secure soc

RESEARCH REPORT

ENGLISH / SEPTEMBER 2026

Comparative Mapping Report.

PART 01

WP2 – SECURESOC

02 September 2026

Social Partners for Resilience and Security
Protecting critical infrastructure, strengthening cybersecurity awareness, and combating disinformation through social dialogue.

securesoc.oegb.at/en

Written by **VÖWG and ÖGB**
Date of publishing: September 2026

ÖGB
Austrian Trade-Union Federation
Johann-Böhm-Platz 1
1020 Vienna, Austria
www.oegb.at

VÖWG
The Association of Public Services and Enterprises Austria
Stadiongasse 6–8
1010 Vienna, Austria
voewg.at

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Directorate-General for Employment, Social Affairs and Inclusion. Neither the European Union nor the granting authority can be held responsible for them.

IN THIS REPORT

Contents

01 EU Cybersecurity Strategy 4

02 Disinformation in the Workplace 19

03 Operational Glossary (Terminology) and Delimiting the Problem 29

↳ Notes 35

01 / REPORT

EU Cybersecurity Strategy

THE EU CYBERSECURITY STRATEGY

Cybersecurity is defined in the *EU Cybersecurity Act* (Regulation (EU) 2019/881) as "all activities necessary to protect network and information systems, the users of such systems and other persons affected by cyber threats". This definition is clarified by Directive (EU) 2022/2555 (NIS 2 Directive) by stating that the security of network and information systems is the ability to resist events that could compromise the availability, authenticity, integrity or confidentiality of the data processed or the services provided via these systems.

To ensure this level of security, the *EU Cybersecurity Strategy for the Digital Decade* establishes the strategic and policy framework for "a global, open, free and secure internet" (European Commission, 2020). Published in 2020, the strategy is structured around three key areas of action:

- Resilience, technological sovereignty and leadership,
- Building operational capabilities for prevention, deterrence and response,
- Promoting a global, open cyberspace (European Commission, 2020).

The following sections explain the three pillars of the EU Cybersecurity Strategy in more detail and review case studies of cyberattacks affecting the EU to clarify the strategy's development.

1. Resilience, technological sovereignty and leadership

This pillar focuses on strengthening the Union's resilience by protecting critical infrastructure, securing technological supply chains and promoting European self-reliance in key technologies (European Commission, 2020). The approach relies primarily on regulatory measures. According to the *WEF Global Cybersecurity Outlook 2026*[1], the EU plays a particularly important role in this regard, as 78% of the CISOs[2] surveyed state that differences between legal systems make it difficult to implement security measures and that a harmonised legal framework would contribute to stability (World Economic Forum, 2026).

In order to strengthen critical infrastructure and services, the EU Cybersecurity Strategy provided for the revision of the original NIS Directive and the creation of a new framework for physical resilience (European Commission, 2020). Subsequently, as part of the strategy, the sister directives[3] (*NIS 2 Directive* and the *CER Directive*) were adopted on 14 December 2022. The *NIS 2 Directive*, the *CER Directive* and the *DORA Regulation* together form the regulatory foundation for the security of critical sectors.

The *NIS 2 Directive* aims to establish a high common level of cybersecurity across the EU and improve the functioning of the single market (Directive (EU) 2022/2555, 2022). As a general rule, the Directive applies to medium-sized and large public or private entities operating in sectors of

high criticality[4] or other critical sectors[5]. These entities are required to implement risk management measures which, according to Article 21, include, amongst other things, a risk analysis framework, incident response procedures and supply chain security.

The *NIS 2 Directive* also introduces multi-stage reporting obligations for significant security incidents[6]. The early warning must be submitted to the relevant CSIRT[7] within 24 hours, followed within 72 hours by an incident notification, which must contain a more detailed description. The final report, including a root cause analysis and the corrective measures taken, must be submitted within one month. According to the NISG[8], operators must report to their sector-specific CERT or[9] to the national CERT[10], which will forward the report to the Federal Ministry of the Interior (Republic of Austria, 2026).

A key aspect of the new Directive is the accountability of management bodies for compliance with cybersecurity risk-management obligations, as well as the requirement for regular training for members of the management bodies (Directive (EU) 2022/2555, 2022). These measures are monitored for essential entities as part of ex-ante and ex-post supervision, whilst important entities are subject only to reactive ex-post supervision. In the event of breaches, authorities may impose fines of up to €10 million or 2 per cent of the previous year's global turnover and may also seek the temporary suspension of certain management functions, subject to the conditions set out in the Directive.

The *CER Directive* (Directive (EU) 2022/2557, 2022) focuses on the physical resilience of critical entities and thus complements the *NIS 2 Directive*. The Directive aims to strengthen resilience and ensure that services essential to vital societal functions or economic activities in the internal market can be provided without hindrance. This resilience is defined in the CER Directive as "the ability of a critical entity to prevent, protect against, respond to, and mitigate the consequences of a security incident, as well as to absorb, manage and recover from such an incident" (Directive (EU) 2022/2557, 2022). This legislation obliges Member States to establish a national framework to ensure resilience. This includes a national strategy, which provides for improvements to the resilience of critical entities. In Austria, this is the Austrian Strategy for the Resilience of Critical Entities (ÖSRKE 2026), implemented through the Critical Entities Resilience Act (RKEG). In addition, regular risk assessments must be carried out and critical entities identified, so that Member States can support these facilities through guidelines, exercises, training and, where necessary, financial resources (Directive (EU) 2022/2557, 2022).

The *DORA Regulation*, adopted in 2022, is a key component of the European cybersecurity strategy, specifically tailored to the financial sector (Regulation (EU) 2022/2554, 2022). The Regulation aims to strengthen the digital operational resilience of financial entities[11] and third-party ICT service providers[12]; this means ensuring they can withstand, respond to and recover from threats such as cyber-attacks or system failures. This is to be achieved through ICT risk management by identifying, assessing and addressing risks that may arise from the use of network and information systems. This includes the reporting of ICT incidents to the financial supervisory authority, digital resilience testing (including advanced, threat-led penetration tests every three years), minimum requirements and monitoring of critical third-party ICT providers by European supervisory authorities, as well as the voluntary exchange of information amongst financial firms.

Another area of the EU cybersecurity strategy is the security of the 'Internet of Things' (IoT[13]), where the strategy seeks to establish the principles of 'security by design' and 'security by default' to prevent insecure devices from becoming a gateway for cyber-attacks (Regulation (EU)

2024/2847, 2024). These principles are enshrined in law by the *Cybersecurity Act* and the *Cyber Resilience Act*.

The Cybersecurity Act (CSA) (Regulation (EU) 2019/881, 2019) was adopted in 2019 and gives the European Union Agency for Cybersecurity (ENISA) a permanent mandate as the Union's reference point for cybersecurity advice and expertise. The legislation establishes the *European cybersecurity certification framework*, which creates a Union-wide framework for the cybersecurity certification of ICT products, services and processes, thereby counteracting fragmentation of the single market. EU cybersecurity certification schemes may specify the assurance levels 'basic', 'substantial' and 'high'.[14] This is intended to strengthen confidence in digital solutions and create uniform standards across the Union.

The *Cyber Resilience Act* (CRA) (Regulation (EU) 2024/2847, 2024) was adopted in 2024 and has been in force since December 2024; its reporting obligations apply from 11 September 2026 and its main obligations from 11 December 2027. Under the Regulation, manufacturers must ensure that products are designed with security in mind from the planning and development stages ('security by design'), that they are provided with a secure default configuration ('security by default'), and that security updates are made available throughout the entire support period (based on the expected useful life, i.e. generally five years). In the case of standalone software, the Commission's guidance specifies that the product is deemed to have been placed on the market as soon as the development phase is complete and the product is offered for download or use for the first time (European Commission, 2026). A key addition here is the inclusion of remote data processing solutions ('RDPS'), meaning that cloud back-ends are legally considered part of the product if they are necessary for its functionality and were developed under the manufacturer's responsibility. The *CRA* also establishes the classification of products into 'important products' (Classes I and II), which are subject to stricter conformity assessments, and 'critical products' (Annex IV), which may require mandatory European certification. A product that has been certified under an appropriate CSA scheme may be presumed to comply with the corresponding CRA requirements to the extent covered by the scheme ('presumption of conformity') (Regulation (EU) 2024/2847, 2024). Subsequent changes are considered 'substantial' if they alter the product's risk profile or intended use, which necessitates a new conformity assessment (European Commission, 2026). Security updates intended solely to address vulnerabilities, on the other hand, are not generally classified as substantial changes.

Another aspect of the first pillar is the development of technological sovereignty and capacity, and one example of this is the DNS4EU project. In order to reduce dependence on a small number of large companies outside the EU, the DNS4EU initiative aims to create a separate public European DNS resolution service[15] as an alternative (European Commission, 2020). The service is designed to comply with the highest security and data protection standards and to adhere to the principles of 'privacy by design'.

ENISA's EU Cybersecurity Index (EU-CSI), developed in collaboration with the Member States, describes the cybersecurity posture of individual Member States and the EU as a whole (ENISA, 2025). The index measures numerous specific indicators and metrics (e.g. incident rates, internationalisation, investment, research, user behaviour) on a scale of 0–100, which are grouped into the main areas ('Policy'[16], 'Capacity'[17], 'Operations'[18] and 'Market/Industry'[19]) in order to make multidimensional concepts quantifiable.

The ‘Policy’ domain assesses, both quantitatively and qualitatively, the extent to which Member States have established the political and legal foundations for cybersecurity (ENISA, 2025). In the 2024 index, ‘Policy’ was the highest-rated area of the entire index, with an EU average of 66.09 out of 100 points. However, there are significant differences between Member States in this area, suggesting that, whilst the regulatory tools exist, the extent of their implementation varies considerably.

2. Building operational capabilities for prevention, deterrence and response

The second pillar focuses on supporting Member States in defending their citizens and their economic and national security interests through enhanced operational cooperation and the mobilisation of technical tools (European Commission, 2020). The WEF Report 2026 confirms the relevance of these measures with statistics showing that only 45% of CEOs in the private sector are confident that their country could respond adequately to cyber-attacks against critical infrastructure (World Economic Forum, 2026).

This relies on a combination of institutional platforms, such as the Joint Cyber Unit and ENISA, specialised networks, such as the CSIRT network, EU-CyCLONe and the NIS Coordination Group, as well as operational tools under the *Cyber Solidarity Act* (“CSoA”) (European Commission, 2020; Directive (EU) 2022/2555, 2022; Regulation (EU) 2025/38, 2025).

The Joint Cyber Unit (“JCU”) was conceived as part of the *EU Cybersecurity Strategy* as a platform to bring together specialist groups that have previously often operated in isolation, within a single framework (European Commission, 2020). These include the NIS authorities (including the specialised networks) at the civilian level, law enforcement agencies such as Europol/EC3[20], the diplomatic service[21] and cyber defence. Through cooperation between these communities, the potential for mutual operational support can be better exploited, thereby helping to ensure shared situational awareness and more efficient coordination of response and recovery. However, the JCU is not a new, independent authority, but acts as a coordination platform where these actors come together to support one another with specialist expertise.

