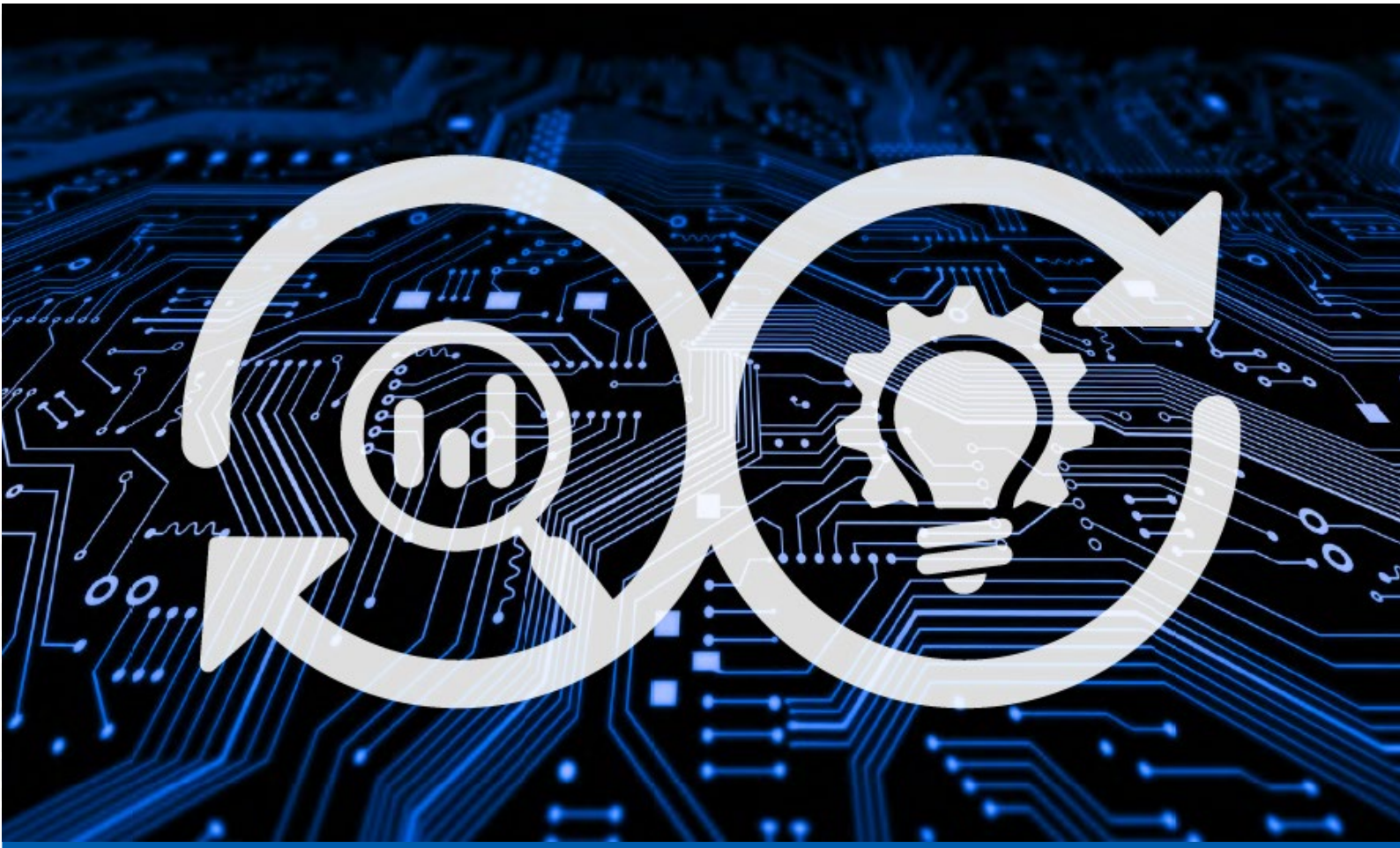
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



RESEARCH AND INNOVATION BRIEF

Annual Report on Cybersecurity Research and Innovation Needs and Priorities

MAY 2022

ABOUT ENISA

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

CONTACT

To contact the authors, please use RIT@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Adrian A. Baumann (ENISA), Corina Pascu (ENISA), Evangelos Rekleitis (ENISA), Marco Barros Lourenço (ENISA), Michal Choraś and Rodica Tirtea (ENISA).

CONTRIBUTORS

Corina Pascu (AI), Jamal Shahin (Policy), Gianluca Misuraca (AI), Luigi Romano (Cryptography), Marco Barros Lourenço (Hyperconnectivity) Panagiotis Rizomilotis (Cryptography), Siguna Mueller (Cyberbiosecurity) and Stavros Ntalampiras (AI).

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The future of the European Union (EU) in the digital age depends on the choices made today and the ability of individuals, businesses and organisations to address challenges and seize opportunities. While Europe and the world recover from a public health crisis, it is vitally important to identify future challenges and opportunities.

This decade, the EU will increase investment in research and innovation (R&I)[1]. One of the focus areas will be the digital transformation of the economy and society that works for people by promoting the European way of life, supporting democracy and values, and protecting its strategic autonomy. In this context, the work of the research community is crucial in creating the knowledge necessary to understand what lies ahead. The EU is a strong player in knowledge and innovation: it accounts for almost 20% of global research and development, publishing and patenting activities[2].

This document offers a forward-looking perspective on some of these challenges and opportunities. It recognises the importance of key structural trends with major implications for the EU's digital ambitions to 2030 and beyond. The multidisciplinary nature of these trends led to the selection of four main themes that form the structure adopted for this report: **hyperconnected world, intelligent systems[3], cybersecurity in life sciences (biotechnology), and computational security**.

Digital hyperconnectivity[4] is a trigger for all other trends and is independent of any particular technology. Ubiquitous connectivity will increase the convergence of industries, products, technologies and services, driven by the accelerated datafication[5] of everything. The growing appetite for data will help make technology smarter as the next frontrunner in the race for greater automation and optimisation in everyday life. In addition, hyperconnectivity, datafication and intelligent automation[6] also contribute to research in the life sciences. This decade, as a result of the pandemic and the efficiency of biotechnology, the EU will increase investment in the research and development of new technologies for the pharmaceutical and health sectors[7].

However, hyperconnectivity and intelligent automation do not come without challenges. While the benefits are well known, the challenges and risks are yet to be fully recognised. Cybersecurity is crucial to ensure that EU citizens, businesses and organisations can enjoy the

[1] https://european-union.europa.eu/priorities-and-actions/actions-topic/research-and-innovation_en, last accessed November 2021.
[2] https://ec.europa.eu/info/publications/science-research-and-innovation-performance-eu-2020_en, last accessed November 2021.
[3] Although they are not the same (intelligent systems could also include AI-based software systems), for simplicity, in the context of this paper we are using the two terms interchangeably.
[4] The term refers to the use of multiple means of communication, such as email, instant messaging, telephone, face-to-face contact and Web 2.0 information services. See for instance Anabel Quan-Haase and Barry Wellman, 'Networks of Distance and Media: A Case Study of a High Tech Firm'. Trust and Communities conference, Bielefeld, Germany, July, 2003; Anabel Quan-Haase and Barry Wellman. 2004. 'Local Virtuality in a High-Tech Networked Organization'. Anaylse & Kritik 26 (special issue 1): 241–57 SEQ CHAPTER \h \r 1; Anabel Quan-Haase and Barry Wellman, 'How Computer-Mediated Hyperconnectivity and Local Virtuality Foster Social Networks of Information and Coordination in a Community of Practice'. International Sunbelt Social Network Conference, Redondo Beach, California, February 2005.; Anabel Quan-Haase and Barry Wellman. 'Hyperconnected Net Work: Computer-Mediated Community in a High-Tech Organization'. Pp. 281–333 in *The Firm as a Collaborative Community: Reconstructing Trust in the Knowledge Economy*, edited by Charles Heckscher and Paul Adler. New York: Oxford University Press, 2006
[5] Datafication (often referred as datafication-of-everything) is about taking a previously invisible process/activity and turning it into data that can be monitored, tracked, analysed and optimised.
[6] Although they are not the same (intelligent automation (IA) uses advanced technologies such as artificial intelligence (AI) to make automated and intelligent decisions), for simplicity in the context of this paper we are using the two terms interchangeably.
[7] https://ec.europa.eu/info/research-and-innovation/research-area/health-research-and-innovation_en, last accessed November 2021.

promised benefits in a reliable and trustworthy environment. This report also aims to identify some of the future needs in protecting data and securing authentication, by creating knowledge in computational security. A summary of the findings across all the thematic areas is presented in Table 1 below.

