schwarz digits

CYBER SECURITY REPORT 2025

PREFACE

THREATS UNLEASHED

Today, no one and nothing is truly safe – politically, economically or digitally. We are living in an age of geopolitical rivalries and economic instability, and the digital space is not spared. Submarine cables and satellites are caught in the crosshairs, IT solutions are pawns in nation state power plays. Attacks on digital supply chains pose a threat to the physical world, triggering unscheduled production stoppages and delivery chaos.

Cyberattacks and misinformation are part of modern conflicts. They endanger critical infrastructure, democracies and economic stability. The number of attacks continues to rise and ransomware remains the most successful way for cybercriminals to generate revenue. Due to a large number of monthly data breaches, our digital and real identities are at risk of being utilized for cyberattacks or identity fraud.

Attackers are well organized, highly professional and sometimes state sponsored. Their objectives are to destroy, steal, blackmail and control. Every vulnerability, lost identity or misconfiguration opens up new ways for successful cyberattacks. Regulatory requirements and the ever-increasing complexity of digital ecosystems are ramping up the pressure on decision-makers and cybersecurity experts to take action.

Cyber defense is a continuous process. The outcomes of our representative survey of 1,000 German companies are alarming – only every second smaller company regularly audits the cybersecurity of its suppliers. Even mid-sized companies only seldom carry out comprehensive technical security checks of their IT systems. Especially the retail and consumer goods companies are lagging behind, both when it comes to the cybersecurity resources at their disposal and the measures they take.

In 2024, around 5.8 billion euros were invested in cybersecurity solutions in Germany. At the same time, cybercriminals inflicted damage totaling almost 179 billion euros. The time has come to rethink our strategy and prioritize proactive defense. Cybersecurity impacts us all and it is not just about technology. Rather, it is about taking responsibility – toward this and future generations. Prevention and education play crucial roles in protecting even the most vulnerable members of society from digital extortion.

Transferring knowledge and implementing concrete measures will be key. Our Cyber Security Report 2025 provides you with an overview. It exposes threats and offers recommendations for action. The digital world is not just a space that we must work together to defend. It is where we are creating a future which is ours to shape, unless we surrender it to those who seek to tear it apart.

As the companies of Schwarz Group, we act ahead and take responsibility. It is important to us to educate and support. We help you with our experience and expertise. Take advantage of this opportunity. Protect yourself.

Let's seize the opportunity to act ahead together.

Gerd Chrzanowski
General Partner Schwarz Group

EXECUTIVE SUMMARY

The cybersecurity landscape evolved at breakneck speed in 2024, with the threat situation increasingly shaped by geopolitical tensions and technological advances. The wars in Ukraine and the Middle East, tensions in the South China Sea and the intensifying formation of political blocs between Europe, the USA, Russia and China continue to have a significant impact on cyberspace. Cyberattacks have now become a key component in hybrid warfare. The rise in state-sponsored attacks on critical infrastructure and the emergence of coordinated disinformation campaigns to exert political influence are especially concerning.

At the same time, attack techniques are becoming increasingly sophisticated. Private and public sector organizations are facing a multitude of threats in parallel, demanding ever higher levels of resilience. The increasing use of artificial intelligence (AI), in particular, is reshaping both offensive and defensive strategies. While AI-assisted threat detection is strengthening defenses, cybercriminals are also leveraging AI technology to automate phishing campaigns and generate deepfake-based social engineering attacks. Having easy access to generative AI capabilities significantly lowers the entry barriers for attackers and fuels the threat situation even further.

Ransomware remains a pervasive threat and has continued to gain in importance thanks to multi-stage extortion tactics and the Ransomware-as-a-Service (RaaS) model. The number of ransomware attacks recorded worldwide rose by 33 percent between July 2023 and June 2024. German companies were especially targeted. In the first half of 2024, a staggering 83 percent of German companies fell victim to ransomware attacks – almost twice the number recorded during the same period the previous year. The rising number of attacks was accompanied by a high level of willingness to pay the ransom.

Along with ransomware, cybercriminals again set their sights on software supply chains. Of particular concern are vulnerabilities in open-source software. These vulnerabilities are systematically exploited and manipulated packages may be inserted. In 2024, more than 6.6 trillion open-source downloads were recorded worldwide. Over the same period, the number of malicious software packages introduced into open-source ecosystems increased by 156 percent compared to the previous year. Cloud services, cybersecurity solutions, IoT environments and industrial control systems are also increasingly targeted by attackers.

In 2024, such cyberattacks inflicted damage totaling around 179 billion euros in Germany. One of 2024's most attention-grabbing events was the faulty update issued by the cybersecurity company CrowdStrike in July, which crippled around 8.5 million computers around the globe running the Microsoft Windows operating system. The resulting chaos was systematically exploited by cybercriminals.

In light of these developments, companies need to continuously reassess their cybersecurity strategies. For this report, a representative survey of 1,001 German companies was conducted in late 2024. It revealed significant discrepancies and differences in cybersecurity measures and perception, depending on the size of the company. While small companies often only have limited resources at their disposal, 42 percent of large companies invest 1 million euros or more in their IT security. The average investment ratio for cybersecurity is 8 percent of the IT budget, with this figure rising to 17 percent for large companies. Despite economic uncertainty, 78 percent of companies have increased their IT security expenditure.