A key stakeholder in the JCU is ENISA (European Commission, 2020). The agency acts as the centre of expertise for cybersecurity in the EU and is the primary point of reference for advice and expertise for Member States and EU institutions (ENISA, 2026). Although it is enshrined in the *Cybersecurity Act*, the proposed *Cybersecurity Act 2* designates ENISA as the ‘Single Point of Expertise’, which will also consolidate tasks arising from the *NIS 2 Directive*, the *Cyber Resilience Act* (CRA) and the *Cyber Solidarity Act* (CSoA) (European Commission, 2026). ENISA currently actively supports the NIS Coordination Group and coordinates the CSIRTs network as well as EU-CyCLONe (Directive (EU) 2022/2555, 2022).

The NIS Coordination Group comprises representatives of the EU Member States, the Commission and ENISA[22] (Directive (EU) 2022/2555, 2022). Together, they draw up a biennial work programme and guidance on the implementation of the *NIS 2 Directive*; they also carry out Union-level risk assessments for critical supply chains and facilitate the exchange of best practices on risk management and reporting obligations.

The CSIRTs network comprises the national Computer Security Incident Response Teams (CSIRTs) of the Member States and CERT-EU[23] (Directive (EU) 2022/2555, 2022). The exchange of technical information on security incidents, cyber threats and vulnerabilities enables more effective coordinated responses to incidents affecting several Member States. This is achieved in

particular through cooperation with the cyber hubs of the "European Cybersecurity Alert System". ENISA provides the secretariat services for this, which include administrative, technical and financial support.

The EU-CyCLONe network is specifically responsible for the coordinated management of large-scale cybersecurity incidents and crises at the operational level and comprises representatives of the Member States' cyber crisis management authorities and the Commission (Directive (EU) 2022/2555, 2022). It acts as the link between the technical level (CSIRTs) and the political level of the EU, and accordingly develops European situational assessments and impact analyses, and supports decision-making at the political level. ENISA provides the secretariat for this network.

ENISA is also responsible for 'Cyber Europe', a series of large-scale, cross-border cyber exercises that has been running since 2010 (Federal Ministry of the Interior, 2025). Every two years, complex cybersecurity incidents, which could develop into large-scale cyber crises, are simulated in order to test the Union's technical and operational defence readiness and to evaluate cooperation between Member States and EU institutions. For example, in 2024, the fictional state of 'Voltaros' and alleged state-sponsored APT actors attempted to shift the political balance of power through cyber-attacks on critical infrastructure. In this way, the *EU Blueprint for Cyber Crisis Management* (the joint European handbook for emergencies) is tested under real-world conditions, and gaps in the standard operating procedures (SOPs) are closed (Federal Ministry of the Interior, 2026). The exercises involve representatives from the public sector (CSIRTs), the private sector (companies from critical sectors) and the EU (Federal Ministry of the Interior, 2025).

The *Cyber Solidarity Act* ('CSoA'; Regulation (EU) 2025/38, 2025) provides specific operational tools and financial resources to ensure that the cybersecurity framework established by the *NIS 2 Directive* can be effectively implemented. This legislative act sets out three instruments. Firstly, the "European Cybersecurity Alert System", which consists of national and cross-border cyber hubs that use state-of-the-art technology to detect cyber threats in real time. These are in contact with the CSIRTs network and EU-CyCLONe. Secondly, the cyber emergency mechanism, which provides the EU Cybersecurity Reserve, a pool of trusted private security service providers who, at the request of a Member State or an EU institution, immediately provide technical assistance with the response and initial recovery following a major attack. This information is passed on to the JCU, and the CSIRT network can also request support here in the event of a crisis. Thirdly, the European cybersecurity incident review mechanism[24], which, at the request of the Commission or the EU-CyCLONe network, reviews and assesses significant or large-scale incidents and formulates recommendations to improve the Union's cybersecurity posture.

In the *EU Cybersecurity Index*, the 'Operations' domain measures how effectively technical and operational measures are implemented in practice to respond to threats and maintain the resilience of critical systems (ENISA, 2025). The EU average of 57.63 points is low relative to the scale's maximum of 100 points, as four of the five indicators for this category are very low. This is evident, for example, in the low uptake of AI technologies for ICT security (score: 3.18), the insufficient investment in cybersecurity by essential entities (score: 7.14), the lack of formal CSIRT certifications (score: 10.31) and the low proportion of companies carrying out systematic risk analyses (score: 32.01). It can therefore be concluded that there is still considerable scope for improvement in operational defence readiness across the EU.

3. Promoting a global, open cyberspace

The third pillar focuses on embedding the European vision of a global, free and secure internet worldwide and establishing the EU as a leading global player in cyber policy (European Commission, 2020). In this context, a strong diplomatic response and deterrence system, technological sovereignty, and international standards and norms are promoted.

The WEF Global Cybersecurity Outlook 2026 highlights the particular relevance of this area. The proportion of respondents who have little confidence in their country's ability to respond to major cyber incidents has risen from 26% in 2025 to 31% in 2026 (World Economic Forum, 2026). This shows that operational capability is not only technically significant but also a matter of confidence in state resilience.

Since 2017, the *EU Cyber Diplomacy Toolbox* ('Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities') has provided a framework within the Common Foreign and Security Policy ('CFSP') for issuing coordinated diplomatic responses to cyber threats (Council of the European Union, 2023). The EU's response is tailored to the severity of the incident (Council of the European Union, 2023). This means that, for example, preventive and cooperative measures such as public awareness-raising, diplomatic dialogue, confidential demarches or confidence-building measures to avoid misunderstandings may be employed (Federal Ministry of the Interior, 2024). However, sanctions, such as the freezing of assets or travel bans, may also be imposed. The use of the toolbox must adhere to several principles, including: ensuring the protection of the EU, its citizens and Member States; taking into account the EU's general external relations with the state concerned; achieving the strategic objectives of EU foreign policy; being proportionate to the scale, complexity and impact of the attack; and complying with international legal standards and human rights (Council of the European Union, 2023).

Provided that compliance with the principles is ensured, the toolbox can be implemented through a multi-stage process (Council of the European Union, 2023). As soon as a threat is identified, information is exchanged (often via the EU INTCEN[25]) and discussed in Council bodies such as the Horizontal Working Party on Cyber Issues ('HWPCI'). In the event of restrictive measures being imposed, the Council of the EU decides on a proposal from the High Representative of the Union for Foreign Affairs and Security Policy. Attribution of the attack is a sovereign political decision of the Member States but can be coordinated at EU level. The *EU Hybrid Toolbox* is an extension of the *Cyber Diplomacy Toolbox* and is used for attacks that go beyond purely cyber-attacks, such as state-sponsored campaigns that combine cyber-attacks with disinformation or economic coercion (Federal Ministry of the Interior, 2025). The *FIMI Toolbox* ("Foreign Information Manipulation and Interference Toolbox") is another such extension, specialising in combating foreign information manipulation and interference (Council of the European Union, 2023).

NATO's response mechanisms are designed to ensure the organisation's three core tasks – deterrence and defence, crisis prevention and management, and cooperative security – are upheld in the digital domain as well (Federal Ministry of the Interior, 2024). Most significantly, a large-scale cyberattack could lead NATO to invoke Article 5 of the North Atlantic Treaty on a case-by-case basis (Lété, 2017). This means that the Allies regard a serious digital attack on one member state as an attack against them all and can respond collectively. In addition to this response mechanism, NATO has an established crisis response system designed to ensure a rapid and coordinated response from the Allies. This is synchronised with the EU, and

information is also exchanged at a technical level via the NATO Communications and Information Agency ('NCIA') and CERT-EU. In the *Cyber Defence Pledge* (adopted in 2016 and updated in 2023), the Allies also commit at the highest political level to prioritising cyber defence, strengthening the exchange of information on threats, and expanding training and education (North Atlantic Treaty Organisation, 2016). These measures, coordinated with NATO, form part of the *EU Cybersecurity Strategy* (European Commission, 2020).

The EU is stepping up its involvement in international standardisation bodies to ensure that technological standards remain safe, ethical and people-centred worldwide, and to prevent technological standards from being set by actors who promote authoritarian models of the internet or mass surveillance (European Commission, 2020). The bodies targeted include, amongst others, the ISO (International Organisation for Standardisation[26]), the ITU (International Telecommunication Union[27]), the IEC (International Electrotechnical Commission[28]), the ETSI (European Telecommunications Standards Institute[29]) and the IEEE (Institute of Electrical and Electronics Engineers[30]).

The EU's approach to responsible state behaviour is an essential part of the EU's foreign and security policy, as the EU explicitly uses its cyber diplomacy tools to support the *UN framework* for responsible state behaviour worldwide and to ensure compliance with it (European Commission, 2020). This means that existing international law and the UN Charter (in particular the prohibition on the use of force and the right to self-defence) apply in full in cyberspace (Council of the European Union, 2023). Furthermore, the EU supports eleven voluntary, non-binding norms that set out what states should do in cyberspace (e.g. aiding in the event of incidents) and what they should refrain from doing (e.g. attacks on critical infrastructure). To translate the often abstract UN norms into practical application, the EU and its Member States are vigorously promoting the *UN Programme of Action to Advance Responsible State Behaviour in Cyberspace* (European Commission, 2020). The aim is to establish a mechanism that regularly monitors and promotes practical compliance with the eleven voluntary UN norms, to facilitate the exchange of best practices between states and to provide developing countries with technical and legal support to enhance their cybersecurity and comply with international standards.

Stepping up international capacity-building is not only relevant within the UN framework; the EU has also developed the *EU Agenda for Cyber Capacity Building* to steer these efforts in line with the UN's *2030 Agenda for Sustainable Development* (European Commission, 2020). To this end, the "EU Cyber Capacity Building Board" was established to monitor progress, identify synergies and address gaps in support for third countries. The EU CyberNet is an EU-funded operational network, which pools expertise for global capacity-building. The aim of these efforts is to support partner countries (particularly in the Western Balkans, the EU's neighbourhood and countries undergoing rapid digital development) in enhancing their own cyber resilience.

The EU views deterrence as inextricably linked to the ability to identify and prosecute cybercriminals worldwide (European Commission, 2020). The *Global Programme on Cybercrime* provides direct support to states in building national capacities to combat crime and is led by the United Nations Office on Drugs and Crime (UNODC), based in Vienna (Federal Ministry of the Interior, 2024). Europol (EC3) and ENISA work closely together in this area to harness synergies between technical cybersecurity and criminal investigation work (European Commission, 2020).

CASE STUDIES OF CYBERATTACKS AFFECTING THE EU

WannaCry (May 2017) – *Windows vulnerability led to a ransomware attack on the NHS*

Incident → On 12 May 2017, the global WannaCry ransomware attack began, ultimately affecting over 200,000 computers in at least 150 countries (House of Commons, 2018). The attack exploited the Windows vulnerability MS17-010[31] using the 'EternalBlue' exploit[32] (EuRepoC, 2026b). This vulnerability in the SMBv1 protocol[33] had been known to the US National Security Agency (NSA) for years before it was leaked by the group 'Shadow Brokers' (Steinberg et al., 2021). Although Microsoft had already released a critical patch in March 2017, this had not been installed on many systems at the time of the attack (EuRepoC, 2026b).

Method → WannaCry possessed worm-like functionality that enabled the malware to spread laterally across networks via the SMBv1 protocol automatically following the initial infection of a device (EuRepoC, 2026b). Once a system had been compromised, the ransomware used asymmetric encryption to lock user files and demand ransom payments. The attack was only halted when a security researcher accidentally activated a 'kill switch' embedded in the code in the form of a domain[34] (House of Commons, 2018).

