



It's not a data breach, it's a surprise backup

Fostering cybersecurity

Authored by:
Teresa Reiter
Dieter Feierabend



Graphic design: Andreas Pohancenik

Publisher:
European Liberal Forum EUPF
Rue d'Idalie 11-13, boîte 6, 1050 Ixelles, Brussels (BE)
info@liberalforum.eu
www.liberalforum.eu

NEOS Lab
Neubaugasse 64–66, 1070 Vienna (AUT)
lab@neos.eu
lab.neos.eu

Published by the European Liberal Forum in cooperation with NEOS Lab. Co-funded by the European Parliament. The views expressed herein are those of the author(s) alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum.

© 2022 the European Liberal Forum (ELF). This publication can be downloaded for free on www.liberalforum.eu. We use Creative Commons, meaning that it is allowed to copy and distribute the content for a non-profit purpose if the authors and the European Liberal Forum are mentioned as copyright owners. (Read more about creative commons here: http://creativecommons.org/licenses/by_nc_nd/4.0)

Printed by Printpool, Austria 2022

ISBN: 978-2-39067-041-4

#It's not a data breach, it's a surprise backup

Fostering cybersecurity

Abstract

According to studies, cybercrime constitutes half of all the crimes perpetrated in some member-state and accounts for losses worth billions of euros per year. Nevertheless, most hacks happen via known exploits, where hackers know the IT networks better than companies. The aim of this publication is to provide measures to strengthen the cybersecurity infrastructure at European and national level. Minimizing cybercrime is generally linked to business preparedness and citizen knowledge. Therefore, these groups are given special consideration in the analysis and policy recommendations.



Teresa Reiter
Author



Dieter Feierabend
Author

Contents

Introduction	3
CHAPTER 1	
Cyber-Crime and Cyber-Security	8
1.1 Cyber-Crime and Cyber-Security – Definitions and Statistics	8
1.2 Actors and Important Legislation	15
1.2.0 Actors	17
1.2.1 EU	17
1.2.2 NATO	19
1.2.3 United Nations	21
CHAPTER 2	
Four subject areas for strengthening cyber-infrastructure in Europe	24
2.1 Resilience, Sovereignty and Strategic Autonomy in the Digital Domain	25
2.2 Defence and Security	36
2.3 Skills and Skilled Workers	42
2.4 Cyber-Economy and Cyber-Security of SMEs	51
CHAPTER 3	
Summary and Outlook	64
All Recommendations at a Glance	65
Outlook	66
Bibliography	68
Abbreviations	76

Introduction

Half of all companies fall victim to ransomware attacks. One in eight companies is targeted almost daily by cyber-type attacks, and 9 per cent experience these kinds of attack several times a month (Deloitte, 2022:4). Ransomware attacks in particular are on the rise. This often involves the encryption of company data in order to extort a ransom. A recent example from Austria is the attack by the ‘Black Cat’ hacker group on the Federal Province of Carinthia (Futurezone, 2022). The attackers stole 250 gigabytes of data and threatened to publish the data if the Federal Province of Carinthia did not immediately pay a ransom of 5 million US dollars.

The state of Carinthia refused to do so, resulting in several releases of data owned by the state. In December 2020, the network management system of the software company SolarWinds was compromised. The attackers were able to collect data over an extended period of time. According to media reports, the stolen information enabled another attack, this time on federal US agencies (Bing 2020, ENISA 2020). In May 2021, the US pipeline operator Colonial Pipeline was the victim of a cyber-attack, resulting in the temporary shutdown of nearly half of the US East Coast fuel supply (Bing & Kelly 2021). These case studies show that cyber-attacks do not have to be isolated individual events and underline the potential damage that successful attacks can cause to peoples’ everyday life. They have been part of the daily threat landscape in Europe and the world for a long time.

However, while such attacks have an everyday political dimension in that they are inconvenient and politically damaging to individuals, parties and governments, the main problem is that they limit the ability of the target of such an attack to act. Even if a company or institution has properly and regularly made backups to secure its data, recovery often involves a lot of time and high costs. During the recovery period, important services for customers might not function, which can lead to further damage. Nor can physical security threats be ruled out as a consequence of such an attack. If such an attack coincides with another crisis and affects crisis management, a cyber-attack can easily have consequences for the security of individuals. While most organisations or companies claim not to pay a ransom, there is probably a high number of unreported cases, as the amount of the ransom often bears no relation to the potential or actual medium- and long-term damage caused by the cyber-attack.

The greatest damage is usually not caused by high-level attacks such as those mentioned above, but by low-level, low-cost attacks on civil infrastructure, private companies and individuals. This shows that cyber-security is an issue for us all, as citizens whose data has been stolen by attacks on public authorities, as entrepreneurs who have to deal with ransomware attacks or as political decision-makers who are increasingly coming into contact with cyber-security in the course of the digitisation of all areas of life. Given the scale of the above, it is not surprising that ENISA, the European Union Agency for Cybersecurity, complains that cyber-security continues to be wrongly treated as purely an IT issue (ENISA 2021). Individual freedoms, prosperity and our security in Europe can no longer be guaranteed without a digital security architecture. Therefore, it is necessary to look at the topic from a different perspective, which is guided by the following two key messages:

- Cybersecurity is an organisational culture issue that goes far beyond IT
- People, not IT, are at the centre of cyber-security

The aim of this publication is to provide measures for strengthening the cyber-security infrastructure at European and national level based on these key messages. This paper is divided into two sections:

The pandemic has also led to changed threat scenarios in connection with cyber-crime. Current threat scenarios are therefore presented and primary threats in the cyber-security area defined at the beginning of the first section. In the past ten years, the Member States of the European Union have created various institutions and instruments to protect the administration, the economy and also individual users from cyber-attacks of different kinds. In addition, NATO and the OSCE, as well as all European nation states, have set up bodies and mechanisms to respond to this challenge which is no longer a new phenomenon. It is sometimes difficult to gain an overall idea of their responsibilities, competences and functioning. As a result, policy makers often call for the creation of more instruments, agencies and co-ordinating bodies without giving much thought to which existing structures could be used, expanded or simply given more support to achieve the goal of greater cyber-security for all. This is particularly relevant as the outbreak of Russia's war of aggression against Ukraine has significantly increased the geopolitical dimension of cyberattacks, as well as attacks by state-sponsored groups (ENISA 2022b).

This paper therefore aims to provide such a representation – a kind of organisational chart of the most important institutions and protective measures in the cyber-domain – including the most important legal measures.

The second section is divided into four thematic areas where the authors believe there is a need for action:

1. Resilience and strategic autonomy are also essential topics in the context of cyber-security. While there is a multitude of laws and regulations relating to this in Europe, there is a lack of specific quantitative metrics with which we can measure the effectiveness and success of the measures.

2. In view of the very different approaches of the USA, Russia and China to cyber-security and cyber-defence, AI and data infrastructure, it is also important to fine-tune the European position in the security and defence sector.
3. As in the ICT sector as a whole, employment figures in the cyber-security sector have also risen dramatically. In view of the ongoing significant increase in the demand for people, the question arises as to how the shortage of skilled workers can be remedied.
4. When it comes to companies and cyber-security, people often only talk about critical infrastructure. At the same time, many small and medium-sized enterprises (SMEs) are exempt from European directives such as NIS 1 and 2. As they too are also significantly affected by cyber-attacks and these companies are the backbone of the European economy, their cyber-security must also be improved.

This paper's target audience is political commentators, liberal European decision makers, liberal-minded citizens and policy think tanks. No one should succumb to the myth that defence against cyber-attacks is cheaper, easier and faster than acquiring heavy weapon systems to fight crime and warfare in analogue space. Rather, we are looking at a future where security strategies and doctrines adapted to cyber-threats could also influence holistic thinking in security and defence. The idea of deterrence, in particular nuclear deterrence, has long shaped the security policy approach of different geopolitical powers. However, it cannot be applied precisely to cyberspace. The accumulation of offensively deployable cyber-weapons does not reduce the risk of an attack. On the contrary: there are prominent examples of cyber-weapons developed for precisely these purposes by major powers being hijacked by attackers and used directly or indirectly against the developer. Another issue that has repeatedly preoccupied liberals in the context of security policy is arms-export control. As the debate on arms deliveries to Ukraine 2022 shows, positions in this regard can be changeable even amongst liberals. Before the last EU parliamentary elections in 2019, many states indicated great support for the position that no weapons should be exported to states involved in an active armed conflict. Here, not only has the wind shifted due to Russia's war against Ukraine, but the debate has also been complicated by possibilities of digital warfare. Traditional arms-export controls have their limits in cyberspace, yet we in Europe and beyond will have no choice but to further develop international rules or consider how existing rules can be applied to this aspect of cyberspace.

Finally, it is important for liberals in particular, but also for all other political forces, to better understand the implications of cyber-crime or cyber-attacks on the economy and in particular on critical infrastructure, and to identify ways to deal with them. The European Union's NIS2 Directive poses significant challenges to the economy and the state, in particular in light of the ICT skills shortage in most countries in Europe, to which they must respond.

There is no one single remedy for threats that have such a complicated and diverse stakeholder and threat-actor landscape as this one. Nevertheless, there

are good examples of how to reduce the number of successful cyber-attacks on a state, its administration, economy and individuals. In implementing these, it is important for Europe's liberals to find, if possible, a common approach that does not disregard a core value of liberalism: the freedom of the individual and his or her fundamental and human rights. The answer to cyber-threats must never be the unconstrained, excessive and unlawful surveillance of citizens. The responsibility to constantly uphold this aspect lies primarily with liberals.



Chapter 1

1.1 Cyber-Crime and Cyber-Security – Definitions and Statistics

The EU Cybersecurity Act defines ‘cyber-security’ as ‘all activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber-threats’ (Cybersecurity Act, 2017: Title 1, Art 2, No 1). This definition should make policy-makers sit up and take notice, because it is clever in that it makes clear that measures to promote cyber-security can encompass virtually everything imaginable and are not limited to the IT context.

Since at least the discovery of the Stuxnet virus in 2008, it has been clear to those who deal with the matter that cyber-security and cyber-defence are not purely IT matters. The ‘Olympic Games’ operation, like the use of the virus in the destruction of Iranian centrifuges for uranium enrichment, exploited physical weaknesses in the facility when deploying the malware. Very simply put, against a system without these physical weaknesses at that time, malware by itself would only have been able to do much less. So it was not the ‘superiority’ of the cyber-weapon that made the attack so dangerous, but the combination of vulnerability and the effectiveness of the targeting weapon. Langner, the security firm famous for discovering the Stuxnet virus, concludes in its analysis that it is unlikely that Stuxnet or any part of it would be applied to copycat attacks on critical infrastructure in the US. For Langner experts, the greater danger lies in the fact that the tactical approach of the attack could be copied, further developed and ‘fired’ at civilian infrastructure (Langner, 2013).

High-level attacks like these provoke great media interest, but they are not commonplace. Attacks of the complexity and costliness of the ‘Olympic Games’ operation are comparatively difficult to carry out. Significant primary threats look different and are defined by ENISA in its periodically published Threat Landscape Report (ENISA, 2022):

Table 1: Key threat scenarios

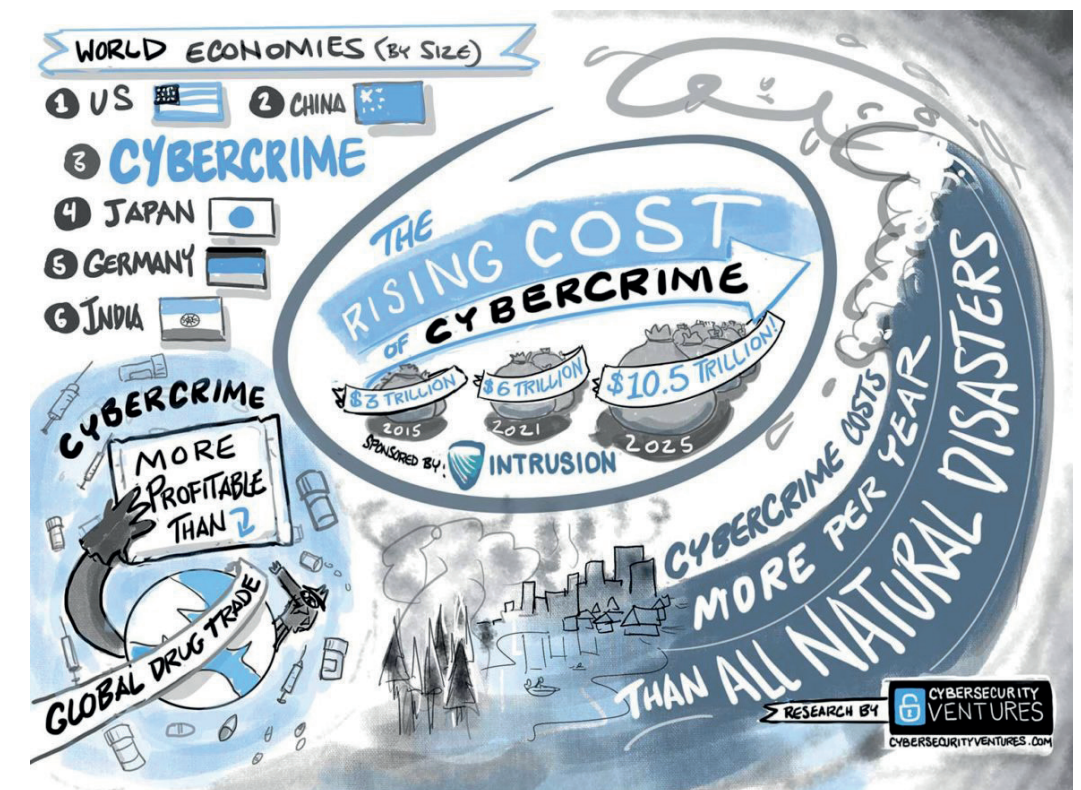
Type	Description
Ransomware	Ransomware is called "extortion software" and allows the attacker to encrypt an organisation's data, thereby effectively holding it hostage. This is accompanied by a request for payment for the restoration of access to the data.
Malware	A malware program is software designed to allow unauthorised access to systems. This access adversely affects the confidentiality, integrity or availability of a system.
Cryptojacking	In cryptojacking (also called covert crypto-mining) criminals use the computing power of their victims without their knowledge to generate cryptocurrency.
Threat to availability and integrity	These include a range of threats and attacks, the stand-out groupings being Denial of Service (DoS) attacks and Web attacks. The objective is often to prevent system availability by depleting resources, resulting in performance loss, data loss and outages.
Threat associated with emails	Attacks linked to emails (electronic mail messages) consist a set of threats that exploit the weaknesses of the human psyche. For example, messages purporting to be from your own bank that there are problems with your account or messages from software companies.
Disinformation-Misinformation	Disinformation and misinformation campaigns are often used in hybrid attacks to diminish social trust in organisations and systems, an important prerequisite for cybersecurity. The increased use of social media platforms and the increased online presence since the outbreak of the pandemic have increased these threats.

Source: ENISA 2022

For several years, ransomware has been the most common threat with several high-profile incidents occurring (see Chapter 1). The relevance of such attacks has been demonstrated both in the European Union and internationally. (ENISA 2021, 2020). Despite broad awareness-raising measures, the danger of malware linked to e-mails remains very high. New forms of crime, such as cryptojacking, a threat that has significantly increased in frequency over the last two years (ENISA 2020, 2021), are contributing towards the threat picture.

In the last ten years, the number of cyber-attacks on civilian infrastructure and military facilities has increased dramatically. According to a study by Accenture (2019), within a single year, the number of successful attacks increased by 11 per cent. The FBI's Internet Crime Report 2021 (2022) shows that the COVID-19 pandemic saw a massive increase in cases. The number of reported cases increased by almost 70 per cent compared to 2019, while the amount of losses doubled within two years. According to the official 2019 annual cyber-crime report by CyberSecurity Ventures, cyber-crime is the biggest threat to every business in the world (CyberSecurity Ventures, 2020). According to their calculations, between 2015 and 2021, the cost of cyber-crime doubled to 6 trillion dollars and forecasts predict that by 2025 the damage will increase to 10.5 trillion. According to analyses by Proofpoint (2022), in 90 per cent of all cases, cyber-attacks start with email messages. According to their analyses, 3.1 billion scam emails are sent per day. Basically, this increase can be explained by several factors. Besides the increasing online presence, the rise of online and cloud-based solutions, the use of emerging technologies, such as artificial intelligence (AI), and the associated complexity of systems and cyber-attacks are a major factor (ENISA 2020, 2021, Stealthlabs 2020).

Figure 1: The rising cost of cybercrime



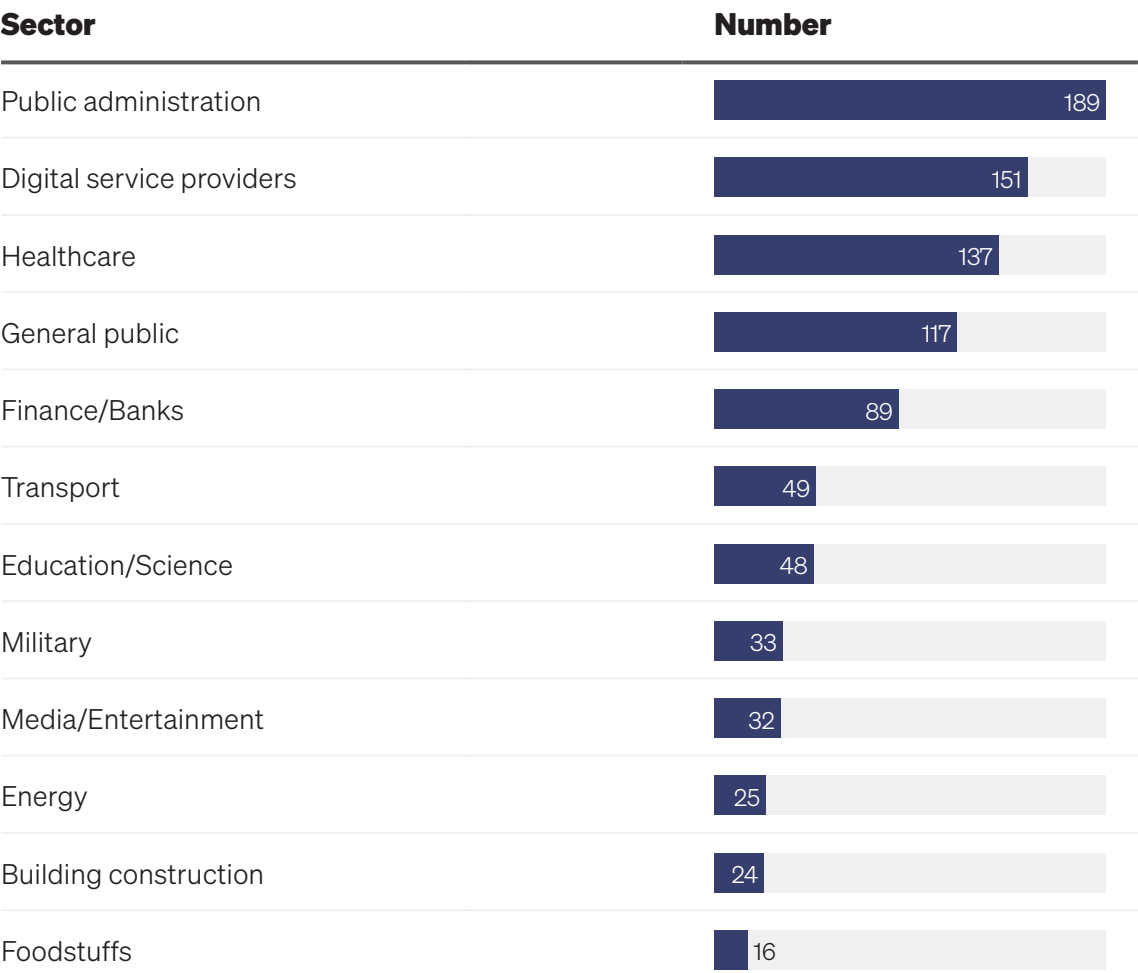
Source: CyberSecurity Ventures

If one compares the economic costs of cyber-crime with the GDP of states on the basis of CyberSecurity Ventures data, cyber-crime would be the third largest economy in the world after the USA and China. This size of the threat, coupled with the massive increase in the amount of damage incurred in recent years, represents the largest transfer of economic wealth in history, according to CyberSecurity Ventures (2021). Within the criminal world, cyber-crime is thus more profitable than the global drug trade.