During 2022, ENISA will promote several initiatives with stakeholders and the community to discuss the challenges and corresponding research needs outlined in this report. These findings will also be used by ENISA to identify funding priorities for the Strategic Agenda and for the work programme of the European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC)[8].

[8] Regulation 2021/887

Table 1: Summary of R&I needs and priorities

	HYPERCONNECTED WORLD	COMPUTATIONAL SECURITY	INTELLIGENT SYSTEMS	CYBERSECURITY IN LIFE SCIENCES (CYBERBIOSECURITY)
NOTEWORTHY CHALLENGES AND GAPS	1. Generating a broader understanding on how hyperconnectivity may influence humanity and the social and political dimensions.	1. Lack of skills in cryptography; 2. Reduced number of market opportunities; 3. The need for standardisation; 4. Efficient support for developers working in the field; 5. Moving of cryptography research from communication fields to being embedded within hardware.	1. Better understating of socio-economic implications with Artificial Intelligence (AI) applied to cybersecurity; 2. Develop technical and regulatory excellence; 3. The need for foresight and development of institutional capacity to deal with AI.	1. Defining the security implications of life science technologies for cybersecurity research; 2. Skills and training for life science researchers; 3. Generating a broader understanding of the implications of cybersecurity for life sciences research.
RELEVANT FUTURE RESEARCH NEEDS AND PRIORITIES	1. The redefinition of the boundaries of human-computer interaction, and the concomitant security risks that are associated with this; 2. Cybersecurity in the context of new generations of mobile communications and data collection or processing methods (evolution from 5G to 6G).	1. Efficient implementation of symmetric key schemes at higher security levels; 2. Planning and preparation for the transition to the Post Quantum era of cryptographic systems; 3. Secure implementations of cryptographic systems are needed that resist side channel attacks; 4. New assumptions and seemingly-impossible results for future cryptographic components that derive from mathematics, physics or hardware limitations; 5. Standards for new quantum resilient safe algorithms and protocols.	1. Linking vertical and horizontal views on AI research (across research teams but also from design to implementation); 2. Design of approaches for monitoring large-scale and possibly interconnected systems; 3. Exploration of biomimetic cybersecurity algorithms; 4. Inclusion of context awareness in machine learning (ML) in order to boost resiliency.	1. The evolving risks and the threat landscape in biotechnology R&I. 2. Risk management framework in the field of public health microbiology (e.g. modern DNA sequencing); 3. Categories of bio vulnerabilities in the context of cyber; 4. Identification of processes and routines throughout the life science fields that require cyber-interfaces and reliance on automation; 5. Pursuit of various activities and initiatives to establish cyberbiosecurity guides and standards.

1. INTRODUCTION

1.1 OBJECTIVES, METHODOLOGY AND TARGET AUDIENCE

The main objective of this document is to identify areas of cybersecurity R&I that are critical to the EU's strategy and ambitions for the digital decade. The report is intended to fulfil ENISA's mandate[9] to advise EU institutions, bodies, offices and agencies, as well as Member States, on new and future research needs and priorities. The information contained in this document will be further developed to help identify funding priorities for future work programmes of the European Cybersecurity Competence Centre and National Coordination Centres.

The four research topics explored in this document were selected primarily through consultation with stakeholders and members of the research community. From a methodological perspective, ENISA would select these topics mainly from trends identified in an annual foresight exercise. However, exceptionally this year and since the ENISA foresight team was taking its first steps, the topics were discussed with stakeholders and agreed internally.

The selected research topics are not exhaustive of all areas where cybersecurity research is needed. They are the culmination of several smaller desktop research activities and consultations with experts carried out during 2021. The work presented here is the consolidated and highly condensed result of several interactions between ENISA members and experts from the research community.

In the first phase, experts were asked to provide input on their research topics, from which a general overview of the cybersecurity research and policy landscape was compiled. This input took the form of written contributions from each expert. In these contributions, the experts outlined key areas for further research in their respective fields. These documents were then consolidated and served as inspiration for a workshop that took place in October 2021. During this workshop, each research topic was discussed and an attempt was made to find a common thread for R&I. This document is based on the contributions and results of this workshop.

This report is targeted at stakeholders involved in the research and innovation area from EU Institutions, Bodies, Agencies, Member States and the wider cybersecurity research community. This report may be especially relevant for:

- members from the eu and national entities involved in funding programmes for research,
- policymakers,
- academics, researchers and R&D actors from the cybersecurity industry.

1.2 EU POLICY CONTEXT

In 2020, the President of the European Commission declared that ‘we are living in Europe’s Digital Decade’10. At the end of 2020, the European Commission and the High Representative presented a Joint Communication on ‘The EU’s Cybersecurity Strategy for the Digital Decade’11. With these guiding documents, the EU is showing that it is proactively reacting to

[9] Article 11 of the Cybersecurity Act, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, last accessed November 2021.
[10] European Commission, ‘COMMISSION STAFF WORKING DOCUMENT Accompanying the Document Proposal for a Decision of the European Parliament and of the Council Establishing the 2030 Policy Programme 'Path to the Digital Decade''.
[11] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN, last accessed November 2021.

the global challenges posed by cyberthreats and presenting the EU as an actor that is aware of the challenges that have to be faced in the forthcoming years.

The EU is fulfilling this role in several ways. Firstly, it is seeking to take a leading role in shaping the global rules for the use of technology and has been doing so for a long time[12]. It seeks, wherever possible, to build global consensus on the tools and mechanisms for developing safe and resilient technologies. The EU works with partners, both state and non-state actors, to build a coherent and trusted framework for cooperation.

Secondly, the EU has developed a discourse of 'open strategic autonomy' that seeks to develop a coherent EU-wide narrative for developing EU-level capabilities to respond to threats in the world. Thirdly, the EU policy toolkit which will be focused on the NIS Directive[13] (currently under revision), the Cybersecurity Act (2019) and the forthcoming Cybersecurity Resilience and Semiconductor Acts[14], is due to be proposed in 2022. The European Council has also called for a Join Cyber Unit[15] to further develop the EU's cybersecurity toolkit.

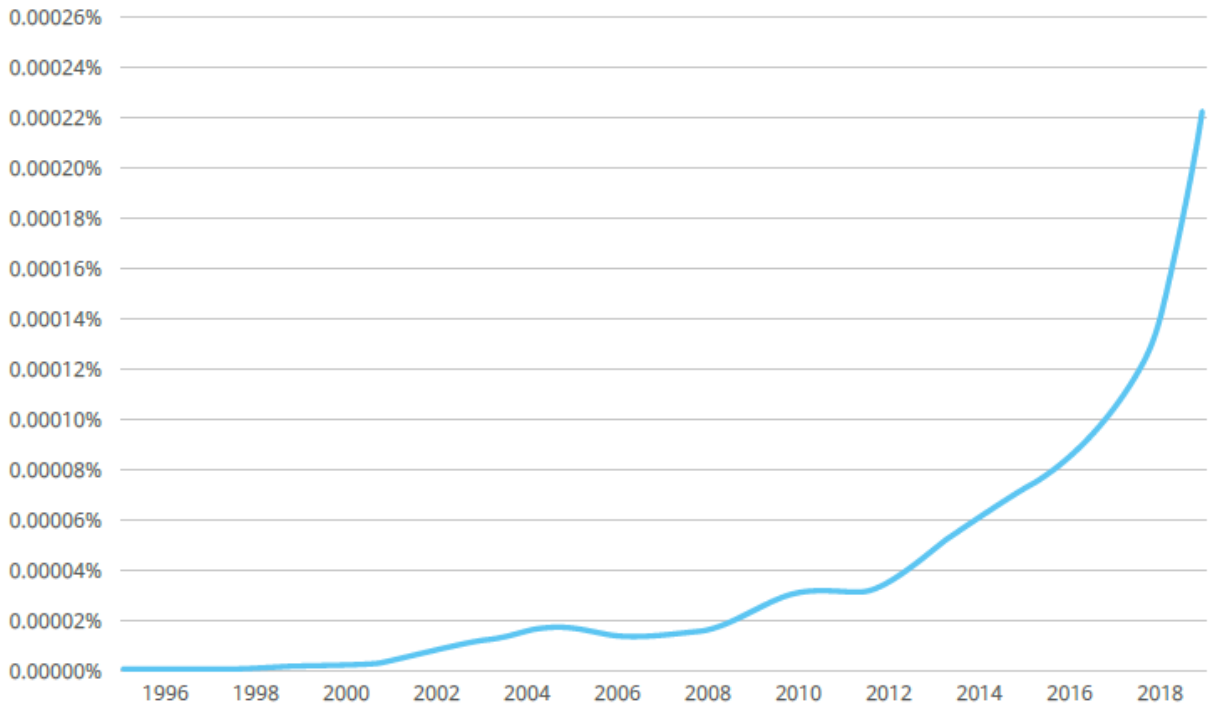
Fourthly, and crucially for the aims of this report, the EU is investing in cybersecurity research and development. The recently established ECCC demonstrates the commitment to this area in a European policy and research context. This includes the development of technological solutions and tools that enable an effective response to current and future risks and cyberthreats. These include new and emerging information and communication technologies and are designed to effectively deploy risk prevention technologies.