Consequences → In the United Kingdom, the National Health Service (NHS) was hit particularly hard. According to the report by the National Audit Office (NAO), at least 81 out of 236 NHS trusts (34%) in England were affected (NAO, 2018). As a result, an estimated 19,494 medical appointments and operations had to be cancelled. In addition, 595 GP practices were infected, and five hospitals were forced to divert ambulances to other locations. The financial losses to the NHS were estimated at around £92 million, whilst the global cost of the attack ran into the billions (EuRepoC, 2026b).

Motive/Perpetrators → Security agencies in the United Kingdom (NCSC), the USA and Canada identified the North Korean hacking group Lazarus as the suspected perpetrators (EuRepoC, 2026b). As the attackers demanded ransoms of between US$300 and US$600 in Bitcoin, a primarily financial motive is assumed. However, given the technical inefficiency of the decryption process, experts also suspect a geopolitical component aimed at destabilisation or serving as a diversionary tactic (Bendiek & Schulze, 2021).

EU response → The incident significantly increased the pressure to implement the *NIS Directive* within the EU (Bendiek & Schulze, 2021). As part of the *Cyber Diplomacy Toolbox*, in July 2020 the Council of the European Union imposed targeted sanctions against the North Korean company Chosun Expo, which had been linked to the Lazarus Group (Council of the European Union, 2020). The measures included an asset freeze against the entity; listed individuals were also subject to travel bans.

Conclusion → Investigations by the NAO and the House of Commons revealed that basic cyber hygiene, such as consistent patch management and[35] the securing of firewalls, could have largely prevented the attack on the NHS (NAO, 2018). It became clear that incident response plans must exist and be tested in advance with local organisations, as communication during the incident was often improvised (House of Commons, 2018). Finally, the findings underlined the need for centralised oversight and clear lines of responsibility to sustainably enhance the cybersecurity of critical sectors.

NotPetya (June 2017) – *Data from banks, public authorities and energy suppliers irreversibly destroyed*

Incident → The NotPetya cyberattack began on 27 June 2017, the eve of Ukrainian Constitution Day (EuRepoC, 2026g). Although the malware appeared superficially to be ransomware, technically it was a wiper designed to irreversibly destroy data on infected systems (Steinberg et al., 2021). The attack spread from Ukraine across the globe and is classified by the US as the most destructive and costly cyberattack in history (EuRepoC, 2026g).

Method → The initial infection occurred via a supply-chain compromise of the Ukrainian accounting software M.E.Doc, which was used by around 80 per cent of companies in Ukraine for tax processing (Steinberg et al., 2021). The attackers exploited backdoors in software updates to inject the malware into users' networks. Once inside the system, NotPetya spread laterally within local networks automatically via the 'EternalBlue' exploit (EuRepoC, 2026g). In addition, the Mimikatz tool was used to extract login credentials from RAM, thereby enabling the malware to spread to systems that had already been patched. The malware not only encrypted files but also overwrote the Master Boot Record (MBR) of the hard drives, making recovery impossible. According to experts, the ransom demand of US$300 in Bitcoin served merely as a political cover for the sabotage (Steinberg et al., 2021).

Consequences → The global financial losses are estimated at a total of over US$10 billion (EuRepoC, 2026g). In the EU and globally, numerous large corporations were severely affected; for example, the Danish shipping giant Maersk suffered losses of between US$250 million and US$300 million and was forced to temporarily close 17 of its 76 international ports (EuRepoC, 2026g). The FedEx subsidiary TNT Express recorded recovery costs of around US$400 million (Steinberg et al., 2021). The pharmaceutical group Merck (MSD) reported losses of US$870 million. Other affected companies included Saint-Gobain (France), Reckitt Benckiser (UK) and Beiersdorf (Germany) (EuRepoC, 2026g). In Ukraine, the radiation monitoring systems at Chernobyl, the metro system in Kyiv, airports, and numerous banks and energy suppliers were knocked out.

Motive/Perpetrator → Security agencies of the Five Eyes countries and Ukraine attributed the attack to the Russian military intelligence unit 74455 (GRU), also known as Sandworm (EuRepoC, 2026g). The motive was the strategic destabilisation of Ukraine as part of the political and military conflict with Russia that has been ongoing since 2014. According to the European Repository of Cyber Incidents, the attack was intended to serve as a warning to companies investing in or doing business in Ukraine.

EU response → The incident was among the cyber operations addressed by the EU's first sanctions under the Cyber Diplomacy Toolbox (EuRepoC, 2026g). In July 2020, as part of the *Cyber Diplomacy Toolbox*, the Council of the EU imposed targeted sanctions for the first time against the GRU's Main Centre for Special Technologies (Sandworm), including the freezing of assets. To improve cross-border coordination in the event of major cybercrime incidents, the *EU Law Enforcement Emergency Response Protocol* was also established under the leadership of Europol.

Conclusion → The NotPetya incident highlights the extreme vulnerability posed by third-party software and inadequate patching cycles, as Microsoft had already released the necessary security patch (MS17-010) three months before the attack in March 2017, yet many organisations had failed to install it (EuRepoC, 2026g). Key preventive measures identified included the need

for strict network segmentation to halt lateral movement, as well as the implementation of robust offline backups (Steinberg et al., 2021). Politically, the attack marked the transition to active EU cyber diplomacy, which aims to deter state actors from future attacks through coordinated public attribution and sanctions (EuRepoC, 2026g).

Brno University Hospital (March 2020) – *Czech hospital's servers locked down during the COVID-19 pandemic*

Incident → The serious ransomware attack on Brno University Hospital (Fakultní nemocnice Brno) took place in March 2020, coinciding with the onset of the first wave of COVID-19 in Europe (NÚKIB, 2021). NÚKIB ("National Cyber and Information Security Agency") classified this incident as the most serious IT security incident of the year in the Czech Republic. The ransomware was activated on 13 March 2020 and encrypted large parts of the server infrastructure.

Method → The attackers used a combination of phishing, ransomware and the exploitation of technical vulnerabilities in the systems (NÚKIB, 2021). In line with an observed trend in modern cyber-attacks, this was not a completely indiscriminate campaign, but rather a targeted attack in which the perpetrators spent time within the network after gaining access to assess the data before initiating the encryption. NÚKIB subsequently issued specific warnings about campaigns exploiting the context of the pandemic.

Consequences → The attack led to massive operational disruptions at three of the hospital's sites: the main hospital in Bohunice, the children's hospital and the women's hospital (NÚKIB, 2021). The IT systems failed completely, forcing the cancellation of scheduled operations and disrupting the care of acute patients due to the need to divert them to other hospitals. As the hospital was one of the country's largest centres for COVID-19 testing, the Czech Republic's pandemic response was immediately weakened. The financial loss was estimated at hundreds of millions of Czech crowns.

Motive/Perpetrators → The attack was attributed to criminal groups whose primary motive was financial gain (NÚKIB, 2021). Such perpetrators often select their victims opportunistically and, during the pandemic, have increasingly targeted the healthcare sector, as they assume that hospitals, due to the vital nature of their services and the high pressure they face, are more likely to pay ransoms.

EU response → In the Czech Republic, the incident led directly to legislative changes, as the *Decree on Providers of Essential Services* was amended to increase the number of regulated hospitals from 16 to around 46 and to significantly tighten their security requirements (NÚKIB, 2021). In November 2020, the Czech Republic also adopted a new national cybersecurity strategy (NÚKIB, 2021). At EU level, the Brno case illustrated the healthcare sector's vulnerability, which the NIS 2 Directive addresses through stronger, harmonised cybersecurity requirements across critical sectors (Directive (EU) 2022/2555, 2022).

Conclusion → This case highlights that critical infrastructure is particularly vulnerable in times of crisis; key preventive measures identified include the need for strict network segmentation, consistent patch management and, in particular, the implementation and regular testing of offline backups (NÚKIB, 2021).

HAFNIUM campaign (March 2021) – EBA Exchange servers compromised

Incident → On 2 March 2021, Microsoft announced that a state-sponsored hacking group from China, identified as HAFNIUM, had attacked on-premises versions of Microsoft Exchange Server worldwide (Winder, 2021). It is estimated that over 250,000 systems were compromised worldwide, but a particularly high-profile victim in the EU was the European Banking Authority, which confirmed on 7 March 2021 that its Exchange servers had been targeted (Feldman et al., 2021).

Method → The attackers exploited a chain of four zero-day vulnerabilities to gain administrative access to the servers without valid credentials (EuRepoC, 2026c). Following the initial compromise, the attackers installed webshells as backdoors to control the servers remotely. Using this access, they exported email accounts, downloaded data from the offline address book and stole credentials from system memory (LSASS process) to ensure long-term access to the victims' networks (Microsoft Threat Intelligence, 2021).

Consequences → In the EBA case, the authority initially said that attackers might have gained access to personal data; as of 10 March 2021, the full extent remained unclear (Feldman et al., 2021). Nevertheless, the campaign caused massive damage globally, particularly to small businesses and public authorities. For the financial sector, the attack was classified as a serious threat to cyber resilience, as the manipulation of key institutions can lead to market instability and a loss of confidence (Feldman et al., 2021).

Motive/Perpetrators → Microsoft attributed the campaign with a high degree of certainty to the HAFNIUM group, which operates as a state-sponsored group from China (Winder, 2021). In July 2021, the EU, the US and NATO issued coordinated statements on the wider campaign; the US and partners linked activity to actors associated with China's Ministry of State Security (EuRepoC, 2026c). The group primarily engages in cyber espionage and has, in the past, specifically targeted US research institutions specialising in infectious diseases, law firms, NGOs and political think tanks (Microsoft Threat Intelligence, 2021).

EU response → As part of a coordinated response, the EU called for the immediate installation of the emergency patches provided by Microsoft (EuRepoC, 2026c). On 19 July 2021, the EU officially condemned the malicious cyber activities as part of the *Cyber Diplomacy Toolbox*. The incident heightened the focus on implementing the NIS Directives and reinforced the case for closer cooperation between national authorities and EU institutions such as the Joint Cyber Unit, with a view to improving operational coordination in cross-border incidents (Feldman et al., 2021).

Conclusion → The HAFNIUM case highlights that patch management alone is insufficient for systems that have already been compromised, as installed webshells remain active even after the vulnerability has been patched (Feldman et al., 2021). Key lessons identified included the need for strict network segmentation to prevent lateral movement, and the critical evaluation of on-premise versus cloud solutions, as Exchange Online was not affected (Microsoft Threat Intelligence, 2021).

Viasat KA-SAT / AcidRain (February 2022) – *Satellite network disrupted at the start of the invasion of Ukraine*

Incident → The cyberattack on the Viasat KA-SAT satellite network began on 24 February 2022, coinciding with the start of the Russian military invasion of Ukraine (Guerrero-Saade & Amerongen, 2022). The attack targeted the satellite ground infrastructure (modems and routers) of the KA-SAT-9A network, leading to widespread outages of broadband services in Ukraine and several EU Member States (EuRepoC, 2026f).

Method → The attackers gained access through a misconfigured VPN appliance and then reached the network's trusted management segment (EuRepoC, 2026f). From there, they moved laterally and used their access and legitimate management commands to deploy the AcidRain wiper to large numbers of modems. AcidRain specifically overwrote data in the devices' flash memory, rendering them inoperable and necessitating either a reinstallation of the firmware or a complete replacement of the hardware.