In its annual report on the cyber-security threat situation, the European Union Agency for Cybersecurity. ENISA, has mapped out significant malicious attacks in addition to providing a basic assessment of the threat situation. These include major incidents, such as the successful attacks on the Federal Province of Carinthia or private companies such as SolarWinds mentioned at the beginning. A continuous increase in major incidents has also become noticeable. Serious attacks doubled in the first year of the pandemic alone, with an increase of 50 per cent observed in the health care sector in particular ENISA (2020, 2021). For the last reporting year, public administration, digital service providers and the health care sector were particularly affected.

Figure 2: Critical attacks on selected sectors

Critical attacks between April 2020 und July 2021



Source: ENISA 2021

The rise in cyber-attacks and increased awareness of cyber-security is driving constant and robust growth in the global market for cyber-security products. While cyber-security solutions accounted for \$83 billion in global sales in 2016, this rose to \$139 billion in 2021, with annual growth rates mostly above 10 per cent (Statista 2022a, 2022b, Zdnet 2022). This makes the cyber-security sector one of the fastest growing markets (Statista 2022b). Within the European Union, the cyber-security market is expected to reach 36.3 billion Euros, with security services accounting for the largest share at 21.1 billion (Statista 2022a).

The Ponemon Institute, in collaboration with IBM, has studied the costs of a successful cyber-attack in 17 states and 17 sectors. According to their analyses, in 2022, companies spent an average of 4.4 million per incident on damage repair, compared to 3.9 million spent in 2020 (Ponemon/IBM 2022). At the same time, the report shows that organisations that were able to identify and repair the damage within 200 days were able to reduce their costs by 1.1 million. So time is of the essence when it comes to detecting attacks.

The greatest damage is usually not caused by high-level attacks, but by low-threshold attacks on civil infrastructure, private companies and individuals that are comparatively inexpensive for the attacker. A high degree of standardisation, which the European Union strives to achieve in various economic and administrative contexts, for example to ensure the functioning of the internal market, to simplify cooperation between EU states or to make life easier for end customers, is sometimes a problem in the context of cyber-security, because it makes copycat attacks very cost-effective for the attackers. Digital systems that have a specific function and were never designed to withstand or repel attacks are growing in relevance for cyber-attackers. An example of this is control systems for monitoring the function of industrial installations. Physical weaknesses in, for example, industrial installations etc. are often not primarily understood as weaknesses in the context of a possible cyber-attack. In terms of military and criminal history, it can be assumed that cyber-criminals and state actors will find creative ways and means to link physical and virtual weaknesses in a target and use them in ever new contexts (Langner, 2013: 19f.). Aspects such as infowar methods are changing alongside our societies' changing communications architecture and behaviour. Platforms, software and digital commodities can easily be 'weaponised', that is, used as a weapon or as an instrument of manipulation, as shown, for example, by the case of the British company Cambridge Analytica, which made headlines for its role in the US election campaign (Chang, 2018).

In addition, the increasing digital networking of private individuals and the state, nationally and internationally, increases the danger of chain reactions, digital pandemics, if you will. The well-known example of the NotPetya attack on Ukraine shows that many computers which were not originally the target of the attack, but were networked with the target architecture in one way or another, were infected and suffered damage. While such high-level attacks usually affect states or larger institutions or critical infrastructure, there is hardly anyone today who can say that they are not also individually affected by cyber-threats, whether they are aware of it or not (Perlroth, 2021).

This is particularly relevant because, according to ENISA (2021b), 84 per cent of all cyber-attacks are based on 'social engineering'. This is a technique where criminal actors obtain security-related data by exploiting human behaviour. Human emotions and characteristics such as trust, helpfulness and fear are exploited to manipulate users, for example to pass on confidential information or to install malware (Kaspersky 2022). The more that is known about users and their habits, the easier it is to instrumentalise these habits. The fact that most people share their preferences, relationships and professional details on social media makes it easier for attackers. Hackers might find that many employees of a company follow a particular restaurant on Facebook and hide their malware in the restaurant's menu link. Social engineering is not a new phenomenon, but the digitisation of our societies allows criminals to reach millions of victims with comparatively little effort. This is particularly striking in small and medium-sized enterprises (SMEs), which, in contrast to large companies, often do not have their own IT department and often have only a few employees. Accenture's ninth

'Annual Cost of Cybercrime' study (Accenture, 2019) reveals that 43 per cent of all successful data leaks take place in small and medium-sized enterprises. An ENISA (2021b) analysis of SME cyber-security shows that, in addition to social engineering, weak passwords (a problem for 56 per cent of all SMEs) and unlocked devices (44 per cent) are among the biggest security risks.

1.2 Actors and Important Legislation

Over the last decade, the EU has adopted a wide range of cyber-security measures. In particular, the NIS 1 Directive in 2016 led to an upgrade of cyber-security in the European Union. Here, industry and relevant institutions were obliged to reduce vulnerabilities from a cyber-security perspective and strengthen resilience. From an institutional perspective, the 'Cybersecurity Act' was of particular relevance, as it represents the establishment of ENISA, the EU Agency for Cybersecurity, in addition to central definitions of terms such as cyber-security, ICT standards and certification processes.

The NIS 2 directive, which is currently being finalised, is intended to minimise differences in cyber-security requirements and guarantee uniform standards in the implementation of cyber-security measures. Particularly noteworthy here is the expansion of the number and type of companies affected by the directive. While on the basis of the current directives, the Member States were responsible for determining which entities fulfil the criteria as operators of essential services, the new NIS 2 directive introduces a size threshold, which means that significantly more companies will be subject to the directives. As public administrations are often also exposed to attacks, NIS 2 also applies to public administrative bodies at a federal and a regional level.

Table 2: Selection of key EU cyber-security initiatives

Date	Initiative	Reference
2013/02	Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Cybersecurity Strategy of the European Union: 'An Open, Safe and Secure Cyberspace	JOIN/2013/01
2015/04	Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – The European Agenda on Security	COM/2015/0185
2016/04	European Parliament and Council of the European Union, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC	Regulation (EU)2016/679
2016/07	Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union	EU Directive 2016/1148
2017/09	European Commission, Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act')	COM(2017) 477 fnal
2018/09	Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres	COM(2018) 630 fnal
2020/02	Shaping Europe's Digital Future White Paper on Artificial Intelligence A European Data Strategy	COM(2020) 65 fnal COM(2020) 66 fnal
forthcoming	Network and Information Security (NIS2) Directive	EU Directive

Source: European Commission, Joint Research Centre

1.2.0 Actors

1.2.1 EU

ENISA

Founded in 2004 and with its headquarters in Athens, the EU Agency for Cyber Security has the rather broadly formulated task of strengthening cyber-security in Europe in general. In practice, it works with business and various organisations to increase trust in the digital economy, strengthen relevant EU infrastructure and protect people living in the EU from cyber-attacks. The agency performs these tasks mainly through capacity building, networking initiatives, certifications, etc. ENISA is not a law enforcement or military organisation. Considering the diverse subject areas ENISA deals with, it has relatively few employees (approx. 60 to 100). In addition, it has various advisory bodies, working groups and a network of national liaison officers (NLOs) in the Member States.

European Cybercrime Center (EC3)

Founded in 2013, the EC3 is an institution of the EUROPOL European police authority. Its mission is to strengthen executive bodies in the fight against transnational cyber-crime. EC3 experts provide strategic, operational, analytical and forensic support to national authorities in the fight against online payment fraud, child pornography and other cyber-crimes. This also includes the fight against illegal activities on the so-called dark web and other dark corners of the digital space.

EU Intelligence and Situation Centre (EU-INTCEN)

EU-INTCEN is a body of the European External Action Service (EEAS) and thus directly subordinate to the High Representative for Foreign Affairs and Security Policy of the EU. Together with EUMSINT (see below), it is the closest thing there is to a European intelligence service. As security remains a nation-state competence, its analyses relate to information it receives from nation-state intelligence services. What information the intelligence services share with their European counterparts is decided by the Member States, unless otherwise regulated (e.g. through reporting obligations following cyber-attacks). In 2016, the so-called 'Hybrid Fusion Cell' was established within this service to provide decision-makers at EU level with analyses and situational awareness briefings regarding hybrid threats. It has a network of national liaison officers who meet twice a year to exchange information and who are coordinators between various departments within the Member States. The Hybrid Fusion Cell also works closely

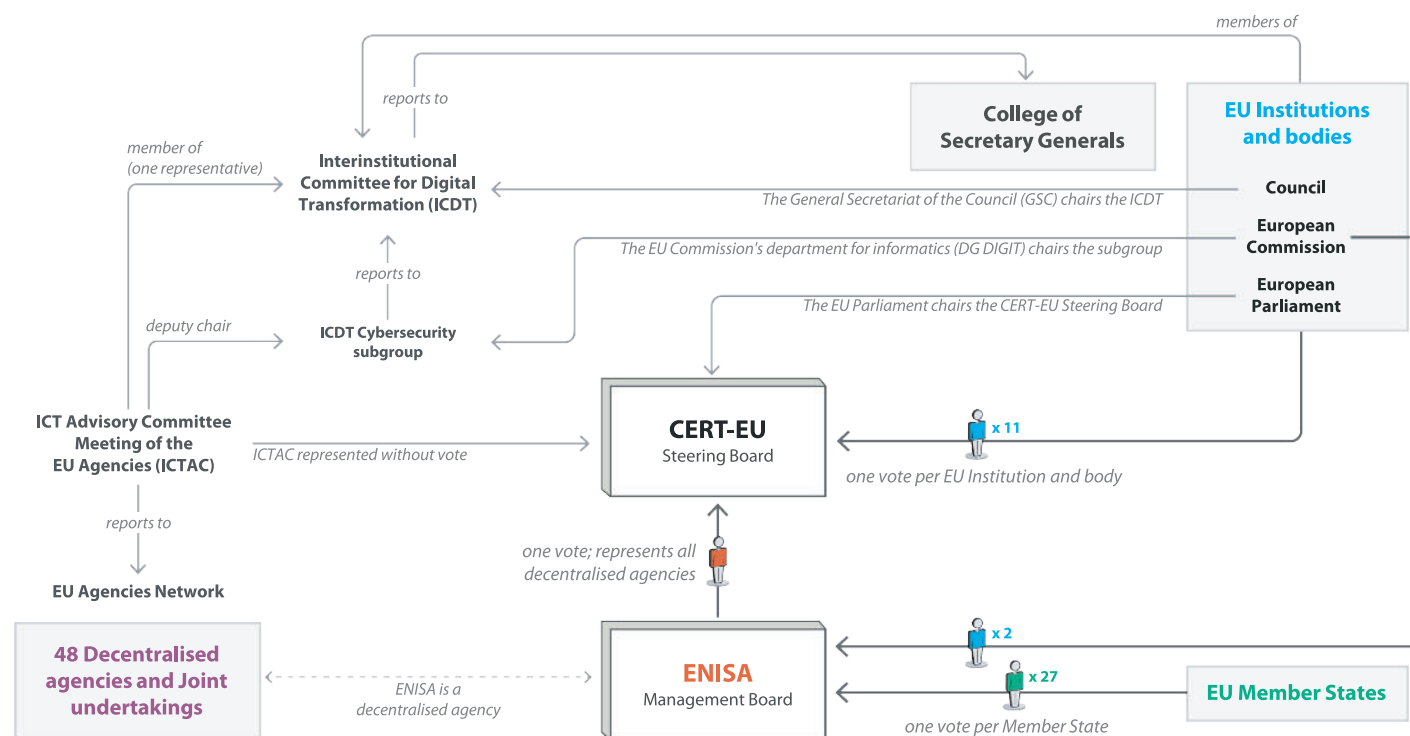
with the Intelligence Directorate of the EU Military Staff (EUMSINT) on cyber-security and defence. Both have expertise in the area of hybrid threats.

Computer Emergency Response Team der Europäischen Kommission (CERT-EU)

This is an IT emergency team of the European Commission which supports all institutions, bodies and agencies of the European Union. Complementary to ENISA, CERT-EU also works in the area of prevention and education and also provides support in the area of incident response. For example, if an EU organisation is acutely affected by a cyber-attack, CERT-EU can coordinate the response, and evaluate, analyse or verify available information. At the same time, the CERT is responsible for identifying and combating vulnerabilities in the technical infrastructure of the EU institutions, etc.. This is done, among other things, through penetration tests and 'ethical hacking techniques'.

Mention should also be made in this context of the European Defence Agency which is making a major contribution in the area of capability building and research and development, just as the European Defence Fund will be doing in the future. In addition, there are several PESCO projects relating to cyber-security or cyber-defence (PESCO, 2022).

Figure 3: Structure of the Computer Emergency Response Team of the European Commission (CERT-EU)



Source: European Court of Auditors

1.2.2 NATO

Cyber-defence has been on NATO's political agenda since 2002. However, it took a while for the Alliance to establish mature policies, structures and governance in this area. Here are some milestones and an overview of current structures.

At the NATO summit in Warsaw in July 2016 cyberspace was officially recognised as a 'domain of war'/'domain of operations', in addition to air, land and sea, which were the existing domains. This step was a significant one in that it meant that NATO would become more focused on developing resources, capabilities and skills in this domain. So this concerned the operational steps that NATO was taking with this recognition. NATO also committed itself to expanding NATO-EU cyber-defence cooperation and to promoting transparency and responsible action by states in cyberspace.

NATO's primary objective in cyberspace is to protect its own networks and operations and support its members and partners in building up resilience. NATO Allies are committed to ensuring that international law applies in cyberspace (NATO, 2022).

Comprehensive Cyber Defence Policy

NATO has a so-called 'Comprehensive Cyber Defence Policy', which aims to strengthen NATO's fundamental defence functions and reinforce a general logic of deterrence, and declares that Article 5 of the NATO Treaty on 'collective self-defence' also applies in the event of a cyber-attack. Furthermore, it states that NATO's response to such an attack will not necessarily be limited to cyberspace (NATO 2022, NATO 2018).

Cyber Space Operations Centre

NATO's Cyberspace Operations Centre, sometimes called 'NATO Cyber-Command' is relatively new. It provides situational awareness support to NATO commanders and coordinates NATO's operational activities in cyberspace, including deterrence. The centre is fully staffed with 70 cyber-experts who are fed information by Member States' intelligence services to provide real-time situational awareness (Emmott, 2018).

Chief Information Officer (CIO)

The NATO Chief Information Officer (CIO) is a new position. The first CIO was appointed in 2021. He/she is responsible for overseeing and coordinating integration and aspects of NATO's information and communication technology systems essential for functioning interoperability and the joint development of new ICT capabilities. He/she also acts as a single point of contact within NATO for all cyber-security matters. This also includes incident management, strategic investments and NATO-wide awareness raising for strategically relevant issues in the cyber-domain (NATO, 2022).

NATO Computer Incident Response Capability (NCIRC)

The NCIRC is housed at NATO's Brussels headquarters and is part of the NATO Communications and Information Agency. It is responsible for protecting NATO's own networks and provides support 24 hours a day in relation to possible cyber-incidents.

Centres of Excellence

NATO has a significant number of so-called 'Centres of Excellence' spread across its Member States. Of particular importance in the cyber-domain is the **Cooperative Cyber Defence Centre of Excellence (CCDCOE)** in Tallinn. Its mission is to provide interdisciplinary expertise for the defence against cyber-threats. This mainly concerns the areas of technology, strategy, operations and law. It is a research, training and exercise centre and also offers non-NATO countries the opportunity to contribute (CCDCOE, 2022). Also relevant in the cyber-domain is the **Strategic Communications (STRATCOM) COE** in Riga, which is very important for combating disinformation and has thoroughly creative approaches to it. For example, STRATCOM developed the online game Newshero (LSE, 2018), to educate in terms of source criticism, and commissioned studies on humour as a weapon against disinformation and propaganda (Ozolins et al., 2017). The centre focusses on Public Diplomacy and Public Affairs and psychological operations (STRATCOM COE, 2022). The **European Centre of Excellence for Countering Hybrid Threats (Hybrid COE)** also plays a role in countering cyber-threats. It works at the interface between NATO and the EU and coordinates joint exercises (Hybrid COE, 2022).

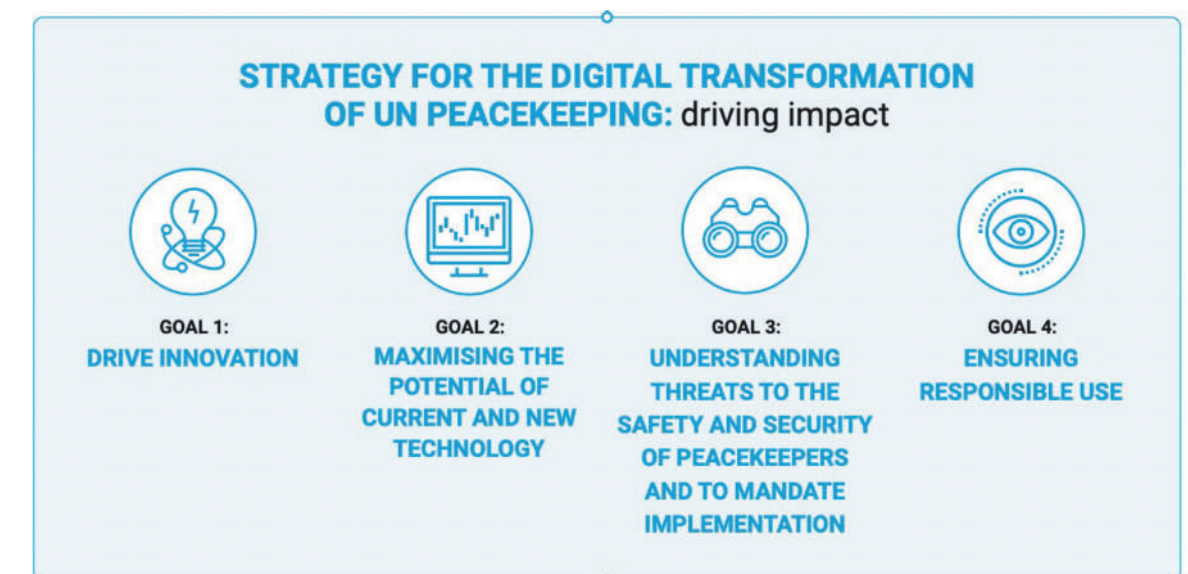
In addition to all these facilities, NATO operates a number of other training centres such as the **NATO School** in Oberammergau, Germany, the **NATO Communications and Information Academy** in Oeiras, Portugal, and the **NATO Defence College** in Rome. Exercises and training in cyber-defence take place at the **NATO Cyber Range** in Estonia. NATO also operates an **Industry Cyber-partnership**, within which it cooperates with private companies to promote the overall resilience of NATO countries (NATO, 2022).

1.2.3 United Nations

Within the United Nations, too, there are bodies and strategies designed to increase cyber-security and avert threats in cyberspace.

The Roadmap for Digital Cooperation was published by the Office of the UN Secretary-General in June 2020. It addresses how the global society can make better use of digital technologies and includes recommendations based on input from Member States, the private sector, civil society, the tech community and others. Its goal: a safer and more equitable digital space for all (UN Office of the Secretary General's Envoy on Technology, 2020). The **UN Data Strategy** aims to improve data sharing with greater levels of protection between Member States, and also serves to promote a data-driven culture within the UN. With the **Strategy on New Technologies**, the UN sought to define how specifically to advance the use of new technologies. **The Action for Peacekeeping (A4P+)** and the **Strategy for the Digital Transformation of UN Peacekeeping** include recommendations and strategies for innovative, digitised and data-driven peacekeeping, and the ICT Strategy focuses on the modernisation, transformation and innovation of the ICT sector (UN Peacekeeping, 2021).

