilitate skills recognition and support employment and employability. The framework should allow for further specification and specialisation by Member States, to accommodate specific needs and requirements, without endangering its pan-European approach, as that would be counterproductive for the single digital market. The framework should be complementary to the United Kingdom's Cyber Security Body of Knowledge ([104]), an important step in formalising cybersecurity concepts.

Alternative approaches may also prove useful for specific domains or for acquiring specific skills without obtaining a formal degree, such as the Rogers Cybersecure Catalyst training programme ([105]). Europe should facilitate the establishment of courses that provide a response to the need for cybersecurity-specialised practitioners and that offer high-level opportunities to people who are looking for a different career path. Collaboration between private and public

Europe should develop its own cybersecurity skills framework, with the aim of creating a common skills language for individuals, employers and training providers.

([100]) ENISA, *Stock taking of information security training needs in critical sectors*, 2017 (https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors).
([101]) https://ecs-org.eu/documents/publications/60101ad752a50.pdf
([102]) https://ec.europa.eu/digital-single-market/en/news/commission-welcomes-women4cyber-initiative-and-launches-progamme-detect-bugs-software-used-all
([103]) Information-technology Promotion Agency, Industrial Cyber Security Center of Excellence, 2017 (https://www.ipa.go.jp/icscoe/campaign1-en.html)
([104]) https://www.cybok.org/
([105]) https://www.ryerson.ca/cybersecure-catalyst/training-program/faq/

entities is essential for such initiatives to be successful and ensure good employment opportunities for trainees who have completed the courses.

To support trainers, Europe could probably fund a few high-level Erasmus Mundus school networks or similar programmes targeted at this specific area.

4.1.3. Ethics and cybersecurity

Beyond technology, cybersecurity curricula should include social and legal dimensions, supporting the view that ethics has a strong link to cybersecurity. As an example, through its teaching material, the CANVAS project ([106]) will ensure that the future generation of cybersecurity experts obtains basic insights into and knowledge of how to tackle ethical and legal dilemmas in cybersecurity.

4.2. LEGAL AND REGULATORY FRAMEWORKS

The GDPR and the Cybersecurity Act provide a strong legal basis for the development of European autonomy. It remains to be seen how these regulations and frameworks will come to be deployed and to be followed by global businesses.

4.2.1. Tools for evaluating GDPR compliance

Beyond the current legal framework, the EU should reflect on and make freely available to users tools that enable them to assess independently and transparently the use of their personal information. The social success of the GDPR among the general public means that the capability to choose between providing information or giving up on a service should become an informed decision, and one that can be exerted at any point, independently of any service, anywhere in the world.

4.2.2. Evaluation of cybersecurity certification schemes

The current European Cybersecurity Act provides a framework for the development of certification schemes for IT products and services. It is impossible to tell at this stage what impact this regulation will have and if industry will embrace the development of new certification schemes that are actually useful to users and that adhere to European values.

In this respect, the new mandate of ENISA on cybersecurity certification ([107]) is a critical step that should sustain European digital strategic autonomy, simplifying certification activities for the industry (thus encouraging certified products in the marketplace) while ensuring that all Member States can rely on EU-wide capabilities.

([106]) https://canvas-project.eu/
([107]) https://www.enisa.europa.eu/topics/standards/certification

ANNEX A: SURVEY METHODOLOGY AND ANALYSIS

This annex documents the methodology followed to select the most important knowledge areas in order to support the EU's digital strategic autonomy.

A.1. METHODOLOGY OF THE STUDY

The methodology followed to develop the document is as follows.