Despite the efforts described above, the security of cyberspace will continue to be an ongoing project. Enormous efforts have been made to develop initiatives that support the development of competences in this area. However, the opportunity and need to diversify the cybersecurity R&I agenda is evident. The effort required to continue to meet the standard missions of government agencies is creating a paradigm shift in the sense that cybersecurity risks and threats are not limited to areas outside of government security. Nor do traditional systems of policymaking apply in our hyperconnected world. Therefore, an approach that crosses the different silos of R&I is needed.

[12] European Commission and European External Action Service, 'Cybersecurity Strategy'.
[13] https://www.enisa.europa.eu/topics/nis-directive, last accessed November 2021.
[14] https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act, last accessed November 2021.
[15] https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit, last accessed November 2021.

1.3 THE EU CYBERSECURITY RESEARCH LANDSCAPE

Figure 1: Google Ngram of the term"cybersecurity" 1995-2021



Cybersecurity R&I is a crucial aspect of research in a number of policy domains. The emergence of this field, witnessed by the exponential growth of literature in the field since around 2013 (with the so-called Snowden revelations), indicates that 'cybersecurity' as a term has emerged in contemporary discourse.

The EU and European research funding agencies contribute a large number of resources to research in the field of cybersecurity. Efforts are driven across a number of agencies, and through a number of different instruments. In a research field that encompasses so many policy fields, the pluralism inherent in the funding and organisational structures is to be expected, and even welcomed. But they are not the world's leading funding agencies for published research in the field by far.

Figure 2 identifies the funding provided by different bodies for research in the field of cybersecurity that has been indexed in the Web of Knowledge (i.e. peer reviewed papers in scientific journals). This clearly shows that US research funding agencies dominate the field, with around 43% of published research in this broad field being supported by public funding from the US government. More recent data, considering only the most cited papers from 2021 and 2022 (pre-prints), shows that European researchers are now emerging in this field, with universities like the Technical University of Delft, Aarhus University, and several universities in Spain generating research output that is being cited by the cybersecurity community.

1.4 MAPPING THE LANDSCAPE

Figure 2: Sources of funding for research in the field of cybersecurity (Source: Web of Science)

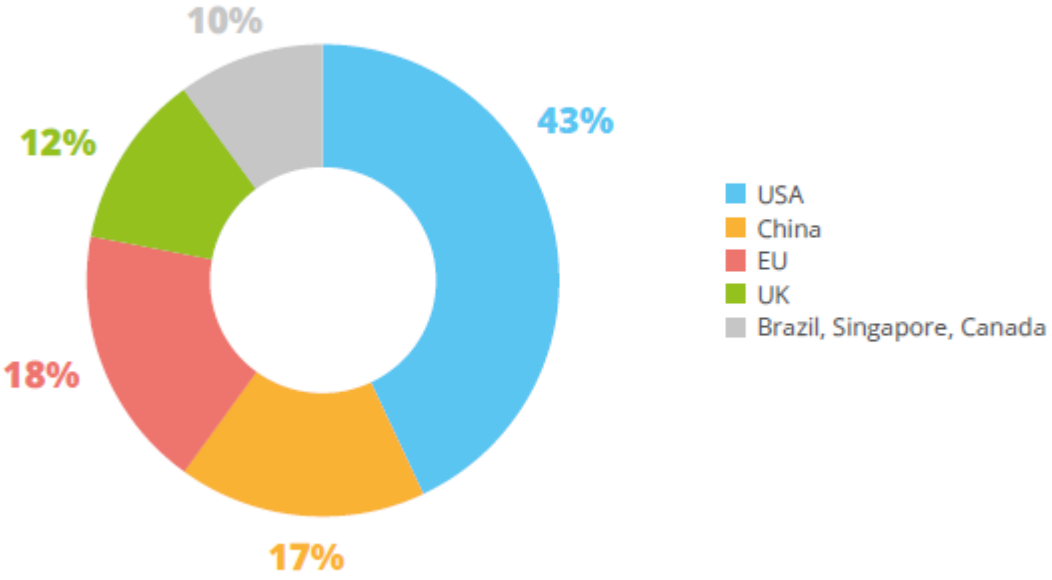


Figure 2 depicts the investment in cybersecurity research from region to region. The European Cybersecurity Atlas[16] highlights the focus of some 750 research centres working on cybersecurity issues in the EU. In terms of education and training, ENISA's own database on cybersecurity in higher education, CYBERHEAD[17], presents well over 100 educational programmes in almost all EU and EFTA Member States. These programmes point to the growing need to develop holistic approaches to dealing with the security threats and risks associated with the increasing importance and emergence of new hyperconnected technologies that are shaping our world. At the same time, many institutes are focusing on the technological expertise needed to be at the forefront of research worldwide. In the European Union, there are a number of projects, initiatives and networks that promote the field of cybersecurity in the EU.

The 2017 Cybersecurity Literacy Survey[18] conducted by DG JRC in collaboration with DG CNECT relied on a survey of over 600 people from European countries to analyse research activities. This identified a large number of research centres and activities engaged in cybersecurity research. This survey was accompanied by the development of a taxonomy of cyberspace to support the categorisation of cyberspace competences. The European Cybersecurity Taxonomy[19] is a useful tool to facilitate the categorisation of the Union's cybersecurity competencies. Cybersecurity is inherently a cross-cutting topic, encompassing many different research areas, academic disciplines and policy fields.

The cybersecurity research landscape is comprised of a wide range of different activities, touching upon technical and social research, as well as policy in this sphere. Integration between these strands of action needs to be addressed holistically in research in order to

[16] https://cybersecurity-atlas.ec.europa.eu/centres-in-europe, last accessed November 2021.
[17] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map/, last accessed November 2021.
[18] https://ec.europa.eu/jrc/en/research-topic/cybersecurity/cybersecurity-competence-survey, last accessed November 2021.
[19] https://publications.jrc.ec.europa.eu/repository/handle/JRC118089, last accessed November 2021.

ensure that outputs have the broadest impact. We need to build bridges between different disciplines and stakeholders in order to ensure acceptance of and engagement with the richness of the research landscape in cybersecurity in the EU.

2. A SECURE AND HUMAN-CENTRED HYPERCONNECTED WORLD

The concept of a hyperconnected world is not defined by technology alone, but by the social, economic and political implications it brings. The notion of hyperconnectivity was originally defined by social scientists[20] to refer to people in networked organisations and societies that are constantly connected through a variety of digital means. Massive connectivity exists in many of our digital environments and represents the interactions between various information systems, data and many devices connected via the Internet. Recent discussions within certain technology platforms and beyond talk about the emergence of a 'metaverse' as an approach to understanding our relationship between immersive, data-driven environments and our daily lives.