Consequences → In Ukraine, thousands of modems failed at the start of the invasion, disrupting communications between the Ukrainian police and military, as well as those of smart weapon systems (Guerrero-Saade & Amerongen, 2022). The incident also had massive spillover effects in the EU; for example, in Germany, 5,800 wind turbines manufactured by Enercon could no longer be remotely controlled or monitored (EuRepoC, 2026f). In total, tens of thousands of users and organisations were affected; Viasat reportedly shipped around 30,000 replacement modems to affected customers, and the total financial loss is estimated to run into millions.

Motive/Perpetrators → The attack is officially attributed to the Russian Federation (specifically the military intelligence service GRU) (EuRepoC, 2026f). According to the European Repository of Cyber Incidents, it seems likely that the motive was the strategic sabotage of Ukraine's leadership and defence capabilities on the first day of a conventional war.

EU response → On 10 May 2022, the EU officially condemned the attack in a statement by the High Representative and, as part of the Cyber Diplomacy Toolbox, called for consequences for the perpetrators (EuRepoC, 2026f). The incident heightened the political focus on supply chain security and reinforced the supply-chain-security requirements reflected in the NIS 2 Directive, which imposes stricter requirements on risk management in supply chains for critical infrastructure.

Conclusion → The case illustrates that cyber-attacks are now an integral part of hybrid warfare and can be used specifically to cause operational paralysis (EuRepoC, 2026f). Commercial satellite systems are proving to be particularly vulnerable due to differing security standards. Sustainable cyber resilience therefore requires close integration of IT security with physical resilience (in accordance with the CER Directive) and the development of effective early-warning systems.

DDoS attack on the European Parliament (November 2022) – *Overwhelming of the Parliament's servers*

Incident → On 23 November 2022, the European Parliament adopted a resolution designating Russia as a state "sponsor of terrorism" (EuRepoC, 2026d). Just a few hours after this vote, the Parliament's official website was paralysed by a large-scale cyberattack. The President of the

Parliament, Roberta Metsola, confirmed the incident on Twitter and described it as a "sophisticated cyberattack", for which a group with links to the Kremlin had claimed responsibility (Der Spiegel, 2022).

Method → The attack was a DDoS (Distributed Denial of Service) attack. The attackers flooded the web servers with millions of requests in order to overload the system resources and render the website inaccessible to legitimate users (Carter, 2022).

Consequences → The website was unavailable or accessible only to a limited extent in Europe and the US for at least one hour (EuRepoC, 2026d). No leak of sensitive data was reported; the attack targeted availability rather than network access (Der Spiegel, 2022). The attack is regarded as a targeted political provocation in direct response to the preceding resolution (EuRepoC, 2026d).

Motive/Perpetrator → The pro-Russian hacktivist group KillNet claimed responsibility for the attack on its Telegram channel (EuRepoC, 2026d). It explicitly justified the action as a response to Parliament's classification of Russia. KillNet is known for similar campaigns against state and private institutions in Western countries (e.g. Norway, the Czech Republic, Lithuania) that have been critical of Russia's actions in Ukraine (Der Spiegel, 2022).

EU response → The EU institutions responded with strong condemnation; Roberta Metsola demonstratively responded to the incident with the hashtag "#SlavaUkraini" (Der Spiegel, 2022). According to the *2024 NIS Annual Report*, DDoS attacks were the leading cause of outages across reported NIS incidents in 2024, which has further highlighted the need for minimum security standards and the accelerated implementation of directives such as *NIS 2* (NIS Cooperation Group, 2025).

Conclusion → The case demonstrates the high political relevance of cybersecurity, as technical attacks are increasingly being used as a tool for symbolic displays of power and propaganda (EuRepoC, 2026d). Even though no data breach or lasting IT damage was reported, the temporary unavailability of the website served to capitalise politically on the disruption of a democratic institution and to publicly call into question the resilience of EU communications.

BIBLIOGRAPHY

Bendiek, A., & Schulze, M. (2021, December). Attribution: A major challenge for EU cyber sanctions. An analysis of WannaCry, NotPetya, Cloud Hopper, the Bundestag hack and the attack on the OPCW (SWP Research Paper 11). Stiftung Wissenschaft und Politik (SWP).

Federal Chancellery. (December 2024). Cybersecurity Report for 2023. Vienna.

Federal Ministry of the Interior. (2025). Cybersecurity Report for 2024. Vienna.

Federal Ministry of the Interior. (2026). Cybersecurity Report for 2025. Vienna.

Federal Ministry of the Interior. (16 January 2026). National Risk Analysis in accordance with RKEG 2026. Vienna.

Federal Ministry of the Interior. (16 January 2026). Austrian Strategy for the Resilience of Critical Infrastructure (ÖSRKE 2026). Vienna.

Carter, D. (23 November 2022). European Parliament website hit by DDoS attack. The Brussels Times.

Council of the European Union. (30 July 2020). Council Decision (CFSP) 2020/1127 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States.

Der Spiegel. (24 November 2022). Hackers cripple the European Parliament's website.

European Commission. (2026, 27 July). Annex to the Communication to the Commission: Approval of the content of the draft Commission Communication – Commission Guidance on the application of Regulation (EU) 2024/2847 (Cyber Resilience Act) (C(2026) 5252 final)

European Commission. (2026). Proposal for a Regulation of the European Parliament and of the Council on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act 2).

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (16 December 2020). Joint Communication to the European Parliament and the Council: The EU Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).

European Union. (17 April 2019). Regulation (EU) 2019/881 of the European Parliament and of the Council on ENISA (European Union Agency for Cybersecurity) and on the certification of the cybersecurity of information and communications technology (Cybersecurity Act). Official Journal of the European Union, L 151/15.

European Union. (14 December 2022). Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity in the Union (NIS 2 Directive). Official Journal of the European Union, L 333/80.

European Union. (14 December 2022). Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical infrastructure (CER Directive). Official Journal of the European Union, L 333/164.

European Union. (2022, 14 December). Regulation (EU) 2022/2554 of the European Parliament and of the Council on digital operational resilience in the financial sector (DORA Regulation). Official Journal of the European Union, L 333/1.

European Union. (23 October 2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Regulation). Official Journal of the European Union, L 2024/2847.

European Union. (2024, 19 December). Regulation (EU) 2025/38 of the European Parliament and of the Council on measures to strengthen solidarity and capabilities within the Union (Cyber Solidarity Regulation). Official Journal of the European Union, L 2025/38.

European Union. (2026, 13 July). Council Decision (CFSP) 2026/1713 amending Decision (CFSP) 2019/797 on restrictive measures against cyber-attacks threatening the Union or its Member States. Official Journal of the European Union, L 2026/1713.

European Repository of Cyber Incidents (EuRepoC). (2026a, 23 February). Incident details: The pro-Russian group Killnet disrupted both state and private targets in the Czech Republic in April 2022 (Last updated).

European Repository of Cyber Incidents (EuRepoC). (2026b, 20 May). Incident details: The North Korean state-sponsored hacking group Lazarus launched a WannaCry ransomware attack, infecting over 200,000 computers in 150 countries... in May 2017 (Last updated).

European Repository of Cyber Incidents (EuRepoC). (2026c, 26 May). Incident details: The China-Nexus group Hafnium exploited ProxyLogon zero-day vulnerabilities in Microsoft Exchange Server globally from January 2021 (Last updated).

European Repository of Cyber Incidents (EuRepoC). (2026d, 26 May). Incident details: Pro-Russian group Killnet took down the European Parliament website with a DDoS attack on 23 November 2022 (Last updated).

European Repository of Cyber Incidents (EuRepoC). (2026e, 10 June). Incident details: A sub-cluster of the Russian APT Sandworm has allegedly been deploying the AcidPour wiper against Ukrainian telecommunications providers since 13 March 2024 (Last updated).

European Repository of Cyber Incidents (EuRepoC). (2026f, 10 June). Incident details: Viasat hack: Russian military intelligence disrupted Ukrainian satellite broadband services in February 2022 (Last updated).

European Repository of Cyber Incidents (EuRepoC). (2026g, 16 June). Incident details: The Russian state-sponsored APT Sandworm initially targeted Ukrainian infrastructure with a wiper campaign called 'NotPetya' from June 2017, affecting targets worldwide (Last updated).

European Union Agency for Cybersecurity. (2025). The EU Cybersecurity Index 2024: EU-level insights and next steps.

European Union Agency for Cybersecurity. (2026). Consolidated Annual Activity Report 2025. Luxembourg: Publications Office of the European Union.

Feldman, L., Thomas, R., Jaffe, P., & Barton, R. (10 March 2021). The Hafnium attack: Evolving risk of cyber-attacks for the finance sector. Freshfields Bruckhaus Deringer.

Guerrero-Saade, J. A., & van Amerongen, M. (2022, 31 March). AcidRain | A modem wiper rains down on Europe. SentinelLabs.

Hogeveen, B. (2022, March). The UN norms of responsible state behaviour in cyberspace: Guidance on implementation for Member States of ASEAN. Australian Strategic Policy Institute.

House of Commons Committee of Public Accounts. (2018, 18 April). Cyber-attack on the NHS: Thirty-second report of the 2017–19 session (HC 787).

Kerttunen, M., & Hemmelskamp, J. (2023a, March). Case study: NotPetya. European Repository of Cyber Incidents (EuRepoC).

Kerttunen, M., & Hemmelskamp, J. (2023b, 4 October). Case study: Viasat. European Repository of Cyber Incidents (EuRepoC).

Lété, B., & Pernik, P. (2017). EU–NATO cybersecurity and defence cooperation: From common threats to common solutions (Policy Brief No. 38). German Marshall Fund of the United States.

Microsoft Threat Intelligence. (2 March 2021). HAFNIUM targeting Exchange Servers with 0-day exploits. Microsoft Security Blog.

National Audit Office (NAO). (24 April 2018). Investigation: WannaCry cyber attack and the NHS (HC 414).

National Cyber and Information Security Agency (NÚKIB). (2021). 2020 report on cyber security in the Czech Republic.

NIS Cooperation Group. (August 2025). Annual report on NIS Directive incidents 2024.

North Atlantic Treaty Organisation. (8 July 2016). Cyber defence pledge.

Council of the European Union. (19 June 2017). Council conclusions on a framework for a joint EU diplomatic response to malicious cyber activities ('Cyber Diplomacy Toolbox') (Document No. 10474/17).

Council of the European Union. (8 June 2023). Revised implementing guidelines of the cyber diplomacy toolbox (Document No. 10289/23).

Republic of Austria. (13 July 2026). Network and Information Systems Security Act – NISG (version of 13 July 2026). Federal Legal Information System (RIS).

Steinberg, S., Stepan, A., & Neary, K. (2021). NotPetya: A Columbia University case study (SIPA-21-022.1). Columbia University School of International and Public Affairs (SIPA).

Winder, D. (2021, 4 March). Microsoft Exchange attacks are declared an emergency by Homeland Security. Forbes.

World Economic Forum. (2026, January). Global Cybersecurity Outlook 2026. In collaboration with Accenture.

