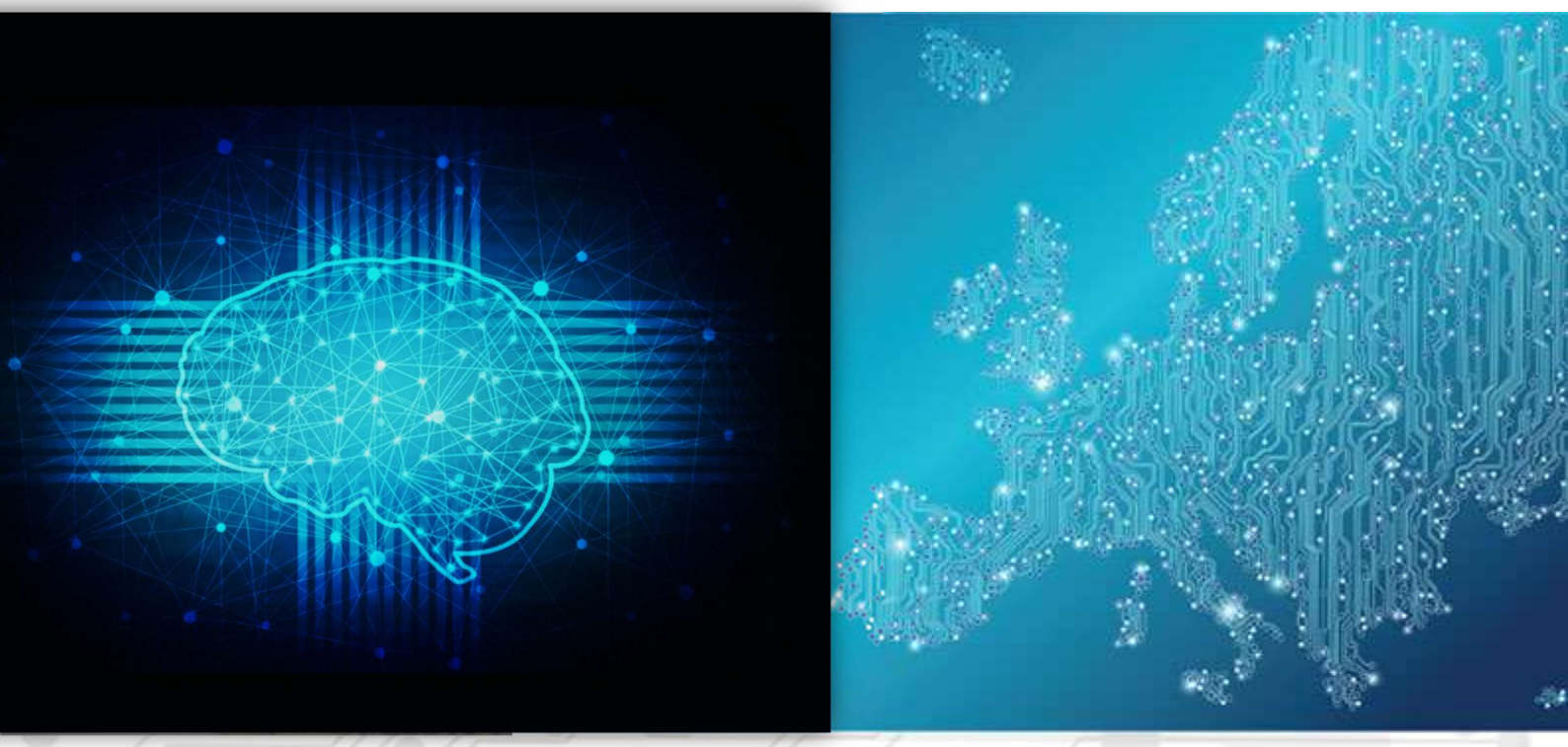

Analysis of the European R&D priorities in cybersecurity

Strategic priorities in cybersecurity for a safer Europe

DECEMBER 2018

www.enisa.europa.eu European Union Agency For Network and Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and EU citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact

For queries in relation to this paper, please contact the author or opsec@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

Author:

Dr. Fabio Di Franco – Fabio.difranco@enisa.europa.eu

Acknowledgements

We would like to thank the list of experts who has provided valuable inputs during the interview or during the review process:
Dr. Robert Atkinson -University of Strathcycle
Dr. Ana Ayerbe – Tecnalia
Dr. Rainer Baumgart - Secunet AG
Dr. Xavier Bellekens - Abertay University
Prof. Giuseppe Bianchi - Università degli Studi di Tor Vergata
Mr. Martin Borrett - IBM
Mr. Scott Cadzow
Mr. Ilias Chantzos - Symantec
Mr. Bruno Chenard- CEN CENELEC
Prof. Michele Colajanni - Università degli Studi di Modena
Prof. Enersto Damiani - Università degli Studi di Milano
Prof. Herve Debar - Telecom SudParis
Mr. Petros Efstathopoulos - Symantec
Dr. Stefanie Frey - Deutor Cyber Security Solutions Switzerland
Mr. Tony Jeffs - Cisco
Mr. Piotr Kijewski - Shadowserver Foundation EU
Mr. Constant Kohler - CEN CENELEC
Dr. Matti Mantere - Forcepoint
Prof. Kai Rannenberg - Goethe University
Dr. Christos Tachtatzis - University of Strathcycle
Ms. Sylvie Wuidart - ST Microelectronics
Prof. Stefano Zanero - Politecnico di Milano

ISBN: 978-92-9204-278-3 doi:10.2824/14357

Table of Contents

Executive Summary

Predicting the future is notoriously difficult. Nevertheless, the main goal of this document is to identify the cybersecurity threats to European society and to identify priorities in research that will lead to mitigations before those cybersecurity threats materialise. By identifying future problem areas, Europe can take a proactive approach in defending against anticipated threats. The security of our information is fundamental and as the pervasive digital transformation takes place, our lives become more exposed to cybersecurity threats.

Based on desktop research and interviews with experts, an effort was made to foresee European society in the near future of 2025, in doing so we have identified the key driving forces and uncertainties, and the changes in society brought by innovation in the digitally connected world. In the effort to explore emerging challenges in a systematic way, a framework has been introduced to guide the analysis. The framework consists of three axes: social aspects, technology and business, along which future developments are forecast. We have recognized the interdependencies among the digital and physical world, the pervasiveness of connectivity in all aspects of society and industries, the evolution of the technologies and their effect on society.

The report focuses on identifying emerging challenges and on those current challenges that are evolving into significant risks to society. Closely related are those challenges in social dynamics brought about by changes in society that have been enabled by technology. Underpinning this is a concern related to education and awareness of the changing threat or risk environment. Based on this analysis, the report identifies the following themes that suggest where future research should be focused on:

- Awareness building – societal challenge
    - Addressing the need, across society, to build awareness of the impact of technological change on social evolution and hence on societal risk
- Capacity building – educational challenge
    - This recognises the shortage of cybersecurity experts and considers means to refresh education at secondary and tertiary levels to bridge the gap
- Existential threats – those threats that if enacted have potential to destroy the directly impacted part of society, industry or business
    - Artificial Intelligence - thanks to the pervasiveness of data collection by the Internet of Everything (IoE), the processing power and storage capacity offered by the cloud, pattern recognition and automatic decision will develop at great speed bringing new opportunities and risks
    - Quantum technologies, where uncertainty is a key characteristic, may be used in both attack against current cryptographic protection methods, and in the development of new computational models for further acceleration of change
    - Complexity of interconnectedness that may lead to cascade fail of multiple systems across the supply chain
    - Cybercrime- thanks to digital transformation, digital identities and valuable assets may become prey during a cyberattack. Detection and mitigation of cyberattacks becomes extremely important
    - The threat to privacy is increasing with “big data” collection and unexpected inference

1. Introduction

The present document provides a series of recommendations for the priorities in the EU for R&D in the domain of ICT security made after analysis of a wide series of interviews with domain experts.

The proposed research priorities have the aim to make Europe, "*a global leader in cybersecurity by 2025, in order to ensure the trust, confidence and protection of our citizens, consumers and enterprises online and to enable a free and law-governed internet*",[1] as stated at the Tallinn Digital Summit in September 2017.

The focus of the report is to highlight and recommend how focussed R&D can address emerging challenges that might pose a severe risk to our society. A key element is the recognition that the world is moving digitally and fast. The speed of adoption of new technologies has a potentially huge benefit resulting in increasing productivity, but at the same time may also pose risks if the technology where used against the best interests of society. Social norms take dozens of years to develop and the digital transformation is creating an increasingly blurred distinction between the digital and the physical world. In the digital world, a small number of corporations, popularly referred to as Internet giants[2], are increasingly required to service the societies of the 21st century. However, this requires a trade-off between the user's data and the internet giants' services: the users allow the digital platforms to track their location, record their interests and monitor their online activities in return for a wide series of services demanded by the users. Data collected from users are used for analytics purposes, which ranges from marketing campaigns and promotions to deep machine learning and data mining.