Figure 4: Key objectives of the Strategy for the Digital Transformation of UN Peacekeeping



Source: UN Peacekeeping

As of 2022, UN Member States are negotiating a new convention on the use of information and communications technologies for illicit purposes. A draft is to be presented by the 'Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes' to the UN General Assembly at its 78th session (UNODC, 2022).

Among the UN institutions dealing with one or more aspects of cyber-security, the following deserve particular attention:

UN Office on Drugs and Crime (UNODC)

Most of the UN's operational activities in the area of combating cyber-threats are carried out by the UN Office on Drugs and Crime (UNODC). Along with the UNODC Cybercrime Repository, this institution also has a comprehensive archive of relevant cyber-crime data. The goals of the UNODC are, for example, well-trained police officers, law enforcement officers and judges in the cyber-domain, international cooperation and information exchange in the fight against cyber-crime. It promotes these goals through training, workshops and also by monitoring of the measures taken by Member States to combat cyber-crime. UNODC also often hosts working groups for the development of new strategies or policies.

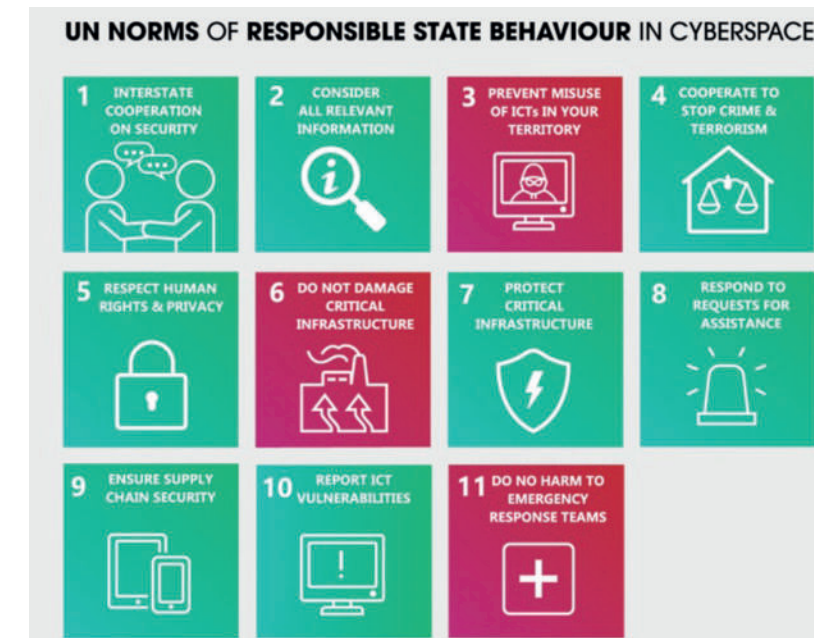
UN Office of Disarmament Affairs (UNODA)

UNODA also has competencies in cyberspace. However, these focus less on the civil component and more on issues of global security and digital disarmament. In this context, the UN Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE), set up by this office, presented a catalogue of 11 standards for responsible state action in cyberspace (Australian Strategic Policy Institute, 2021). These are essentially action guidelines for self-regulation by UN Member States.

Office of Information and Communications Technology (OICT)

The UN Office of Information and Communications Technology (OICT) reports to the Office of the Assistant Secretary General of the UN and is responsible for a 'better, safer, more sustainable future through innovative technology'. Analysis of new technologies, technology assessment and strategic tasks are among the core tasks of the OICT (Unite, 2022).

Figure 5: Standards for responsible state action in cyberspace



Graphic: Australian Strategic Policy Institute, ASPI, 2021

Chapter 2

Four Subject Areas for Strengthening Cyber-Infrastructure in Europe

As Chapter 2 has shown, the response to the increasing cyber-threat situation has been global with investments in cyber-security, new laws and new organisations. With new technological possibilities and the de facto dominance of information and telecommunication technologies in our daily lives, further development of cyber-security remains a key task for political decision-makers.

As Chapter 1 has shown, the response to the increasing cyber-threat situation has been global with investments in cyber-security, new laws and new organisations. With new technological possibilities and the de facto dominance of information and telecommunication technologies in our daily lives, further development of cyber-security remains a key task for political decision-makers. While resilience has become a buzzword in recent years, it is clear that in many cases it is too late for effective resilience-building and that our societies are some distance from the resilience ideal. The remaining obstacles to European sovereignty in the digital space and how they can be resolved are explained in chapter 3.1. Even though cyber-security should not be confused with cyber-defence, the two are inextricably linked. Chapter 3.2. is dedicated to essential subject areas on the basis of which cyber-defence improves cyber-security policy in Europe. There has been talk for years of a shortage of skilled workers in the ICT sector not least due to demographic change. In hardly any other sector is this as evident as it is in cyber-security. Not least because of the strong growth in a few years, there are personnel capacity problems worldwide. How this shortage of skilled workers can be resolved is described in chapter 3.3. Since the emergence of cyber-attacks, critical infrastructure such as energy operators have gradually become more and more the focus of an effective cyber-security policy. There is a good reason for this, as shown by the example of the US pipeline operator Colonial Pipeline where almost half of the fuel supply to the US East Coast can be temporarily forced to shut down due to a cyber-attack. Nevertheless, empirical evidence shows that more than 40 per cent of all successful cyber-security attacks affect small and medium-sized enterprises. The security of small and medium-sized enterprises is of fundamental interest to Member States of the European Union, as SMEs account for 99 per cent of all enterprises in the EU and employ over 100 million people (European Commission 2022a). Chapter 3.4 illustrates measures to strengthen the cyber-security of small and medium-sized enterprises.

2.1 Resilience, Sovereignty and Strategic Autonomy in the Digital Domain

In European language usage, there is sometimes a degree of confusion when it comes to the subject of the capacity to act in the security sector. Terms that are at different semantic hierarchy levels are often used synonymously, or the translation into many a member state's language makes it difficult to clearly distinguish between different terms and concepts.

The *Strategic Compass* of the European Union is the strategy to make the EU a *sovereign/autonomous* planning and acting entity. On the one hand, this means that the EU must be secure from unsolicited outside interference in order to guarantee the security of its citizens. On the other hand, the Union must be as independent as possible from other powers which might be pursuing other strategic goals. In times of global production and supply chains, this is a difficult task and it should be noted that independence does not mean protectionism and isolation. However, the example of gas dependence on Russia and the consequences for the European Union since the start of the Russian war of aggression in Ukraine in February 2022 is a good illustration of a situation that should be avoided. If one considers the activities that, for example, the US company Apple is undertaking to reduce its dependence on China, which has become problematic in terms of production due to long lockdowns (Jennings, 2020), a certain diversification, namely a distribution of essential production to different countries, ideally those countries that are, for example, alliance partners in NATO or otherwise have a close relationship to the home state, could be a solution.

According to ENISA (2021c), digital sovereignty, or freedom of action, is based on three components: individual data sovereignty, political sovereignty to influence norms and standards, and the sovereignty of the data-driven industry. Accordingly, it defines digital strategic autonomy as Europe's ability to source products and services which meet its needs and values without undue influence from external actors (see ENISA 2021c).

There are different aspects to achieving the twin goals of independence and resistance to external influence in order to establish strategic autonomy in the digital sector. On the one hand, it is essential for Europe to implement cyber-policies that are oriented towards European values and the realities of the European single market. Both are not always easy to reconcile and require an

active balancing of interests.

Having as much European production as possible of digital products (software and hardware) and services important for the security and functionality of European democracies and economies increases our resilience, as does having our own European digital infrastructure for business and administration.

In addition, there is a need to continuously raise awareness and build trust among the citizens of Europe in order to minimise external influence.

Finally, the training of skilled workers and the ability to subsequently retain them on site are also an important cornerstone of the European capacity to act in the digital sphere. This also includes real-life capacity building amongst people of all ages who are not active in the ICT sector. Chapters 3.3 and 3.4 deal with this aspect.

‘Resilience’ is the buzzword of security policy in the 2020s. The idea that it is more effective and efficient to immunise a state, an organisation and also individuals against cyber-threats of all kinds to such an extent that they cannot be harmed by any attacks etc. in the first place, is an excellent one. Unfortunately, the Western world has only now discovered the concept for itself. In many areas relevant to security, it is now either too late to effectively build resilience without any gaps, or too costly in economic and sometimes political terms (Erhardt, 2019).

Infrastructure

An example of this is the debate about the smartphone app TikTok, which is particularly popular among young people worldwide. The app belongs to the Chinese company *ByteDance*, which always insists in its statements that it is not controlled by the Chinese government (BBC, 2020). The company is suspected of passing on user data to the Chinese government, which *ByteDance* spokespeople always deny. However, a BuzzFeed investigation in June 2022 showed that there is legitimate reason to doubt the company’s assertions. Leaked audio recordings of more than 80 internal TikTok meetings held by the parent company *ByteDance* indicate that so-called ‘master users’ located within China have accessed non-public data of US TikTok users, implying access rights which not even *ByteDance*’s US employees have. The period from September 2021 to January 2022, when the data access is alleged to have taken place, coincides precisely with the testimony of a senior TikTok executive before the US Senate. In it, he swore that a team of world-renowned, US-based experts decided who would get access to the data. In one of the leaked audio recordings of TikTok employees, someone openly says: ‘Everything is seen in China’ (Buzzfeed, 2022). To protect the company from greater harm, *ByteDance* announced shortly afterwards that it would store all US users’ data in the US from that point onwards by handing over all data to the US company Oracle. Even though many experts called this a clever move, the distrust by Western governments has not gone away.

According to an analysis by netzpolitik.org (Meineck and Fanta, 2022), what is new about the BuzzFeed investigation is not that this data access exists – this had

previously been spoken about by TikTok itself – but how extensive the access is. The authors also point out that the *Bytedance* group is not automatically synonymous with the Chinese government, but that the Chinese regime owns shares in the company and ‘regime loyalty is mandatory for Chinese companies’. According to an investigation by *Wired* magazine TikTok collects a lot of data without specifically telling users what data is shared with third parties. *Wired* quotes Proofpoint’s Vice President of Threat Research as saying that the number of permissions TikTok requests from its users is greater than other platforms. While it is possible to deny this access, this limits the app’s functionality (O’Flaherty, 2021). TikTok has over 1.5 billion active users of whom the Chinese government may be well aware, regardless of whether US data was moved to Oracle this year (Bloomberg, 2022). Regardless of how much a state invests in building resilience against such data access, the knowledge about users active up to this point can no longer be erased.

There are even more far-reaching consequences of decisions, some of which were made years ago, in the area of infrastructure. This concerns 5G infrastructure on the one hand, but also Chinese direct investment in Europe. The Strategic Compass of the European Union (2022) states that it needs ‘a specific and realistic plan for Europe to develop, own and control all essential cyber-infrastructure itself, so that strategic autonomy in cyberspace can be secured as far as possible.’ The decision to jointly explore 5G infrastructure with China was taken in 2015 (European Commission, 2015). To date, several EU countries have jointly identified a high risk potential that some 5G providers may be used for manipulation by foreign intelligence services. There is also the fear of a hidden ‘switch’ in this infrastructure that China could use to cut off the West’s network. For this reason, some governments around the world (Australia, New Zealand, Israel, South Korea, Japan, Vietnam) have excluded China from their 5G infrastructure production chains (Gorman, L., 2020). Realistically, both the US and Europe have to face the fact that China is rolling out its 5G network much faster than the West, although not without problems. If they want to keep up with China’s technological progress, they will have to make great leaps forward in the next few years and themselves create an infrastructure that is strategically autonomous (Strumpf, 2020).

Other failures in the past also influence the resilience of our societies against cyber-attacks today. Another example is that when schools were digitised, insufficient attention was paid to protecting them against cyber-attacks, as a school did not seem a particularly worthwhile target for hackers. However, poorly secured schools are very well suited as vehicles for botnet attacks on other institutions. This also applies to any small business with computers and employees who, at best, have a basic knowledge of network threats. In most companies whose core business is not IT, there is no mandatory, regular cyber-training.

The European data situation

While a large number of directives and laws have been passed at European and national level in the last ten years, in practice there are often still very heterogeneous approaches to central topics such as raising cyber-security awareness. Since more than 80 per cent of all cyber-attacks are based on social engineering, awareness communication and knowledge transfer are of central importance. As ENISA illustrates in a country comparison study (2021d), both the objectives and the population groups to be addressed are defined very differently from country to country. While the goal in Luxembourg is to build trust in the digital world and protect human rights online, the Latvian cyber-security strategy aims to build an information society (ENISA 2021d). While all strategies aim to increase the awareness of the general population, specific measures often only target specific groups. While Slovakia defines measures to improve the cyber-understanding of public servants and IT professionals, the Finnish cyber strategy also includes the NGO sector and Latvia focuses on students and teachers (ENISA 2021d). In practice, this means that in each Member State, different targets and target groups are addressed in everyday operations, making measurability and comparability difficult. This makes it more difficult for the EU to address potential weaknesses in awareness-raising.

Basically, heterogeneity among target groups is understandable, due, amongst other things, to the geopolitical situation and the various associated threat perceptions. Different economic structures in the individual Member States also play a role. Nevertheless, the fundamental goals and measures must definitely be harmonised, especially when it comes to the general population. A case study for low-threshold information and awareness-raising is the 'Cyber Weather Report' of the Finnish National Cyber Security Centre (NCSC 2022). The Cyber Weather Report provides an update on the most important information-security incidents and threat situations of the month. Based on a weather forecast, all areas are assigned to one of three categories: calm, worrying or serious. The uniformity of the format raises its profile among the population and the clear categorisation helps the population to assess risks. The measure is also comparatively inexpensive and can be easily implemented via public broadcasting.

As in all areas, effective measures cannot be taken in cyber-security without any evidence. In the case of cyber-security awareness communication and knowledge transfer, Eurobarometer regularly collects data for all Member States. These are often supplemented by national surveys. While Estonia, for example, collects questions on cyber-crime awareness annually, Belgium collects data on cyber-security practices (ENISA 2021c). Not least because of the threat posed by social engineering, it is also advisable to collect data on attitudes and behaviours, yet basic data of this kind is often lacking in Europe. According to ENISA, the lack of a common measurement methodology across the EU-27 creates uncertainty about what the relevant cyber-security culture indicators really are (ENISA 2021c).

Another example of what should be included in a cyber-security taxonomy is better data on foreign direct investment (FDI). Over the past decades, these investments have generated global growth, boosted development, created jobs and improved

prosperity. Removing barriers to capital inflows means that recipient countries must manage the potential risk to national security or public order (OECD 2009). China's importance to Europe is not based on its cyber-capacities. It is vital to screen investments from China from a European perspective (Herpig 2021), in particular in the areas of economic and competitive espionage or espionage for political reasons, and to restrict them if necessary. The practical impacts of this are illustrated by a report by the German Marshall Fund (Christiani, D. et. al 2021).

In recent years, China has made massive investments in Hungary's railway infrastructure and Greece's port infrastructure, amongst others, as part of the Belt and Road Initiative. Both countries have prevented the EU from condemning China for human rights violations, including the alleged torture of human rights lawyers. Both Hungary and Greece rejected a common EU position on the conflict in the South China Sea in 2016 (Christiani, D. et. al 2021). It is of vital interest for digital sovereignty to screen investments from abroad, in particular when it comes to key digital infrastructure. As illustrated by a report from the European Think-tank Network on China (ETNC), there is massive dependence on China in some Member States, in particular in the 5G sector, which has led to Austria, Hungary and Greece blocking measures against the Chinese company Huawei (Seaman, J. et. al 2022).

But apart from such reports, we often know little about foreign direct investment. According to RHG FDI.Monitor, from 2000 to 2016, more than 1400 individual FDI transactions by Chinese investors were registered in the EU with a total value of 101 billion Euros, while Eurostat lists 58 billion Euros (Seaman, J. et. al 2022). In both the 2000-2009 and 2010-2016 periods, 15 per cent of Chinese FDI went to the European ICT sector, while an increase in the transport and infrastructure sectors has been observed, particularly in recent years (ENTC 2017).

Such data are often estimated, and granular data, in particular at the Member State level, are often not available (ENTC 2017, 2022). Reliable information on FDI from China will be crucial in addressing a wide range of policy challenges in EU Member States. In order to minimise dependencies, for future trade and investment agreements, the expansion of market access for European companies in China could take place and legal certainties for investors could be strengthened in return in those areas in which China invests heavily.

As this example shows, it requires a mix of structural indicators (e.g. FDI in key technologies), data on attitudes and behaviours in the cyber-security sector, and indicators relevant to security policy such as zero-day incident statistics. Waldron (2019) argues that a system of metrics is needed which decision-makers can use and which are accepted within the relevant stakeholder groups. This requires a taxonomy, as well as a common understanding of what we mean by 'European digital sovereignty' and what contribution cyber-security actors need to make here. Last but not least, quantitative and qualitative indicators need to be developed which allow an evaluation to be made of how well directives and regulations have been implemented in the Member States.

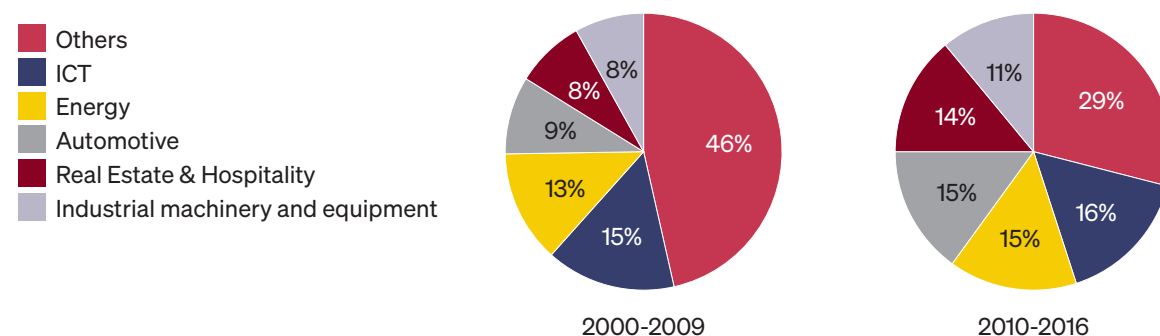
Another essential factor for European strategic autonomy in the digital sector

is cloud computing. This facilitates the provision of computer services via the Internet. This means that companies buy licences to use certain programmes online without having to store them on-site. This allows organisations and companies to access resources more flexibly (depending on location and consumption) and to benefit from scaling effects. Similarly, their data can be stored at a lower cost. Gartner (2019) predicts that by 2025, approximately 80 per cent of organisations will close their traditional data centres in favour of cloud computing. This development is accompanied by a significant increase in the value of the European data market. This is the market where digital data are exchanged as products or services from raw data. According to estimates by the European Commission, the data market in the EU27 is expected to reach 82.5 billion Euros by 2027, with an average annual growth rate of 5.8 per cent (European Commission 2020). The infrastructure in which this data is stored and used is therefore very important.

The United States and China are central to this. As data from the UN Digital Economy Report (UNCTAD 2021) shows, the two countries together own 50 per cent of global Hyperscale data centres, have the highest 5G implementation in the world, own 90 per cent of the market capitalisation of major digital platformers and are responsible for 94 per cent of the funding of AI start-ups. As the European Liberal Forum (ELF) illustrates in its publication 'Cybersecurity in Context', US cloud service providers dominate their European competitors both in terms of business volume and technological innovation (Gamal, N., Martino, L., Nestoras, A. 2022).

Figure 6: China invests heavily in Europe's ICT-Sector

Chinese direct investment in Europe



Source: RHG FDI Monitor

GAIA-X was founded in 2019 to minimise this disparity and to develop a data infrastructure according to European standards. GAIA-X is an international NPO based in Belgium that describes itself as an organisation which wants to network cloud providers in Europe on the basis of 'European values'. Currently, 1800 participants from over 500 institutions participate in GAIA-X (GAIA-X 2022). GAIA-X was massively pushed by the governments of Germany and France in 2019 to create a cloud infrastructure for the European market which facilitates data exchange within the EU based on its laws. The aim is to build a 'powerful, competitive, secure and trusted data infrastructure for Europe' which meets the 'highest aspirations for digital sovereignty while fostering innovation' (UNCTAD 2021). This should also facilitate a single data market in the European Union, which in turn will enable European cloud providers to strengthen the monetisation of data, and thus their international competitiveness.