02 / REPORT

Disinformation in the Workplace

Risks of Digital Transformation in the Workplace

The technological innovations of recent years offer enormous potential for the workplace, but are inextricably linked to new, profound sources of stress (EPRS, 2025). This tension in the digital workplace arises from the drive to boost efficiency dramatically through innovation, while employees are increasingly confronted with systematic intensification of work and invasive surveillance (Garben, 2017). Digital technologies are already used regularly at work by 89% of European employees (Dragano, 2024). Widespread consequences of this transformation include a sense of constant surveillance, a deteriorating working environment, and a growing threat from disinformation. These symptoms indicate that economic risk is increasingly being shifted onto employees, thereby creating a new type of workplace relationship.

Technostress Arising from Algorithmic Management

Algorithmic management (AM) refers to the use of systems that partially or fully automate traditional management functions such as issuing instructions, monitoring, or evaluating employees (EPRS, 2025). There are various levels of technological autonomy: In AI-supported management, AI provides data and analyses, while the human manager retains full decision-making authority. In AI-augmented management, the system generates suggestions or recommendations that must be reviewed by humans. The highest level is AI-automated management, which makes decisions independently with minimal human intervention. According to an EPRS analysis based on the 2024 EWCS[36], 42.3% of workers in the EU are already affected by AM, and this figure is expected to rise to 55.5% in the medium term. The prevalence varies greatly by region, ranging from 70.1% in Denmark to 27.2% in Greece. There are also significant differences by sector, as AM is particularly prevalent in the finance and transport sectors, while it is used less frequently in agriculture. Large companies also use the technology more often than small businesses[37] (53% versus 31%).

While this technology can simplify decision-making processes, it also places a significant burden on employees, particularly in the form of so-called “technostress” (EPRS, 2025). This phenomenon refers to the psychological strain resulting from working with digital technologies (Dragano, 2024). It is characterised by various stressors: constant uncertainty due to chronic digital transformation processes (“techno-uncertainty”), stress caused by increasing complexity (“techno-complexity”), stress resulting from technical unreliability (“techno-unreliability”), and the fear of being replaced by technology or more qualified personnel (“techno-insecurity”). The European Parliamentary Research Service found that being exposed to AM is statistically linked to a 6.2% increase in stress levels (EPRS, 2025).

This stress is driven largely by factors such as “techno-overload,” which is characterised by a fast pace of work dictated by digital technology, constant interruptions, and stressful multitasking expectations (Dragano, 2024). According to the European Commission’s Joint

Research Centre, the pace of work is already directly determined by digital technologies for 52.3% of EU workers (González Vázquez et al., 2024). Equally decisive is the "techno-invasion," which through constant availability via mobile devices and the resulting blurring of the boundaries between work and private life promotes an omnipresent "always-on" culture that severely disrupts employees' necessary recovery periods (Dragano, 2024). The European Law Institute and the European Commission emphasise that this requires a regulatory response, which is why the right to disconnect is increasingly understood as an integral part of occupational safety and health.

AM systems are primarily programmed for maximum efficiency, often ignoring human factors such as fatigue, traffic jams, or social needs (EPRS, 2025). This forces employees to maintain a consistently high pace and severely limits their individual judgement and professional creativity. A particular point of criticism here is the "black box" effect, which is the lack of transparency in algorithmic decision-making processes (European Commission, 2021). According to the 2024 EWCS survey, among the 26% of employees whose work is influenced by computer programs, only slightly more than half—15% of all respondents—report that their company has a clear procedure for challenging automated decisions. This makes it considerably more difficult to effectively challenge unfair assessments or sanctions (European Commission, 2021).

In light of these challenges, Members of the European Parliament are calling for a horizontal "Directive on Algorithmic Management" to establish a coherent, workplace-specific framework that ensures the entire workforce is protected from the risks of digital control (EPRS, 2025). A key element of this call is the "human-in-command" approach, which stipulates that significant employment decisions—such as dismissals or salary changes—must never be made solely by an algorithm but must always be subject to human review.

Case Study: AI-Based Triage and Workforce Planning in the French Healthcare System

Following the COVID-19 pandemic, algorithmic-management systems such as Kronos[38] were expanded to compensate for staff shortages and high patient volume (EPRS, 2025). They are primarily used for workforce planning, meaning algorithms determine shift rotations, task assignments, and leave requests. In emergency rooms, AI-based triage systems assign medical staff to patients in real time. However, this technology limits staff's ability to prioritise tasks independently or respond to patients holistically, leading to a sense of micromanagement. The constant digital notifications also cause "alert fatigue" and increase the risk of burnout, particularly among nurses and junior staff.

Case Study: Maximising Efficiency in the Italian Logistics Sector

The intense time pressure and dynamic environment in the logistics sector was the main motivation for the introduction of AM (EPRS, 2025). Companies use platforms such as Kronos or Hubstaff [39] to automate delivery schedules and routes in real time. Real-time dashboards visualise drivers' locations, monitor performance metrics, and optimise routes based solely on efficiency, often ignoring human factors such as necessary breaks, traffic stress, or the challenges of urban navigation. This leads to a massive intensification of work and constant pressure from surveillance, as low-performance scores can automatically trigger disciplinary measures. Furthermore, AM promotes precarious working models in this sector that resemble a "gig economy." [40]

Case Study: Record Fine for Invasive Surveillance by Amazon France

Amazon deployed an extremely precise system that measured interruptions during package scanning down to the second and continuously monitored work speed (EPRS, 2025). In December 2023, the French data protection authority (CNIL) imposed a fine of €32 million for this violation, as the system contravened the principle of data minimisation (GDPR) because the monitoring of break times was deemed excessive. The authority also criticised the lack of transparency, as employees had not been adequately informed about the intrusive evaluation system.

Digital Surveillance in the Workplace

Technological advances in the digital age have transformed systematic workplace monitoring, expanding it from the mere tracking of work output to comprehensive monitoring of the individual, which often conflicts with the fundamental right to privacy (EPRS, 2025). Modern surveillance technologies can track employees' locations and movements using GPS, smartphones, and wearables, a practice particularly common in logistics and platform work (Ball, 2021). Software can analyse keystrokes and click patterns to determine how and when work is being performed (EPRS, 2025). There are now even systems that analyse facial expressions, tone of voice, heart rate, or brain waves to measure attention or stress (Global Workplace Law & Policy, 2024).

The data analyses obtained in this way can be used for "social sorting", a system in which electronic profiles are created to make automated decisions about future work assignments, compensation, or even the likelihood of termination (Ball, 2021). The extent of this trend is illustrated by the fact that, during the pandemic, search queries for software to monitor employees working from home temporarily increased 17-fold (Ball, 2021). In this context, the Austrian Trade Union Federation warns against the proposed 'EU Digital Omnibus', which could weaken workers' rights and the right of works councils to participate in decision-making regarding the introduction of such monitoring systems (ÖGB, 2025).

This constant visibility in the workplace, made possible by digital technologies, creates a psychological dynamic known as the Panopticon effect (Ball, 2021). This means that employees feel constantly observed and are therefore under constant stress. Since surveillance is often

opaque, employees try to pre-emptively adjust their behaviour in a way that will earn them a positive evaluation from the algorithm. This form of unpaid labour (actively shaping one's own digital image) is defined as "scopic labour." The resulting "surveillance anxiety" can lead employees to skip necessary breaks, which in turn significantly increases the risk of stress, exhaustion, and burnout (EPRS, 2025).

According to the EPRS, 37% of employees report increased surveillance through these technologies in their workplace. However, Professor Kurt Pärli of the University of Basel points out that employees have a legitimate expectation of privacy and that any intrusions into privacy must be based on a clear legal basis, serve a legitimate purpose, and be proportionate (Pärli, 2020). The EU AI Act prohibits the use of emotion-recognition systems in the workplace, except for medical or safety reasons. It also gives people affected by decisions based on the output of certain high-risk AI systems a right to clear and meaningful information about the role of the AI system and the main elements of the decision (European Union, 2024).

Example Box: Location and Movement Data

Deliveroo is an online delivery service that connects customers with meals from local restaurants and supermarkets via an app (Ball, 2021). According to reports from 2016/2017, drivers are continuously monitored during the delivery process. Data are collected on the average time taken to accept orders, travel time to the restaurant, waiting time for customers, and the number of late or unassigned orders.

Uber is a ride-hailing service that connects passengers with licensed rental car and taxi companies via an app (Garben, 2017). According to studies, the company has been collecting GPS and accelerometer data from drivers' smartphones since 2015, and risky driving behaviour—such as rapid acceleration or abrupt braking—can result in the automated deactivation of an account.

Example Box: Keystroke and Behavioural Monitoring

During the pandemic (2021), the global call centre provider Teleperformance used webcams to take photos of employees at their home desks at regular intervals, a practice that was criticised as a disproportionate intrusion into employees' private lives (Ball, 2021).

Between 2017 and 2019, Barclays Bank piloted a system in the United Kingdom that tracked employees' computer usage, having previously installed "black boxes" under desks to monitor physical presence (Ball, 2021).

Example Box: Biometrics and Emotion Recognition

Companies such as HireVue[41] and Cognisess[42] use algorithms to analyse facial expressions, tone of voice, and body language in video interviews, which can form the basis for hiring decisions (Ball, 2021). Their use has increased since 2017.

The British consumer goods company Unilever manufactures and distributes everyday products in the areas of nutrition, personal care, beauty, and household goods (Global Workplace Law & Policy, 2024). Starting in 2018, it made extensive use of AI-powered video interviews to efficiently pre-screen thousands of applicants. Under the EU AI Act, AI systems used in recruitment are classified as high-risk, while emotion-recognition systems in the workplace are prohibited subject to limited exceptions (European Union, 2024).

Threats Posed by Disinformation

With the use of generative AI, the threat of disinformation in the workplace has reached new and unprecedented levels. Disinformation is defined as information that is demonstrably false or misleading and is created, presented, and disseminated with the intent to deceive the public or to gain economic advantage (EDMO, 2024). The scale and sophistication of such attacks are increasing, threatening both social stability and the integrity of businesses (EDMO, 2024; European Commission, 2026). For example, the use of large language models has dramatically increased the effectiveness of social engineering attacks[43] (ENISA, 2025). AI enables attackers to compose emails that are virtually indistinguishable from genuine ones, without the grammatical or spelling errors that were once typical, making them much harder to detect. By early 2025, AI-powered phishing campaigns already accounted for more than 80% of all social engineering activity observed worldwide (ENISA, 2025). The concept of Phishing-as-a-Service (PhaaS) is being driven by platforms such as "Darcula"[44] or "Lucid,"[45] which automate the creation of phishing kits and thus enable even technically less-savvy actors to launch complex attacks against hundreds of organisations simultaneously (ENISA, 2025).

The increased volume of AI-generated content is also fundamentally changing the information ecosystem. As early as November 2024, the volume of AI-generated content surpassed that of human-created content for the first time, and by May 2025, AI-generated content accounted for 52% of all digital content (Bentzen, 2025). This flood of synthetic data is making it increasingly difficult to distinguish fact from fiction and is fuelling the so-called "Liar's Dividend," in which actors exploit the existence of deepfakes to dismiss genuine evidence against them as forgeries. Disinformation campaigns are coordinated operations, often orchestrated by state or non-state actors, designed to disseminate manipulative narratives on a massive scale (EDMO, 2024). Generative AI makes it possible to scale manipulative narratives cost-effectively, which can systematically undermine trust in institutions and internal business decision-making (Abendroth Dias et al., 2025). For example, deceptively realistic deepfakes of executives can be used to manipulate markets or damage a company's reputation through fabricated scandals (Abendroth Dias et al., 2025). This manipulated information can lead to flawed decision-making processes and significant financial losses (Hoxtell, 2024).