In computer networking, hyperconnectivity refers to all things communicating through a network, encompassing person-to-person, person-to-machine and even machine-to-machine communications. This will be possible with the massive increase in network coverage, input/output communication (MIMO) and bandwidth. Current and future generations of mobile communications such as 5G and 6G offer that possibility.

The introduction of 6G wireless communications is still about a decade away. Nonetheless, the first discussions about new technologies and potential applications for this next generation have already begun. Broadly speaking, the current question is whether 6G should be an improvement on 5G in terms of core features, or whether it should go beyond existing coverage into new areas, such as underwater and in space, or even at the molecular level.

Moreover, the increasing digitisation of business and society, with the advent of online shopping, FinTech, cryptocurrencies, social media and many other transformative technologies, are harnessing connectivity everywhere, all the time. With hyperconnectivity, the digital economy and society will increasingly rely on the network to transform the way companies do business and the way we all live.

With an increasingly connected digital economy and society, cybersecurity will also become increasingly important. The frequency and sophistication of cyberthreats will continue to challenge many individuals and organisations. Hyperconnectivity has increased the vulnerability of connected individuals, institutions and nations. It represents a new challenge to humanity in how it defines scale with hundreds of millions of connected individuals.

Multidisciplinary and future-oriented research will be required to facilitate the transition to this inevitable hyperconnected world.

Foresight has an important role to play in providing early insights into the technological and social changes that will shape this future, and in taking actions that will help define a desirable and globally beneficial hyperconnected future. Cybersecurity research will lay the foundations for building a trustworthy and reliable hyperconnected world.

[20] https://en.wikipedia.org/wiki/Hyperconnectivity, last accessed November 2021.

2.1 THE DATAFICATION OF EVERYTHING

The process of digitalisation - often referred to as digital transformation - is profoundly changing our economy and society. It will continue affecting individuals, businesses and organisations throughout this decade. The wake-up call for all the future research challenges and opportunities described in this document occurs at a time of growing political awareness of digital dependency in the economy and society.

The most noteworthy pattern in this digital transformation is the data-driven world we live in, a world that will be always on, always tracking, always monitoring, always listening and always watching – because it will be always learning. What we perceive to be randomness will be bounded into patterns of normality by sophisticated algorithms that will take our data to deliver the future in new and personalised ways. Data are often considered to be an asset but we see that, in contemporary society, data are emerging as a space of contestation that goes beyond the 'data is the new oil' debate, pushing us towards conceiving of data as the 'new air'[21].

An important discussion is how hyperconnectivity will the drive the datafication-of-everything with the expansion of use cases, data collectors and data processors. The list below highlights some of the challenges in the coming decades.

- **The appetite for personal data:** with hyperconnectivity, the opportunities for data collection increase significantly. Among the most sensitive are personal identifiable information and geolocation which, if breached or stolen, may cause severe impacts on citizens' privacy, the economy and society.
- **A growing interest in surveillance of citizens:** there is a general concern about the increasing interest of private (corporate) and state-sponsored agents in the surveillance of citizens and organisations. With hyperconnectivity and the growing appetite for data, eavesdropping could become a major threat, compromising the privacy and protection of users' data.
- **The use of technology to expand the risks affecting the fundamental rights of EU citizens:** the rapid increase in the use of artificial intelligence to explore data collected and maintained by digital platforms may pose risks to the fundamental rights of citizens. It may lead to infringements of privacy, data protection and equal treatment, particularly when it comes to the growing use of Big Data through the rapid advances in machine learning.

Questions pointing to research needs and priorities in the context of an hyperconnected world:

- What are the consequences for humanity in a hyperconnected world?
- How will hyperconnectivity affect the security of cyberspace?
- What are the conceptual frameworks required before transitioning to a hyperconnected world?

[21] 'Answering Europe's Call: Storing and Processing EU Data in the EU'. 2021. EU Policy Blog. 6 May 2021. https://blogs.microsoft.com/eupolicy/2021/05/06/eu-data-boundary/.
Bello-Orgaz, Gema, Jason J. Jung, and David Camacho. 2016. 'Social Big Data: Recent Achievements and New Challenges'. *Information Fusion* 28: 45–59. https://doi.org/10.1016/j.inffus.2015.08.005.
Organisation for Economic Cooperation and Development. 2013. 'Exploring Data-Driven Innovation as a New Source of Growth' 222 (June). https://doi.org/10.1787/5k47zw3fcp43-en.
Roxana Radu and Jean-Marie Chenou. 2015. 'Data Control and Digital Regulatory Space(s): Towards a New European Approach'. *Internet Policy Review* 4 (Issue 2). https://doi.org/10.14763/2015.2.370.
'The Debate - Battle for Our Data: European Leaders Call for Digital Sovereignty'. 2019. France 24. 15 November 2019. https://www.france24.com/en/business/20191114-battle-for-our-data-european-leaders-call-for-digital-sovereignty-1.
Roxana Radu and Jean-Marie Chenou. 2015. 'Data Control and Digital Regulatory Space(s): Towards a New European Approach'. *Internet Policy Review* 4 (Issue 2). https://doi.org/10.14763/2015.2.370.
'The Debate - Battle for Our Data: European Leaders Call for Digital Sovereignty'. 2019. France 24. 15 November 2019. https://www.france24.com/en/business/20191114-battle-for-our-data-european-leaders-call-for-digital-sovereignty-1.

- What are the policies and technological possibilities to help in mitigating economic and social consequences with unquestionable implications for the security of cyberspace due to an unequal rollout of hyperconnected technologies?

Possible research focus:

- The redefinition of boundaries of human-computer interaction, and the concomitant cyber risks that are associated with this;
- Cybersecurity in the context of new generations of mobile communications and data collection or processing methods (evolution from 5G to 6G).

3. THE AGE OF INTELLIGENT SYSTEMS

Artificial intelligence (AI) is one of the most transformative forces of our time and key to the EU's ambitions and strategy for the digital decade. The importance and expansion of its influence is referenced in various parts of this document. AI will continue to transform the way businesses and organisations work, manage data and interact with users through a blend of advanced technologies, such as machine learning (ML), natural language processing (NLP) and cognitive computing. There are still areas where more research and development is needed to promote trustworthy and reliable AI that supports the rights of EU citizens and respects EU values.

In order to map the domain, defined by a complex and open-ended relation with cybersecurity, we made a clear distinction between 'AI used to harm' and 'AI used to protect'.

Potential offenders are highly innovative and may develop algorithms, solutions or procedures that eventually become new standards in the cybercrime arena. Moreover, even a 'secure and trustworthy' system may later be hijacked by a different actor with malicious intent.

Participants at the intersection of cybersecurity and AI often find themselves caught between the creation of knowledge and market initiatives, such as academic research being mingled with R&D in a more blurred way than usual, peer-reviewed literature coexisting with major players involved in AI and cybersecurity issues on their own terms, major advisory agencies and consultants (often former or active C-level executives), all contributing to the collective progress of this research field.

AI in cybersecurity applications can be classified in the following categories: AI-powered defence mechanisms, cyberthreats exploiting AI, attacks against AI-based security mechanisms (mechanisms using AI to promptly detect, identify and accommodate the consequences of cyberattacks) and defences for AI-based protection mechanisms (to secure and protect AI-based mechanisms from malicious attempts).

To lay the groundwork for this exploration, a case analysis has been conducted on two focus areas that are of particular importance as they demonstrate a strong interdependence between AI and cybersecurity issues.

3.1 AI TO IMPROVE CYBERSECURITY DEFENCES

A first research focus should be on using AI to improve cybersecurity defences. In this regard, research should focus on common cybersecurity tasks, such as the prediction and prevention of attacks, detection of threats and intrusion, response, planning and other areas, and in what ways AI and ML tasks, techniques and methods can be applied to address them.

AI tools offer high performance at low cost and in real time. Areas of cybersecurity for which AI/ML offer promising solutions include applications that require the processing of large amounts of data. In particular AI/ML can automate threat detection (both known and emerging threats), using pattern recognition and anomaly detection methods. AI approaches can be used for spam, intrusion, and malware detection and classification. Support Vector Machine (SVM) is one of the most prominent algorithms for anomaly detection and pattern recognition (malware,

spam, and intrusion detection[22]). Other algorithms have also been used for spam and intrusion detection[23]. Ensemble methods, which combine multiple ML tools, have been used to detect malware[24] and intrusions[25].