In this regard, Europe is at a crossroads when it comes to also further developing strategic autonomy within the context of cloud computing. Either Europe's response to the massive dominance of China and the US is to codify standards that apply within the EU, in which case GAIA-X must be developed into an EU-wide standard that must also be used by global cloud providers, which is currently not the case (UNCTAD 2021). This will lead to massive political tensions, especially with the US and its cloud providers. Alternatively, GAIA-X can be further developed so that it is made available to European cloud providers free of charge so that they can implement it in their business models and become more competitive internationally.

The example of cloud infrastructure is just one of many where significantly different access can be observed worldwide between the major global markets in Europe, the US and China. As UNCTAD (2021) shows, in the United States market-based accesses have priority. Data protection and privacy issues are considered from a market perspective and competition policy plays a minor role. In China, the dominance of state intervention is evident; for the state, access to data is essential. Within the EU, regulation based on individual rights of market participants is preferred and competition law is seen as fundamental. Individual rights, which are central within the EU, for example, are therefore not very compatible with US companies, whose business model and regulations are based on the free exchange of data, and Chinese social media applications, where the state has unfettered access to data and content. Conversely, European companies which are confronted with robust regulations are often not competitive globally. Similarly, access by national security agencies varies greatly. As these are fundamentally different accesses, economic, foreign and security policies are therefore inseparable.

The fact that such accesses do not only concern data and its infrastructure, but are a fundamental access to digital elements, can be demonstrated by the example of artificial intelligence, the existence of which massively depends on digital infrastructure and good data (Paschunder and Feierabend 2019). As a result, from a geopolitical perspective, Europe must improve the coordination of foreign, security and economic policy, as European strategic digital autonomy

inevitably elicits tensions with the current technology and market leaders in the USA and China. This is highly relevant, in particular from a security perspective, because within the context of economic espionage, internationally established rules and norms on which cyber-activities constitute legitimate or illegitimate behaviour are largely lacking (Hoffman & Maurer, 2019).

Table 3: International accesses to data-related regulations

	USA	China	European Union
Growth and developement of the digital economy	Mainly market-based	Strong state interventions	Regulations and support within the "recovery plan" after COVID 19
Data protection and privacy	Not historically prioritised; no comprehensive federal laws, but comprehensive laws in some states (California, Virginia)	Regulation focused on enterprises	GDPR on the basis of individual rights
National security	Data for national security is a clear priority	Comprehensive access and control by the state	In principle, competency of the respective Member States
Competition policy	Data is not generally viewed as a competition issues, but is currently subject to antitrust investigations and legal proceedings	Unclear rules as whether data fall under competition rules	Data are part of competition policy
Cross-border exchange of data	Promotion of the free exchange of data	Extensive restrictions	Free within the EU and with some states; trade policy promotes data exchanges, but initiatives which currently promote restrictions

Source: UNCTAD

Table 4: Comparative overview of AI focus in North America, China and the European Union

North America	China	European Union
Public R&D building tech giants	Ambition to become global leader	Focus on responsible, trustworthy AI
Big data collecting monopolies	Social Credit Score	Legal, social, ethical standards
Commercial interest and venture capital	Governmental standardized assessment of citizens, corporate economic and social reputation	GDPR on the basis of individual rights
(Federal Communications Commission) & FTC (Federal Trade Commission) as regulatory bodies	Big data used for disciplinary purposes	Focus on transparency and explainability
Canada: Personal Information Protection and Electronic Documents Act (PIPEDA)	Leapfrogging on Europe and US	Civil law rules for robotics

Source: Puaschunder & Feierabend / ELF 2019

Recommendations

Resilience has been the buzzword in security policy for years, but in Europe, measures were often instigated too late, which meant that an improvement in resilience was not possible. To prevent this from happening in the context of strategic digital autonomy, the following measures are necessary:

- A common understanding of central goals and measures to strengthen awareness communication and knowledge transfer for cyber-security in Europe. In particular, low-threshold proposals, such as the ‘Cyber Weather Report’ of the Finnish National Cyber Security Center, must be established.
- The European Cybersecurity Taxonomy must be expanded to include measurable cyber-security indicators. This must include a mix of structural indicators, data on attitudes and behaviour in the cyber-security field and indicators relevant to security policy.
- In the field of cloud computing, a decision must be reached on whether GAIA-X should be the standard that must also be applied by global cloud providers in Europe or whether GAIA-X should be an infrastructure to improve the competitiveness of European cloud providers.
- The coordination of foreign, security and economic policies must be improved in order to strengthen European digital sovereignty. At the international level in particular, the priority must be to establish which norms and behaviour constitute illegitimate behaviour in the context of economic espionage.
- Europe must invest massively in its own connectivity to create and control its own 5G and fibre infrastructure and be more secure from possible Chinese manipulation.

2.2 Defence and Security

While a few years ago there was still talk among security experts of a blurring of the line between war and peace, now the ‘age of perpetual conflict’ is upon us (Kolbe, 2020). While it is easy for autocratic governments to exploit the open, global system and close interconnectedness of liberal democracies, the very freedom of the global West and other democracies often ties their hands behind their backs when it comes to defending themselves against attackers (Bunde, 2022; Cooley and Nexon, 2022). Liberal democracies have good reasons not to engage in mass surveillance of Internet users and filtering of Internet content, but they pay a price for preserving the fundamental rights and freedoms of their citizens.

Democracies are easier to attack because they have to be defended against fears and conspiracy theories which are easily fanned by digital mass media. A large proportion of the disinformation campaigns aimed at influencing free elections can be clearly traced back to Russia (Nakashima and Timberg, 2020). This fact is now also known to the general public. But the knowledge of this does not provide immunity against these attacks. When, for example, approval ratings for sanctions against Russia slowly began to fall in Austria at the end of August 2022, this was partly the result of visual Russian propaganda showing an icy Europe. Russia easily managed to embed the link between sanctions against Russia and the supposedly immediate consequence of freezing to death in a winter completely without gas (Metzger et. al., 2022).

Cyber-attacks, which in the broadest sense also include disinformation campaigns, can be used as a method of hybrid warfare, even if most cyber-attacks do not reach the level that one could define as an act of war. However, if there is a cyber component to a military conflict, recent examples in particular show that it is not necessarily just the countries involved in the conflict themselves that are affected. On the one hand, spillover effects are possible (Cerulus, 2022). On the other hand, partner states that support one conflict party without themselves directly participating in the conflict can also be the target of cyber-attacks within the context of a violent conflict of this kind. Using the example of Western support for Ukraine through arms deliveries, it is easy to explain that networks of industrial producers of equipment important for Ukraine would be a worthwhile target of cyber-attacks by Russia. This is now where defence and security considerations overlap in terms of defence against and deterrence of cyber-attacks by other

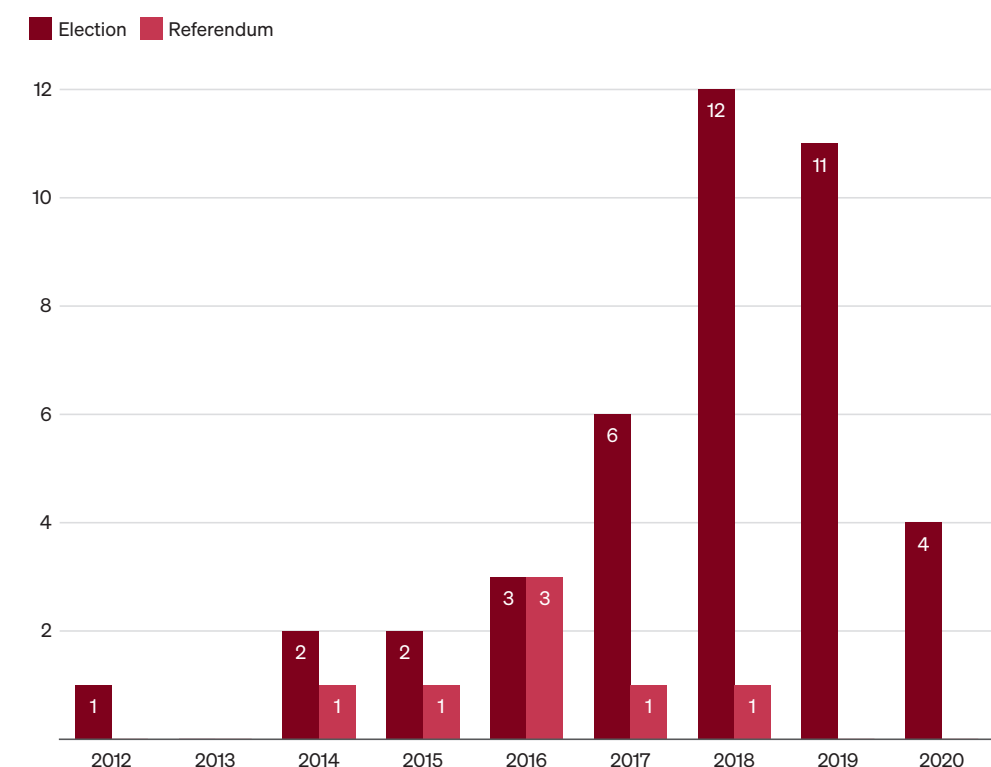
states or non-state actors. Cybersecurity is not the same as cyber-defence, but the two are closely related.

In recent years, various European states have publicised the fact that there have been cyber-attacks on their networks, apparently with the aim of manipulating elections. The methods used vary, ranging from spear phishing to data theft, malware, DDoS attacks and the threat most commonly cited: disinformation spread over the Internet (ENISA, 2019:6).

The international Cyber Policy Centre of the Australian Strategic Policy Institute (ASPI) think tank has identified 41 elections and 7 referendums between January 2010 and October 2020 which were affected by cyber-attacks in the broadest sense (i.e. including disinformation campaigns, etc.). The majority of these attacks took place in highly digitised states of the global West, especially in European states and the USA. Insofar as the attackers were identified, the ASPI data show that the world is divided into cyber-zones of influence as far as attacks with a cyber-component are concerned. According to the data, Europe’s biggest threat is Russia, and many Asian states, in particular Taiwan, are struggling with cyber-attacks probably originating from China. Attacks from Iran hit the USA, the UK and Israel. The USA is also being targeted by China, Russia and North Korea (ASPI: 13f). Hostile military intelligence services play a major role in the attacks.

Figure 7: Elections and referendums are becoming targets of cyber-attacks more frequently

Cases of foreign interference through cyberattacks by year and type of political process



Quelle: Australian Strategic Policy Institute

Figure 8: Regional distribution of politically motivated cyber-attacks on elections and referendums



Source: Australian Strategic Policy Institute

The extent to which various states are vulnerable to cyber-attacks on elections and referendums does not just depend on their cyber-capacities. As explained at the beginning of this paper, the cyber-focus is on the individual. Trust of the individual in the institutions of the state and in the information architecture (state-owned and through privately run media companies) is therefore essential. In addition, the general health of a political system also counts. Very politically divided societies in particular are often more vulnerable (Lim and Hansen, 2018). Furthermore, the degree of digitisation of a state, as mentioned above, also plays a role (Conley et. al., 2020).

While in traditional armed conflicts, despite often huge collateral damage to civil society, a large part of the conflict took place between the militaries of hostile states, cyber-attacks focus on civil targets. Democratic processes, administration and all sorts of sectors of the economy are directly targeted. In the defence against such attacks, predominantly non-military actors also play the main role. Successful defence is to a large extent small-scale and requires that the various actors within a state should be made immune towards attacks. In addition to societal measures and military defence, foreign policy instruments, if used properly, are also effective.

The issue of attribution in particular – public identification of the attacker – plays a major role in this regard, as well as (cyber) sanctions as a consequence. The European Union, often not the important actor in foreign policy that it would like to be, could play an essential role in the fight against cyber-threats in the world. As a community of states built, at least on paper, on values of peaceful coexistence and respect for the rights of others, the EU could act as an advocate for de-escalation

in the cyber-domain worldwide. Peaceful conflict resolution, dialogue, capacity building in the defensive sector and various preventive measures could become the Union's trademark in the cyber-domain. The knee-jerk reaction of political decision-makers, even in the cyber-domain, is to focus on rearmament for the purpose of deterrence. However, the EU's response must be de-escalation. The more malware that enters the world through digital armament, the greater the risk of its theft and use by the wrong people. Deterrence does not work in the digital space through armament, but through strong alliances, attractive locations for IT professionals, by making an attack as costly and time-consuming as possible through strong defensive components. This may not sell well politically, but it is the only way Europe can become more cyber-secure.

Furthermore, the EU and its Member States could deter cyber-criminals from attacking by standing united and demonstrating that it is prepared to punish attackers for their actions, or to make the cost of such an attack prohibitive for the attackers. The first deployment of the EU Cyber Rapid Response Team in Ukraine together with US partners was a first step in this direction (Liedekerke and Laudrain, 2022). Further cooperation with NATO, which also has 24-hour rapid response teams, also makes sense.

While the overwhelming majority of international legal experts agree that international law is also applicable to cyberspace, there are often even fewer consequences for virtual breaches of law, if that were possible. One difficulty here is the so-called attribution – that is, the assignment of a specific attack to the country from which it originated. In the past, there have sometimes been various reasons for the silence of entire governments about the identities of the perpetrators. On the one hand, a successful cyber-attack on a government or a large company is accompanied by a certain loss of face, because one has obviously not protected oneself well enough against it. This can also have political costs for those in power. Companies, on the other hand, suffer reputational damage. Suffering a major data leak is already a tragic event for most companies. If it happens more than once, it is natural for the company's clients to think that their data is not in good hands. Another reason for not naming the perpetrator after an attack, which particularly concerns attacks at state level, is that no state can simply let such an attack on its systems go unanswered. The state which has suffered the damage and can name the attacker is expected to defend itself, whether by means of retaliation, economic sanctions or other means. States which have economic interests in the aggressor country are often particularly reluctant to take public steps against it. Developments in recent years, in particular in connection with Russian attacks, but also Chinese, Turkish and Iranian attacks, suggest that Europe in particular could act differently in the future on the issue of attribution.

Another way to deter attacks on the European Union would be for the EU to act quickly and in a coordinated manner when it comes to naming attackers (Liedekerke and Laudrain, 2022). This does not only apply to attacks against the Union itself. The EU could choose for itself the role of publicly naming illegal or irresponsible behaviour in cyberspace, such as espionage or sabotage, or the

irresponsible export of offensive cyber-weapons (ALDE 2022). Since conventional arms export control is not possible for cyber-weapons, the only form of control is the exposure of such exports by other stakeholders. The goal must be a world in which powerful states regulate themselves and invest more in defence than in offensive weapons, while helping more vulnerable states build effective cyber-defences.

Europe has a cyber-sanctions regime which has proven to be very dynamic in that it was used shortly after its establishment. Improvements can be made here in terms of accuracy. Cyber-sanctions target potential attackers' freedom to travel and assets existing within the EU, but attackers are often individuals who neither have assets in the EU nor wish to enter the EU.

The Strategic Compass (Council of the European Union, 2022), adopted by the European Union in spring 2022, aims to make the EU stronger and more resilient so that it can better protect its citizens and credibly advocate for peace and security on the international stage. The Strategic Compass is intended to be the roadmap which leads the Union towards strategic autonomy. It also envisages close cooperation with partners who share European values. It is possible, however, that the EU will also have to cooperate with countries which do not share its values but have a common security interest with Europe, particularly in the area of cyber-security/cyber-defence. This will only be possible through ad hoc cooperation and not through the conclusion of international treaties, as has been the customary multilateral practice up to now.

Recommendations

- As can be seen from its actions against Russia since the invasion of Ukraine, the Union is most effective when it is united and determined. For this to be possible in the area of cyber defence, there are a number of points on which the Member States must quickly reach agreement. One of these is that the Union should have a common approach to the issue of exploits or zero days. Exploits traded on the digital black market are a dangerous offensive cyber-weapon. The European Union should establish common rules on whether governments can buy exploits and use them, or not. In addition, at least two EU states have been publicly stating that they are developing offensive cyber-weapons. A kind of 'internal' mutual control within the Union prevents any arbitrariness and creates trust between states.
- In order to curb the resale of exploits among cyber-criminals, the EU should offer financial incentives to find and report exploits to the operators concerned before they can be acquired by attackers and used in an attack. This measure can also be implemented at Member State level if consensus cannot be found at EU level.
- There will be no Union without offensive cyber-weapons, which already exist in some countries. In the spirit of a de-escalation, peacemaking and general security-promoting policy, EU states should aim to conduct offensive operations only with a view of deterring an adversary from launching an attack against the EU or a Member State.
- At the same time, it is important to be self-assured vis-à-vis larger partners such as the Five Eyes states. Europe should be the only power that determines under which conditions partner states outside the EU are allowed to operate in European networks. There needs to be a standard process including Prior Notification between Europe and its partners, so that such any intervention in the sovereign digital space of a state, whether justified or not, is carried out systematically and is not determined by the law of the strongest.

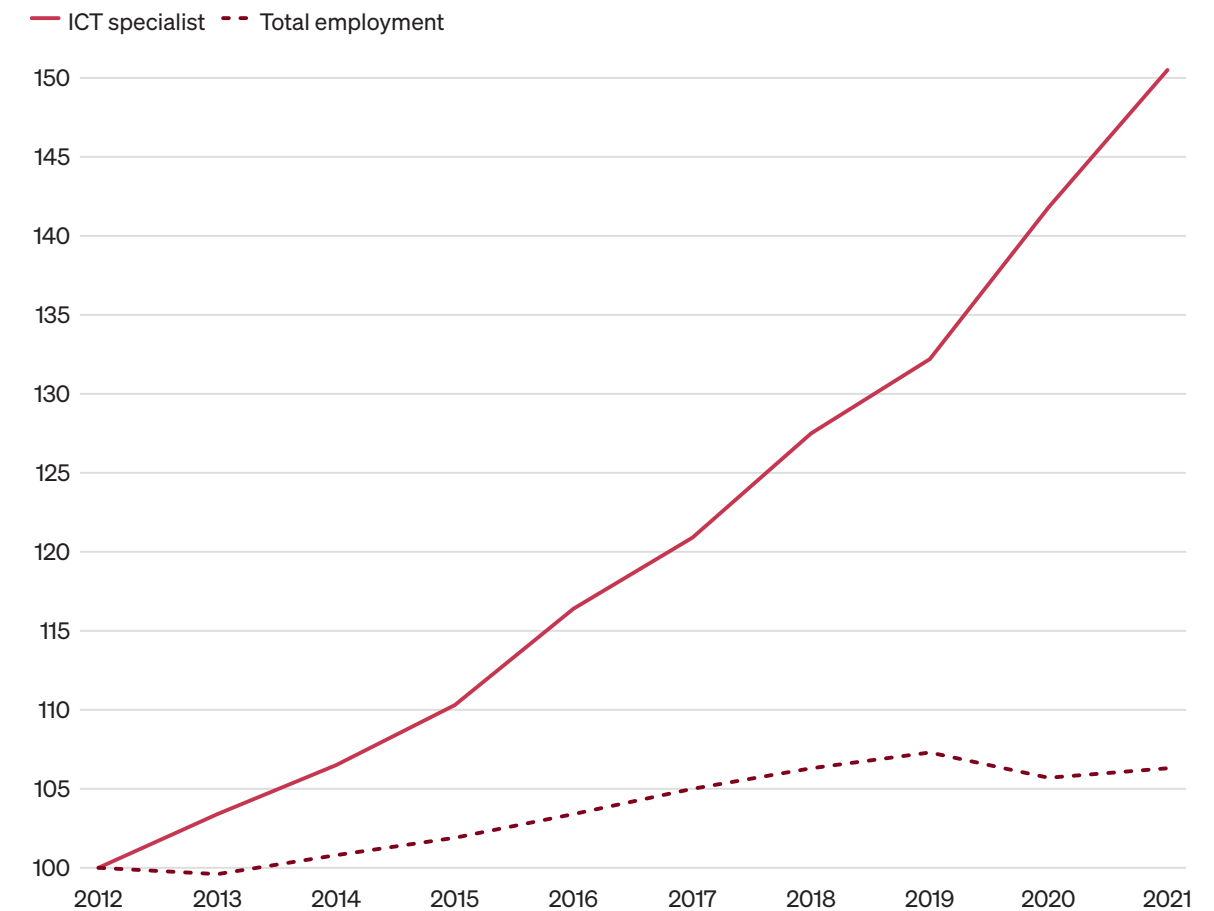
2.3 Skills and Skilled Workers

With growth rates mostly in excess of 10 per cent and a European market worth over 36 billion Euros, the cyber-security sector is one of the fastest growing markets (Statista 2022a, b). This also means that a corresponding workforce potential is necessary to meet the demand for security solutions. There are many parallels here with the supply or shortage of skilled workers in the Information and Communications Technology (ICT) sector. This sector has expanded massively in recent years. Between 2012 and 2021, the number of ICT specialists in Europe grew by more than 50 per cent, while the total workforce increased by 6.3 per cent in the same period, meaning that there are now almost 9 million people working in the ICT sector in the European Union (Eurostat 2022).