In the workplace, informal communication channels often serve as entry points for cyberattacks. In practice, employees often resort to informal messaging platforms, such as private chat groups, to coordinate workflows (EPRS, 2025). This bypasses official IT security controls and creates new vulnerabilities for disinformation and targeted attacks within the company. Women, in particular, are more frequently negatively affected by the increased use of generative AI, as 99% of people targeted by non-consensual sexual deepfakes are women (Bentzen, 2025). According to the EPRS, these attacks are often intended to intimidate and drive women out of the public sphere, cause severe psychological trauma, and cause lasting damage to their reputation. To counter these threats, the *EU AI Act* already establishes transparency requirements for deepfakes and prohibits certain manipulative AI practices (European Union, 2024). In addition, the Digital Services Act (DSA) requires large platforms to actively mitigate systemic risks posed by disinformation (Bentzen, 2025).

Example Box: Espionage and Disinformation on LinkedIn

One infiltration technique involves fake IT workers and fabricated recruitment profiles (ENISA, 2025). A prominent actor is the state-affiliated North Korean group Famous Chollima, which has been increasingly observed attempting to gain employment as IT staff in EU companies, particularly in sensitive government and defence sectors. The group uses generative AI to create deceptively authentic LinkedIn personas, which serve both to communicate with target organisations and to distribute malware via malicious job postings or applications. In addition to cyber espionage through strategic data collection, these actors have also been observed using extortion tactics after the end of their contracts to generate revenue.

Example Box: Disinformation in AI via Manipulated Information on Wikipedia

Disinformation can enter everyday work through supposedly trustworthy knowledge sources whose credibility is exploited for manipulative purposes (Bentzen, 2025). Analyses by DFRLab and CheckFirst of the Russian Pravda network ‘Portal Kombat’ showed that, since the start of Russia's war of aggression against Ukraine, actors have increasingly placed links to Portal Kombat domains in Wikipedia references to launder manipulative narratives and circumvent sanctions against state-controlled Russian media. Since Wikipedia, due to its multilingual nature and enormous scope, is one of the central resources for training large language models, this practice leads to systematic data poisoning. This means that manipulated information is fed directly into AI chatbots, which employees are increasingly using as tools for daily research or decision-making in the workplace—a trend that, in the long term, jeopardises the integrity of internal business processes and the quality of digital public goods.

Example Box: Deepfakes of the Italian Prime Minister

In May 2026, Italian Prime Minister Giorgia Meloni responded to a wave of AI-generated images showing her in underwear that were passed off as genuine (Tagesschau, 2026). A social-media user shared the image as if it were genuine and told Meloni that she should be ashamed. The incident illustrates how quickly deepfakes can cause significant reputational damage.

Deterioration of the Work Environment

The ongoing digitalisation is leading to a fundamental change in the social fabric of the workplace, bringing specific stresses that can worsen the work environment and endanger employees' health.

Since the COVID-19 pandemic, a profound shift in work culture has been observed, characterised by a massive increase in working from home and remote work (ELI, 2023). To meet work demands, highly skilled workers tend toward "voluntary self-exploitation" in situations where work and personal life are blurred, with 27% of people working from home reporting that they regularly work during their free time (Klammer et al., 2017). According to OSH Pulse 2025 data, 43.5% of EU workers report working in isolation, which can weaken team cohesion and increase the risk of depression and burnout (EU-OSHA, 2025). Part of this trend is 'disintermediation', which occurs when human supervisors are increasingly replaced by algorithmic platforms, which undermines social support in times of crisis and leads to a loss of appreciation (Ball, 2021; Heider & Streithofer, 2022).

The strong focus on increasing efficiency is significantly increasing competitive pressure on the workforce. Digitalisation often aims to eliminate downtime, which leads to a significant intensification of work and an acceleration of the pace of work (Heider & Streithofer, 2022). According to the OSH Pulse survey, 52% of workers report that digital technologies directly determine the pace of their work (EU-OSHA, 2025). At the same time, gamification techniques and leaderboards are used to influence employees and encourage them to work faster through "nudges," causing colleagues to be perceived as competitors rather than team members (EPRS, 2025). Customer reviews are also sometimes used directly for disciplinary purposes or to assign tasks, thereby transferring customer biases unfiltered onto employees.

The digital workplace also has measurable effects on physical health. According to Statistics Austria, 86.4% of the working population in Austria is exposed to at least one physical or mental health risk (Heider & Streithofer, 2022). About 37% of EU workers report general exhaustion resulting from chronic stress (EU-OSHA, 2025). In Austria, 37.3% of workers cite significant eyestrain as the main risk of the digital workplace (Dragano, 2024). Prolonged sitting, a hallmark of the digital workplace, can exacerbate musculoskeletal problems (back pain), especially when suitable ergonomic equipment (chairs, lighting) is not provided. Data show that 42% of women and 39% of men spend at least three-quarters of their working hours sitting (EU-OSHA, 2025).

Example Box: Communication in Banking

In Austrian banking operations, digitalisation illustrates the loss of interpersonal communication and the weakening of team cohesion (Madner, 2019). In the past, team members communicated in person to solve problems or coordinate their efforts, but with the introduction of digital management systems, every task is now assigned individually through the system, and employees often no longer even know who else is working on the overall project besides themselves. Questions about work are also handled only within the system and can hardly ever be clarified in person. Social support within the team is dwindling dramatically, as informal conversations and personal exchanges are being replaced by anonymous, standardised system processes.

Example Box: Staff Scheduling in Fashion Retail

In brick-and-mortar fashion retail, computer-assisted staff scheduling—based on weather data or prior-year sales—is so tight that “minimum staffing” is often intentionally planned (Madner, 2019). Digitalisation serves as an argument for further intensification here; for example, the time allotted for a payment transaction has been reduced from 27 seconds to just 22 seconds in order to offset staffing costs. This means that when customer traffic increases, employees effectively have to “work faster” to meet the targets. This leads to enormous stress and, as a result, a drastic deterioration in working conditions.

The increasing use of digital platforms and AM structures is giving rise to a model of “atomised working time,” in which labour is purchased in the smallest of units and only “active” seconds are compensated (EPRS, 2025). This threat is exacerbated by disinformation campaigns and AI-powered phishing, with health and psychosocial consequences for workers. Therefore, shaping the digital future requires a coherent regulatory framework to ensure that efficiency is not maximised at the expense of health and privacy. Future digital resilience in the workplace should be enhanced through a “human-in-command” approach, the promotion of AI literacy, and the early involvement of the workforce. The central challenge remains to manage digital innovations in a way that fully harnesses their potential to ease the burden of work without eroding the foundations of social protection and human well-being (EPRS, 2025).

Bibliography

Abendroth Dias, K., Arias Cabarcos, P., Bacco, F. M., Bassani, E., Bertoletti, A., et al. (2025). Generative AI Outlook Report: Exploring the Intersection of Technology, Society, and Policy. European Commission, Joint Research Centre.

AnySecura. (2026, 7 June). Hubstaff review: Core features, pros, and cons. https://www.anysecura.com/blogs/hubstaff.html

Ball, K. (2021). Electronic monitoring and surveillance in the workplace: Literature review and policy recommendations. European Commission, Joint Research Centre.

Bentzen, N. (2025). Information Manipulation in the Age of Generative Artificial Intelligence (Briefing PE 779.259). European Parliamentary Research Service (EPRS).

Dragano, N. (August 29, 2024). Health Risks and Prevention in the Digital Workplace: Technostress, Ergonomics, and Accident Prevention. Aus Politik und Zeitgeschichte (APuZ)/bpb.de.

Dragano, N., Riedel-Heller, S. G., & Lunau, T. (2021). Do Digital Technologies at Work Affect Mental Health? *Der Nervenarzt*, 92(11), 1111–1120.

European Agency for Safety and Health at Work [EU-OSHA]. (2025). OSH Pulse: Occupational Safety and Health in the era of climate and digital change (Flash Eurobarometer).

European Commission. (2021). First-phase consultation of social partners under Article 154 TFEU on improving working conditions in platform work (C(2021) 2611).

European Commission. (2026). Code of Conduct on Disinformation. Shaping Europe's Digital Future.

European Digital Media Observatory [EDMO]. (2024). How Is Disinformation Addressed in the Member States of the European Union? 27 Country Cases.

European Law Institute [ELI]. (2023). Guiding Principles on Workers' Right to Disconnect.

European Parliament. (2021). Report on fair working conditions, rights, and social protection for platform workers —new forms of employment in the context of digital development (2019/2186(INI)).

European Parliamentary Research Service [EPRS]. (2025). Digitalisation, artificial intelligence and algorithmic management in the workplace: Shaping the Future of Work (PE 774.670).

European Union. (2016). Directive (EU) 2016/943 on the protection of undisclosed know-how and business information (trade secrets).

European Union. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).

European Union Agency for Cybersecurity [ENISA]. (2025). ENISA Threat Landscape 2025.

Eurofound. (2025). European Working Conditions Survey 2024: First Findings (A. Parent Thirion, B. Gerstenberger, J. Cabrita, F. Eiffe, S. Riso, K. Fric, J. Hurley, & C. White). Publications Office of the European Union.

Garben, S. (2017). Protecting workers in the online platform economy: An overview of regulatory and policy developments in the EU. European Agency for Safety and Health at Work.

Global Workplace Law & Policy. (2024). The Prohibition of AI Emotion Recognition Technologies in the Workplace under the AI Act.

González Vázquez, I., Curtarelli, M., Anyfantis, I., Brun, E., & Starren, A. (2024). Digitalisation and workers wellbeing: The Impact of Digital Technologies on Work-Related Psychosocial Risks (JRC138992). European Commission, Joint Research Centre.

Heider, A., & Streithofer, P. (2022). Worker protection I: Inter-company worker protection (Labour Law Lecture Notes 08A). Vienna: Verlag des ÖGB GmbH.

Hoxtell, W. (2024). Umgang mit Desinformation in Europa: Herausforderungen und Gelegenheiten für zivilgesellschaftliche Organisationen und Privatsektor. Bertelsmann Stiftung.

Klammer, U., Steffes, S., Maier, M., Arnold, D., Stettes, O., Bellmann, L., & Hirsch-Kreinsen, H. (2017). Work 4.0 – The Impact of Digitalisation on the World of Work. Wirtschaftsdienst, 97(7), 459–476.

Netcraft. (2025, 17 September). Inside the Lighthouse and Lucid PhaaS campaigns targeting 316 global brands. https://www.netcraft.com/blog/inside-the-lighthouse-and-lucid-phaas-campaigns-targeting-316-global-brands

Austrian Trade Union Federation (ÖGB). (December 2025). EU Digital Omnibus: A Threat to Workers' Rights (Fact Sheet). https://www.oegb.at

Pärli, K. (2020). The ECtHR's Case Law on the Protection of Privacy and Against Surveillance in the Workplace. European Journal of Labor Law (EuZA), 224–235.