It is a major challenge to imagine how society will be in a few years from now, and to consider the threats to society at that time. In order to frame this, the broad assumption is that ICT will reach further into society with more connectivity, further integration with everyday life activities through ICT, and this will demand a response in both the design of ICT and the cybersecurity features of ICT products and services. The concerns of the next few years however stretch far beyond the remit of only security technology and many of the recommendations in the present document extend to gaining better understanding of how ICT in general, and in particular, ICT incorporating cybersecurity features impact daily life.

Encouraging R&D in ICT security is essential to respond to the societal challenges that will arise from a fast developing and fast changing ICT centred world that both contributes to, and threatens, the sustainable development of the global economy and, particularly global social stability. The concern for making the activity of the world secure, and the role of ICT technologies in supporting that world, is complex and cannot be simply addressed in technology, thus this report asserts that the R&D focus has to be wider than simply technology and address wider societal issues. In security, it is essential to consider the golden triangle of People, Process, and Technology. If just one element of the three is missing, the risk rises significantly.

[1] https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf

[2] Realistically this includes the largest companies quoted in the stock exchanges: Amazon with Amazon Web Services and Alexa products; the Alphabet corporation, which owns the Google search engine, the YouTube platform and the Android operating system for smartphones; Microsoft with operating systems and the Azure web service platform; Apple with their ecosystem; Facebook with Instagram which dominates the social network in the western world. In combination, their market capitalisation exceed of $3trilion in market, close to 20% of the combined GDP of the EU28.

Unfortunately, it is a generally held view that security is a cost only exercise, and that making people pay for security is often difficult. In fact, it is not always clear if the investment in security is effective, rather than an attacker simply failing to carry out a successful attack. Thus, the cost effectiveness of working security is often considered as hard to quantify.

In order to be able to prioritise research topics, and, perhaps more importantly, to be able to see the larger picture and develop research programmes that are capable of addressing society challenges also a broader, a high-level overview is needed, that shows how the many topics relate to each other. In that light, *Chapter 2 contains a narrative scenario that sketches a broad picture of society in 2025*.

Based on this scenario, *Chapter 3 provides a short description of the identified challenges and the existential threats along with the associated recommendations to mitigate them*.

A detailed analysis of the identified strategic topics and the related research questions are discussed in Annex A: Awareness and education challenges and Annex B:Existential Threats.

Annex C concludes with the methodology used in the report, the European policy context and European funding scheme for research and development.

2. Our Europe in 2025: a plausible scenario

Europe in 2025. Devices are connected to the internet and have permeated everywhere. All the essential operators in all sectors (i.e. energy, transport, banks, digital infrastructure, hospitals), in all public administrations and across industry are providing connected services. 80 billion devices (10 per person on the planet) are connected through the internet and the quantities of data produced has been doubling every 2 years. *Internet of everything (IoE)* has transformed the ecosystem where we live and smart objects have brought about an increase in productivity. It is common to use *wearable devices* controlled by voice to reserve a table on line for a dinner, as well as having a *5G-connected autonomous shared car* driving to a business meeting. Education and training have been made more effective thanks to *augmented reality* and *gamification*, which guarantee an immersive sensation and leverage the natural desire for socializing, learning and competition. Important societal strategies have been identified to increase cybersecurity and strengthen resilience to cyber-attacks. People's awareness, knowledge and motivation to be secure online have been strengthened as media have been drawing attention to the issue. Community initiatives to promote security by design in local infrastructures and systems have flourished, and companies and public administrations have been developing procedures and implementing training programmes. However**,** this has created a workforce of cyber-aware elites and a sub-culture of less aware workers that has increased social tensions.

Governments are now demanding online-only access to taxes, pension and benefits, that require all citizens to have and to use *digital identities*. Massive computing power and storage capacity are available on the cloud and maintained in huge server farms that place significant demands on power and telecommunications infrastructure. Industries have increased productivity by introducing sophisticated sensor networks, machine-to-machine communication, additive manufacturing, robotics, machine intelligence, analytics, and others enabled by smart sensors, cloud technology and virtualisation of processes. More automation has been introduced across almost all forms of businesses. This automation has been augmented by the application of *artificial intelligence* to provide significant levels of behavioural analysis to the data captured from the always-online society, to provide greater insight and understanding of consumer and business behaviour, and to develop ever more products and services to respond to their needs.

In a completely digitized Europe, the internet giants have been able to assert even more control over the economy, but additionally their platforms underpin almost all aspects of society (government, commerce, health, transport, etc.). They are not only able to respond to customer demands, but they are the engines that drive customers' desires, making the customer both the product and the source of revenue driving society. This has raised major concerns in government and in society regarding not just the power of the internet giants but also regarding who leads and governs society. Some activists are refusing to use internet at all driven by concerns regarding privacy risks, others are paying for hiding their online behaviours.

As society has become more experienced in the use of the internet to share information, the already evidenced poisoning of information has become increasingly widespread and controlled by both organised crime and rogue states (or rogue elements in nation states). Using a number of psychologically informed triggers to enforce confirmation bias through "fake news" and by the ability to filter out any contrary opinion, bad actors are actively removing informed societal debate. This has led to the spread of digital ghettos of like-minded people on social networks that are seen as a risk to democracy by removing the

search for, and agreement on, a consensus, often requiring concessions for the greater good, that is required in democratic societies.

In spite of the proliferation of a connected society, many public authorities still face the challenge of large and complex, and in some cases, outdated ICT systems making it difficult to guarantee their security. Citizens, business, and government have been increasingly the target of sophisticated attacks by malicious parties. The capability to respond to cyber-attacks has been enhanced although the impact of cyber-attacks and cyber-crimes have been devastating. Law enforcement still do not have the capability to act as fast as the criminals, who move freely in cyber space and take advantage of the uncertainty of geographical location to keep ahead of law enforcement and of attempts to mitigate their actions.

The percentage of global reliance on ICT is difficult to judge. The growing dependence on an always digitally connected society, where all sectors are dependent to some extent on ICT may lead to consider a failure in ICT as an existential crisis. In fact, ICT is the binding critical infrastructure and a loss of ICT through cyber-attack could lead to failure of all other critical infrastructures.

Quantum computing is still perceived as both an opportunity and a threat. Mastering quantum computing might allow solving classes of problems that cannot be solved with classical computing in a reasonable time. The public-key cryptographic solutions resistant to quantum computers has been emerging although the wider problem of migration has no viable solution in sight.

Given the huge number of network-enabled relationships on which EU citizens' and governments rely, cybersecurity and privacy are areas of major policy concern.

3. Key Messages and Recommendations

In this chapter, the identified threats are briefly explained based on the scenario of Europe in 2025, which has been presented in the previous chapter. Associated with each threat, an area of intervention that might mitigate the emerging threat is proposed. This constitutes the base of our recommendations for the strategic priorities in research and development. A detailed analysis of the identified strategic topics and the related research questions are further discussed in Annex A: Awareness and education challenges and Annex B: Existential Threats.

Awareness building – societal challenge

Any irrevocable societal change takes time to become a behavioural norm. Digital transformation is an example of an irrevocable societal change that is rapidly changing how we behave. The pace of transformation has left too many unaware of the impact of that change and the consequent risks that the new behaviour introduces. Up to now, cybersecurity campaigns have not had the desired outcome and many still do not know how to behave safely in the digital world.

Cybersecurity must become a shared responsibility and all the actors should facilitate a secure and responsible digital world. However, to achieve that, it is essential to have a thorough understanding of related risks and threats, as well as ways to secure and protect against them. This requires a deep understanding of the human behaviour and psychology of change, of how societies work and of social science in general. Bringing these disciplines together is one path to ensure that the changes wrought by increasing digitisation of society, and the resultant change in threat and risk, can be safely managed.

Recommendations on the societal challenge: awareness building

Promote an understanding of how people use and adapt to technology, in order to better model both risk perception and risk reality with a view to providing a concrete basis of why cyber-security technology is required and what its limitations are.

Promote systems that are designed with security and privacy protection features in place and have intuitive user interfaces

Encourage innovations on communicating cybersecurity risks

Based on these high-level recommendations, we identified specific research actions:

- Multi-disciplinary research is needed to model and design future systems in such a way that they are more easily comprehended. This needs a strong collaboration between experts in social disciplines (e.g. anthropology, psychology, sociology) in economics (e.g game theory) and in technology. Large-scale demonstrators should be used to prove the research solutions are valid in real social environments. The intent of this field of research is to gain understanding of how people adopt and use new technology and how risk is perceived in the digital world.
- Research and experimentation in the field of social science is needed to create more awareness of security risks. Moreover, it should be understood how people perceive threats in the digital world and how that perception is used to generate both conscious and impulsive mitigations. Some help in this area is likely to come through the use of simulation experiments (perhaps employing artificial intelligence) to allow greater understanding of the unconscious and intuitive reactions to threats. For that, cognitive modelling and augmented reality could be used to improve the understanding of

appropriate interaction of the users. However, any classroom bias (in which participants are aware they are in a simulation and exhibit false behaviour in gaming the experiment) has to been removed.