According to an analysis by ENISA (2020b), about 13 per cent of all ICT jobs are in the cyber-security sector and on the basis of Eurostat data, it can be assumed that almost 1 million jobs within the EU are related to cyber-security. At the same time, the ICT sector is the one sector which finds skilled workers particularly difficult to recruit across Europe. According to surveys by Eurostat (2022b), 55 per cent of all companies have problems hiring suitable ICT specialists. This is particularly true in the Czech Republic (76 per cent), Austria (74 per cent) and the Netherlands (71 per cent).

Figure 9: Massive increase in ICT employment compared to total employment

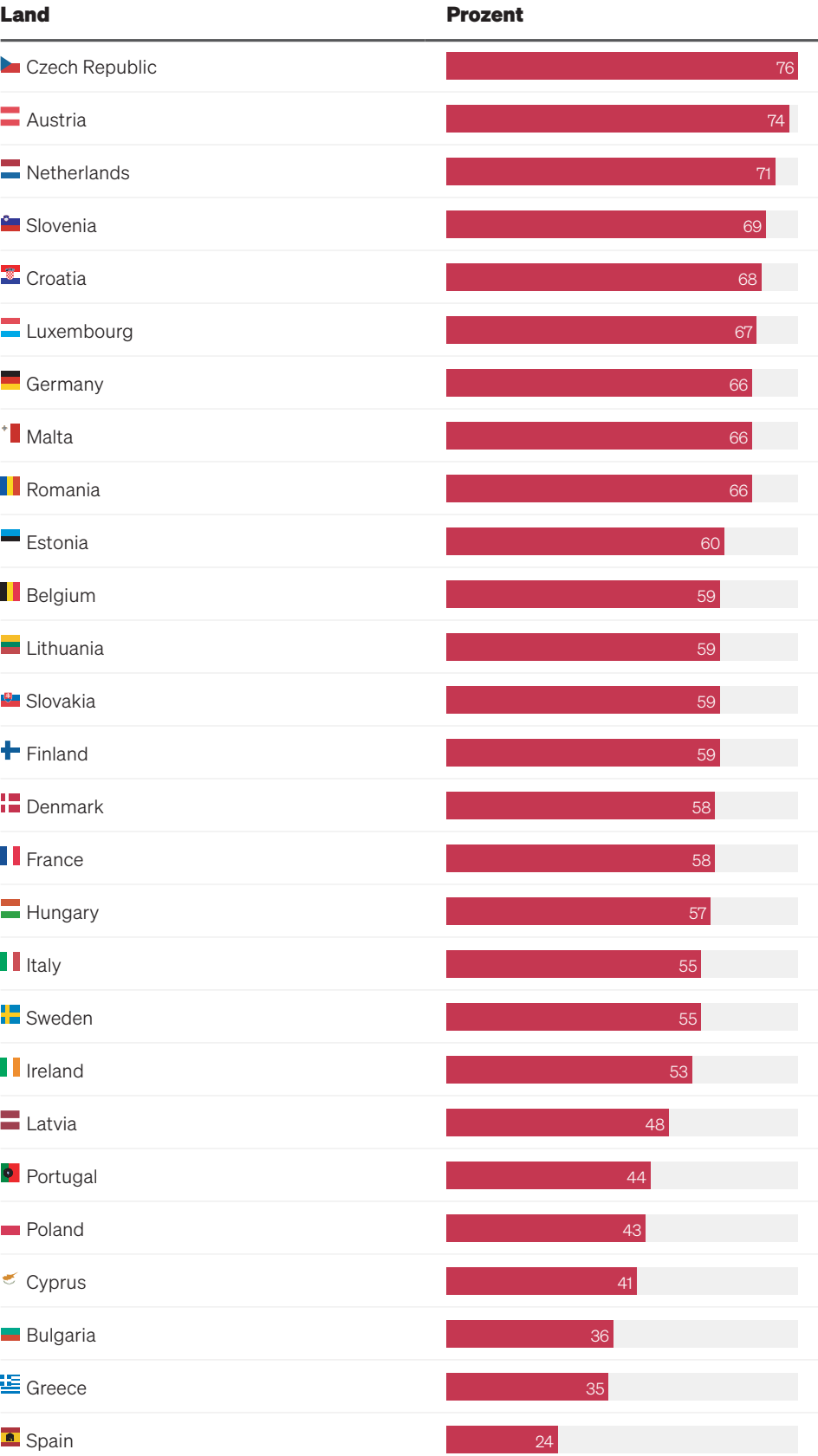
Relative development of employment, 2012=100



Source: Eurostat

Figure 10: Many parts of Europe have significant shortage of ICT skilled workers

Percentage of companies that have difficulties filling vacant ICT positions

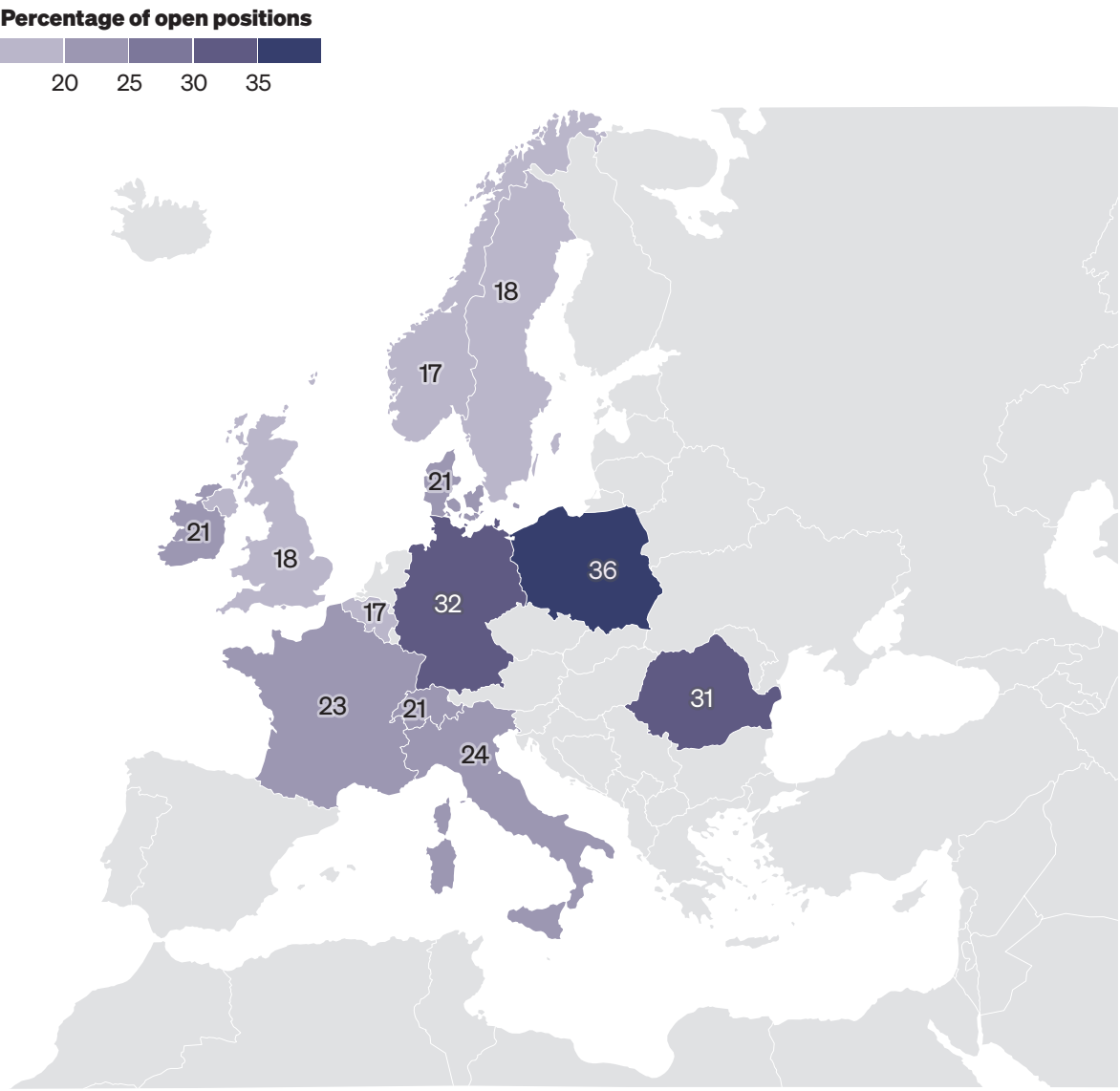


Source: Eurostat

Looking at the figures and focussing on company size, small and medium-sized enterprises in particular have difficulties filling positions (Eurostat 2022b). These problems are also found in the cyber-security sector. Based on an analysis of LinkedIn data in 12 EU Member States, Microsoft forecasts that these countries will have more than 60,000 vacancies. The situation is exacerbated by the fact that within one year (2021 to 2022) the demand for cyber-security skills has increased by 22 per cent (Microsoft 2022).

Figure 11: Many open cybersecurity positions across Europe

Analysis of unfilled positions on LinkedIn



Source: Microsoft & LinkedIn

The European Cyber Security Organisation ESCO (2022) estimates that, in the European Union as a whole, there is a shortage of up to 500,000 skilled workers. That this is not just a European problem is indicated by international surveys which suggest that there are also up to 3.5 million vacancies worldwide, that the gap between vacancies and the workforce has risen by around 13 per cent and that the potential workforce would have to increase by 80 per cent in the coming years to meet current demand (Gamal, N., Martino, L., Nestoras, A. 2022).

At the European level, huge efforts are being made to address this shortage of skilled workers. ENISA has for many years been working on programmes to raise awareness of cyber-security measures and on training programmes for cyber-security specialists (ENISA 2020b, 2021d). The 2020 EU Cybersecurity Strategy has a significant focus on cyber-security research and training and has allocated 2 billion Euros to the ‘Digital Europe Programme to Advance the Digital Transition’ (European Commission 2021, Gamal, N., Martino, L., Nestoras, A. 2022). According to ENISA (2021e), this has meant that, in the coming years, the number of university-trained specialists will double.

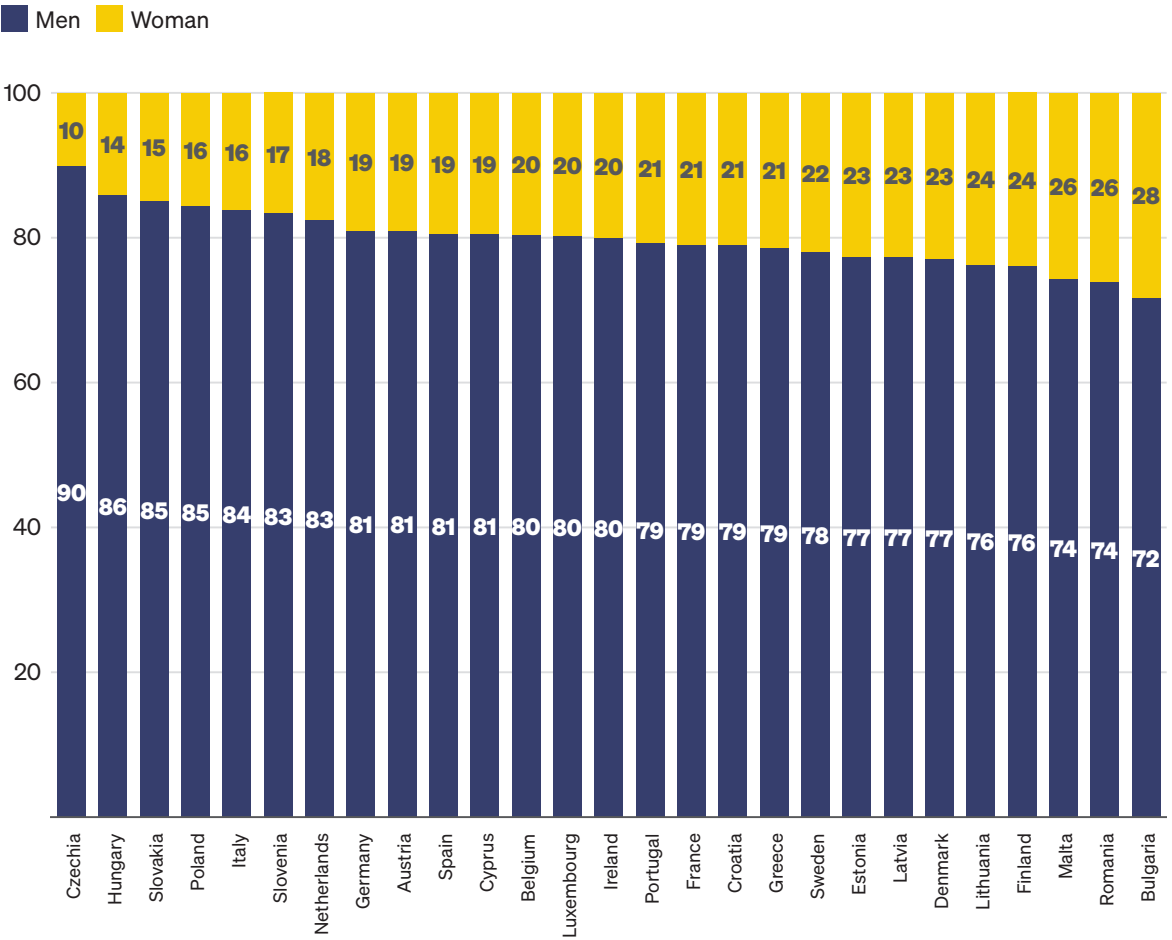
Although progress is being made, this far from covers the number of skilled workers needed. The reasons for the workforce shortage are manifold, but one aspect in particular stands out: the unequal distribution of men and women in the ICT and cyber-security sector compared to other industries. According to Eurostat (2022), over 80 per cent of all ICT workers are men.

In the cyber-security sector, analyses suggest that in the last five years the proportion of cyber-security workers within the ICT sector has more than doubled from 11 to 25 per cent (Gamal, N., Martino, L., Nestoras, A. 2022). According to these analyses, the deficit is particularly high in Europe, where only 11 per cent of all jobs are filled by women. Microsoft (2022) is coming to similar conclusions. In the countries studied, the proportion of women ranged from 13 (Poland) to 25 per cent (Italy). The increasing demand for skilled workers can therefore only be met if the proportion of women is massively increased. This is all the more urgent as the Russian war of aggression has significantly increased cyber-attacks in Europe (Gamal, N., Martino, L., Nestoras, A. 2022).

Alongside the gender gap, the second major area ripe for development in the skilled worker sector is education and training and related curricula and certification schemes. The ENISA Higher Education Database (ENISA 2022) is the largest verified database of academic training programmes in the European area. As of September 2022, 124 programmes can be taken in 25 EU Member States. There are two problems which are immediately apparent: Firstly, an obviously uneven distribution between EU Member States. While Germany, with over 80 million inhabitants, has only two courses, Spain has 23. With 10 courses, Austria has about the same number as all the Nordic countries put together. Secondly, specialisations within the framework of a Master’s programme make up the majority of the courses. Four out of five programmes are Master’s programmes, while EU-wide, there are only 20 Bachelor’s

Figure 12: Large gender gap in the ICT sector

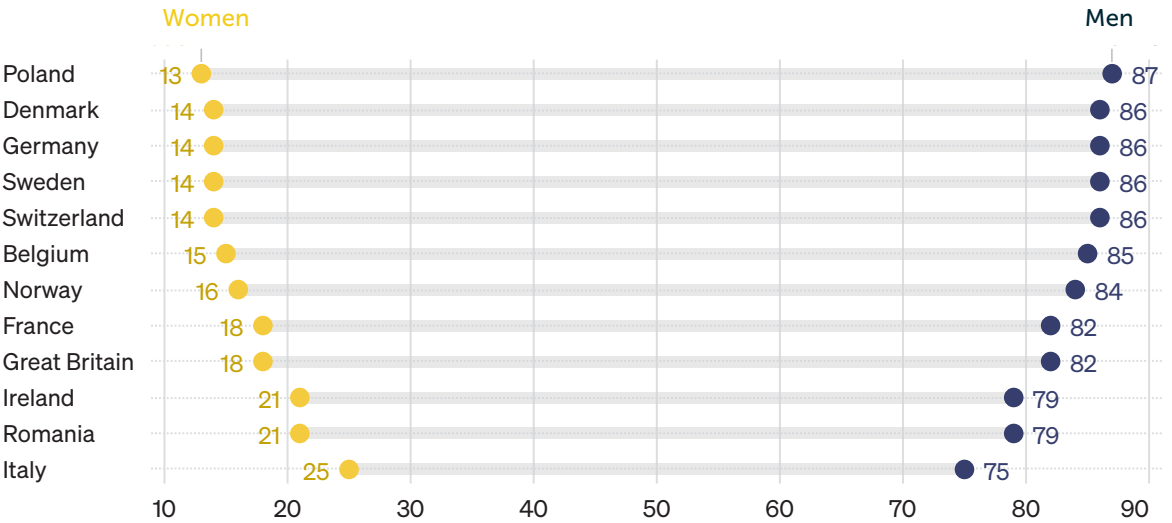
Distribution of ICT workers by gender, 2021



Source: Eurostat

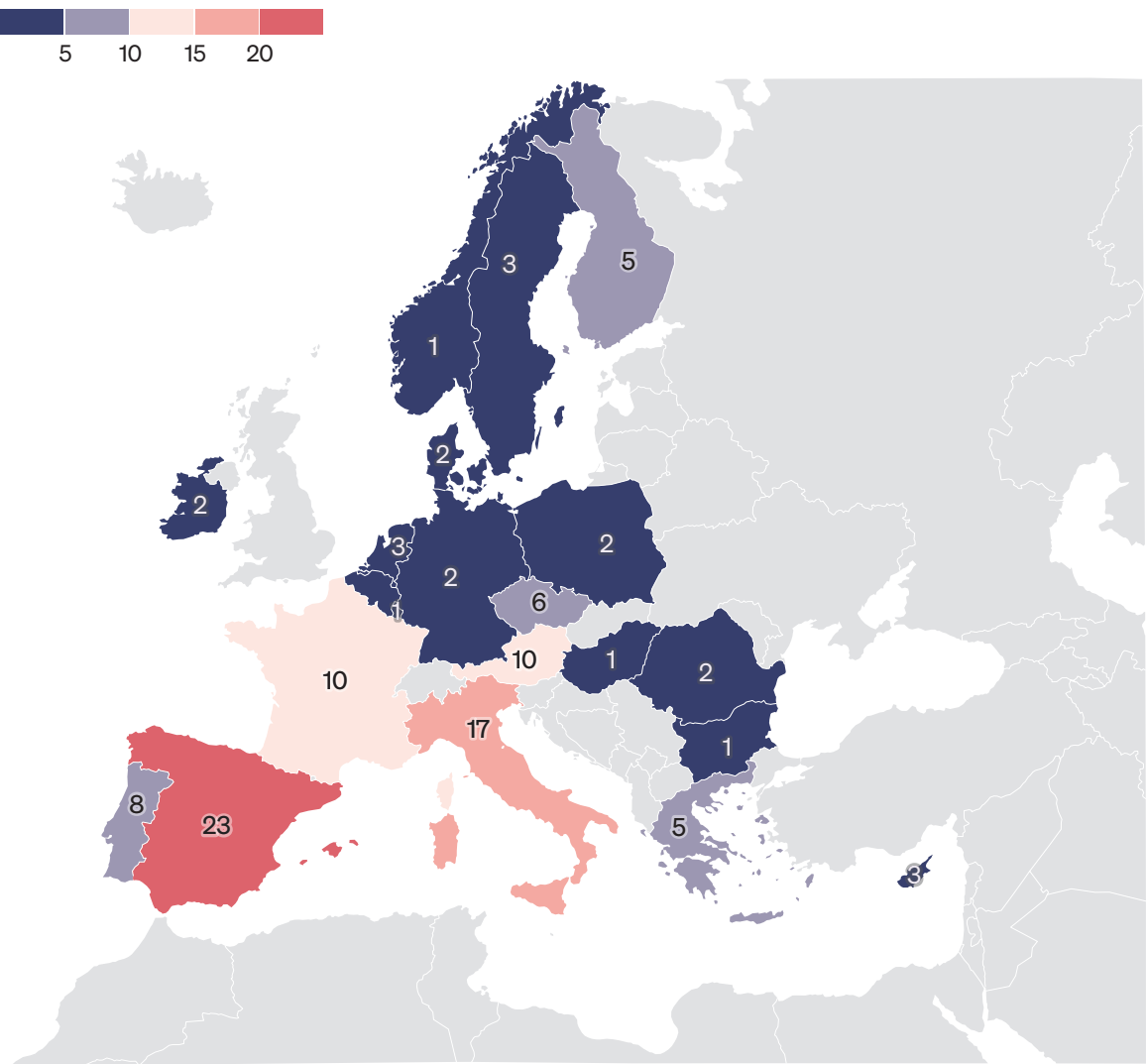
Figure 13: Proportion of women in the cybersecurity sector

Distribution of cybersecurity workers by gender



Source: Microsoft & LinkedIn

Figure 14: Number of cybersecurity study programs in Europe



Source: ENISA

programmes. This is a problem in particular with regard to accelerated career entry. In addition, there are no minimum standards for curricula (Gamal, N., Martino, L., Nestoras, A. 2022, ENISA 2020b, 2021e).