Reifinger, I. (2021, 7 October). The future of work: Faster, more, and increasingly digital [Interview conducted by P. Leinfellner]. oegb.at. https://www.oegb.at

Riso, S., & Litardi, C. (2024). Employee monitoring: A moving target for regulation. Eurofound.

Swiss Cybersecurity. (March 28, 2024). Phishing-as-a-Service platform sends iMessages on behalf of hundreds of brands. https://www.swisscybersecurity.net/news/2024-03-28/phishing-as-a-service-plattform-verschickt-imessages-im-namen-hunderte

Tagesschau. (2026, 6 May). Kampf gegen Deepfakes: Meloni verurteilt KI-Bild als politischen Angriff. https://www.tagesschau.de/ausland/europa/meloni-ki-deepfakes-100.html

Yun Chee, F. (2025, 4 February). EU lays out guidelines on misuse of AI by employers, websites, and police. Reuters.

03 / TERMINOLOGY

Operational Glossary (Terminology) and Delimiting the Problem

To ensure a common understanding across all partner countries, the project's key terms are defined for the purposes of this survey as follows. This section establishes the terminology used in the research design.

Disinformation

Definition: Disinformation is the deliberate dissemination of false or misleading content through digital communication channels with the aim of deceiving recipients (link). Disinformation must be distinguished from "misinformation" (false information shared unintentionally) and "malinformation" (genuine information used with harmful intent, e.g. through leaks or deliberate shifts in context). (link)

Forms of disinformation:

Fake news: The politically charged term fake news is often used as a synonym for disinformation. Here, the focus is on viral dissemination to reach a broad audience ("clickbait"). Typical features include highly emotive headlines, simplistic blame attribution and the exploitation of existing prejudices or uncertainty. (link)

Example: Russia's war of aggression against Ukraine: In the first year of the war, CORRECTIV's fact-checking team reviewed more than 150 claims spread by Russian state media and Kremlin-linked accounts. Its fact checks have included claims that Zelenskyy had bought a casino in Cyprus and that live footage from Ukraine was staged or taken from the video game Call of Duty. (source) Such narratives seek to systematically undermine trust in democratic institutions and the media, with implications for European security and foreign policy.

Example: 5G and COVID-19: One claim linked the rollout of the 5G mobile standard in Wuhan to the emergence of the coronavirus. Independent research has found that 5G causes neither cellular damage nor flu-like symptoms. (link)

Deepfakes: Deepfakes are AI-generated, manipulated images, videos or audio recordings that convincingly imitate an individual's biometric characteristics, such as appearance, facial expressions or voice. (link) As generative AI becomes more widely available, the barrier to creating such manipulations falls considerably, making them harder to detect.

Example: 2023 Slovak parliamentary election campaign: An AI-manipulated audio recording purported to capture leading politician Michal Šimečka explaining how he intended to rig the election. Political opponents circulated the recording to discredit Šimečka before the election. (Guardian)

Example: attempted interference in a US election: Ahead of the 2024 New Hampshire presidential primary, 73-year-old Gail Huntley received a call using the voice of US President Joe Biden, which advised her to "save" her vote for later. This AI-generated call attracted attention because it demonstrated how advanced and readily deployable the technology had become. (Guardian) (see Vishing below)

AI-generated deepfakes were also used as political propaganda during Ireland's 2025 presidential election and in the Netherlands. (link) The EU has responded, among other things, through legislation such as the Digital Services Act (DSA), which places greater responsibility on platforms to combat disinformation.

Decontextualisation and selective statistics: When content is removed from its original context, it often loses its original meaning and can be used as an instrument of manipulation. (link) Accurate data may be selectively chosen, distorted or misinterpreted to support an incorrect conclusion. In business settings, for example, such distortions of labour-market data or corporate metrics can lead to poor decisions. See Section 3.

Motives: Communication scholar Schulz-Tomančok identifies two central motives: economic interests, where emotive false reports generate advertising revenue, and political objectives aimed at influencing public discourse. (link)

Workplace relevance: Conspiracy theories and populist narratives often spread among colleagues and can significantly worsen the working environment because decisions lack a shared factual basis (link). If an entire company becomes the target of a disinformation campaign, the resulting loss of trust can have legal and financial consequences. (link) If essential occupations in critical infrastructure are affected, this can impair or threaten security of supply and resilience.

Reputational attacks: A common form of disinformation is a targeted campaign against a particular company, individual or group with the aim of damaging its reputation. Defamation, fabricated reviews and artificially generated online outrage are used to influence public opinion. (link)

Rumours

Definition: Rumours are claims passed on without verifiable evidence of their accuracy, although they often appear to be objective information (link). They fall within the category of misinformation: false or misleading information shared without a deliberate intention to deceive (link). Rumours often arise in situations of uncertainty or insufficient information. They perform a social function by attempting to fill "knowledge gaps", even when their content has not been verified. In digital working environments, such as internal chats and social networks, they spread much faster and can quickly reach large parts of the workforce.

Examples from the workplace: Rumours about plant closures are currently circulating at Volkswagen (VW). Following a sharp fall in profits, the group brought in McKinsey to support a "far-reaching restructuring". (link) Employee representatives criticised potential plant closures as irresponsible threats. Such threats generally increase feelings of job insecurity, which numerous studies associate with adverse effects on mental and physical health. (link)

In Germany, section 111 of the Works Constitution Act (BetrVG) requires employers to inform the works council comprehensively and in good time about planned operational changes. Where applicable, a social plan is subsequently drawn up to mitigate adverse effects on employees. The works council can therefore serve as a reliable source of information.

At EU level, employees also have information and consultation rights (e.g. under Directive 2002/14/EC), which are intended to promote transparency and reduce rumours. (link)

Examples from politics: Rumours are also an important tool for influencing public opinion in the political sphere. Claims that Annalena Baerbock wanted to ban pets or abolish widows' pensions were false reports originating in right-wing and conspiracy-oriented communities on social networks and messaging services; sharepics and posts carried them into the mainstream. According to one study, 71% of the false or misleading claims concerning the three candidates for chancellor targeted Baerbock. Traditional media unintentionally amplified such reports by framing them as questions or "debates", even after fact-checkers had identified them as false. The case illustrates how disinformation originating on social media can be amplified by mainstream reporting. (link)

Generative AI, Social Media Algorithms and Filter Bubbles

Social media, AI and the algorithms associated with them use personalised recommendation systems to maximise user engagement, thereby creating "filter bubbles" and a highly distorted picture of reality. These systems analyse large volumes of data, such as click behaviour, dwell time and interactions, and optimise content for the attention it generates rather than its accuracy. (link)

Generative AI: AI makes it substantially easier and cheaper to mass-produce plausible texts, comments and "news"; create deepfakes and synthetic avatars (virtual representations or stand-ins for a person in the digital world, such as profile pictures); and generate content in many languages tailored to different target groups. (link)

Filter bubbles: Social media platforms use recommendation algorithms to rank content in ways that increase the likelihood that users will spend as much time as possible on their platforms. Once users have consumed politically polarising content, they are often shown more of it. This system tends to favour polarising and emotive material, giving it a systematic advantage and creating a distorted information environment. (link)

Search engines and AI: Algorithms operating in the background can influence the visibility of different content. Ranking criteria, personalisation and commercial interests all play a central role. AI-powered search systems, such as answer systems rather than lists of links, can further narrow the selection of information presented.

Study on political candidates: According to a study by Epstein and Robertson, a political candidate's visibility correlates with voting intention. Manipulating search-engine rankings can influence undecided voters to support a particular candidate without being aware of the influence. On average, this affected 20% of undecided voters in the study (the "Search Engine Manipulation Effect"). (link)

Example: DeepSeek AI: According to a technical document published by China's national cybersecurity standards committee, Chinese generative AI systems such as DeepSeek must not contain material that violates the country's "core socialist values". This includes content that

"incites to subvert state power and overthrow the socialist system" or "endangers national security and interests and damages the national image". (link)

International relevance: Political groups and state actors exploit social media algorithms to artificially boost selected topics (see selective information) or disinformation. (link) In its 2024 Global Risks Report, the World Economic Forum identified misinformation and disinformation, amplified by AI, as the leading global risk over the following two years. (link)

Example: influence on the 2024 Indonesian election: Reuters reported that OpenAI's products were widely used in the election to create campaign materials, monitor sentiment on social media, develop interactive chatbots and target voters. (Guardian)

Example: pro-Trump campaigning: In 2026, US media identified hundreds of AI-generated "influencers" depicted as young men or women - some as immigration officers, some scantily clad - who discussed issues such as abortion or the war with Iran from a pro-Trump perspective. The content illustrated how hyper-targeted, personalised political messaging could be used to influence public opinion. (Standard)

Workplace relevance - OECD study: Although the AI boom prompted fears of job losses, the technology has so far led more often to job reorganisation, affecting working conditions, opportunities and skill requirements. The OECD study highlights several dominant trends: repetitive, rule-based or hazardous tasks are increasingly automated, while workers are expected to develop greater AI competence. This suggests that the AI transition affects the labour market unevenly, as some groups are more exposed to automation or have less access to training and are therefore more vulnerable. Increased work intensity is another concern: workers report a faster pace, greater surveillance (see Section X) and a sense of being "always connected". (link)

Social Engineering - Fraud Schemes and Scams

Definition: Social engineering is a strategy used to manipulate and deceive people into disclosing sensitive information, such as passwords, financial information or personal data, or into taking actions that compromise their security. It relies on psychology and human behaviour rather than technical vulnerabilities. (link)

Identity fraud: Identity fraud occurs when attackers use an individual's personal data without that person's knowledge or consent to enter into contracts, order goods or carry out similar transactions. Identity fraud is often facilitated by hacking or social engineering. (link)

Pretexting and deception: Attackers often pose as trusted persons to exploit their target's vulnerabilities. Typical roles include IT support staff, managers and external service providers. (link)

Methods:

Phishing: In phishing attacks, deceptive emails, messages or links to apparently legitimate websites are used to induce recipients to disclose sensitive information, such as login credentials, bank details or personal data. (link)

Spear phishing: Spear phishing is a highly personalised form of phishing. Attackers tailor their messages using information about the target that can be found on social media, such as the person's workplace, current projects, hobbies or holiday destinations. (link)

Vishing: Vishing is a form of phishing conducted through voice communication, usually telephone calls. (link)

Angler phishing: In angler phishing, users of social networks are targeted with deceptive messages, often relating to popular or topical subjects so that they appear relevant and trustworthy. (link)

Quishing: Quishing is a form of phishing that uses malicious QR codes to direct victims to fraudulent content. (link)

Clone phishing: In clone phishing, a copy of a legitimate email previously sent by a trusted organisation is created and its legitimate link is replaced with a malicious one. (link)

Whaling: Whaling is targeted phishing directed at senior executives or other people in leadership positions. (link)

Baiting: Baiting uses an enticing offer to induce people to disclose sensitive information or download malware onto their device. Examples of bait include promised gifts, free software and substantial discounts. (link)

Extortion: Extortion involves threatening to disclose sensitive information or disrupt systems unless a ransom is paid. Attackers create fear to put pressure on their victims. (link)

Malware: Malware is an umbrella term for any type of malicious software.

Ransomware: Ransomware is malware that encrypts data on a device or blocks access to storage systems. Attackers demand a ransom to restore access to the data. (link)

Computer virus: A computer virus is a program that replicates itself by infecting other files or programs and can spread across networks and data systems.