- We analysed recent relevant cybersecurity research roadmaps (such as the NIS Working Group 3 strategic research agenda ([108]); the European cybersecurity strategic research and innovation agenda for a contractual PPP ([109]); AEGIS – *White Paper on Research and Innovation in Cybersecurity* ([110]); and SecUnity – *Cybersecurity Research: Challenges and course of action* ([111])) and other national initiatives.
- Through this analysis, 17 research challenges stood out (listed in Section A.2). We considered that this list of challenges represented the collective opinion of stakeholders of the EU ecosystem with respect to cybersecurity research.
- To find out which of these 17 research challenges were the most important, we created a survey, which was hosted on a designated web page (https://ec.europa.eu/eusurvey). The survey was widely disseminated among the cybersecurity community, with the aim of prioritising the research challenges involved in the support of EU digital sovereignty and thus autonomy. To ensure that we had a prioritised list at the end of the survey, the survey respondents were asked to rank the five most important challenges.
- The results of the survey (see Section A.3) led to the selection of the seven most highly ranked research challenges.
- A first document was then drafted that elaborated on the seven challenges.
- To receive feedback, the document was circulated and reviewed by experts in the field.
- An open validation workshop was organised in Brussels on 30th January 2020, which led to the final round of comments and finalisation of the document.

A.2. SURVEY OBJECTIVE

The objective of the survey was to obtain from members of the community their opinions on the importance of each research challenge with respect to the EU's strategic autonomy. Although all research challenges may be potentially important, some may be less critical to autonomy than others.

([108]) European NIS Platform, *Cybersecurity Strategic Research Agenda – SRA*, 2015 (https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents/strategic-research-agenda-draft-v02.63/at_download/file).
([109]) European Cyber Security Organisation, *European cybersecurity strategic research and innovation agenda (SRIA) for a contractual public–private partnership (cPPP)*, 2016 (https://ecs-org.eu/documents/ecs-cppp-sria.pdf).
([110]) AEGIS, *White Paper on Research and Innovation in Cybersecurity*, 2018 (http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-White-Paper-on-Research-and-Innovation-in-Cybersecurity.pdf).
([111]) https://it-security-map.eu/en/roadmap/secunity-roadmap/

The 17 challenges described in Table A.1 were extracted from the literature to form the basis of the survey and positioned with respect to the taxonomy of the European Commission's Joint Research Centre (JRC) ([112]).

Table A.1: Survey challenges

Challenge text	Position in the JRC taxonomy
Securing cryptographic systems against emerging attacks (including post-quantum cryptography, basic cryptographic building blocks and cryptographic protocols)	Domains: Cryptology Sectors: Most of them Applications: Most of them
Trustworthy hardware platforms (including bootstrap security, hardware bugs, side channel attacks and hardware-anchored cybersecurity tools)	Domains: Software and hardware security engineering Sectors: Most of them Applications: Most of them
Trustworthy software platforms (including operating systems, middleware, software vulnerabilities, malware and botnets, and system virtualisation security)	Domains: Software and hardware security engineering Sectors: Most of them Applications: Most of them
Secure system lifecycle (despite the potential use of less trustworthy components), including software runtime verification and enforcement	Domains: Software and hardware security engineering Sectors: Most of them Applications: Most of them
Data security (including vulnerabilities of AI, machine learning and big data aspects, data security and privacy, data aspects of social networks and explainable AI)	Domains: Data security and privacy Sectors: Most of them Applications: Big data, AI
Data-centric computing and networking (including MPC, FHE, ZKP, quantum computing, blockchain and related technologies)	Domains: Software and hardware security engineering Sectors: Most of them Applications: Most of them
Digital communication security (including network services as critical infrastructure, network security, IoT security and virtual networks)	Domains: Network and distributed systems Sectors: Most of them Applications: Most of them
Authentication, authorisation and identity management	Domains: Identity and access management Sectors: Most of them Applications: Most of them
Digital forensics (including legal support for cybersecurity)	Domains: Operational incident handling and digital forensics Sectors: Most of them Applications: Most of them

([112]) Nai, F., Neisse, R., Hernandez Ramos, J. L., Polemi, N., Ruzzante, G. L., Figwer, M. and Lazari, A., *A Proposal for a European Taxonomy*, JRC118089, Publications Office of the European Union, Luxembourg, 2019 (https://ec.europa.eu/jrc/en/publication/proposal-european-cybersecurity-taxonomy).