However, the lack of minimum standards is not limited to the university sector. Similarly, there are no standardised and certified occupational profiles within the European Union (Gamal, N., Martino, L., Nestoras, A. 2022, ENISA 2020b, Blažič 2021). This is, however, central to ensuring the long-term demand for skilled workers in Europe is met. Every occupation can be divided into work activities. In order for a work activity to be performed successfully, certain skills are needed (Eder/Feierabend 2017, Blažič 2021). Competency and role profiles help to define essential occupations into fields of work and to standardise which work activities and skills are necessary for the respective occupation (Blažič 2021).

In the United States, competency and role profiles are defined in the NICE initiative (National Initiative for Cybersecurity Education). NICE defines seven specific areas of expertise and at least two areas of expertise are assigned to each role profile. For each job profile, work activities are then defined in all categories and the skills required with them are specified (Blažič 2021). The NICE scheme simplifies the search for employees in the US and allows for a granular representation of existing and missing competencies. As noted by both ENISA (2020b) and a variety of other institutions and publications (Gamal, N., Martino, L., Nestoras, A. 2022), the lack of a European NICE equivalent is one of the most significant structural barriers to addressing the skills shortage in the EU. The basis for a Europe-wide scheme could be previous voluntary certification schemes such as the 'NIS (Network and Information Security) driving licence' being developed by ENISA or the results of a pilot project of the CCN network (Blažič 2021).

It is important to bear in mind that role profiles do not only comprise technical skills. Martin and Collier (2019) argue that an interdisciplinary approach which goes beyond technical skills is preferable as it allows for a better understanding of cyber-security challenges. Similarly, Dawson and Thomson (2018) argue that the complex challenges in the cyber-domain need more consideration of social aspects. They define skills that are particularly relevant for cyber-security skilled workers: systematic thinking, good communication, ability to collaborate, continuous learning and a minimum level of knowledge of basic rights and democratic values. This would also make it possible to strengthen an area that has often been neglected in the discussion about skilled workers: adult education. In contrast to the cyber-security sector, with the European Qualification Framework (CEDEFOP 2022), Europe has an excellent programme for defining learning objectives, knowledge, skills and not least, a comparability of education and training. This is the place to start and define tailor-made training programmes on the basis of a European NICE equivalent. In particular, in view of the obvious shortage of skilled workers, it would be a relief for European companies if existing staff could take over certain work activities.

One of Europe's greatest strengths to date has not yet been exploited: apprenticeship training. In many countries, it is an essential building block for economic and labour market policies. While many ICT occupational fields have apprenticeship training, it is lacking in the cyber-security sector. Countries such as Germany or Austria, which have a long tradition of dual education, could develop appropriate training courses here within the framework of pilot projects. Formal school education can also be used as a starting point. Austria, for example, has a type of secondary school known as the Höhere Technische Lehranstalten (HTL) or Higher Technical Education Institute, which focusses on technical training. This makes it possible to embed skills within school education.

Recommendations

The massive growth of the cyber-security industry leads to problems similar to those experienced by the entire ICT sector: an ever-increasing shortage of skilled workers, diversity problems and often weak political countermeasures. Even though the number of skilled workers available is growing, the following measures are indispensable:

- At university level, EU-wide minimum standards for curricula must be established. The number of Bachelor's programmes and academic in-service training initiatives must also be expanded.
- The massive gender gap must be reduced. This can be done, for instance, by linking funding with diversity measures, expanding awareness-raising initiatives or internships.
- Weaknesses in the certification area must be addressed. A standardisation of professions, their work activities and the associated skills is needed, similar to the NICE initiative in the USA.
- Pure academisation will not resolve the problem of skilled workers. Therefore, adult education must be strengthened by providing specific training for professionals already working in the field. If certain work activities can consequently be taken over, this will relieve the burden on European companies.

2.4 Cyber-economy and Cyber-Security of SMEs

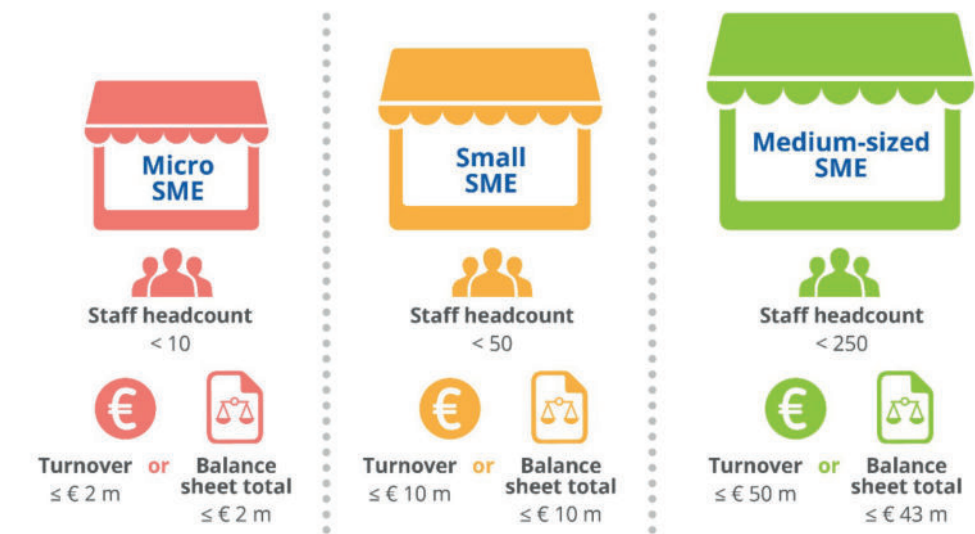
The European Union is the largest single market in the world and an economic superpower. This makes it all the more crucial to recognise cyber-attacks as one of the greatest threats and also to build a cyber-security infrastructure that will secure the continent's future economic prosperity. Hardly any other industry shows such growth rates as the IT sector.

New technologies such as mobile or cloud computing are not only revolutionising the IT markets, they also pose challenges for cyber-security. ENISA (2016) estimates that a lack of cyber-security could cost the EU up to 640 billion Euros in the event of large-scale coordinated attacks, for example on smart grids, which would lead to Europe-wide blackouts. Faced with the prevailing cyber-threats, security concerns play a central role in politics, administration and business. If these cannot be resolved through adequate infrastructure and trained personnel, the adoption of innovative technologies in Europe will slow down even more, preventing European companies from making the most of innovations to increase their economic efficiency and become globally competitive.

Worth 36.3 billion Euros, the EU cyber-security market is itself a key economic driver with security services accounting for the largest share at 21.1 billion Euros, which compares favourably to the cyber-security markets in other regions around the world. At the same time, the annual growth rate in Europe is lower than in other regions, in particular the United States (Statista 2022a, ENISA 2016). The weaker growth can only be explained by lower spending by small and medium-sized enterprises, as the larger European firms spend similar amounts on cyber-security as large firms from other regions around the world (ENISA 2016). However, many standards and specifications only apply to 'critical infrastructure' and large companies. The NIS 2 Directive currently under negotiation also excludes SMEs from its regulatory framework. It is, therefore, all the more important to ensure the security of small and medium-sized enterprises by expanding knowledge and disseminating ICT security standards. SMEs form the backbone of the European economy. According to data from the European Commission, 99 per cent of all companies in the EU are small or medium-sized enterprises. They employ around 100 million people across Europe and generate more than half of the European gross domestic product (European Commission 2022b). At 93 per cent, so-called micro SMEs (companies with fewer than ten employees) are the

predominant company size.

Figure 15: SME definitions



Source: ENISA (2021)

There is a widespread perception that cyber-attacks are only carried out on large organisations, possibly because that is where there seems to be the most to gain. However, this is not correct. Organisations can be attacked in similar ways regardless of their size. SMEs are often even more vulnerable in particular because high profits can be gained from ransomware at a relatively low cost (ENISA 2021b). Statistically, large companies are more likely to report being exposed to cyber-attacks. However, successful attacks that lead to data leaks often take place in small and medium-sized enterprises, as Accenture’s ninth ‘Annual Cost of Cybercrime’ study (Accenture 2019) shows. In addition, as a media investigation in Germany recently made abundantly clear, there are also glaring deficiencies on the part of the authorities, specifically the police, in the training of officers responsible for recording cyber-crimes. Today, cyber-threats have also become a recognised business risk for small and medium-sized enterprises. According to a representative Europe-wide survey of small and medium-sized enterprises, 41 per cent of respondents said they had already been the victim of phishing emails, and web-based attacks and malware are also tools frequently used to attack SMEs.

Figure 16: Distribution of cyber-security incidents based on their origin



Source: ENISA (2021)

Successful attacks also target weak passwords (this was a success factor in 56 per cent of all successful attacks on SMEs) or unlocked devices (44 per cent). This shows that it is often not complex technical problems that lead to security breaches. In general, ICT security has a high priority in European enterprises. Eurostat surveyed seven ICT security measures such as strong password authentication or data backup in a separate location. 92 per cent of all companies use at least one of the surveyed security measures (Eurostat 2022c). However, security processes are often neither documented (only one third of all companies do this) nor are they regularly evaluated.

Table 5: ICT security in Europe’s enterprises

	At least one ICT security measure used	Documents on ICT security measures, practices or procedures	The ICT security documents were defined or reviewed within the last 12 months
EU-27	92	33	24
 Belgium	94	34	27
 Bulgaria	85	18	13
 Czech Republic	94	32	26
 Denmark	97	56	42
 Germany	97	37	27
 Estonia	86	27	18
 Ireland	93	54	42
 Greece	74	15	10
 Spain	92	33	25
 France	94	26	18
 Croatia	90	41	25
 Italy	93	34	28
 Cyprus	83	32	24
 Latvia	98	42	25
 Lithuania	93	36	22
 Luxembourg	93	27	22
 Hungary	86	17	13
 Malta	92	32	25
 Netherlands	96	42	32
 Austria	91	36	28
 Poland	87	23	18
 Portugal	98	28	21
 Romania	73	17	11
 Slovenia	84	35	26
 Slovakia	90	28	22
 Finland	97	44	35
 Sweden	95	52	39

Source: Eurostat

Table 6: Many cybersecurity standards are not used in small and medium-sized business

Less than 30% of SME	More than 70% of SME
Employ a security officer	Regular backups
Removable media management	Antivirus program installed
Incident response structure	Firewall
Information Security Management System	Systematic updating of software
Business continuity and Disaster recovery plan	
Regular cyber information for employees	

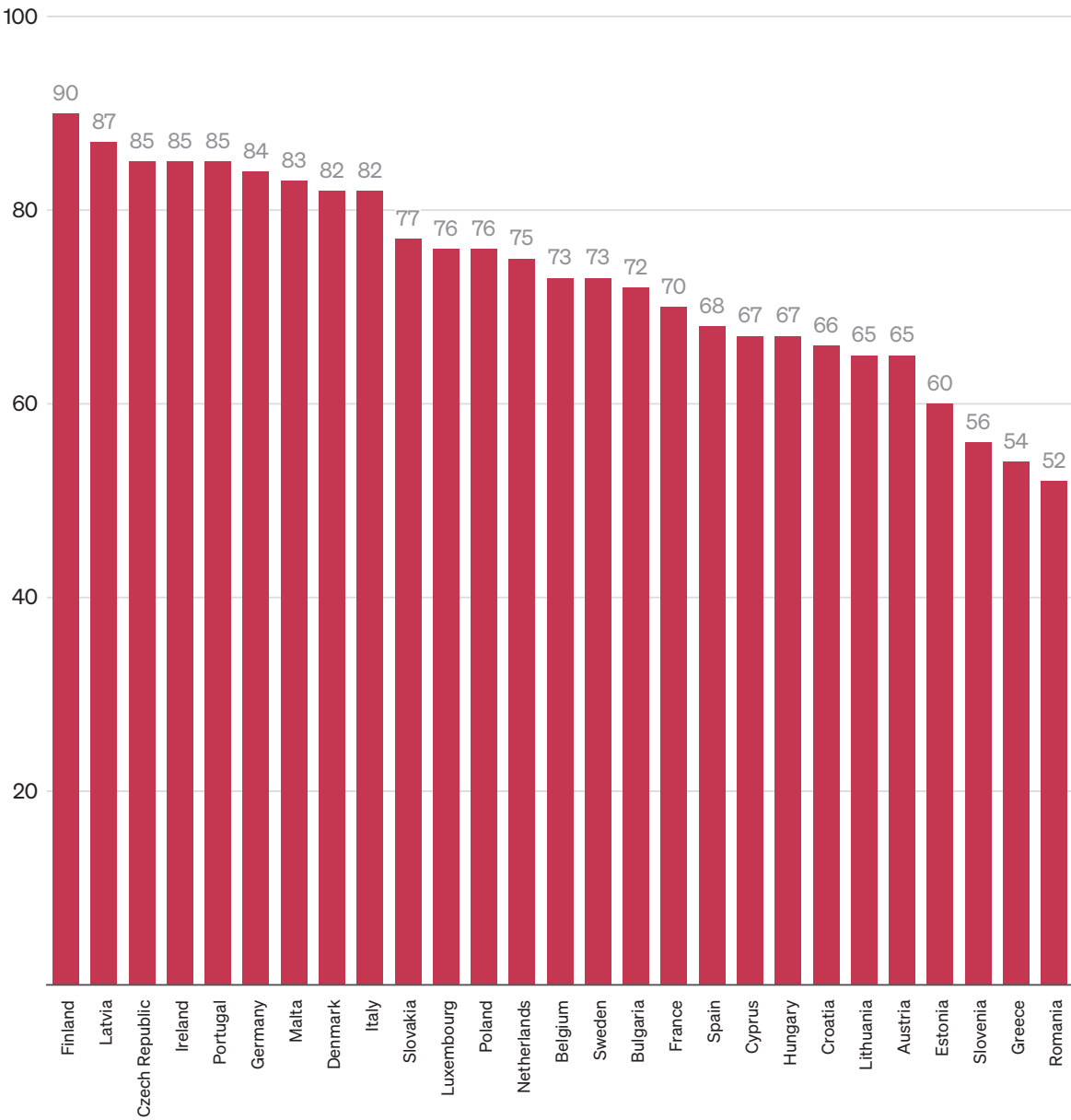
Source: ENISA

In principle, this also applies to small and medium-sized enterprises. In a survey of small and medium-sized enterprises in Europe commissioned by ENISA, over 70 per cent of the companies stated that they made backups, installed an anti-virus programme or regularly updated the software used. (ENISA 2021b). However, other security practices such as a employing a security officer or drawing up plans to use mobile data carriers are not widespread. Less than 30 per cent reported making use of them.

While weak passwords are often a major key to successful cyber-attacks, 76 per cent of all European small and medium-sized enterprises have authentication systems that require strong passwords. At the same time, there are significant differences between businesses within the European Union. While nine out of ten Finnish SMEs have implemented this standard, this is the case for barely half of all small and medium-sized enterprises in Greece (54 per cent) and Romania (52 per cent).

Figure 17: Small and medium-sized enterprises with secure passwords

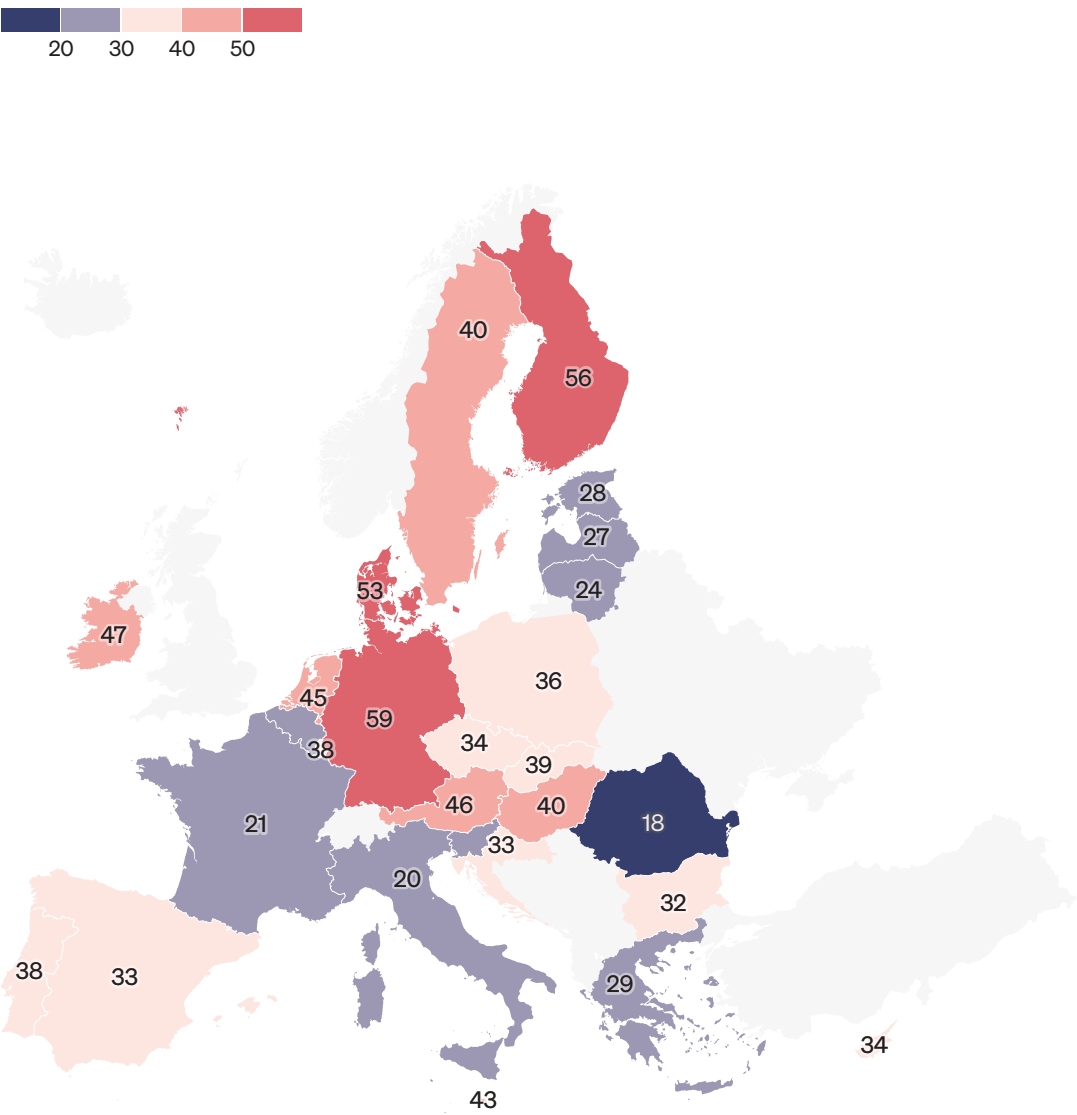
Percentage of small and medium-sized enterprises that state their company's use standards for strong passwords



Source: ENISA

Small and medium-sized enterprises are much less likely to use data and email encryption, which has become a common practice for protecting data and sensitive information. Only 37 per cent of all SMEs use this and significant differences within the European Union can also be seen in this regard. While a majority of SMEs in Germany (59 per cent), Finland (56 per cent) or Denmark (53 per cent) use encryption, this is only the case for one in five companies from France or Italy.