Capacity building – educational challenge

On the education side, the principle of security by design and security by default should be the norm and should embrace all phases of the development lifecycle. We identify that the challenge is manifold: cybersecurity has not been considered a disciplinary subject; software security is not included in standard education programmes in computer science, and the effectiveness of the courses might be improved using realistic environments.

Cybersecurity capacity building should not be tackled only from the technological point of view because it has a holistic perspective. Future cybersecurity experts should not only focus on technology, but also on people behaviour at individual and social level (psychology/sociology) and on organisational aspects (processes). Unless cybersecurity experts learn, either individually or in groups, to be experts across disciplines (i.e. technical, human behaviour, organisational and regulatory), the ability to build a socially inclusive secure future for ICT will be lacking. Addressing this problem at the root through education, can contribute to unifying cybersecurity initiatives between these groups. Security is a complex issue that must be considered across every component during the lifecycle of the product. It must also be addressed from a systems perspective, to ensure that the composition of secure individual components into an integrated system yields the desired security properties through the testing and deployment. Integrating security concepts in computer science courses will create a new generation of professionals who understand the security basics and are able to create software with security and privacy in mind. Specialist courses for cybersecurity practitioners should also use simulated realistic environments in order to improve the efficacy of the training including multidisciplinary elements.

Annex A.2 presents in more details the education challenge and the rationale behind our recommendations.

Recommendations on the educational challenge: capacity building

Encourage the transfer of knowledge from specialized security experts to the wider academic environment, particularly in ICT domains, but also across all societal sciences.

Facilitate the teaching of security principles in all computer science and software engineering courses in such a way that the new generations of software engineers have security principles integrated in their course curricula.

Promote the development of new teaching environments that encourage the design, implementation and validation of new methods, technologies and processes.

Foster the development of multi-disciplinary curricula in cybersecurity

Artificial Intelligence – an opportunity and an existential threat

Artificial intelligence (AI) has at its core the promise of huge benefit with similarly huge risk. Enabled by the massive amount of collected data by the evolving Internet of Everything (IoE), the ubiquitous fast connectivity and cloud infrastructure, new applications using artificial intelligence are proposed every day.

Whilst closely related to the concept of "big data", AI is able to pick out patterns and make automatic decisions through the sub-disciplines of Machine Learning and Deep Learning. That is where both opportunity and risk lie – the decision may be beneficial, or it may be catastrophic. A false or misleading assertion by AI could lead to significant harm to the intended societal beneficiary. However, the attraction of building new business on AI is considerable and the reach of AI is immense. It is this depth of intrusion of AI into everyday life that requires a focus of technological research.

Main Recommendation on Artificial Intelligence threat

Promote a robust, safe, secure and inclusive Artificial intelligence where humans can understand the rationale and trust the results.

Foster verification, validation, security, control of the machine learning algorithms and input data have not been manipulated

Annex B.1 contains a more detailed analysis on the applications, opportunities and risks of AI for the security of society. Based on that, more specific research actions are summarized here:

- Research in developing AI techniques that produce more explainable models while maintaining prediction accuracy (usually called in research Explainable Artificial intelligence).
- Research in verification, validation, security and control of the machine learning algorithms for preventing safety issues.
- Research in adversarial machine learning in order to avoid wrong results due to the introduction of false data (either in the algorithm or in the trained data) in the machine.
- In applications where machine learning is unsupervised and there is an interaction with people, AI experiments have shown bias and unfair results. Research is needed how to build inclusive and no discriminatory AI.

It is also considered that longer term research is necessary in the field of having ethically 'correct' Artificial intelligence. The rationale is that as AI becomes increasingly trusted, following the results from the areas highlighted above, it will increasingly become involved in areas of decision making where in conventional human discourse an ethics panel may sit.

Quantum technology

The impact of quantum technology on security can be divided into 2 classes:

1. Techniques to provide resistance to attacks using quantum computing - post-quantum cryptography or Quantum Safe Cryptography (QSC);
2. Techniques taking advantage of quantum effects (e.g. superposition, entanglement, uncertainty) as typified by Quantum Key Distribution (QKD).

The first of these has been identified as a reaction to an existential threat – that by defeating, absolutely, any security claims made against the asymmetric cryptography used today in digital transactions. In other words, quantum computers might be able to undermine the security that underpins e-commerce, e-government.

The second class of quantum technology uses quantum technologies to agree on a secret key in order to establish a secure communication channel resistant to attacks by quantum computers. Although QKD technology has several limitations, including the dependence on physical channels and the need for intermediate trusted node, development of innovative QKD systems might create a niche market in high secure digital communications.

Whilst there are a number of extant research projects into both classes of quantum technology, relevant fundamental research challenges and development issues are present and it might need many years of R&D to bring substantial results. Moreover, when quantum safe cryptographic solutions emerge, further effort and research will be needed to adapt solutions for each user case. Obviously, this priority might need to be reassessed based on the advancement of quantum computers and their practical ability to break current asymmetric cryptography.

Main Recommendations on Quantum technologies

Facilitate the research on post quantum cryptography and their successive applications when candidates will become available

Support the development of Quantum Key Distribution geographical high-speed networks (by using satellite and terrestrial links) for high security communications

The state of the art research in quantum technologies for cybersecurity and the underlying research issues are described in Annex B.2.

Complexity, cascade and supply chain threats

The digital transformation has engendered a subtle transformation that has made all sectors increasingly dependent on digital infrastructures. For example, cloud providers offer many services now and any unavailability, loss of integrity, or violation of confidentiality, may have serious consequences for businesses or governments who use their services. In the same way, the unavailability of financial operations – due for instance to a denial of service attack - has the potential to affect the operations and economy of most countries and businesses.

Unfortunately, the security of systems cannot be guaranteed to 100%. But efforts must be done to secure the systems in order to reduce the risk at an acceptable level and guarantee resilience and business continuity.

Main Recommendations on Complexity threat

Foster the development of a new approach for impact assessment of complex and interdependent systems.

Promote the definition of secure and interoperable interfaces among critical infrastructures to prevent cascading effects.

Based on these high-level recommendations, we identified more specific research actions (as also detailed in Annex B.3) :

- New approaches for dependency and interdependency impact assessment
- Research on the cybersecurity measurements (by catching meaningful parameters from empirical data analytics) might be extremely important to determine trends to better utilize security resources and judge the success or failure of implemented security solutions.
- Convergence of safety, security and quality elements that might be used to assess the maturity model and the resilience of the system
- Define secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.
- New approaches to mitigate against the increasing value of attacks as a result of data centralisation

Cybercrime: Detection, Mitigation and Attribution of Cyber-attacks

Criminal activity is common in all areas of life and it is not a surprise that criminal activity has spread to the digital world. With the digital transformation, many valuable assets are online and they may become the prey of cybercriminals. Some of the attacks use methodologies and attack vulnerabilities that are already known; others, the most sophisticated ones, use creative solutions and unknown techniques. Cyber-attack patterns need to be better recorded and understood in order to apply effective mitigation measurements.

Main Recommendations on Cybercrime: Detection, Mitigation and Attributions of Attacks

Facilitate the research on technical prioritization of security efforts and the development of innovative situational awareness tools

Help the development of independent evidence-based cyber threat intelligence and understand the trends through historical data.

Based on these high-level recommendations, further R&D investment is needed on these topics (also described in Annex B.4):

- Research on technical prioritization of the security effort (e.g. Advanced threat intelligence which simplify the process of combining and prioritizing alerts from multiple sources)
- Development of novel approaches for providing organisations the appropriate situational awareness in relation to cyber security threats allowing them to detect and quickly and effectively respond to sophisticated cyber-attacks.
- Development of novel techniques to collect forensic information
- Development of independent evidence-based cyber threat intelligence for fighting cybercrime, understand the trends through the position of sensors able to do sinkholing and collect malware samples
- Research and development on malware /attack prediction using data analytics and machine prediction. That will need the creation of very large updated data sets of labelled malware to train the machine predictor.

Privacy threat

Privacy is a fundamental right cited in the Universal Declaration of Human Rights[3] and in the European Convention of Human Rights[4], and many efforts have been made in regulation and legal frameworks to protect those rights. The most recent important example in Europe being the General Data Protection Regulation (GDPR) [5], which had a considerable impact on how corporations and organisations manage personal data. The GDPR introduce a risk-based approach that encourages organizations to implement appropriate measures corresponding to the level of risk of their data processing activities. That might be seen as an administrative burden, but if it helps to protect the privacy that is always at risks in this always more connected data-centric digital world. The forthcoming Regulation on Privacy and Electronic Communications may reinforce the legal basis for the protection of privacy in electronic communications.

Main Recommendations on Privacy threat

Promote and diffuse Privacy Enhancing Technologies (PETs) across different components (e.g. big data, cloud, IoT) and through application domains (e.g. healthcare, transportation, energy)

Promote the development of privacy assessment tools for guaranteeing appropriate measurements are in place to protect private information.