Challenge text	Position in the JRC taxonomy
Cyber threat management and response (including cyber threat intelligence, cybersecurity analytics, situational awareness, attack detection and mitigation, deception, cyber defence, and post-design and post-perimeter defence strategies)	Domains: Security management and governance, operational incident handling and digital forensics Sectors: Most of them Applications: Most of them
Quantifying cybersecurity (including quantitative aspects of security, and risk assessment and management)	Domains: Security measurements and assurance, audit and certification Sectors: Most of them Applications: Most of them
Cybersecurity certification lifecycle management (including incremental certification, certification for critical infrastructure, and certification of complex systems and services)	Domains: Assurance, audit and certification Sectors: Most of them Applications: Most of them
Security and safety co-design	Domains: Security management and governance Sectors: Most of them Applications: Most of them
Digital business models for a fair and secure economy and society	Domains: Security management and governance Sectors: Most of them Applications: Most of them
Accountability and transparency of information quality	Domains: Human aspects Sectors: Most of them Applications: Most of them
User-centric security practices and tools (including privacy tools, privacy-enhancing technologies, usable security, human-centred security and privacy, security visibility, social engineering and human errors in cybersecurity)	Domains: Human aspects and cryptology Sectors: Most of them Applications: Most of them
Capacity building and **awareness building** (including training technologies and training platforms)	Domains: Education and training Sectors: Most of them Applications: Most of them

The survey was open for 20 days in October 2019, and its existence was widely communicated to the community through different mailing lists, including those of the four pilot projects (Concordia, CyberSec4Europe, ECHO and SPARTA) of the 2018 Horizon 2020 cybersecurity call 'Establishing and operating a pilot for a European Cybersecurity Competence Network' ([113]).

A.3. ANALYSIS OF THE RESULTS

The survey received 94 responses. Several participants indicated that it was difficult to choose between the challenges, which forced them to think about those that are most important in the cybersecurity domain.

([113]) https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

Participants were asked to rank what they thought were the five most important challenges by order of importance (from highest to lowest). Each of the challenges was scored according to the following formula: the highest-scored challenge received 1 point, the second highest 0.8, and so on, down to 0.2 for the fifth choice. The remaining challenges were awarded a score of 0. The score for each challenge was then averaged over the 94 responses. The scores for the seven most highly ranked challenges are provided in Table A.2.

Figure A.2: Survey scores for the seven most important challenges

Challenge text	Position in the JRC taxonomy	Score	Ranked by	Number prioritising this first
Data security (including vulnerabilities of AI, machine learning and big data aspects, data security and privacy, data aspects of social networks and explainable AI)	Domains: Data security and privacy Sectors: Most of them Applications: Big data, AI	0.39	50	16
Trustworthy software platforms (including operating systems, middleware, software vulnerabilities, malware and botnets, and system virtualisation security)	Domains: Software and hardware security engineering Sectors: Most of them Applications: Most of them	0.32	43	11
Cyber threat management and response (including cyber threat intelligence, cybersecurity analytics, situational awareness, attack detection and mitigation, deception, cyberdefence, and post-design and post-perimeter defence strategies)	Domains: Security management and governance, operational incident handling and digital forensics Sectors: Most of them Applications: Most of them	0.27	40	11
Trustworthy hardware platforms (including bootstrap security, hardware bugs, side channel attacks and hardware-anchored cybersecurity tools)	Domains: Software and hardware security engineering Sectors: Most of them Applications: Most of them	0.26	37	11
Securing cryptographic systems against emerging attacks (including post-quantum cryptography, basic cryptographic building blocks and cryptographic protocols)	Domains: Cryptology Sectors: Most of them Applications: Most of them	0.25	36	9
User-centric security practices and tools (including privacy tools, privacy enhancing technologies, usable security, human-centred security and privacy, security visibility, social engineering and human errors in cybersecurity)	Domains: Human aspects and cryptology Sectors: Most of them Applications: Most of them	0.24	37	9
Digital communication security (including network services as critical infrastructure, network security, IoT security and virtual networks)	Domains: Network and distributed systems Sectors: Most of them Applications: Most of them	0.22	34	5

Data security is a clear winner, with an overall average score of 0.39 and having been cited as the highest priority by 16 respondents out of 94. This clearly reflects the importance of data and the sensitivity of data-driven services.