Trojan: A Trojan is malicious software disguised as a legitimate or useful program; once installed, it can covertly provide attackers with access to a system.

Cyber Threats

Cybersecurity: Cybersecurity is the practice of protecting digital infrastructure, including software, servers, data and devices, against malicious attacks, unauthorised access and damage. At its core is the protection of confidentiality (access to data only by authorised persons), integrity (protection against unauthorised alteration of data) and availability (reliable access to functioning systems). This "CIA triad" (confidentiality, integrity and availability) underpins modern security concepts. (link) Cybersecurity is not merely a technical issue; it has major strategic, political and economic consequences.

Cyberattacks: Cyberattacks exploit technical vulnerabilities and human error to damage digital infrastructure, steal data, disable systems or extort ransom. (link) Critical infrastructure sectors, including energy, health, transport and finance, as well as public administrations, SMEs and individuals, all depend on these systems functioning reliably.

Threats to availability: Threats to availability render systems or services unusable through resource exhaustion or network overload, for example by overwhelming servers with large volumes of requests in denial-of-service attacks (DoS/DDoS). (link)

Ransomware: Attackers use ransomware to gain control over systems and extort victims of cyberattacks, including individuals, public institutions and companies. This may involve encrypting data and threatening to publish it or destroy it permanently. (link)

Data compromise: Unauthorised access to sensitive or protected data, for example through hacking, phishing, insider misuse or inadequate access controls, constitutes a compromise of data. (link)

EU examples:

Attack on the European Parliament: In 2022, the European Parliament's website was hit by a sophisticated cyberattack for which a pro-Kremlin hacker group claimed responsibility, shortly after Members of the European Parliament designated Russia a state sponsor of terrorism. The attack disrupted services, although Parliament's IT staff were able to contain it. The incident highlights the growing threat posed by state-sponsored cyberattacks in the EU. (link)

Attack on essential public services: French hospitals - the Centre Hospitalier Sud Francilien in Corbeil-Essonnes near Paris, Cannes Hospital and the Centre Hospitalier de Versailles - were repeatedly targeted by ransomware attacks. In such attacks, hackers encrypt systems, demand a ransom and threaten to publish sensitive patient data. In some cases, hospitals had to turn away emergency patients. (eca.europa)

Attack on IT infrastructure: In July 2021, the Anhalt-Bitterfeld district was hit by a ransomware attack that encrypted central servers and paralysed its administration. The district temporarily suspended social-benefit payments and was unable to provide many public-facing services normally for more than 200 days. The total cost was approximately EUR 2.5 million, and some data have still not been fully recovered. (link) (link)

EU Cybersecurity Strategy: The EU Cybersecurity Strategy and the NIS Directive prompted the adoption of national rules. Key elements include establishing national CERTs/CSIRTs (Computer Emergency Response Teams/Computer Security Incident Response Teams), incident-reporting obligations, requirements for operators of critical infrastructure, and support for research, innovation and awareness-raising. (link)

Cyber threats in the workplace: Employees are often the "entry point" for attacks and also the first to be affected by outages, data breaches or extortion. Common workplace risks include weak passwords, missing software updates and opening suspicious attachments. (link)

Election interference in Slovenia: Ahead of Slovenia's 2026 parliamentary election, the Israeli private intelligence and surveillance company Black Cube was suspected of working with local actors to use covert recordings and compromising material to support corruption allegations against the Golob government and influence the election. (link)

REFERENCE NOTES

Notes

1. The World Economic Forum (WEF) is an international organisation for public-private cooperation that brings together leading figures from the worlds of politics and business to shape global agendas (World Economic Forum, 2026). Its annual report, the 'Global Cybersecurity Outlook', assesses the global cyber threat landscape as well as the perceptions and preparedness of global decision-makers (World Economic Forum, 2026).
2. CISO (Chief Information Security Officer): The senior executive within an organisation responsible for information security, who oversees the strategic and operational management of cyber risks (such as ransomware or supply chain resilience) and acts as the link between the technical defence layer and senior management (World Economic Forum, 2026).
3. The NIS 2 and CER Directives are referred to as 'sister directives' in the proposed Cybersecurity Act 2 (2026) (European Commission, 2026). Physical and digital security are inextricably intertwined (Directive (EU) 2022/2557, 2022). There is mutual recognition whereby entities identified as 'critical' under the CER are automatically classified as 'essential entities' under NIS 2, ensuring a uniformly high level of protection (Directive (EU) 2022/2557, 2022). To avoid duplication of effort and minimise the administrative burden on businesses, the Directives also require close cooperation between authorities and the exchange of information on incidents, thereby effectively preventing redundancies in supervisory and reporting processes (Directive (EU) 2022/2557, 2022).
4. Energy (electricity, gas, oil, hydrogen), transport (air, rail, road, sea), banking, financial market infrastructures, healthcare (hospitals, laboratories, pharmacies), drinking water supply, wastewater management, digital infrastructure (data centres, cloud, DNS, IXPs), public administration (central and regional levels) and space (Directive (EU) 2022/2555, 2022).
5. Postal and courier services, waste management, the manufacture, processing and distribution of chemical substances, the manufacture, processing and distribution of medicinal products, the manufacture, processing and distribution of medical devices, the processing and distribution of foodstuffs, public electronic communications networks and services, and providers of certain digital services (e.g. social media platforms, search engines, online marketplaces) (Directive (EU) 2022/2555, 2022).
6. Incidents involving serious operational disruptions or significant financial losses (Directive (EU) 2022/2555, 2022).
7. CSIRT (Computer Security Incident Response Team): A specialised unit responsible for detecting, analysing and managing security incidents, providing technical support in responding to attacks, and acting as a central information hub for operational cooperation (European Commission, 2026a).
8. NISG is the Austrian implementation of the NIS 2 Directive.
9. A CERT (Computer Emergency Response Team) is a specialised group of experts dedicated to ensuring the security of network and information systems, which supports organisations in preventing, detecting and responding to cyber risks and security incidents (Directive (EU) 2022/2555, 2022).
10. In Austria, this is CERT.at and/or GovCERT (Federal Ministry of the Interior, 2024).
11. These include credit institutions (banks), payment institutions, investment firms, providers of crypto-asset services, insurance undertakings and central securities depositories (Regulation (EU) 2022/2554, 2022).

12. Third-party providers that supply critical ICT services to the financial sector (e.g. cloud providers such as Amazon Web Services or Microsoft Azure) also fall within the scope of the supervisory framework (Regulation (EU) 2022/2554, 2022).

13. IoT (Internet of Things): Electronic devices (such as smart household appliances, wearables or industrial sensors) that are connected to the internet to enable automation, data collection and remote control; however, because they are connected, they often present new vulnerabilities to cyberattacks (Federal Ministry of the Interior, 2026).

14. ENISA draws up 'candidate schemes' on behalf of the Commission, which are then formally adopted by the Commission through implementing acts (Federal Ministry of the Interior, 2024).

15. A DNS service provider is an organisation that provides publicly available recursive domain name resolution services to end-users of the internet, or authoritative resolution services to third parties (Directive (EU) 2022/2555, 2022).

16. Development and implementation of cybersecurity policies and strategies (ENISA, 2025).

17. Measured by society's ability to detect cyber threats and prevent incidents (ENISA, 2025).

18. This section assesses a Member State's ability to carry out cybersecurity operations and ensure resilience (ENISA, 2025).

19. The measure assesses the private sector's ability to prevent, detect and analyse cyber threats and incidents (ENISA, 2025).

20. The European Centre for Combating Cybercrime supports national authorities. In Austria, the Cyber Crime Competence Centre (C4) within the Federal Criminal Police Office is the relevant authority for IT investigations and digital forensics (Federal Ministry of the Interior, 2024).

21. This includes the European External Action Service, headed by the High Representative of the European Union for Foreign Affairs and Security Policy. You can find out more about the Cyber Diplomacy Toolbox in Pillar Three.

22. The European External Action Service is attending as an observer.

23. The Commission is participating as an observer.

24. The review is conducted by ENISA.

25. EU-INTCEN is the Union's civilian intelligence analysis centre and forms the backbone of situational awareness in cyberspace (European Commission, 2020).

26. It develops globally recognised standards in almost all technical and non-technical fields (European Commission, 2020).

27. The International Telecommunication Union is a specialised agency of the United Nations for information and communication technologies (European Commission, 2020).

28. The International Electrotechnical Commission is responsible for global standardisation in the field of electrical engineering and electronics (European Commission, 2020).

29. The European Telecommunications Standards Institute is an officially recognised European standardisation organisation based in France (ENISA, 2026).

30. The IEEE is a global professional association of engineers in the fields of electrical and information technology (European Commission, 2020).

31. A security-related flaw in the Windows operating system that may arise as a result of its design, implementation or configuration (Bendiek & Schulze, 2021).

32. An exploit is a method or a specific piece of program code designed to take advantage of a security vulnerability (weakness) in hardware or software components. This enables attackers to execute unintended commands, such as causing a program to crash, escalating user privileges or executing arbitrary malicious code (Bendiek & Schulze, 2021).

33. A network protocol is a standardised set of rules governing the exchange of data between devices on a network. It enables, for example, shared access to files or printers (Steinberg et al., 2021).

34. A mechanism embedded in the WannaCry code; by registering a specific web address, a security researcher halted the malware's further spread and encryption (House of Commons, 2018).

35. Processes for the systematic installation of software updates to address security vulnerabilities such as MS17-010 (EuRepoC, 2026b).

36. The EWCS (European Working Conditions Survey) is a comprehensive survey conducted by Eurofound to monitor the quality of work in Europe (EPRS, 2025).

37. Large companies are those with more than 250 employees, and small businesses are those with fewer than 50 employees.

38. Kronos is a specialised software platform for algorithmic management (AM) that is increasingly being used in sectors such as logistics and healthcare to automate human management functions (EPRS, 2025).

39. Hubstaff is a time-tracking and productivity-monitoring software platform for teams, used to log hours, track activity through screenshots, and automate related workflows like reporting or payments (AnySecura, 2026).

40. The gig economy refers to a segment of the labour market in which small jobs are arranged on short notice through digital platforms and assigned to independent contractors, freelancers, or part-time workers (Dragano et al., 2021). A key problem is that workers are often classified as self-employed, even though they are subject to a level of control through algorithms similar to that of employees (European Commission, 2021).

41. HireVue is an AI-powered video interview and recruiting platform that enables companies to prescreen and evaluate candidates via on-demand or live video (Guardian, 2018).

42. Cognisess is a provider of cognitive tests and psychometric assessments used in recruiting to evaluate skills, aptitude, and potential (Guardian, 2018).

43. Social engineering attacks refer to psychological manipulation tactics that attackers use to trick individuals into unwittingly or involuntarily granting access to systems, data, or financial resources (Abendroth Dias et al., 2025).

44. Darcula is a Chinese-language phishing-as-a-service platform for global fraud campaigns via SMS, iMessage, and RCS that creates fake websites for well-known brands (Swiss Cybersecurity, 2024). It impersonates more than 200 organisations worldwide and uses automated phishing kits to display login pages that look deceptively real to employees (ENISA, 2025).

45. Lucid is a phishing-as-a-service platform operated by the Chinese cybercrime group XinXin (Netcraft, 2025). It focuses on mobile messaging services (iMessage and RCS) and has used them to target victims in over 88 countries (ENISA, 2025).