As described in Annex B.5, the research challenge are manifold:

- New anonymization privacy models and methods are required
- New Analytics tools where the principle of data minimisation is applied.
- New Model of safeguarding mechanisms following the privacy by design and by default requirements

[3] http://www.un.org/en/universal-declaration-human-rights/
[4] https://www.echr.coe.int/Documents/Convention_ENG.pdf
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679

Annex A: Awareness and education challenges

A.1 Awareness building – societal challenge

The digital world has a different pace. Understanding this, being aware of it, is the key to progress and improvement. Cybersecurity represents both risk and opportunity. In the physical world, society has spent many centuries developing both awareness and understanding of the environment and developing coping mechanisms to manage both risk and opportunity. The digital world and its inherent risks and opportunities have been with us for at most a few decades. The pace of its arrival has meant that unlike in the past the older generation has time to learn and teach the next generation a set of coping behaviours. In the digital age all generations are experiencing and learning at the same time – this tends to encourage sharing experiences and behaviours amongst peers.

The call to "Don't take candies from strangers", "Don't talk to strangers"? is in many societies used throughout childhood to teach risk aware behaviour and became part of the social norms upon which society is built. The viability and success of these forms of teaching has taken many years to develop but on occasion still fail: Children still accept candies from strangers and in some occasions place themselves at extreme risk as a result. In contrast, the digital world is comparatively new and is evolving too fast for simple social teaching and social norms to develop in order that learned protections become native. Moreover, in this context the threats are continually changing.

In many cases, people cannot translate what is safe and polite behaviour in the physical world to the digital world[6]. There are some demographic generalisations that may apply: Exposure only as adults with limited desire to become safe and protected digital citizens; A younger generation has been born using technology as the basis of learning and communicating (i.e. mobile phones and computers are the new norms). There is also a general expectation that the ICT infrastructure (the services, the network) will work as intended, and that failure has no hard consequences, other than requiring a reboot. There is also a significant mind-gap between pure IT appliances (telephones, computers, TVs, tablets), whose life expectancy is relatively small, and physical-IT appliances (cars, fridges, heaters, AC unit, etc.) which have a long lifetime, and are even supposed to be used by multiple owners and have resale value. Ensuring that the ICT part of these objects follows the same principles as the physical part, which can be sold without leaving "traces", is certainly difficult.

Typical reactions to advice on cybersecurity are generally negative: "the interfaces are too complicated", "I did not know", "it is too boring", "I know but I don't care". The lesson of this appears to be that people find the concept of cybersecurity both difficult and of no interest. In the physical world, safety is provided for them or is learnt through both direct and indirect exposure to risk. Taking all of the risk management onboard as an individual is not acceptable so it is often discounted as somebody else's responsibility. So, the question is either:

- how can citizens be empowered with the knowledge and a sense of shared responsibility to practice safe and informed behaviours on the Internet? or,

[6] The European Cybersecurity Month initiative has been promoting awareness in cybersecurity since 2011. It advocates for change in the perception of cyber-threats by promoting data and information security, education, sharing of good practices and competitions. In particular the slogan STOP. THINK. CONNECT.™ aims to educate all Internet users to be more vigilant about practicing safe online habits; to ensure that Internet safety is perceived as a shared responsibility at home, in the workplace, and throughout our communities. https://cybersecuritymonth.eu

- how can citizens be assured that they are not exposed to risk?

Further research is required to answer either of these questions with any degree of certainty.

A.2 Capacity building – educational challenge

Cybersecurity experts are in high demand and it is predicted that more than 350K additional experts will be required by 2022[7]. Cybersecurity education will play a fundamental role for forming a new generation of experts.

A.2.1 Enabling the multidisciplinary approach

Cybersecurity is a multidisciplinary subject, well described in the Camino[8] H2020 project as formed by these aspects:

- **Technical** - related to technology, concrete technological approaches and solutions that can be used to fight against cyber-crime and cyber-terrorism,
- **Human** - related to human factors, behavioural aspects, privacy issues, as well as raising awareness and knowledge of society with regards to cyber-crime and terrorism threats,
- **Organisational** - related to processes, procedures and policies within organisations, as well as cooperation (public-private, public-public) between organisations,
- **Regulatory** - related to law provisioning, standardisation and forensics.

Very simply unless cybersecurity experts learn, either individually or in groups, to be expert across all of these disciplines and their many sub-disciplines, the ability to build a socially inclusive secure future for ICT will be lacking. Quite simply as has been shown in the research to date, experts focusing on different cybersecurity aspects often find it difficult to communicate effectively together because their incentives, languages, knowledge bases, and worldviews are different. Addressing this problem at the root through education, can contribute to unifying cybersecurity initiatives between these groups[9]. The assertion is that it is known what needs to be done, that is to become multidisciplinary, the challenge is to enable it.

An approach in this direction is the Cyber Security Academy [10] where students are required to learn the relations between technical, legal and social scientific aspects of cybersecurity, so they can come to effective and sustainable solutions for cyber risks and threats and contribute effectively to sustainable strategies for digital defensibility and security of society as a whole. ***An effective way to achieve this goal appears not to have a clear answer as to what must be done. This guarantees that is has to be a priority in research.***

A.2.2 Cybersecurity in computing

If the assertion is made that ICT embraces cybersecurity, and that ICT is enabled by computing, then it follows that cybersecurity and computing should be addressed together.

Every day developers release code that contains defects. Whilst not all defects are necessarily security flaws, many of them may be exploited to become security or safety concerns. Even if a defect or bug exists the functional goal of the code may be achieved, and the existence of the defect may not be seen in

[7] Global Information Security Workforce Study 2017
[8] http://www.fp7-camino.eu/
[9] Ramirez, R, 'Making cyber security interdisciplinary : recommendations for a novel curriculum and terminology harmonization', MIT 2017
[10] https://www.csacademy.nl/en/

conventional use and deployment. The existence of defects that may become vectors of attack should not be a surprise given that ***software security is usually not included in the standard educational programs in computer science and security and privacy by design are too often taught only in specialized optional courses.*** Findings such as those of the CSEC2017 Joint Task Force[11] recommending that efforts be made to standardize curricula for the programme in cybersecurity, and by doing so to restructure the curricula in Computer Engineering, Computer Science, Information Systems, Information Technology, Software Engineering and introduce cybersecurity concepts in specialized classes, are a significant step forward.

Security must be considered from the top to the low level, across every component, between every component from the architecture of the systems, through the testing and operation and deep into the silicon that carries out the computing. That is a not trivial exercise. The issue in programming is complex and range from architectural security issues to a single bug exploit by a creative attacker, this is also true for decisions regarding the use and reuse of library code where the reuse may disclose defects not present in the originally targeted use.

Recently DevSecOps[12] [13] has gained traction in IT development: it indicated the development, security and operation team work together in agile way and they think about security and application from the start. It is all about introducing the security elements sooner in the life cycle of application development[14] to minimize vulnerabilities and have everyone involved become responsible for security. The idea is to automate core security tasks by integrating security processes and controls earlier in the development side. That is also beneficial the overall quality of the products and services offered.

Security by design should be the norm along and should embrace all phases of the lifecycle. The research interviews that informed the present report indicated **a need of *material with updated examples and guidelines that might facilitate the transfer of the knowledge from specialized security expert to the wider computer science*.**

In particular, development of guidance and education material for computer science is needed to ensure education in the following fields:

- Validation methods which can trap and eradicate known vulnerabilities (e.g. built in immunity to SQL injection attacks)
- Authentication, authorization, and session management in order to remove mechanisms by which an attacker gains unauthorized access (prevention of privilege escalation).
- Secure programming including characteristics of each language that impact security including cryptographic utilities, the storing and access to sensitive information, protecting data in memory.

[11] https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf
[12] https://www.redhat.com/en/topics/devops/what-is-devsecops
[13] https://www.csoonline.com/article/3245748/devops/what-is-devsecops-developing-more-secure-applications.html
[14] Microsoft has develop a Security Development Lifecycle that introduces security and privacy early and throughout all phases of the development process including an Agile approach: https://msdn.microsoft.com/en-us/library/windows/desktop/84aed186-1d75-4366-8e61-8d258746bopq.aspx

- Methodology for software development, which takes into consideration security in the lifecycle of the software - from design through development to deployment, maintenance by secure software update until both the end of life, and reassignment of life[15].
- Static analysis automatic tools to identify insecure code (e.g. Potential buffer overflows, tainted inputs and integer overflows) and perform security and vulnerability testing

Research is also needed to use artificial intelligence to analyse software both in static and runtime modes in order to provide intelligent insights such as application stability, failure patterns, defects and failure prediction.

A.2.3 Simulation and visualisation

Cybersecurity skills need to be continuously advanced at all levels and the experts need to adapt their expertise to a constantly evolving landscape with increasingly sophisticated and novel cyber-attacks, against a widening attack surface of exposed ICT systems and services. A mechanism that may achieve refinement of skills is through the cyber range, a form of war-gaming where procedures, technical elements and coordination activities can be exercised and responses validated. War gaming has long been an accepted practice in the training of armies, emergency services and civil response units. In this context, an example is offered by the European Cyber Security Challenge initiative[16] that through a sort of war gaming among national teams tries to mitigate the shortage of skill in cybersecurity and at the same time encourage young people to pursue a career in cybersecurity.