The next five items were also highly ranked, despite achieving relatively lower scores.

The final item that we retained – digital communication security – attracted less attention than the others in terms of its ranking position. Despite this, it achieved a significant score (one that was very close to the score of the challenge that ranked sixth), as many respondents included it in their list of priorities.

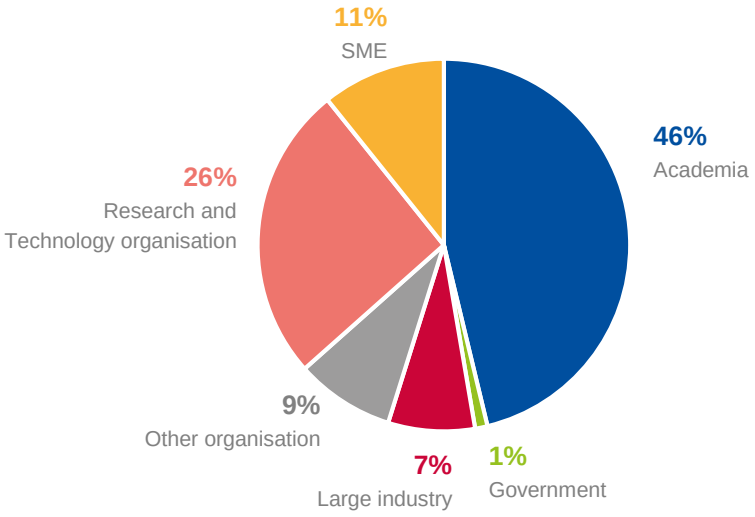
The eighth priority, 'Authentication, authorisation and identity management', achieved a score of 0.18 only, so it was considered that this priority was of less interest to the community and less important to the EU's digital strategic autonomy.

All 17 priorities were voted for by at least 50 respondents, indicating that all of them were relevant to the topic.

A.4. RESPONDENT ANALYSIS

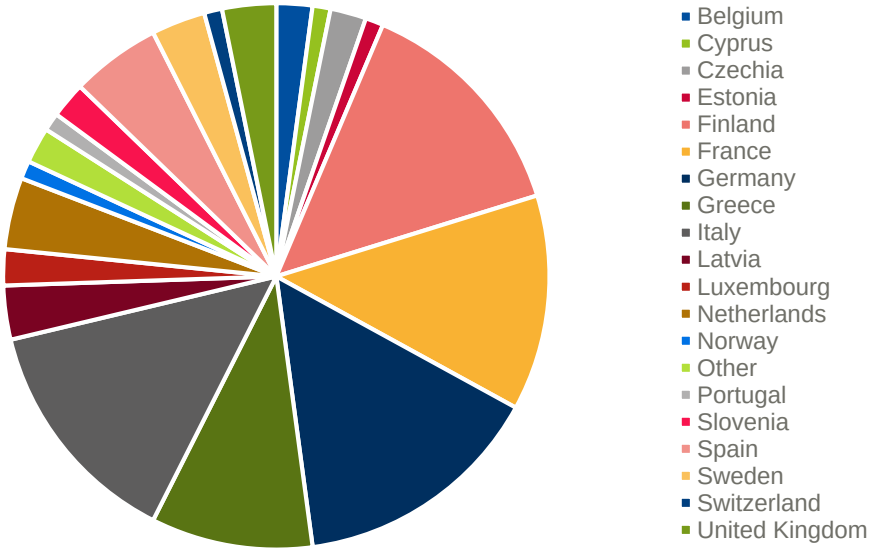
Overall, ninety-four respondents completed the survey. The respondents came from a variety of organisations, as indicated in Figure A.1.

Figure A.1: Respondents by organisation type



The majority of the responses came from people working in academia and research and technology organisations.

Figure A.2: Respondents by country



Five countries (Germany, Greece, France, Italy and Finland) provided over half of the survey answers, with 20 countries represented out of the 27 Member States (Figure A.2).

TP-03-20-868-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found on its website https://www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-458-9
DOI: 10.2824/43660