AI-based defences that use supervised and unsupervised approaches, as well as bio-inspired algorithms[26] and auto-encoders, may prevent attacks such as Distributed Denial of Service (DDoS), ransomware, zero-day attacks[27].

In addition, AI-based systems may also predict the most vulnerable points of attack, enabling operators to plan and allocate resources accordingly. In general, manual responses cannot keep up with the increasing number of automated threats, and this is exactly where AI-based solutions show great potential. However, the efficiency of such tools depends on the availability and quality of data. In most cases, not all the necessary information is available to feed the algorithms in advance, e.g. attack data within the proper context.

3.2 AI TO ORCHESTRATE CYBERATTACKS

A second research focus should be on protecting AI against its possible use to orchestrate cyberattacks, as well as against attacks on AI-based mechanisms and tools[28]. Attackers exploit AI to increase the attack efficiency, discover vulnerable points of entry, identify previously unknown weak points, automate the attack mechanism and extend its impact. Examples of such attacks include malicious personalised tweets or Deep-Fakes[29] using Generative Adversarial Networks[30] (GAN). AI can also be used to improve the efficiency of malware by using, for example, reinforcement learning techniques.

Based on current assumptions, such as the availability of a vast amount of high-quality data and stationarity over time, R&I efforts should focus on small data, end-to-end solutions and on minimising the need for domain expertise. R&I should regularly assess the validity of the developed model(s), be able to incorporate non-stationarities (i.e. changes in the time variance of system states), carefully examine the available dataset to detect and eliminate existing biases and imbalances, as well as develop standardised datasets, to reliably reproduce and compare existing AI-based solutions.

[22] Baigaltugs Sanjaa and Erdenebat Chuluun. Malware detection using linear svm. In Ifost, volume 2, pages 136–138, 2013. doi:10.1109/IFOST.2013.6616872; Min Yang, Xingshu Chen, Yonggang Luo, and Hang Zhang. An android malware detection model based on DT-SVM. Security and Communication Networks, 2020:1–11, December 2020. doi:10.1155/2020/8841233; Kinan Ghanem, Francisco J. Aparicio-Navarro, Konstantinos G. Kyriakopoulos, Sangarapillai Lambotharan, and Jonathon A. Chambers. Support vector machine for network intrusion and cyberattack detection. In 2017 Sensor Signal Processing for Defence Conference (SSPD), pages 1–5, 2017. doi:10.1109/SSPD.2017.8233268.

[23] *k*-means clustering and Hidden Markov Models (HMM) are useful for intrusion detection, while NB can be used for classification tasks in cybersecurity. See for instance Ye Du, Huiqiang Wang, and Yonggang Pang. HMMs for anomaly intrusion detection. In Computational and Information Science, pages 692–697. Springer Berlin Heidelberg, 2004. doi:10.1007/978-3-540-30497-5_108.

[24] Sanjay Kumar, Ari Viinikainen, and Timo Hamalainen. Evaluation of ensemble machine learning methods in mobile threat detection. In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), pages 261–268, 2017. doi:10.23919/ICITST.2017.8356396.

[25] See for instance Abdulla Amin Aburomman and Mamun Bin Ibne Reaz. A novel SVM-kNN-PSO ensemble method for intrusion detection system. Applied Soft Computing, 38:360–372, January 2016. doi:10.1016/j.asoc.2015.10.011..

[26] Anas Arram, Hisham Mousa, and Anzida Zainal. Spam detection using hybrid artificial neural network and genetic algorithm. In 2013 13th International Conference on Intelligent Systems Design and Applications, pages 336–340, 2013. doi:10.1109/ISDA.2013.6920760; Hossein Gharaee and Hamid Hosseinvand. A new feature selection ids based on genetic algorithm and svm. In 2016 8th International Symposium on Telecommunications (IST), pages 139–144, 2016, doi:10.1109/ISTEL.2016.7881798.

[27] https://en.wikipedia.org/wiki/Zero-day_(computing), last accessed November 2021.

[28] ENISA AI threat landscape (https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges/@@download/fullReport) and ENISA study on Securing ML algorithms (forthcoming)

[29] https://pt.wikipedia.org/wiki/Deepfake, last accessed November 2021.

[30] https://towardsdatascience.com/understanding-generative-adversarial-networks-gans-cd6e4651a29?gi=329f3a60610f, last accessed November 2021.

There are several datasets[31] facilitating diverse application of AI technologies in the cybersecurity domain. These cover a wide spectrum of cybersecurity applications and represent real-world conditions to some extent.

AI tools and mechanisms are the attack points themselves, i.e. through their own vulnerabilities in open-source software libraries, data poisoning (attacks that poison training data), adversarial attacks based on GAN, as well as reverse-engineering of the trained model[32].

Finally, there are a number of AI-specific requirements that are particularly relevant when addressing cybersecurity applications. AI-based tools and methods should be verifiable, reliable, explainable, robust against adversarial attacks, auditable and unbiased. At the same time, to effectively address these requirements, AI should integrate multidisciplinary perspectives such as socio-technical, economic, regulatory, cultural and cognitive points of view.

Importantly, the work produced for this document identified existing gaps and provided directions for future research that will ensure intelligent and effective deployment of AI as a tool for increased cybersecurity.

Questions pointing to research needs and priorities in the context of intelligent systems:

- How to use AI to design intelligent defence solutions able to detect and identify attacks against systems, networks and programs?
- How to understand the use of AI in orchestrating cyberattacks?
- What about the validation value chain that is particular to science and scientists? How can the work of researchers be validated through different forms of publication, such as blogs, independent websites, relays of big companies' presentations, in other words, a huge debating grey literature, discussing a truly fast-changing reality?

Possible research focus:

- Development of a standardised performance evaluation framework;
- Design of approaches for the monitoring of large-scale and possibly interconnected systems;
- Exploration of biomimetic cybersecurity algorithms;
- Incorporation of the security-by-design concept (assess the security of the protection mechanisms against a standardised framework considering diverse malicious attempts);
- Preservation of the privacy and confidentiality of the information flow;
- Inclusion of context awareness in ML in order to boost resiliency.

[31] a) KDD Cup 99 and DEFCON serving research on intrusion detection and modelling, b) CTU-13 covering real botnet traffic, c) Spambase and SMS Spam which are collections of SMSs and e-mails facilitating spam classification purposes, d) CICIDS2017 providing full-packet traffic data recorded at the Canadian Institute for Cybersecurity, e) CICAndMal2017 dataset which encompasses trustworthy and malware applications and f) the Android Validation dataset which captures accurately the relationships existing between various applications from a Cybersecurity point of view.
[32] For a more detailed list of threats, see ENISA AI threat landscape available at https://www.enisa.europa.eu/publications/artificial-intelligence-cybersecurity-challenges/@@download/fullReport

4. COMPUTATIONAL SECURITY

Computational security is a large and emerging area of research that is heavily influenced by our increasing reliance on communication technologies. The security of the processing systems that stitch together our increasingly hyperconnected world is dependent on processors and the way in which they process data.

Computational security encompasses issues of hardware security and cryptography. Hardware security for protecting data and applications even from attacks by privileged users, such as cloud providers or system administrators, is becoming increasingly important, as evidenced by famous security breaches, such as that of Verkada[33] in March 2021. In this breach, access was given to over 150,000 security camera feeds in various public and private locations.

One of the most important debates in cryptography research is the extent to which it could be seriously affected by the potential of quantum information processing, since the security of most cryptographic primitives in use today relies on the hardness of computational problems that can be easily broken by adversaries who have access to a quantum computer. Some of the identified challenges include the following.