In this simulated environment, whilst it can offer a platform for research into the design, implementation and validation of new security measures, most usefully it offers an opportunity to teach the role of the multidisciplinary elements of cybersecurity.

In this simulated environment, research must be done on the design, implementation and validation of new methods, technologies and processes in order to achieve a higher level of security to increase the resilience against the growing threat of cyber-attacks. The simulated environment will also help for training activities, by developing skills that can be immediately used in the real world environment.

[15] Many ICT devices are re-purposed for a second life after their primary purpose is fulfilled, this may be as simple as passing a laptop from parent to child when the former upgrades, but also has to address the second hand market in ICT tools and technologies

[16] https://www.europeancybersecuritychallenge.eu/

Annex B: Existential Threats

B.1 Artificial intelligence: the new frontier in cybersecurity

B.1.1 Artificial Intelligence in the world of Internet of Everything

Artificial Intelligence (AI) is a significant new frontier of technology that is developing at great speed and becoming applied as an integral element in the software of all environments and industries. The promise of these advances is that AI acts as a transforming capability in all sectors bringing innovative solutions to the market. As AI capabilities advance and as AI systems take on increasing importance in societal functions, the fundamental challenges discussed below are expected to become increasingly significant.

It is necessary to refine what is meant by AI. In the present document, AI refers to the broad sweep of technologies in which a machine demonstrates intelligence leading to an optimal, or close to optimal, solution for a given problem (e.g. machine learning, deep learning). As AI develops it will be the root of many applications that are proposed to be introduced where machines act in increasingly autonomous modes, i.e. responding to and interacting with their environment in flexible, resilient and self-learning ways.

The core characteristic of AI-enabled machines is that they analyse and interpret data in order to solve a problem, or to gain insights from data[17]. AI is assumed to learn in real time through trial and error, in the same way humans do, and for that requires massive amounts of "cleaned" data to train the model.

However Artificial Intelligence has been talked about forever. The only difference is that now the fast processing, the fast networking and the massive amounts of generated data sets enables AI to reveal the full potential.

In fact, citizens are living in smart houses, driving autonomous cars, wearing smart wearables and enormous quantities of data are produced and processed by AI-enabled machines. The core concept of "*Big Data*" analytics using AI is able to transform unstructured data into meaningful information and a trained AI model is able to take real-time decisions based on previous behaviours. Many of the major cloud providers have already started to provide Artificial Intelligence as a Service[18] [19] [20] [21]. Whilst it may require further effort to discover viable solutions for all business cases, the direction is set.

Unfortunately, AI does not only offer opportunities but it also poses security threats and safety risks that will impact efforts to create a defence for the beneficial use of AI.

B.1.2 A few applications of AI today

Autonomous vehicles

Autonomous cars are now becoming a reality. They use a variety of sensing technologies including radar, optical recognition, which can function in tandem with GPS and inertial measurement sensors to model

[17] The field of big data and data analytics, which allows gaining insight from data to take better decision, is often a different considered a separate field of study and development.
[18] https://www.ibm.com/cloud/machine-learning
[19] https://azure.microsoft.com/en-us/services/machine-learning-service/
[20] https://cloud.google.com/products/ai/
[21] https://aws.amazon.com/machine-learning/

the current dynamic behaviour of the vehicle. Moreover, the sensor data can provide accurate estimates of the location and direction of the vehicle. This facilitates convergence with a cooperative Intelligent transportation systems (ITS) to build up a detailed dynamic map of the operating environment and its relation to the planned route of the vehicle. AI technologies are abundant in the vehicle to enable this dynamic map and to estimate the behaviour of other vehicles with either human or AI drivers in order to maximise the safety of the vehicle and its environment.
However, cybersecurity might not have been a priority area of research in the development of autonomous vehicles since the exploit of autonomous cars have been extensive: hackers taking control of the car[22], modifying the system into not following the posted traffic signs[23], lock the systems for ransom[24]. The AI itself could be taught to act in a way that makes the driving environment unsafe or dangerous to both the AI controlled vehicle and its environment. As AI becomes closer to some meaning of sentience different AIs may behave in similarly random ways to the human intelligences that they seek to replace[25]

Image and video manipulation
Now it is possible to produce synthetic images that are nearly indistinguishable from real photos. Soon probably, humans might not be able to distinguish which videos are created artificially from the real one. As production and dissemination of high-quality forgeries becomes increasingly low-cost, synthetic multimedia may constitute a large portion of the media and information ecosystem and they might spread using social networks. Obviously, the advance in machine learning might allow the detection of synthetic multimedia with a greater level of accuracy.

Surveillance
Surveillance systems have been developed that can follow trajectories of individuals, count people and predict where crowd congestion may occur without[26] human intervention[27]. Many deployed CCTV systems have the technical ability to deploy AI processing to perform a number of tasks including gait recognition and facial recognition that recognize particular individuals. Whilst technically available not all such technologies can be deployed due to legal restrictions – however their existence suggests a particular challenge in assuring citizen privacy[28].

Concern of dual use
Artificial intelligence is a dual-use area of technology. It can be used in both an attacking and defending role, for civilian or military application, and more broadly, toward both beneficial and harmful ends. For example, systems that examine software for vulnerabilities have both offensive and defensive applications. The DARPA's Cyber Grand Challenge[29] created a "Capture the Flag" tournament where autonomous machines attacked the other six machines participating at the tournament while defending their own system. This required breakthrough approaches in a variety of disciplines, (e.g. computer security, program

[22] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
[23] Eykholt, K, 'Robust Physical-World Attacks on Deep Learning Models', Corr, 2017
[24] https://www.wsj.com/articles/the-dangers-of-the-hackable-car-1505700481
[25] There is necessary overlap between AI in autonomous vehicles and the establishment of ethical AI that is addressed in more detail later in this report. http://moralmachine.mit.edu/ provides a website for building a crowd-sourced picture of human opinion on how machines should make decisions when faced with moral dilemmas and for discussion of potential scenarios of moral consequence.
[26] https://spectrum.ieee.org/the-human-os/robotics/artificial-intelligence/hacking-the-brain-with-adversarial-images
[27] https://www.theverge.com/2018/1/23/16907238/artificial-intelligence-surveillance-cameras-security
[28] http://www.hitachi.com/New/cnews/month/2017/03/170327.html
[29] https://www.darpa.mil/program/cyber-grand-challenge

analysis, and data visualization) to perform automatic identification of software flaws, formulation of patches and deployment on the network in real time.

Unsupervised AI and bias
There have been a number of examples of unsupervised AI that have made news headlines due to unwanted behaviour:

- The twitter chatbot used to test and improve Microsoft's understanding of conversational language was suspended after 16 hours when it began to behave in an unforeseen and unintended manner[30].
- Amazon's proposed automatic tool for recruitment was scrapped due to it exhibiting signs of sexual discrimination[31].
- In a study analysing the risk of using Northpointe's AI assisted tool COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) it was discovered that the AI tool was introducing racial discrimination[32] by wrongly identifying black defendants at higher risk of reoffending (recidivism) than white defendants thus reinforcing custodial sentencing for black offenders.

Examples exist of social-media sites filtering news that amplify behavioural biases by showing only media that reinforces natural confirmation bias and, by design, protect the reader from being challenged with contradictory sources of news. That opens questions at moral and ethical levels: How to ensure a fair and equal representation in the data used to train AI data across all dimensions of diversity, racial, cultural, gender, linguistics in order to avoid discriminations, racism, extreme political views? How can AI decisions be made that achieve fair and inclusive views and balance different positions? How to engage and support the marginalized people and the most vulnerable in our society?

The conclusion here is that research is needed in order to de-bias AI and to ensure that training schemes for AI do not inherit biases from their programmers.

B.1.3 Research for an explainable robust and safe AI

Artificial intelligence offers tremendous opportunities in all sectors. "*The risks, however, are also substantial and plausibly pose extreme governance challenges. These include labour displacement, inequality, an oligopolistic global market structure, reinforced totalitarianism, shifts and volatility in national power, strategic instability, and an AI race that sacrifices safety and other values*"[33]. In this document, the scope is narrower and focusses on a few technical elements that are related to the technology centric security aspects. To be accepted in a society, an AI machine has to be trusted[34]. Research is desired to lead to proof that an unsupervised AI performs robustly as desired and the results are in line with the expectations. This can be translated into 4 areas of research: [35]

- **Verification**: How to prove that a system satisfies certain desired formal properties. (Did I build the system right?)

[30] https://en.wikipedia.org/wiki/Tay_(bot)
[31] https://www.bbc.com/news/technology-45809919
[32] https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm
[33] Dafoe, A.,'AI Governance: A Research Agenda', Future of Humanity Institute, University of Oxford, 2018
[34] Samek, W et at, 'Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models', ITU Journal: ICT discoveries, Oct 2017
[35] Russell, S et al, "Research Priorities for Robust and Beneficial Artificial Intelligence", AI Magazine 36, No 4, 2015 https://futureoflife.org/static/data/documents/research_priorities.pdf?x93895

- **Validity**: How to ensure that a system that meets its formal requirements does not have unwanted behaviours and consequences. (Did I build the right system?)
- **Security**: How to prevent intentional or unintentional manipulation by unauthorized parties.
- **Control**: How to enable meaningful human control over an AI system after it begins to operate.
- **Traceability**: How to be able to trace how the AI system has taken a certain decision.