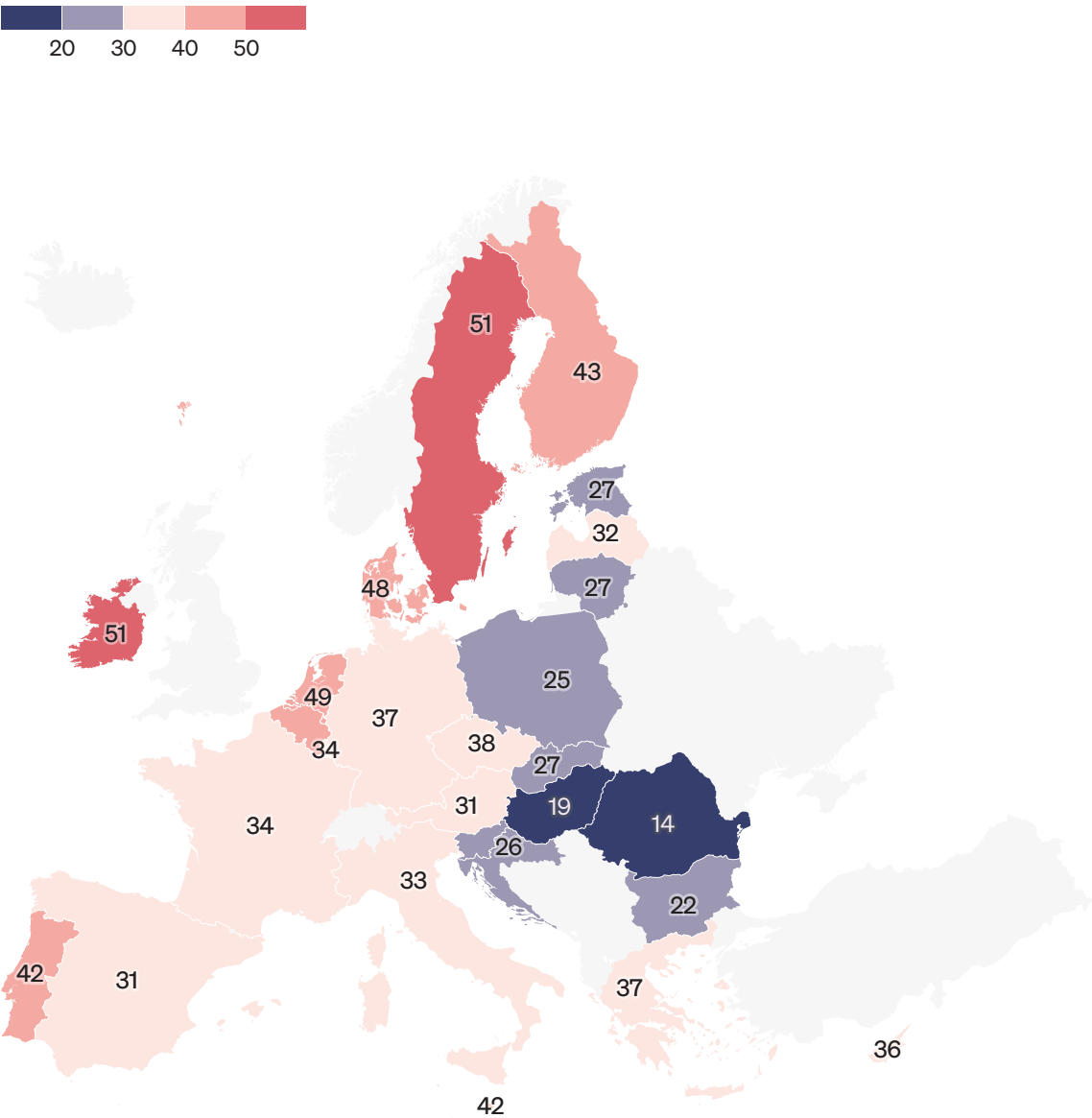
Figure 18: SMEs which use encryption techniques for data, documents or emails



Source: Eurostat

Besides software solutions, security procedures and tests, for example performing penetration tests or a test of backup systems, play a vital role. Similar to the situation with encryption techniques, small and medium-sized enterprises throughout Europe are having to play catch-up. Only just under one in three SMEs regularly carries out security tests. These are widespread in Sweden (51 per cent), the Netherlands (49 per cent) and Denmark (48 per cent), while SMEs in Bulgaria (22 per cent), Hungary (19 per cent) and Romania (14 per cent) hardly ever carry them out.

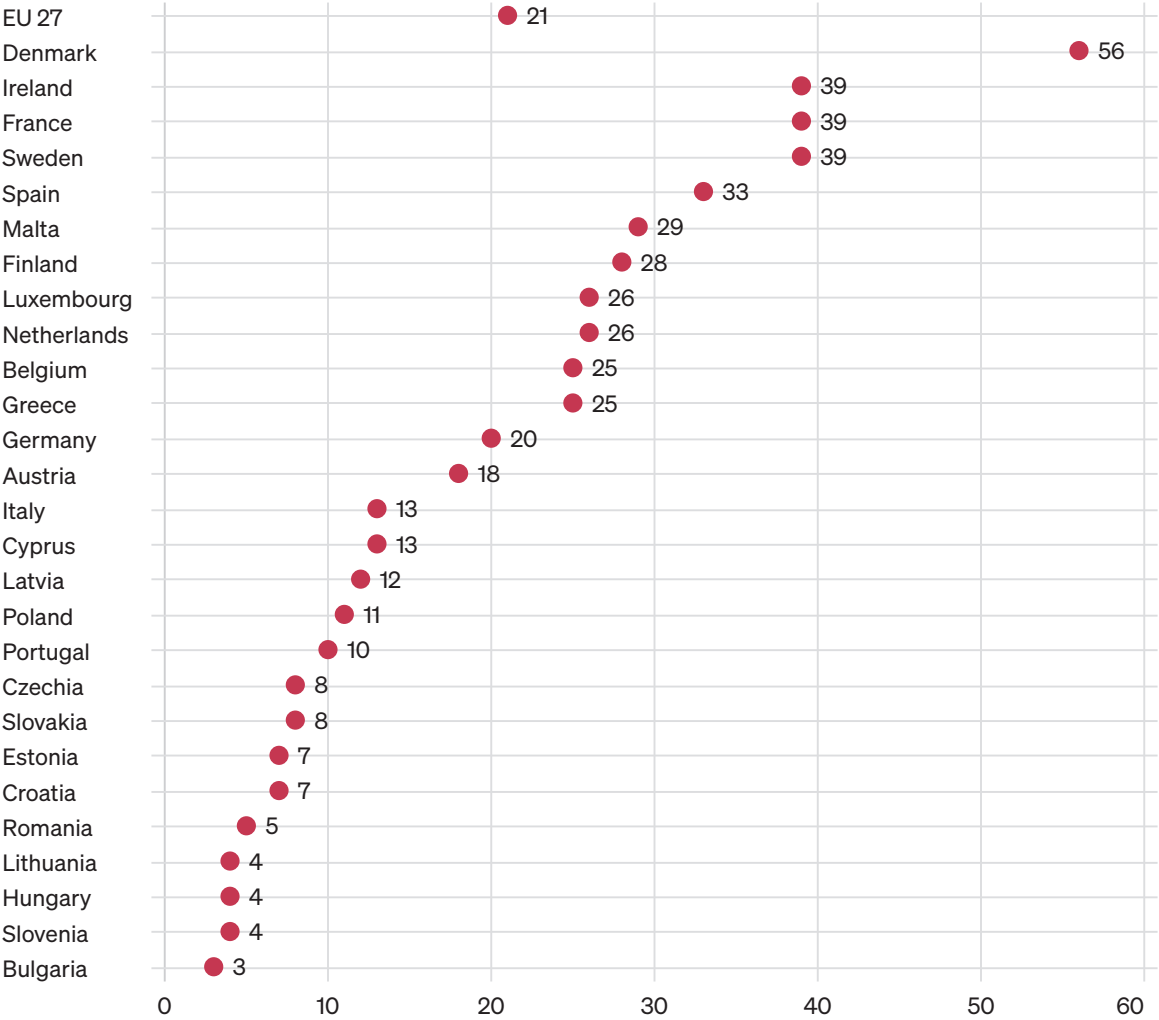
Figure 19: SMEs which carry out security tests



Source: Eurostat

In view of the high costs in the event of damage (see chapter 2.1.) and the frequency with which companies are exposed to cyber-attacks, insurance solutions for ICT damage claims are becoming increasingly relevant. However, Eurostat data show that only every fifth company has this kind of insurance. Only in Denmark (56 per cent), Ireland (54 per cent) and Sweden (52 per cent) do a majority of companies have this sort of insurance. In 13 EU countries, however, not even every third company has insurance, and in Bulgaria, Romania, Hungary and Greece not even every fifth company has insurance. This can lead to considerable business risks and, in view of average damage costs of 4.4 million Euros per attack (Ponemon/ IBM 2022), threaten the existence of many companies.

Figure 20: Percentage of SMEs insured against cyberattacks



Source: Eurostat

Broken down by company size, it shows that 35 per cent of all large companies have insurance against ICT damages, with this being the case for 28 per cent of medium-sized companies. However, this is only the case for one in five smaller companies. But even within sizes of company, there are clear country-specific differences. As an analysis by the OECD (2022) shows, country-specific differences play a major role. For example, almost 60 per cent of Danish micro-enterprises have ICT insurance, but less than 20 per cent of German or Austrian small businesses. The goal must therefore be to strengthen the European insurance market. This applies in particular to countries with previously weak insurance rates. At the European level, a transfer of knowledge between Member States should be encouraged; Denmark in particular can serve as a model for many states.

In addition to the expansion of ICT security solutions and the European insurance market, an analysis by ENISA (2021b) shows that in practice poor guidelines for SMEs are a major hurdle. In recent years, institutions at a European and national level have drawn up many guidelines for small and medium-sized enterprises. Often the level of awareness of these documents in the target group is low and they are usually very abstract and written in a language that does not give the individual entrepreneur a clear recommendation for action. Qualitative analysis shows that companies are often advised to 'implement backups' or to appoint an 'information security officer' without explaining how to 'implement' a backup or what an 'information security officer' actually does (ENISA 2021b). In practice, documents of this kind are ineffective. A positive case study would be Belgium, whose guide for small and medium-sized enterprises contains over 70 detailed measures, including basic elements such as a secure password, as well as advanced measures (CCB 2022). Across Europe, the goal must be to make certain security practices such as the 3-2-1 rule known in all SMEs. This rule means that there should be at least three copies of all data on two different storage locations, one of which is on the cloud.

It is of fundamental importance that cyber-security is affordable, in particular for small and medium-sized enterprises. This means that support systems must be expanded or joint procurement by SMEs promoted. Likewise, a push for cloud-based solutions is vital, as a cloud provider must guarantee cyber-security measures and the user thus automatically benefits from a certain level of protection. When concluding such 'fixed Service Level Agreements' for the use of such services, SMEs have a negotiating disadvantage due to their size. Pooling (the voluntary association of several companies) could reduce costs in this case (ENISA 2021b).

Figure 21: 3-2-1 Model for securing data



Source: ENISA (2021)

Europe has the largest single market in the world and is the largest economy. This means that cyber-security is of key importance to businesses, as European companies are an attractive target for Europe's competitors and cyber-criminals acting for personal gain. Small and medium-sized enterprises, contrary to public perception, are often affected by cyber-attacks, but are not covered by legislation such as the NIS Directive, which aims to improve protection. As they generate more than half of Europe's Gross Domestic Product, improving the cyber-security of Europe's small and medium-sized enterprises is crucial.

Recommendations

- Europe-wide expansion of essential security mechanisms such as data encryption. It is evident that there are significant differences between countries in all the measures analysed. It is therefore particularly important to minimise these.
- Since claims are associated with high costs, the insurance market for ICT claims must be strengthened throughout Europe. Denmark stands out as a best-practice example from which other EU countries can learn.
- Guidelines, if they exist, must be revised and made practical. European and national institutions are recommended to develop these together with the target group, namely small and medium-sized enterprises, so that they become effective in practice.
- Essential security standards such as the 3-2-1 strategy for securing data must be propagated throughout Europe and made known to small and medium-sized enterprises, as they represent effective, low-cost solutions.
- The affordability of cyber-security measures must be strengthened for SMEs. This starts with the revision of funding schemes, but solutions should be promoted at national and European level to facilitate joint procurement thereby reducing costs for SMEs.
- Since most small and medium-sized enterprises have fewer than ten employees, the motto is: strengthening the cyber-security of the people means strengthening SMEs. Strategies for awareness communication and knowledge transfer should therefore explicitly convey practical examples taken from everyday work.



Chapter 3

Summary and Outlook

In Eurobarometer surveys, a majority of the citizens surveyed now regularly state that they are concerned about potential fraud online or cyber-attacks on democratic elections. The issue has therefore finally registered with the majority of the population. Now is the time to go on the offensive and reiterate the necessary measures, with the greatest possible transparency and with due regard for Europe's security interests. In realistic terms, decision-makers can immediately accept that, when it comes to combating cyber-threats, the future will continue to be characterised by trials and tribulations.

Just think of the debate on upload filters (automatic filter systems that control uploads) at the European level, which many experts criticise as misguided. Likewise, every step and every measure must be accompanied by a realistic picture of the necessary expenditure in the field of cyber-security and defence. In 2022, no one can still be under the illusion that digital defence will be cheaper in the long run than the use of traditional police and military means.

Starting from the premises that

- cyber-security is not a monopoly of the IT departments of this world and it is not possible for them alone to secure cyberspace,
- people, their behaviour, decisions and perceptions play the central role in cyber-security,

this paper has identified current problem areas and possible solutions. It is essential for Europe's liberal society that it manages without surveillance measures and excessive restrictions of Europeans' freedoms

All recommendations at a glance

- The coordination of foreign, security and economic policies must be improved in order to strengthen European digital sovereignty.
- A common understanding of central goals and measures to strengthen awareness communication and knowledge transfer for cyber-security in Europe. In particular, low-threshold proposals, such as the 'Cyber Weather Report' of the Finnish National Cyber Security Center, must be established.
- Develop a cyber-security taxonomy. This must include a mix of structural indicators, data on attitudes and behaviour in the cyber-security field and indicators relevant to security policy.
- Fundamental decisions to be made on the future of European cloud computing (GAIA-X standard in Europe or tool to improve the competitiveness of European cloud providers)
- Massive investment in Europe's network connectivity to create and control its own 5G and fibre infrastructure and be more secure from any outside manipulation.
- Minimum standards for university curricula and expansion of Bachelor's programmes and academic in-service training in Europe.
- Close the gender gap by linking funding to diversity measures, awareness raising and internships.
- Address weaknesses in the certification area. Similar to the NICE initiative for the US, it needs standardisation of professions, their work activities and associated skills.
- Strengthen adult education by establishing specific further training for people already in working life.
- Pilot projects to introduce apprenticeships within the cyber-security sector.
- Strengthen the insurance market for ICT claims throughout Europe in order to cushion high loss amounts for companies which have been victims of a successful cyber-attack.
- Revise and simplify practice guidelines of national and European institutions in the field of cyber-security.
- Europe-wide implementation and promotion of essential security standards (e.g. data encryption, 3-2-1 strategy, for securing data), especially for SMEs.
- Improve the affordability of cyber-security measures for SMEs.
- Strategies for awareness communication and knowledge transfer with explicitly practical examples taken from everyday working life.

Outlook

This paper does not yet shed light on many of the topics that informed our deliberations. In this respect, the following is a brief outlook which touches on those aspects of the debate which were not examined this time, but which are sure to play a key role in Europe's digital future.

Skilled immigration

As a location for the cyber-security service industry, Europe is struggling with giants in the East and West and has sometimes made it difficult for itself (for good reasons). The orientation towards European values, basic rights and human rights, and the ideal of a successful competition policy for the European single market sometimes disadvantages Europe's global competitiveness. Legal processes take longer, European monopolies which can compete with US or Chinese competitors do not (yet) exist in many areas of the digital economy. As a location for industrial skilled workers, Europe is also in a worse position in terms of the industry and also in terms of legal restrictions in the area of innovation as well as skilled immigration. It is easy to forget that skilled workers are people who do not choose their place of residence solely on the basis of industrial conditions. Europe is a continent worth living in, where social balance plays a specific role. The rule of law, good school systems, cultural activities, a clean environment and diversity make Europe competitive in other ways when it comes to skilled workers. However, the European Union needs to reform its policies and bureaucratic barriers to skilled immigration from other parts of the world as soon as possible.

Trust

The next buzzword in the field of security, which is already commonplace in circles familiar with the issue, could be 'trust'. Standards, self-regulation, control, transparency, etc. can make trustworthy digital applications stand out from all others. If the battle for a digital space in which rules apply, are adhered to and where rule-breaking is fully sanctioned has often been lost, it is still possible to build 'islands' of trust within it. Let's call them 'digital zones of protection', in which the greatest asset of the providers operating there is their trustworthiness and adherence to high standards. However, only the public sector can guarantee this, and even then, there may be incidents resulting in security breaches. An example of this kind of technology is the idea of a low-threshold, simple European identity, including European login solutions for online shopping or administrative services.

Deterrence

In addition to becoming an attractive place to live for ICT skilled workers, it would also serve as a deterrent if Europe made further progress in intelligence pooling. While some information is already shared with partners through EU and NATO reporting systems, for example, mistrust between European intelligence services is still clearly present. A secure Europe needs European intelligence services to trust each other and work closely together. The path to this may be an arduous and lengthy one, but Europe will benefit from it.

Technological impact assessment

Digital transformation is in full swing. In order to make a better assessment of future developments and societal impacts, a combination of a technological impact assessment and ethical principles needs to be developed as a 'compass'. A realistic technological impact assessment that policy-makers, businesses and civil society can work with, is based on two key principles: Firstly, technological impact assessments must be considered in scenarios with clearly defined parameters, and must clearly define what the limitations of the respective models are. Secondly, when evaluating technological impacts, it is necessary to define clear objectives: desired effects. This is where ethical principles come into play. The potential of such solutions is illustrated by Ptaschunder and Feierabend (2019b), who compare historical legal systems in terms of the usability of interactions between automated AI and humans.

The future, one might sometimes think, no longer exists. Not because we as human beings do not have a future, but because the acceleration of progress has meant that no innovation is as illusory and distant as it used to be. So when implementing the proposed measures, there is no need to think of a distant tomorrow. The future is now.