- **The design and standardisation of new public key systems:** in the Post Quantum era, all popular public key solutions will be broken and new systems must be designed based on problems that are conjectured to remain hard in the quantum computational model. These mathematical problems must be studied well and extensively evaluated against quantum algorithms.
- **The design and standardisation of new symmetric key systems:** while public-key schemes will be broken, it seems that symmetric key cryptography is significantly less affected. The impact of Grover's quantum algorithm can be compensated by just doubling the key size in order to achieve the desired level of security. However, it doesn't mean that it will be just another day in crypto paradise. Doubling the key size has a significant impact on the performance of the cryptographic module and in some cases using them will be prohibitive.

4.1 SUSTAINABLE CRYPTOGRAPHY

The catastrophic impact that quantum computing is expected to have on cryptography and cybersecurity in general proves that the pursuit of security is a marathon race that requires constant effort and awareness.

Research for new cryptographic primitives, algorithms and protocols must be a never-ending task.

Some of the identified challenges include:

- **Quantum Cryptography:** this is a significant paradigm-shift because security in the area of cryptographics is based on physics. More precisely, quantum cryptography covers a vast range of cryptographic algorithms that are based on theories of quantum mechanics. Quantum key distribution is the most well-known application of quantum

[33] https://www.bloomberg.com/news/articles/2021-03-09/hackers-expose-tesla-jails-in-breach-of-150-000-security-cams, last accessed November 2021

cryptography as it has reached production phase. However, it is still hard to scale and the security of the scheme, though unconditionally secure in theory, is subject to several assumptions in practice.

- **New mathematical problems:** since the introduction of the public key paradigm in the middle 1970s, several mathematical problems have been proposed to be used in public key schemes. However, the public key technologies have been dominated by two main hard mathematical problems, the factorisation of integers and variants (field, elliptic curve) of the discrete logarithm problem. The expected implementation of quantum computing has forced the cryptographic community to invest its research efforts in new problems or to revisit old ones that did not gain sufficient attention over the last four decades.

4.2 PRIVACY PRESERVING BLOCKCHAIN TECHNOLOGIES

Blockchain technology offers the possibility of implementing a public digital ledger of transactions. The main security feature of this structure is that it allows append-only operations with cryptographic guarantee, i.e. the security of a cryptographic hash function protects the integrity of the structure. The technology has been widely adopted in many applications and offers users the ability to deal directly with each other without an intermediary.

Cryptocurrencies and finance in general are the sectors that have recognised the importance of such a technology and the areas in which the technology has proven its power. However, several improvements are in order and user's privacy has been identified as one of the most important among them. While the main goal of blockchain-based cryptocurrencies is transparency, in many situations individuals or companies want to protect the privacy of the information surrounding a transaction. After all, finances and transactions are generally held to be private information. Some of the challenges identified include the following.

- **Verifiable computation:** the scope of verifiable computation (VC) is to verify the output of an outsourced operation. The client wants to outsource the computation of some function to an untrusted machine and be assured that the computed outputs are correct. The client aims for efficiency and integrity. One of the main application areas is cloud computing, as cloud data processing results may be incorrect and cannot always be trusted.
- **Standardisation of ZKP schemes:** every year several new schemes appear improving previous works or introducing new properties. The ZKP schemes come into various flavours and each one is tailored to a specific use case. For the moment, it does not seem that there is one scheme to rule them all. It is clear from the plethora and variety of schemes that a clarification of the field is required. Guidelines are needed to facilitate the selection of the optimal ZKP scheme for each use case[34].

4.3 ENHANCED PRIVACY - USER CONTROLLED ENCRYPTION

There is an ongoing debate regarding encryption and its effect on the ability of law enforcement to access data. While there is no silver bullet that can solve the problem, the discussion regarding encryption policy or, even better, user-controlled encryption remains alive. EU Member States are asked to find a balance between 'security through encryption and despite encryption'. Legally, EU-wide legislation on strong encryption is identified as a possible measure to ensure the security of human rights. Some of the challenges identified are shown below.

- **Privacy preserving market:** EU Member States must find a balance between privacy and the prevention of criminal activity. They are invited to protect both privacy and the

[34] In 2018, actors from the industry and academia jointly formed the ZKProof standardisation effort. The main goal is to 'standardise the use of cryptographic zero-knowledge proofs'. To this day, it is still an on-going effort.

legal rights of EU citizens and EU market clients. The challenge is both technical and regulative in nature. From the technical point of view, several issues must be resolved, i.e. key management and data access control.

4.4 HARDWARE-ASSISTED SECURITY

Even the most secure algorithm is vulnerable if the computing environment where it is executed is not adequately protected. Effective protection mechanisms must be provided throughout the data cycle, i.e. data must be handled securely at all times and in all locations. This results in stringent requirements for confidentiality and integrity, not only when data is 'in transfer' (e.g. when it is exchanged over a network connection) or 'at rest' (e.g. when it is stored on a disk) but also when it is 'in use' (e.g. it is loaded in RAM or in the CPU for executing a computation).

While protection of data in transfer and at rest is relatively easy to achieve, protection of data in use is still - to a large extent - an open issue.

Hardware-assisted security does not mean hardware security. The term hardware security refers to the protection of physical systems from harm, not to the protection of software which runs on the hardware of a computer system. In hardware-assisted security instead, features of the hardware are used to support software security, typically by means of Trusted Computing (TC) features. A key concept of TC is the chain of trust. A chain of trust is established by validating each component of hardware and software from the end entity up to the root of trust. Some generally agreed upon features of TC include trusted boot, sealed storage, curtained memory, attestation, integrity measurement and secure I/O.

Trusted Execution Environment technologies (TEE) provide an application-layer designed for security aware developers, who partition their application into security critical parts (which are executed in processor-hardened enclaves and/or protected memory areas) and non-critical parts (which are executed normally). TEE has received great attention from developers, software vendors and original equipment manufacturers (OEM) and software ecosystem partners. What makes TEE attractive is its capability to provide protection for the integrity and confidentiality of data-in-use, even against super-privileged software and users. Notably, not only is this effective against malware but it also removes the need for trusting third parties, such as the system administrator or the cloud provider.

4.5 PRIVACY PRESERVING AI

AI inference systems are expected to become an integral part of the vast majority of modern systems deployed and operating in the cloud, on the core network and on devices. Both the training and prediction phases of AI models pose new risks to client privacy. Many AI models are optimised by embedding their clients' preferences into the training data, while even the raw training data may contain private information (gender, location, religion, political views). In the inference phase, the client's inputs are used unprotected, while in several cases even the AI model and its coefficients (e.g. weights and biases, architecture) require IP protection. It is no surprise that the protection of privacy has been identified by the industry as one of the key factors for the wide adoption of ML inference technology[35]. The list below identifies the main areas in the research of privacy in AI.

1. **Practical fully homomorphic encryption:** homomorphic encryption (HE) is a form of encryption that permits users to perform computations on encrypted data without first decrypting it. The problem has been studied for the last four decades and an FHE solution was first proposed in 2009. Since then, more and more promising schemes have been proposed.
2. **Multi-party computation:** in secure multi-party computation (MPC) cryptography, multiple participants can correctly execute a computation together without revealing their respective

[35] https://arxiv.org/abs/2008.04449, last accessed November 2021.

inputs. The field was introduced in the early 1980s, and since then a lot of theoretical work has been done.

3. **Standardisation:** an open consortium of industry, government and academia to standardise homomorphic encryption exists[36]. The standardisation effort aims to facilitate the adaption of the HE technology and to present the security properties of the standardised scheme(s) in a clear and understandable form. All the schemes that have been proposed for standardisation so far belong in the second category. Besides the fact that the field of MPC protocols is more mature than HE, the standardisation effort is very limited.
4. **Hardware implementation:** in the last decade, the performance of HE schemes has impressively improved up to five orders of magnitude thanks to advances in the theory and to more efficient implementations. Despite the impressive improvements that took place during the last decade, both MPC protocols and HE schemes impose significant computational overhead that cannot be ignored. Hardware implementation of the complicated operations and large operands seems to be the solution for efficient MPC and HE modules.
5. **Compilers:** realising HE or MPC based computations is complex for the non-expert, there has been huge progress in the last decade and several compilers have been introduced that produce efficient protocols. In order to facilitate the work of developers, HE compilers have been proposed to offer high-level abstraction.