Poor design of AI systems may cause unsafe and harmful behaviour. The following list shows some of the research problems regarding a safe AI[36]:

- Avoiding negative side effects: How to ensure that an AI agent will not cause unintended and destructive effects to the rest of the environment?
- Avoiding Reward Hacking: "*How can we ensure that an AI agent will no game its reward function? For example, if we reward the robot for achieving an environment free of messes, it might disable its vision so that it won't see any messes, or cover over messes with materials it can't see through, or simply hide when humans are around so they can't tell it about new types of messes*"[37]
- Distributional shift: How can it be ensured that an AI agent behaves robustly when its test or deployment environment differs from the training environment? [38]
- Safe exploration: How can an AI agent be built that respects constraints and limits?
- Absent supervisor: How can an AI agent ensure that it does not behave differently depending on the presence or absence of a supervisor?
- Safe interrupt ability: How to ensure an AI agent, in order to achieve its goal, does not disable any designed in kill switch?[39]

All these issues for safety and security can be better managed through ***explainable robust AI***. This field of research aims to produce more explainable models in the way that humans can understand the rationale, trust the results and be able to predict how the AI will behave in the future.

B.1.4 Adversarial machine learning intelligence and the challenge to recognize the unknowns

Adversarial machine learning in which an attacker produces carefully perturbed input samples aimed to mislead detection at deployment is an additional area in which research is required. There have been reported cases where a Black Box attack has been carried out in closed systems surveillance systems, autonomous car, and speech recognition[40] as examples of adversarial machine learning. Adversarial AI often deals with unknown unknowns wherein on deployment they misclassify never-before-seen inputs that are sufficiently different from known training data[41]. This threat needs further research in order to avoid a false sense of security in the mitigation and detection of attacks done using AI where unknown unknowns poses a risk of misclassification on the defence monitoring tool.

---

[36] See some of the works done for the AI Safety Research programme: https://futureoflife.org/ai-safety-research/
[37] Amodei, D et al, "Concrete Problems in AI Safety", 2016, https://arxiv.org/abs/1606.06565
[38] Leike ,J, "AI Safety Gridworlds", 2017, https://arxiv.org/abs/1711.09883
[39] Orseau, L et Amstrong, S. "Safely Interruptible Agents", Proc. of Conference on Uncertainty in Artificial Intelligence 2016, New York City. Machine Intelligence Research Institute, 1 June 2016, https://intelligence.org/files/Interruptibility.pdf
[40] Narodytska, N et Kasiviswanathan, S. "Simple Black-Box Adversarial Perturbations for Deep Networks, 2017, https://arxiv.org/abs/1612.06299
[41] Biggio, B et Roli, F, "Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning", 2018, https://arxiv.org/abs/1712.03141

B.1.5 Artificial intelligence and ethics

A more provocative area of research is the relation between AI and ethics.

Robots will increasingly gain intelligence and the resulting robots may be used in the future as defence tools. A first question is how to define an AI that can recognize what is ethically 'correct' or not. Any solution that eliminates the uncertainty of sentience, such as creating programs with explicitly formulated rules, rather than asking a robot to derive its own, is defeating the rationale for sentient or autonomous AI. There are many ways to consider and gamify ethical dilemmas. The challenge to be faced in research is that of providing a structure of ethics that allows a robot to interact with humans (and other sentient things (machine or animal). An ethical black box, which is able to maintain a record of the inputs and actions that led to any decision, may be critical to the process of discovering why and how a robot caused an accident, and thus an essential part of establishing accountability and responsibility [42]. Society's acceptance of such machines will depend on whether they can be programmed to act in ways that maximize safety, fit in with social norms, and encourage trust. However, a more philosophical set of question remain: Can machines have sentience? How can a sentient machine be recognised? This restates the Turing test: Can machines think?[43] How to distinguish a human from a machine?

The resultant codification of AI, of Ethics, has to be interoperable across a wide range of technologies and there has to be a very close relationship between R&D and exploitation or deployment. This has to address such issues as codification in policy and legislation as well as in the ICT requirement to share knowledge and information.

B.2 Quantum technology

. The current state of the art in asymmetric cryptography is predicated on “hard” problems, that is problems which have no feasible means of being solved. If these hard problems can be solved then the security assumptions are made null and void. Research in the field of quantum computing and the application to such problems has produced credible threats to the underlying assumptions behind these “hard” problems to such an extent that research has been focussed in recent years on identifying alternative schemes to the existing pervasive cryptosystems of RSA and Elliptic Curve Cryptography.

The impact of quantum technology on security can be divided into 2 classes:

3. Techniques to provide resistance to attacks using quantum computing - post-quantum cryptography or Quantum Safe Cryptography;
4. Techniques taking advantage of quantum effects (e.g. superposition, entanglement, uncertainty) most often demonstrated in Quantum Key Distribution (QKD)

State of the art

In June 2015, ETSI has released a survey of current cryptographic principles, the possible impact of quantum computing on their effectiveness and what can be done to mitigate the risks in an economically and technically practical manner[44]. This study has been followed up by a large number of ETSI

[42] Winfield, Alan et Jirotka, Mrina, “The Case for an Ethical Black Box”, Part of the Lecture Notes in Computer Science book series (LNCS, volume 10454)
[43] Turing, Alan, "Computing Machinery and Intelligence", Mind, LIX (236): 433–460, Oct 1950, doi:10.1093/mind/LIX.236.433, ISSN 0026-4423
[44] http://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf

publications[45] on the threat from quantum computing and on characterisation of cryptographic primitives that enable resistance against attacks using quantum computers[46].

In parallel ETSI ISG QKD has developed a number of specifications[47] relating to the physical layer capabilities of quantum-based data transfer that allow for a completely secure means to achieve agreement on some shared random data, the most obvious semantic form for this random data is a key for use in a future cryptographic function. Note that QKD only addresses the threat of capture of a key in transit and does not address any further distribution of the key once agreed. It should be stressed that QKD is a purely physical phenomenon whereas QSC is able to be applied at any abstracted layer in the conventional OSI model.

Whilst in April 2016 NIST published "NIST Interagency Report (NISTIR) 8105: Report on Post-Quantum Cryptography"[48], which indicated the status of quantum computing and post-quantum cryptography up to that point, it also outlined NIST's initial plan to move forward in this space. The next steps have been seen in the invitation for assessment of future quantum safe cryptographic algorithms which are undergoing detail analysis[49]. Submissions include some that were (co-)designed by PQCRYPTO[50] and SAFEcrypto[51], two H2020 projects completed in 2018 with a focus on developing post quantum cryptography solutions.

The contrast between quantum technology in security and resistance to the application of quantum computing to defeat security has to be stressed. Very simply there are no visible developments in the application of quantum mechanics in security – in this context the role of QKD is that of key establishment and does not of itself address security (the nature of QKD is that a secret is exchanged between 2 parties but that secret is not known in advance nor it is part of a recoverable key management scheme).

In 2016 the EU commission prepared a communication "Commission Staff Working Document on Quantum Technologies"[52] which reviews current issues in creating industrially and societally relevant Quantum Technologies and discusses concerns to be addressed by a roadmap for turning Europe's global leadership in research into a future world-class European Quantum Industry.

The Commission Expert Group on Quantum Technologies – High Level Steering Committee - has delivered in June 2017 the Quantum Technologies Flagship Final Report[53]. It focuses around four mission-driven research and innovation domains, representing the major applied areas in the field: Communication, Computation, Simulation, as well as Sensing and Metrology. The Quantum communication involves generation and use of quantum states and resources for communication protocols (i.e. quantum random number generators (QRNG) for secret keys and quantum key distribution (QKD) for their secure distribution).

---

[45] See the work done in ETSI related to cybersecurity: https://www.etsi.org/technologies-clusters/technologies/cyber-security

[46] This work was conducted by the ETSI TC CYBER and the ETSI ISG QSC group, now integrated as a specialist working group of ETSI TC CYBER

[47] https://www.etsi.org/technologies-clusters/technologies/quantum-key-distribution

[48] https://doi.org/10.6028/NIST.IR.8105

[49] https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization

[50] https://pqcrypto.eu.org/

[51] https://www.safecrypto.eu/

[52] ec.europa.eu/newsroom/dae/document.cfm?doc_id=15270

[53] https://tinyurl.com/QT-/HLSC-report

Based on Quantum Technologies Flagship Report, the EU commission has recently opened some calls:

- H2020-FETFLAG-2018-2020 to build a strongly networked European Quantum Technologies [54]-Ramp-up phase in H2020 to further develop R&D in Quantum Technologies
- SU-ICT-04-2019 QKD testbed call for building an experimental platform to test and validate the concept of end-to-end security, providing quantum key distribution as a service. This will be a pilot to determine the maturity of QKD to identify the practical implementation issues[55]

All these initiative goes in the right direction and both Quantum Key Distribution (QKD) and post-quantum cryptography present relevant fundamental research and development challenges and might need many years of research to bring substantial results. Moreover, when quantum safe cryptographic solutions will emerges, further efforts is needed to adapt the best solutions for each user case. Obviously, this priority might need to be reassessed based on the advancement of quantum computers and their capability to break the current asymmetric cryptography[56].