Bibliography

Accenture (2019): The state of cyber-security resilience 2021. Last accessed 17 September 2022: <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>

Alliance of Liberals and Democrats for Europe (2022): A liberal response to current and emerging cyber threats. ALDE Party Secretariat, June 2022, Dublin. Last accessed 17 September 2022: https://assets.nationbuilder.com/aldeparty/pages/5805/attachments/original/1654356480/006_-_A_liberal_response_to_current_and_emerging_cyber_threats_%281%29.pdf?1654356480

Australian Strategic Policy Institute (2020): Cyber-enabled foreign interference in elections and referendums. Last accessed 17 September 2022: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-10/Cyber%20enabled%20foreign%20interference_0.pdf?QnX7Dz7akMiLSP5xHWYYo8ZitxOt2_i7=

Australian Strategic Policy Institute (2021): UN Norms for Responsible State-Behaviour in Cyberspace. Last accessed 18 September 2022: <https://www.aspi.org.au/report/un-norms-responsible-state-behaviour-cyberspace>

BBC (2020): TikTok: We are not 'under the thumb' of China. Last accessed 17 September 2022: <https://www.bbc.com/news/business-53469766>

Bing, C. et. al (2020): 'Powerful tradecraft': how foreign cyber-spies compromised America. Reuters. Last accessed 17 September 2022: <https://www.reuters.com/article/us-global-cyber-usa-insight-idUSKBN28T0XV>

Bing, C. and Kelly, S. (2021): Cyber Attack Shuts down U.S. Fuel Pipeline 'Jugular', Biden Briefed. Reuters Last accessed 17 September 2022: <https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/>

Blažič, B.J. (2021): The cybersecurity labour shortage in Europe: Moving to a new concept for education and Training. In: Technology in Society, Volume 67,

Bloomberg (2022): The TikTok War Didn't Cause the TikTok Boom. Last accessed 17 September 2022: <https://www.bloomberg.com/news/articles/2022-04-07/tiktok-user-growth-surged-before-russia-ukraine-war>

Bunde, T., et. al (2022): Munich Security Report 2022: Turning the Tide – Unlearning Helplessness. Munich Security Conference. Last accessed: 17 September 2022: <https://doi.org/10.47342/QAWU4724>

Buzzfeed (2022): Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China. Last accessed 17 September 2022: <https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>

CCB (2022): Cybersecurity Guide for SME. Last accessed 17 September 2022: <https://ccb.belgium.be/en/document/guide-sme>

Chang, A. (2018): The Facebook and Cambridge Analytica scandal, explained with a simple diagram. Vox. Last accessed 17 September 2022: <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>

CEDEFOP – European Centre for the Development of Vocational Training (2022): European qualifications framework. Last accessed 17 September 2022: <https://www.cedefop.europa.eu/en/projects/european-qualifications-framework-eqf>

Christiani, D. et. al (2021): The Security Implications of Chinese Infrastructure Investment in Europe. GMF. Last accessed 17 September 2022: <https://www.gmfus.org/sites/default/files/2022-01/Cristiani%20et%20al%20-%20report%20%281%29%20Updated.pdf>

Cerulus, L. (2022): Cyber 'spillover' from Ukraine looms in the Baltics. Last accessed: 17 September 2022: <https://www.politico.eu/article/baltic-cyber-spillover-ukraine-russia-attack/>

Conley, H. et. al. (2020): Countering Russian & Chinese influence activities, Center for Strategic & International Studies. Last accessed: 17 September 2022: <https://www.csis.org/analysis/countering-russian-chinese-influence-activities>

Cooley, A. & Nexon, D. (2022): The Real Crisis of Global Order: Illiberalism on the Rise. Foreign Affairs 101:1 (2022), 103–118. Last accessed 17 September 2022: <https://perma.cc/U8N3-43XH>

Couture, S. & Toupin, S. (2018): What does the concept of 'sovereignty' mean in digital, network and technological sovereignty?. paper presented at GigaNet: Global Internet Governance Academic Network. Annual Symposium 2017

Council of the European Union (2022): A Strategic Compass for Security and Defence – For a European Union that protects its citizens, values and interests and contributes to international peace and security. General Secretariat of the Council, Brüssel, 21. März 2022. Last accessed 17 September 2022: <https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/en/pdf>

CyberSecurity Ventures (2020): The official annual cybercrime report. Last accessed: 17 September 2022: <https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/>

CyberSecurity Ventures (2021) The official annual cybercrime report. Last accessed: 17 September 2022: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

Dawson, J. Thomson, R. (2018): The future cybersecurity workforce: going beyond technical skills for successful cyber performance *Frontier Psychology*. Vol. 12.

Deloitte Services Wirtschaftsprüfungs GmbH (2022): Deloitte Cyber Security Report 2022. How Austrian companies deal with increasing cyber threats. Last accessed 17 September 2022: <https://www2.deloitte.com/content/dam/Deloitte/at/Documents/risk/cyber-risk/at-cyber-security-report-2022.pdf>

Eder, G. & Feierabend, D. (2019): You had one job – Transforming social security systems into the digital working age. *European Liberal Forum (ELF)*

ENISA (2016): Cybersecurity as Economic Enabler. Last accessed 17 September 2022: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/cybersecurity-as-an-economic-enabler#:~:text=The%20EU%20Cybersecurity%20Market%20is,than%20all%20other%20major%20regions>

ENISA (2019): Election Cybersecurity: Challenges and Opportunities. Last accessed 17 September 2022: <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/election-cybersecurity-challenges-and-opportunities>

ENISA (2020): Threat Landscape for Supply Chain Attacks. Last accessed 05 August 2022: <https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>

ENISA (2020b): Cybersecurity Skills Development in the EU. Last accessed 17 September 2022: <https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union>

ENISA (2021): Threat Landscape 2020/21. Last accessed: 05 August 2022: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>

ENISA (2021b): Cybersecurity for SMEs – Challenges and Recommendations. Last accessed: 17 September 2022: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>

ENISA (2021c): Research Directions for Digital Strategic Autonomy Last accessed: 17. September 2022: <https://www.enisa.europa.eu/publications/cybersecurity-research-directions-for-the-eu2019s-digital-strategicautonomy>

ENISA (2021d): Raising awareness for cybersecurity Last accessed 17 September 2022: <https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity>

ENISA (2021e): Addressing Skills Shortage and Gap Through Higher Education Last accessed 17 September 2022: <https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education>

ENISA (2022): CYBERHEAD – Cybersecurity Higher Education Database. Last accessed 05 September 2022: <https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/>

ENISA (2022b): Threat Landscape 2022. Last accessed: 5 November 2022: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022>

Erhardt, M. (2019): Alternatives to Huawei are expensive and cost time. *Deutschlandfunk*. Last accessed 18 September 2022: <https://www.deutschlandfunk.de/5g-technik-alternativen-zu-huawei-sind-teuer-und-kosten-zeit-100.html>

European Commission (2015): The EU and China signed a key partnership on 5G, our tomorrow's communication networks. Last accessed 17 September 2022: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_15_5715/IP_15_5715_EN.pdf

European Commission (2020): The European Data Market Monitoring Tool. <https://data.europa.eu/doi/10.2759/72084>

European Commission (2021): Commission to Invest Nearly €2 Billion from the Digital Europe Programme to Advance on the Digital Transition. Last accessed 17 September 2022: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_5863

European Commission (2022): SME definition. Last accessed on 17 September 2022: https://single-market-economy.ec.europa.eu/smes/sme-definition_en

European Commission (2022b): Entrepreneurship and small and medium-sized enterprises (SMEs). Last accessed 17 September 2022: https://ec.europa.eu/growth/smes_en

Eurostat (2022): ICT specialists in employment. Last accessed 17 September 2022: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_in_employment

Eurostat (2022b): ICT specialists – statistics on hard-to-fill vacancies in enterprises. Last accessed 17 September 2022: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises#Employment_and_recruitment_of_ICT_specialists

Eurostat (2022c): ICT security in enterprises. Last accessed 17 September 2022: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises

European Parliament (2019): Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Last accessed 08 August 2022: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

- FBI** (2021): Internet Crime Report 2021. Internet Crime Complaint Center. Last accessed 17 September 2022: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
- Puaschunder, J. & Feierabend, D.** (2019): Artificial Intelligence in the Healthcare Sector. European Liberal Forum (ELF).
- Puaschunder, J. & Feierabend, D.** (2019b): Ancient Legal Codes as Basis for Artificial Intelligence Regulations in the 21st Century. *Scientia Moralitas*. Vol. 5. Last accessed 17 September 2022: <http://scientiamoralitas.com/index.php/sm/article/view/51>
- Futurezone** (2022): Further data from cyber-attack on Carinthia published. Last accessed 17 September 2022: <https://futurezone.at/digital-life/weitere-daten-cyberangriff-kaernten-ransomware-veroeffentlicht-leak/402044563>
- GAIA-X** (2022): The GAIA-X project. Last accessed 08 August 2022: www.bmw.de/Redaktion/EN/Publikationen/DigitaleWelt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6;
- Gamal, N., Martino, L., Nestoras, A.** (2022): European Cybersecurity in Context. A Policy-Oriented Comparative Analysis. European Liberal Forum (ELF).
- Gartner** (2019): The Data Center is (Almost) Dead. Last accessed 17 September 2022: <https://www.gartner.com/smarterwithgartner/the-data-center-is-almost-dead/>
- Gorman, L.** (2020): 5G Is Where China and the West Finally Diverge. Last accessed 17 September 2022: <https://www.theatlantic.com/ideas/archive/2020/01/5g-where-china-and-west-finally-diverge/604309/>
- Hansen, I. & Lim, D.** (2018): Doxing Democracy: Influencing Elections Via Cyber Voter Interference. *Contemporary Politics*. Last accessed 18 September 2022: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3310974
- Herpig** (2021): Cybersecurity and the People's Republic of China. Stiftung Neue Verantwortung. Last accessed 17 September 2022: <https://www.stiftung-nv.de/de/publikation/cybersicherheit-und-die-volksrepublik-china-ein-ueberblick-aus-deutscher-perspektive>
- Hoffman, W., & Maurer, T.** (2019): The Privatization of Security and the Market for Cyber Tools and Services. Centre for Security Sector Governance Last accessed 17 September 2022: https://www.dcaf.ch/sites/default/files/publications/documents/Carnegie_MaurerHoffmann_July2019.pdf
- Jennings, R.** (2020): Apple's Assemblers Are Looking To Shift Some Operations From China To India. *Forbes*. Last accessed 18 September 2022: <https://www.forbes.com/sites/ralphjennings/2020/09/18/apples-assemblers-are-looking-to-shift-some-operations-from-china-to-india/?sh=180275c83a37>
- Juncker, J.-C.,** 'The hour of European sovereignty', State of the Union 2018. Last accessed 17 September 2022: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-speech_en.pdf

- Kaspersky** (2022): What is Social Engineering? Last accessed 17 September 2022: <https://www.kaspersky.de/resource-center/definitions/social-engineering>
- Kolbe, P.** (2020) 'With Hacking, the United States Needs to Stop Playing the Victim,' *The New York Times*. Last accessed 17 September 2022: <https://perma.cc/9FJF-JZTK>
- Langner, R.** (2013): To Kill a Centrifuge. A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group. Last accessed 07 July 2022: <https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf>
- Lee-Makiyama, H. & Forsthuber, F.** (2020): Europe's dependency on China? European Centre for International Political Economy. Last accessed 17 September 2022: <https://ecipe.org/blog/europes-dependency-on-china/>
- Liedereke, A. & Laudrain, A.** (2022): Russia's Cyber War: What's Next and What the European Union Should Do. Council on Foreign Relations. Last accessed 14 September 2022: <https://www.cfr.org/blog/russias-cyber-war-whats-next-and-what-european-union-should-do>
- Martin, A., Collier, J.** (2019): Beyond Awareness: the Breadth and Depth of the Cyber Skills Demand. Center for Technology and Global Affairs Oxford University. Last accessed 17 September 2022: <https://www.ctga.ox.ac.uk/files/wp10thebreadthanddepthofthecyberskillsdemandpdf>
- Meinek, S. & Fanta, A.** (2022): Leaked recordings incriminate TikTok. *netzpolitik.org*. <https://netzpolitik.org/2022/china-sieht-alles-geleakte-mitschnitte-belasten-tiktok/>
- Metzger, M.** (2022): Who is behind alleged Gazprom video? ZDF online. Last accessed: 17 September 2022: <https://www.zdf.de/nachrichten/politik/propaganda-gazprom-video-desinformation-ukraine-krieg-russland-100.html>
- Microsoft** (2022): The urgency of tackling Europe's cybersecurity skills shortage. Last accessed 17 September 2022: <https://blogs.microsoft.com/eupolicy/2022/03/23/the-urgency-of-tackling-europes-cybersecurity-skills-shortage/>
- Nakashima, E. & Timberg, C.** (2020): Russian Government Hackers Are behind a Broad Espionage Campaign that has Compromised U.S. Agencies, Including Treasury and Commerce. *The Washington Post*, December 14, 2020. Last accessed on: 14 September: <https://perma.cc/N7BG-GKFJ>
- OECD** (2022): Helping the Austrian business sector to cope with new opportunities and challenges in Austria. <https://doi.org/10.1787/18151973>

Office of the UN Secretary General (2020): Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation. Last accessed 18 September 2022: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/51/PDF/N2010251.pdf?OpenElement>

NCSC (2022): Cyber weather. Last accessed 17 September 2022: <https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather>

OECD (2009): OECD Legal Instruments. Last accessed 17 September 2022: <https://www.kyberturvallisuuskeskus.fi/en/ncsc-news/cyber-weather>
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0372>

O’Flaherty, K. (2021): All the ways TikTok tracks you and how to stop it. Wired. Last accessed 17 September 2022: <https://www.wired.co.uk/article/tiktok-data-privacy>

Perlroth, N. (2021): This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Books.

PESCO (2022): Project list. Last accessed 18 September 2022: <https://www.pesco.europa.eu/>

Ponemon/IBM (2022): Cost of a Data Breach Report. Last accessed: 17 September 2022: <https://www.ibm.com/uk-en/security/data-breach>

Proofpoint (2022): What is Email Spoofing? Last accessed 01 September 2022: <https://www.proofpoint.com/uk/threat-reference/email-spoofing>.

Prodaft (2021): Ransomware Group In-Depth Analysis’. Last accessed on 18 November 2022, <https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis>

Statista (2022a): Cybersecurity – EU-27. Last accessed: 17 September 2022: <https://de.statista.com/outlook/tmo/cybersecurity/eu-27#analystenmeinung>

Statista (2022b): Cybersecurity – Worldwide. Last accessed: 17 September 2022: <https://de.statista.com/outlook/tmo/cybersecurity/weltweit>

Seaman, J. et. al (2022): Dependence in Europe’s Relations with China. Weighing Perceptions and Reality. ENTC. Last accessed 17 September 2022: https://www.ifri.org/sites/default/files/atoms/files/etnc_2022_report.pdf

Stealthlabs (2020): Top 10 Cybersecurity Trends in 2022 and Beyond! Last accessed 17 September 2022: <https://www.stealthlabs.com/blog/top-10-cybersecurity-trends-in-2021-and-beyond/>

Strumpf, D. (2020): U.S. vs. China in 5G: The Battle Isn’t Even Close. Wall Street Journal. Last accessed 17 September 2022: <https://www.wsj.com/articles/u-s-vs-china-in-5g-the-battle-isnt-even-close-11604959200>

UN General Assembly (2020): Road map for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation. Last accessed 18 September 2022: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N20/102/51/PDF/N2010251.pdf?OpenElement>

UN Office of the Secretary General’s Envoy on Technology (2022): Roadmap for Digital Cooperation. Last accessed 18 September 2022: <https://www.un.org/techenvoy/content/roadmap-digital-cooperation>

UN Peacekeeping (2021) Strategy for the Digital Transformation of UN Peacekeeping. Last accessed 18 September 2022: https://peacekeeping.un.org/sites/default/files/20210917_strategy-for-the-digital-transformation-of-un-peacekeeping_en_final-02_17-09-2021.pdf

UNCTAD (2021): Digital Economy Report 2021. Last accessed 17 September 2022: <https://unctad.org/webflyer/digital-economy-report-2021>

UNITE (2022): Mission Statement. Last accessed 18 September 2022: <https://unite.un.org/about>

UNODC 2022 https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

Vakakis, N. et al. (2019): Cybersecurity in SMEs. The smart-home/office use case. IEEE International Workshop on Computer-Aided Modeling, Analysis, and Design of Communication Links and Networks. Last accessed 17 September 2022: <https://ieeexplore.ieee.org/document/8858471>

Waldron, K. (2019): Resources for Measuring Cybersecurity, R Street, October 2019. Last accessed on 17 September 2022: <https://www.rstreet.org/wp-content/uploads/2019/10/Final-Cyberbibliography-2019.pdf>

ZDNET (2022): Global security spending to top \$103 billion in 2019. Last accessed 17 September 2022: <https://www.zdnet.com/article/global-security-spending-to-top-103-billion-in-2019-says-idc/>

Abbreviations

DDoS – Distributed Denial of Service (Attack)

ENISA – European Union Agency for Cybersecurity

EU – European Union

ICT – Information and Communication Technology

IT – Information Technology

NATO – North Atlantic Treaty Organisation

OECD – Organisation for Economic Cooperation and Development

PESCO – Permanent Structured Cooperation

SME – Small and Medium-sized Enterprise

Authored by

Teresa Reiter is a journalist by training and a member of the Europe's Futures programme at the Institute of Human Sciences in Vienna. She works at the crossroads of European and security policy and digitalisation. She co-developed the Friedrich-Naumann-Foundation's Liberal Defence Expert Network and is the co-host of their podcast "The Defence Café". Previously, she worked as a journalist, was the Head of Communications and Marketing at the European Forum Alpbach and a policy advisor for foreign and European affairs, defence, migration and development cooperation for the liberals NEOS in the Austrian Parliament. She holds degrees in news journalism from Kingston University in London and in advanced international studies from the Diplomatic Academy of Vienna.

Dieter Feierabend works as scientific director at NEOS Lab. He holds a PhD in Social Sciences and a BSc in Statistics from the University of Vienna. In his studies, he focused on the relationship between policy issues and electoral behaviour. Furthermore, he is a graduate of the postgraduate program "Multi-Level Politics in Europe" at the Institute for Advanced Studies in Vienna. Before joining NEOS Lab, he worked as a freelance consultant i.e. for the Austrian Academy of Sciences (Institute for Technology Assessment).

INSTITUTIONS

The European Liberal Forum (ELF) is the official political foundation of the European Liberal Party, the ALDE Party. Together with 46 member organisations, we work all over Europe to bring new ideas into the political debate, to provide a platform for discussion, and to empower citizens to make their voices heard.

ELF was founded in 2007 to strengthen the liberal and democrat movement in Europe. Our work is guided by liberal ideals and a belief in the principle of freedom. We stand for a future-oriented Europe that offers opportunities for every citizen. ELF is engaged on all political levels, from the local to the European.

We bring together a diverse network of national foundations, think tanks and other experts. At the same time, we are also close to, but independent from, the ALDE Party and other Liberal actors in Europe. In this role, our forum serves as a space for an open and informed exchange of views between a wide range of different actors.



www.liberalforum.eu

NEOS Lab is the political academy of the liberal grass-roots movement NEOS, and an open laboratory for new politics. The main objective of NEOS Lab is to contribute to enhancing political education in Austria by providing a platform for knowledge exchange and liberal political thinking on the key challenges and pathways of democracies and welfare states in the 21st century. Particular emphasis is placed on the core topics of education, a more entrepreneurial Austria, sustainable welfare systems and democratic innovation. NEOS Lab conceives itself as a participatory interface between politics and society insofar as it mediates between experts with scientific and practical knowledge on diverse policy issues and interested citizens. A network of experts accompanies and supports the knowledge work of the diverse thematic groups and takes part in the think tank work of NEOS Lab. Additionally, NEOS Lab provides several services, such as political education and training, workshops and conferences and a rich portfolio of inter- and transdisciplinary research at the interface between science, politics, economy and society.

NEOS Lab is the successor of the Liberal Future Forum, which was previously a member of ELF.

lab.neos.eu

A liberal future in a united Europe

 /europeanliberalforum
 @eurliberalforum
#ELFevent

ISBN: 978-2-39067-041-4

liberalforum.eu

Copyright 2022 / European Liberal Forum EUPF.

This publication was co-financed by the European Parliament. The European Parliament is not responsible for the content of this publication, or for any use that may be made of it.