Possible research focus:

- Quantum resilient or safe and efficient public key schemes;
- Efficient implementations of symmetric key schemes that possess a higher level of security;
- Standards for new quantum resilient/safe algorithms and protocols;
- Planning and preparation for the transition to the Post Quantum era of cryptographic systems;
- Hardware assisted security, more specifically on CPU technology, transparent application support and the combined use of Trusted Execution Environment technologies and Homomorphic Encryption (HE);
- Compilers that produce efficient and secure multi-party computation (MPC) and HE protected code;
- Standardisation of HE schemes and MPC protocols;
- Hardware acceleration of MPC protocols and HE schemes;
- New assumptions and impossibility results that derive from mathematics, physics or hardware limitations, as a basis for future cryptography;
- Secure implementations of cryptographic systems that resist side channel attacks.

[36] www.homomorphicencryption.org, accessed November 2021.

5. CYBERSECURITY IN LIFE SCIENCES (BIOTECHNOLOGY)

Governments and security experts have identified the life sciences sector as particularly vulnerable to cybercrime. The importance of reviewing cybersecurity related issues in life sciences, and in biotechnology in particular, is no different from many other critical infrastructures (e.g. the chemical industry, nuclear physics, etc.). However, the lack of awareness and of specific cybersecurity controls to address the risks and the long term implications that may have implications for life itself lends a sense of urgency to the need to review this topic from a research perspective.

When it comes to cybersecurity, innovation is quickly becoming a double-edged sword for life sciences customers. Recently, a cybersecurity researcher uncovered[37] the threat posed by two Advance Persistent Threat (APT) groups that gained access to a leading pharmaceutical company's environment for up to three years before being discovered. They stole IP and business data from the victim, information on bio culture products, cost reports and other details related to the company's overseas operations. There is nothing more important to a pharmaceutical company than the formula for one of its new drugs.

5.1 THE URGENCY OF CYBERBIOSECURITY

Most broadly, cyberbiosecurity aims to identify and mitigate security risks fostered by the digitisation of biology and the automation of biotechnology. What exactly is meant by this needs to be explained further. Cyberbiosecurity was first defined[38] as understanding the vulnerabilities to unwanted surveillance, intrusions, and malicious and harmful activities which can occur within or at the interfaces of commingled life and medical sciences, cyber-physical dimension, supply chain and infrastructure systems, and developing and instituting measures to prevent, protect against, mitigate, investigate and attribute such threats as they pertain to security, competitiveness and resilience. We have reached new milestones in our understanding of how biological systems work and have also found ways to manipulate these systems to our advantage or needs in meaningful ways. Biotech tools such as gene editing can intentionally introduce heritable genetic traits into wild populations, offering a new way to escape certain vector-borne diseases.

Several areas in Biotech are of particular concern for cyberbiosecurity. Gene editing tools such as CRISPR-CAS9[39] (Clustered Regularly Interspaced Short Palindromic Repeats associated protein-9 nuclease) for example, are used worldwide for rapid and precise gene editing. Researchers like to use computers to analyse Deoxyribonucleic acid (DNA)[40], operate lab machines and store genetic information. In healthcare, the digitisation of biology and metabolic engineering is accelerating the development of new vaccines, drugs and painkillers. Agriculture is becoming smarter and digital, with farmers relying on data-driven decisions gained from

[37] https://www.darkreading.com/threat-intelligence/state-sponsored-cyberattacks-target-medical-research, last accessed November 2021.
[38] Randall S Murch, William K So, Wallace G Buchholz, Sanjay Raman, and Jean Peccoud. Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. Frontiers in bioengineering and biotechnology, 6:39, 2018.
[39] https://www.nature.com/articles/nprot.2013.143, last accessed November 2021.
[40] https://en.wikipedia.org/wiki/DNA, last accessed November 2021.

sensors implanted in the soil, satellites controlling tractor movements and other new practices. But these new possibilities also bring a whole new category of vulnerabilities and risks.

In the last five years, the technological barriers to acquiring and using biological weapons have been significantly lowered. The security implications of biotechnological advances extend beyond bioweapons. For example, developments in metabolic pathway engineering also offer ways to produce illicit drugs such as heroin. Scientists have already figured out how to make the active ingredients in other narcotics, such as cannabis and precursors to Lysergic acid diethylamide (LSD). What if a terrorist group or despotic regime tries to spread modified organisms aimed at attacking troops, scaring civilians, or throwing food production into disarray?

Recently, researchers outlined in a study[41] the risks of using gene sequencing technologies to corrupt databases by altering sequences or annotations. In this article, computer scientists designed a DNA sample that, when sequenced, resulted in a file that allowed the hacker to remotely control the sequencing computer and make changes to DNA sequences. These changes could delay a research program, resulting in capital and labour losses, or could be used in a terrorist act to produce toxins or infectious agents in an uncontrolled manner. To mitigate these risks, the culture of the life sciences community must change from blind trust to a highly aware and educated community. This also requires intricate relationships between the computational and experimental dimensions of product development workflows.

The multiplicity of pathogens and toxins with their potential to be used as bioweapons (BW) agents[42] could be due to several factors. These include infectivity (the number of organisms required to cause disease), virulence (the severity of the disease caused), transmissibility (the ease of spread from person to person) and incubation time (the time from exposure to a biological agent to a disease outbreak). All these attributes are manageable by modern biotechnology, and information about such experimental series is key to any covert attack that uses them as bioweapons.

Similarly, in cyberspace, there are a variety of malicious codes. These include viruses (programs that replicate in target machines); worms (self-sustaining programs); and carriers such as a Trojan horse that perform a legitimate function combined with malicious activity. Additionally, botnets or networks of computers infected with malicious code can be coordinated to perform distributed denial-of-service attacks.

For biological weapons, means of delivery range from advanced aerial spraying to contamination of food or water, while malicious code can be transmitted in cyberspace through user portals, email, web browsers, chat clients, web-enabled applications, and updates. The cyberthreat has expanded dramatically in recent years through a series of damaging incidents.

Bioinformatics software is still not hardened against cyberattacks. There is a need to promote the widespread adoption of standard software best practices for security, such as input sanitisation, use of memory-safe languages or bounds checking on buffers and regular security audits. Patching remains a challenge because analytics software often resides in individually managed repositories and is not regularly updated.

[41] Randall S Murch, William K So, Wallace G Buchholz, Sanjay Raman, and Jean Peccoud. Cyberbiosecurity: An emerging new discipline to help safeguard the bioeconomy. Frontiers in bioengineering and biotechnology, 6:39, 2018.
[42] Biological weapons are microorganisms like virus, bacteria, fungi or other toxins that are produced and released deliberately to cause disease and death in humans, animals or plants, WHO (https://www.who.int/health-topics/biological-weapons#tab=tab_1).

5.2 A MAPPING OF KNOWN CYBERBIOSECURITY CHALLENGES AND EXISTING GAPS

Exploitable technology and a range of (still under-assessed) attack vectors include (a) databases (including genomic, list of dangerous genes or organisms), design-build-test libraries and rules, simulations, test data, sample records, (b) individual personal computers, lab equipment and processes, mission-critical devices and hardware (e.g. assemblers, synthesisers, sensors), (c) mission-critical software (e.g. workflow controls, process controls), (d) local and remote networks, and (e) raw materials, supplies and actual biomatter[43].

Notably, many of the devices used throughout the biotech sector are portable, and most are connected to the internet. Challenges arise not only at the level of application but even during research as well as at the design, build and test level.

Thanks to the inherent vast variation in nature, biological processes are difficult to grasp. Computerised or automated results (e.g. molecular diagnostic tests) are next to impossible to verify with the naked eye. Yet more traditional tests and processes throughout the life-science fields have been replaced by computer technology. Practical skill and hands-on experience are no longer the focus. Furthermore, more credence is often given to a computerised output (e.g. in diagnostics) than to clinical observations. While biological or medical decision making was traditionally based on consensus and expert opinion, computer simulations or automated processes could easily be distorted and manufactured without anyone being able to tell the difference. Examples of known attacks show how easy it is to compromise sensors and protocols and to, for example, achieve misdiagnosis of skin cancer, referable diabetic retinopathy and pneumonia by automated processes.