B.3 Complexity, cascade effect and supply chain threat

The complexity of networks and systems has increased dramatically over the last years, and there is no reason to suggest that this trend will stop. It is already challenging to consider the relations in each of big monolithic or small-interconnected systems, but the complexity increases exponentially when it involved complex systems from different sectors and cross borders. It is necessary to look at the complexity and interdependency in different areas that are critical for our society and economy. In fact, a loss or damage will lead to significant negative impact on the safety, security or health of the population.

A domino effect, in which the failure of one component can instantiate a chain of failures across a wide set of loosely connected components should be addressed in design. A more technical definition of the domino effect is cascade failure. The impact of security incidents may propagate across sectors via such cyber dependencies and interdependencies.

Due to the digitisation of services, all major sectors have an increasing level of dependency on digital infrastructures. For example, many services now are offered by cloud providers and any unavailability, loss of integrity, or violation of confidentiality, may have serious consequences for businesses or governments who use their services. The use of multitenant cloud storage also poses security risks that cannot be completely unconsidered. Moreover, the unavailability of financial operations – due for instance to a denial of service attack - has the potential to affect the operations and economy of most countries and businesses.

Another example of the complexity and the dependencies in our everyday life is shown by the supply chain attack[57]. An instance is the NotPetya attack[58], where a compromised software posed a single point of

[54] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/fetflag-03-2018.html
[55] https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/su-ict-04-2019.html
[56] BSI in 2017 has published a comprehensive study on the evolution of quantum computers in order to understand the status of the art, the actors and the current technology to build a Quantum Computer - https://www.bsi.bund.de/qcstudie
[57] Examples of supply chain attacks: https://www.enisa.europa.eu/publications/info-notes/supply-chain-attacks
[58] https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ reports that at least four hospitals in Kiev, six power companies, two airports, more than 22 Ukrainian banks, ATMs and card payment systems in retailers and transport, and practically every federal agency were affected. And the attack had serious consequence in other countries and in important businesses.

failure for the security of several entities that offered critical services. Strictly related to it, it is the failure of assurance that products introduced in the supply chain do not present cybersecurity defects (at any layer from the silicon to the customer interface), which when exploited can create failures with domino effects.

Unfortunately, the security of systems cannot be guaranteed to 100%. But efforts must be done to secure the systems in order to reduce the risk at an acceptable level and guarantee resilience and business continuity. A risk-based approach is the most used methodological approach for security although it is often not difficult to quantify the risk brought by interdependencies.

The present report therefore suggests the following areas for research:

- New approaches for dependency and interdependency impact assessment starting from the Identification and Modelling of Dependencies and Interdependencies, through the Analysis and Measurement (e.g. Network based approaches that capture information flows among individual components to depict dependencies and interdependencies)
- The quantitative measurements in cybersecurity[59] are extremely difficult and most often organizations use metrics which may include a subjective attribute. Research on the cybersecurity measurements (by catching meaningful parameters from empirical data analytics) might be extremely important to determine trends to better utilize security resources and judge the success or failure of implemented security solutions.
- Convergence of safety, security and quality elements that might be used to assess the maturity model and the resilience of the system
- Define Secure, interoperable interfaces among different critical infrastructures to prevent from cascading effects.
- New approaches to mitigate against the increasing value of attacks as a result of data centralisation.
- Development of system-wide attack mitigation patterns that should be included in systems to provide graceful failure modes instead of catastrophic modes.

B.4 Cybercrime: Detection, Mitigation and Attribution of attacks against Cyber threats

As cyberspace grows in size and complexity and digital transformation evolves, the risk of cyber-attack for business and individuals increases[60]. The economic benefit for the attackers is reported very high and risk for individuals might include not only a financial or cyber dimension but also a physical one (e.g. the theft of personally identifiable information or biometric data may be used for a criminal impersonation).

High-profile data breaches[61] have made headlines recently and the growing number of incidents require extra effort for detecting and mitigating the attacks. The fight against cybercrime can be approached at different levels (policy, regulatory, technical, organizational, etc.) although the present report focusses on the technical level.

[59] The ETSI Information Security Indicators ISG is already publishing standards in the area of quantitative evaluation of cybersecurity performance for organizations. The work already done includes indicators, a maturity model, and in the future, they might propose data analytics to compute part of the indicators automatically.
[60] The Global Risk Report 2018 from the World Economic Forum has identifies cyber-attacks as the most probable risks after natural disasters in a 10 period time https://www.weforum.org/reports/the-global-risks-report-2018
[61] Largest data breaches in the last years :
https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/

To effectively tackle ever more sophisticated cyber threats requires an understanding of the actors, their determination or motivation, in order that the defenders have a clear understanding of the attack surface and how it can be reduced.

One of technical issue for both government and business protecting against cyber-attack is the relative inefficiency of threat analytics. Whilst solutions such as the Security Information and Event Management (SIEM) have existed for an extended period of time, the complexity of the systems, the inability to extract information from noise, the lack of skilled resources to interpret and the analyse the available data, and sometimes the sophistication of attacks has left many attacks undetected for long periods of time, and this results in discrediting of the tools at hand. Research into new predictive security analytic machines may play a significant role by utilising the tools of big data analytics to provide an analyst with everything they need to know or make an automated decision based on the measured elements[62].

However, the fight against cyberattacks should not be underestimated: the adversary can be creative (e.g. zero-day attacks), might not follow any rules, the knowledge of labelled data on malware or attacks is limited to a few cyber security companies and new sample might be available too late in certain critical environment. Research and development in this field is necessary although that might be proved extremely challenging considering that categorize the unknowns is not possible and it is extremely challenging to predict an attack who has not been before. However, a concrete move in this area to might be beneficial to provide an effective first layer of defence. The higher level of security might still only be offered by whitelisting the known software and connections to reputable partners and leaving an expert or another algorithm to judge the other cases. Anyway in many environments, defence-in-depth approach as well as cyber resilience and response capabilities appear as the only solutions viable to respond to the threats and limit the damage.

There is also a significant trade-off between security controls and ease of use. Monitoring and detection provide a solution that enables users to carry on with their work, while detecting anomalies and supporting corrective measures later.

The present report therefore suggests the following areas which need further R&D investment:

- Research on technical prioritization of the security effort (e.g. Advanced threat intelligence which simplify the process of combining and prioritizing alerts from multiple sources)
- Development of novel approaches for providing organisations the appropriate situational awareness in relation to cyber security threats allowing them to detect and quickly and effectively respond to sophisticated cyber-attacks.
- Development of novel techniques to collect forensic information
- Development of independent evidence-based cyber threat intelligence for fighting cybercrime, understand the trends through the position of sensors able to do sinkholing and collect malware samples
- Research and development on malware /attack prediction using data analytics and machine prediction. That will need the creation of very large updated data sets of labelled malware to train the machine predictor.

[62] Hanan, et al. "A Taxonomy and Survey of Intrusion Detection System Design Techniques, Network Threats and Datasets." arXiv preprint arXiv:1806.03517 (2018) presents a taxonomy of Malicious Traffic for Intrusion Detection Systems and they highlight the difficulty to evaluate them due to a shortage of open–source datasets representing accurately network traffic and their associated threats.

B.5 Privacy threat and the innovation brought by the GDPR

GDPR has had a considerable impact on how corporate manages personal data. Perhaps one of the most significant issues behind this success is the punitive nature of violations by data controllers and processors. It may be argued that fear of punishment of itself is the driver for more care in the design of processing but it might offer an economic incentive to minimize the risk. The GDPR introduces a risk-based approach: the higher the risk (for the rights and freedoms of data subjects), the more rigorous the measures that the controller or the processor needs to take (in order to manage the risk).

GDPR provision for a risk-based approach is horizontal as there are not exemptions or light weight approaches based on the organization size, availability of recourses and capabilities. That means that all individuals, SME and big corporate has this legislative obligation that can be seen as a costly administrative burden. However, GDPR might offer a competitive-advantage for companies: applying effectively the principle of ***privacy-by-design*** can help to build and retain customer trust. GDPR compliance tools can facilitate the privacy assessment and automatic tools give power to consumers to own their data and have a choice of whom they share this with and for what return.

The forthcoming Regulation on Privacy and Electronic Communications is expected to give new impetus to the way privacy is protected in electronic communications.

However further innovation is needed in different fields which can contribute at a more effective data protection and at creating business opportunities.

Technical elements such as **Privacy-Enhancing Technologies (PETs**), e.g. encryption, protocols for anonymous communications, attribute based credentials and private search of databases are the primary areas of research. In addition there are very important ground for *research on how to guarantee data portability in an online platform, prevent online and mobile tracking, consent management in a multi-ownership environment, guarantee in automatic way the subject's right, e.g. right to erasure, access and correction, data deletion especially in a cloud environment*[63].

In a big data and Artificial intelligence environment, the challenges at technical level for research are further more[64] [65]:

- New anonymization privacy models and methods are required when data are continuously and massively collected.
- New encryption techniques are necessary to efficiently allow search and do other computations over the stored data without decrypting the data (e.g. Attribute-Based-Encryption, Encryption search, Privacy preserving computations).
- New Analytics environments where the principle of data minimisation are applied.
- New Model of data protection and privacy requirements where policy definition and enforcement is automatic in a way that one party cannot refuse to honour the policy of another party in the chain of co-controllership and information sharing

[63] For instance, blockchain technology might offers individuals greater sovereignty over their data and allow them to manage and own their data on a shared ledger.
[64] https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design
[65] The Norwegian Data Protection Officer has prepared a report on AI challenges and GDPR: https://www.datatilsynet.no/en/about-privacy/reports-on-specific-subjects/ai-and-privacy/

While the technical research community is continuing improving existing building blocks, interdisciplinary research is needed for connecting privacy to economics, law, ethnography, psychology, medicine, biotechnology, human rights. Obviously, PETs need to be rooted in a data governance strategy for unfolding their full benefit for privacy and data protection. In big corporation, the new obligation can help to think break down organisation barriers and might create a fertile ground for innovation with data.

Annex C: Methodology, policy context and R&D funding scheme

C.1 Methodology used in the report

This study was carried out using a four-step methodology starting from the scope definition, the initial information gathering, the collection of expert opinion and ending with the development of a report.

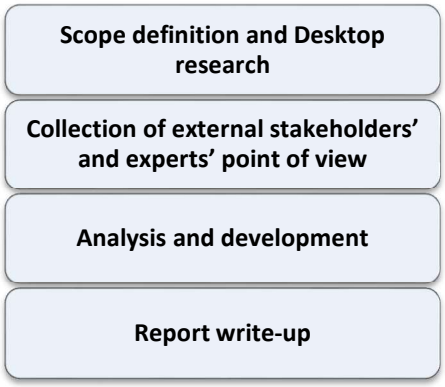

Figure 1 Steps used in the methodology of the report

1. **Scope definition and Desktop research:** The first step was to establish the report's scope and perimeter. In parallel an investigation was carried out to identify existing publications and information on the topics and to conduct brainstorming session with ENISA experts in different fields, so as to gather their input and knowledge in relation to the objectives of this report.
2. **Collection of external stakeholders' and experts' point of view:** A series of interviews were conducted with the selected experts from ENISA permanent stakeholder group and selected member of academia and industry. In the interview, the experts express their opinions on the strategic research priorities in cybersecurity for a safer Europe. It was also asked to give the rationale behind these chooses and their supporting evidences.
3. **Analysis and development:** The results from the desktop research and the interviews were analysed and contrasted to align them with the objectives of the report. A qualitative approach was used to prioritize the identified research topics and to evaluate the supporting evidence. The analysis included triangulation of the data across different stakeholder groups and with validation by ENISA experts. A critical assessment of contributions was made since the stakeholders may vest interest.
4. **Report write-up:** The last step was to synthesise all the findings from the desktop research and the interviews with the experts, shaping this report.

C.2 European Policy Context

The current approach to Critical Information Infrastructure Protection (CIIP) and resilience within the EU has its roots in the Commission communication of 2009, entitled "Protecting Europe from large-scale

cyber-attacks and disruptions: enhancing preparedness, security and resilience"[66]. In 2013, the Commission released the Cybersecurity Strategy of the EU, which laid down a number of fundamental principles that support the EU approach to cybersecurity, including the need of achieving cyber resilience, strong and effective legislation on the cyber domain, the promotion of a Single Market for cyber security products, and fostering R&D investments and innovation.

The Directive on security of network and information systems (NIS Directive)[67] was the first piece of EU-wide legislation on cybersecurity. It provided legal measures to boost the overall level of cybersecurity in the EU forcing all the EU member states in adopting a national strategy on the security of network and information systems, to create a cooperation group in order to support and facilitate strategic cooperation and the exchange of information among Member States, to introduce security measures and incident reporting obligations for operators of essential services and digital service providers.

On 13 September 2017, the Commission adopted a cybersecurity package[68]. The Commission identifies that "*the scale and cross-border nature of the threat make a powerful case for EU action providing incentives and support for Member States to develop and maintain more and better national cybersecurity capabilities, while at the same time building EU-level capacity. This approach is designed [..] to give cybersecurity the priority it needs to build resilience and deliver a better EU response to cyber-attacks".*

The cybersecurity package created a focus on:

- Building EU resilience to cyber-attacks and stepping up the EU's cybersecurity capacity through a reinforced ENISA with the mandate to put in place and implement the EU-wide cybersecurity certification framework
- Stepping up EU's cybersecurity capacity by establishing an European Cybersecurity Research and Competence Centre, acting as a blueprint for how Europe and its Member States can respond quickly and encourage cooperation as a means of developing stronger cyber defence capabilities
- Creating an effective response in criminal law
- Strengthening global stability through international cooperation

The package builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response.

The EU General Data Protection Regulation (GDPR)[69] who came into effect in May 2018 was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens with regard to data privacy. It reshaped how organizations approach data privacy for all the European citizens (independently of where the company is located) and mandate a number of security approaches, such as:

- Privacy by Design and by Default
- New transparency requirements: the condition for consent (where required) must be clear and easily intelligible
- More control over personal data for individuals: right to rectification, to be forgotten, to data portability, to object to automated individual decision making and profiling
- Notification of a data breach that is likely to affect the rights and the freedom of individuals

[66] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149
[67] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
[68] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
[69] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN

- Serious Penalties for infringement

The new regulation on Privacy and Electronic Communications (ePR), which at the time of writing is still in EU trilogue process, aims at aligning Europe's ePrivacy regime more closely with the regime set out in the General Data Protection Regulation (GDPR). Its focus however is on a high level of privacy for all electronic communications, regardless of the technology used, thus addressing the IoT and M2M domains explicitly, and independently whether it contains personal or non-personal data. Moreover, it aims to simplify rules on cookies and to encourage the developers of web browser to ensure clear and open access to users to set their browser settings that are also correctly implemented in the web services they navigate to.

C.3 R&D activities and funding schemes

As a key priority to foster R&D and innovation across Europe, a structure of research facilities and funding schemes is in place to provide expertise and management to research and innovation projects, and to promote synergies between these activities, to benefit both economic growth and the EU citizenship. The beneficiaries of the funding programmes include SMEs, research centres, universities, large companies, the types of funds range from supporting start-ups to various clusters.

Horizon 2020- known also as H2020- has been the biggest running EU research and innovation programme with 75 billion euro of funding available over a seven year period (2014 to 2020). H2020 has been focusing on supporting EU competitiveness through the delivery of ideas and development of technology to help achieve smart, sustainable and inclusive economic growth. The goal is to ensure that Europe produces world-class science and technology, removes barriers to innovation and makes it easier for the public and private sectors to work together in delivering solutions to big challenges facing our society.

The new program for EU research funding called Horizon Europe has a proposed budget of €97 billion for 2021-2027. The commission has also proposed to allocate €13 billion to the European Defence Fund and specifically €4.1billion for funding of collaborative defence research to address emerging and future security threats.

The Commission has also identified a "*new programme dedicated to increasing and maximising the benefits of the digital transformation for all European citizens, public administrations and businesses*"[70] called Digital Europe. Its aim is to provide a spending instrument that is tailored to the operational requirements of capacity building in the areas of high-performance computing, artificial intelligence and cybersecurity. This programme will focus on large-scale digital capacity and infrastructure building, with the objective of wide uptake and deployment across Europe of critical existing or tested innovative digital solutions. €2 billion "*will be invested into safeguarding the EU's digital economy, society and democracies through boosting cyber defence and the EU's cybersecurity industry, financing state-of-the-art cybersecurity equipment and infrastructure as well as supporting the development of the necessary skills and knowledge*"[71] in the period 2021-2027.

It is acknowledged that whilst cyber-security is not the sole beneficiary of such funding it should also be taken into account that any project proposal requiring network connectivity, or which makes use of network resident resources, should take security and privacy concerns into account. This does not suggest that every research project is a health and safety (H&S) project, or that every research project is an ICT/cybersecurity project, but rather, that H&S and ICT/cybersecurity are essential elements of every

[70] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the Digital Europe programme for the period 2021-2027 - COM(2018) 434 final
[71] http://europa.eu/rapid/press-release_IP-18-4043_en.htm

project. This insistence at the genesis of a project on addressing H&S and ICT/cybersecurity is an essential step in moving towards security by default, privacy by design, and safe by design.

ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Catalogue Number TP-05-18-145-EN-N

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-278-3
doi:10.2824/14357