5.3 A LARGELY UNRECOGNISED BIOTECH THREAT LANDSCAPE

The most studied cyberbiosecurity danger probably involves pathogenic databases. Several studies have shown extensive cybersecurity vulnerabilities which are exacerbated by the human interface (errors and social engineering attacks). The danger is not only that bad actors could ‘create’ dangerous microorganisms from unsecured digital information. Just as concerning is the fact that erroneous or manipulated data can compromise international research activities and public health responses during outbreaks of disease (e.g. when trying to understand, model and detect new pathogens).

More generally, cyberbiosecurity vulnerabilities can lead to disruption of CIA[44] at all levels (including biosynthetic pathways and processes, software, hardware, mission-critical devises etc.) and scales (from biological processes at the molecular level to genetically-modified plants, microbes or animals). Notably, as biotech is only able to work with small biological snippets (e.g. ‘marker genes’ or ‘DNA signatures’, which are believed to represent the whole organism), establishing genuine ‘integrity’ of biological entities or processes (e.g. genuine GMOs[45] versus illicit or manipulated ones) is in many cases technically impossible.

Impairment of the confidentiality of biologic data can, for example, leak pathogenic data. Illicit access to, for example, synthetic processes or critical biomatter can result in the hazardous distribution of biological agents with a potential global impact.

Making only manipulated devices or processes available can lead to erroneous medical treatment or misdetection attacks - whereby the device or service could appear to be functioning while it actually provides false results. For example, with modern sequencing technologies, this could lead to false diagnostics. Such attacks could even have a global impact when no other molecular tests are available, as is often the case with novel pathogens. On the

[43] https://en.wiktionary.org/wiki/biomatter, last accessed November 2021.
[44] CIA - Confidentiality, Integrity and Availability.
[45] Genetically Modified Organism.

other hand, lack of availability (including supply chain attacks) can result in shortages of drugs, medical supplies, food, knowledge and others.

Questions pointing to research needs and priorities in the context of cyberbiosecurity:

- What is the level of exploitability of biotechnology R&D?
- Which attack vectors could compromise biotechnology R&D?
- What are the most critical digital assets used in biotechnology?

Possible research focus:

- The evolving risks and the threat landscape in biotechnology R&D;
- Risk management framework in the field of public health microbiology (e.g. modern DNA sequencing);
- Categories of cyberbiosecurity vulnerabilities (i.e. distinguishing the more traditional ones from those that are outside existing methodologies);
- Identification of the processes and routines throughout the life science fields that require interfaces and reliance on automation.

6. INTERDISCIPLINARITY IN THE RESEARCH OF CORE FIELDS

Many common research challenges as well as gaps emerge across all four themes outlined in this paper (intelligent systems, cyberbiosecurity, computational security and hyperconnected world).

Key issues focus on the interdisciplinarity of researchers in core areas, and the incorporation (or reinforcement) of basic cybersecurity principles such as privacy, confidentiality and trustworthiness. Trust is also a theme that runs through all the major research themes.

Skills, education and awareness in all areas are mentioned in each of the research themes. New and emerging technologies provide opportunities not only for innovation (societal and market) but also for abuse. Education and awareness of the potential misuse of these technological developments must also focus on providing developers and users with the most appropriate skills.

Many stakeholders are involved in all four research themes, which are identified as crucial areas that will have an impact on the resilience of our societies. These research themes should not be interpreted as silos for independent research. Given the nature of the research challenges, collaboration between the various stakeholders is required, and this needs to be addressed at a fundamental level in understanding the interactions between technical, political, societal and economic approaches in these areas. One way is to ensure that this is done with multidisciplinary teams representing different stakeholders. All these research themes involve stakeholders at different stages of theory building, conceptualisation, development and production and should therefore all be integrated into research and innovation activities.

6.1 CONVERGENCE OF AI WITH OTHER EMERGING TRENDS

As the digital ecosystem continues to expand with the Internet-of-Things (IoT) and other devices connecting individuals, organisations and value chains via mobile phones, central systems, data centres and also airborne devices, AI can be seen as both a key driver and the underlying technology in several areas (without claiming to be exhaustive) such as, among others, next generation mobile telecommunications, computer security and biotechnology (e.g. cyber biosecurity and synthetic biology).

The development of 6G is expected to reach technological maturity and standardisation over the next decade, impacting how people interact with the digital world beyond 2030. 6G will go beyond mobile internet to support ubiquitous AI services from the core to the network terminals. In fact, 6G can be expected to be ‘AI-enabled’ in the sense that it will both rely on AI for its core physical layer function and enable a wide range of new AI-based applications.

AI will play a critical role in the development and optimisation of 6G architectures, protocols and operations. At the same time, AI will be increasingly necessary for the IoT, either to run some local and relatively closed systems or to monitor the value of the global ecosystem with many more or less open systems over the Internet, in a cloud or at the edge. AI is undoubtedly an excellent set of tools to mitigate IoT risks, whether by investigating vulnerabilities, anticipating

problems (or even predicting them through self-reporting capabilities), controlling cross-network issues, orchestrating traffic and flows, and more generally, the risks of threats.

Cryptography is the foundation of computer security and one of the most important research areas in cybersecurity. One of the most important discussions in cryptography research is how it could be seriously affected by the potential of quantum information processing.

The increasing convergence of biotechnology and AI is also an emerging area to exploit. The ability to collect and process enormous amounts of data, which underpins AI, machine learning and deep learning, combined with advances in biotechnology such as gene editing, DNA sequencing and synthesis, is leading to a leap forward at the heart of the next industrial revolution. Precision medicine, enhanced bio surveillance[46], synthetic biology are all technologies that will increasingly benefit from the intersection of these two fields. Some advances being made in the bio-AI synergy may also raise ethical concerns.

In addition to the above, a space for discussions on the perspectives of societal challenges for the abovementioned research themes needs to be created. These 'perspectives' will continuously engage with the present, critically assessing our design, use, and adoption of technology, rather than just looking through technologically-determined lenses toward the future.

Possible research focus:

- Build systematic anticipatory capacities e.g. **launch multidisciplinary Delphi** surveys to address **key challenges as they emerge and as they can be anticipated;**
- **Adopt a 'broad eye' lens** for AI as the ecosystems we are evoking are constantly expanding, for example cybersecurity and AI, in the age of quantum cryptography;
- Design roadmaps involving AI capacities for, for example, cryptographic or cyberbiosecurity challenges over the next 10-15 years.

[46] Biosurveillance is an aspect of biodefense relating to the detection of biological threats, including bioterrorist threats, https://en.wikipedia.org/wiki/Biosurveillance, last accessed November 2021.

7. CLOSING REMARKS AND NEXT STEPS

This document highlights some of the key R&I needs and priorities identified by ENISA in consultation with the expert community. The four suggested themes for this year encompass some of the key trends identified by ENISA for the next 10 to 20 years. It invites researchers and industry to develop their knowledge on key challenges by identifying the aspects that will result from a decade of investment in the digitisation of the economy and society in Europe. Addressing some of the challenges raises some concerns and requires a strong position and commitment from policy makers and researchers to include them in the R&D programmes and roadmaps.

Although Europe is at the forefront as a global contributor to R&I, there are several challenges that need to be addressed, which are highlighted in this report. The first concerns interdisciplinarity, where excellent research is conducted in disciplinary silos. The second is linking basic research in advanced and niche areas with broader implementation initiatives, which are evident in EU funding instruments and beyond. The third is the organisation and coordination of research efforts in a global context.

The main objective of this document is to serve as a compass for ENISA to advise different stakeholders, including the EU Commission, the ECCC[47] Governing Board and Member States, on these important requirements for cybersecurity R&I. This document is only a brief overview of the first edition of the annual report, which summarises the main challenges and research opportunities in the field of cybersecurity.

During the upcoming years, ENISA will publish separate reports assessing these topics individually to provide more contextual and technical information on the challenges and research needs outlined in this report. In parallel, ENISA will continue to engage with stakeholders and the research community to discuss these and other topics relevant to cybersecurity. The topics will be identified beforehand from a foresight exercise to be conducted with stakeholders and the community. The results of these discussions will be reviewed and described in the form of an annual brief to be published towards the end of the year.

[47] https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-competence-centre, last accessed November 2021.

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

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

enisa.europa.eu