Staff shortages, however, remain a challenge. While 63 percent of all companies have their own IT departments, almost half of small companies have no internal IT security capacity. This lack of qualified staff not only makes it difficult to implement preventive measures, but also to respond quickly to acute threats.

Implementing the NIS 2 Directive poses challenges for many companies, especially smaller ones. Two thirds of all companies consider themselves well or very well prepared for cyberattacks, although 60 percent regard government support to be insufficient.

More than half of companies do not perceive any significant cyber risks associated with their suppliers or external partners. Only 16 percent of small companies

have defined binding cybersecurity requirements for all suppliers, compared with 40 percent of large companies. Across all companies, 49 percent audit their suppliers regularly or occasionally for compliance with security standards.

When selecting providers, large and small companies adopt differing strategies. While 88 percent of large companies pursue a multi-vendor strategy, 93 percent of small companies rely on a single provider. Only 6 percent of small companies perceive reliance on a single source as a risk, compared with 33 percent of large companies. To avoid disadvantageous dependence on a provider, more than half of the companies surveyed rely on open standards or regularly evaluate alternative vendors.

Simultaneously, the market for cybersecurity tools has experienced substantial growth over the past 25 years. There are over 3,500 providers worldwide, but many companies encounter difficulties in identifying and integrating the most fitting solutions. On average, companies are using up to 83 different security products from 29 providers, and in certain cases as many as 336 products from 57 providers. However, this diversity does not only provide benefits, with 64 percent of IT security teams reporting that the products they use are not optimally designed for interoperability, resulting in inefficiency and gaps in security.

Investment in cybersecurity has continued to rise. In Germany, spending on cybersecurity solutions totaled 5.8 billion euros in 2024, while the global market is projected to grow to between 247 and 292 billion US dollars by 2029. Despite this surge in investment, the number of successful cyberattacks has continued to rise. This is partly due to the fact that haphazardly evolving security infrastructures often create more vulnerabilities than they mitigate. There is no single product able to fulfill all requirements for automation, pricing or seamless integration. Companies are faced with the challenge of choosing between specialized best-of-breed stand-alone solutions or an integrated platform. While the latter reduces the administrative workload, it increases the risk of vendor lock-in.

Organizations often invest more than necessary, while essential functions offered by their security products remain unused. Pricing often lacks transparency – antivirus or EDR solutions are comparatively affordable, ranging between 1 and 30 euros per device (e.g., server, workstation). Firewalls are also available from as little as 100 euros, but they can also cost in excess of a million euros.

While companies are struggling to define effective security strategies for their organizations, global infrastructures are increasingly becoming targets of hybrid warfare. Especially submarine cables and satellites, on which most communication, energy and transport systems are heavily dependent, constitute potential targets. Undersea cables, which carry more than 95 percent of global Internet traffic, are a particularly critical target. When such systems are sabotaged, the economic and political consequences may be profound, as shown by incidents in the Baltic Sea in which suspected Russian actors damaged submarine cables. A recent GPS spoofing attack on a passenger flight clearly demonstrated that digital threats could pose direct risks to security in the physical world.

However, it is not just companies, government agencies or political parties that are impacted – individuals are also increasingly targeted in cyberattacks, making it necessary to raise awareness about protecting digital identities and activities in cyberspace in addition to safeguarding digital information environments. The upsurge in sextortion, a form of digital blackmail which couples psychological manipulation with modern technologies, is particularly alarming. While sextortion impacts people of all ages and social backgrounds around the world, teenagers are especially at risk. Perpetrators specifically use social networks, online games and dating platforms to establish contact.

In 2023, at least 12,600 victims reported being targeted by sextortion offenders in 2023, and 20 suicides were documented. With only a fifth of victims reporting the crime, the number of unreported cases remains high. Moreover, these crimes are not reflected in many police statistics. Technological developments have made it

even easier to commit this type of crime. Eleven percent of the content used in sextortion cases is already fake. Moreover, perpetrators use encrypted communication platforms and hard-to-trace cryptocurrencies to evade prosecution.

It is especially important to protect the most vulnerable members of our society through targeted prevention, technological innovation and resolute social action. Only a concerted effort by politicians, educational institutions, tech companies and law enforcement agencies can effectively prevent these attacks.

CONTENTS

CHAPTER 1

STATE OF PLAY
CYBERSECURITY TRENDS 2025

Top threats in 2024

Misconfigured systems
38%

Zero-day vulnerabilities
30%

Lateral movement by adversaries
28%

31%
Vulnerabilities in apps developed in-house

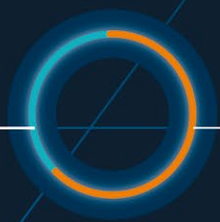
29%
Known software vulnerabilities

Cybersecurity outlook for 2024:
Biggest impact on cybersecurity

AI / MACHINE LEARNING
66%

- Convergence of IT and OT security — 13%
- Cloud technologies — 11%
- Quantum technology (computing, encryption) — 4%
- Decentralized technologies (e.g., blockchain) — 3%
- Satellite technology (communication, GPS, internet) — 2%
- Other — 2%

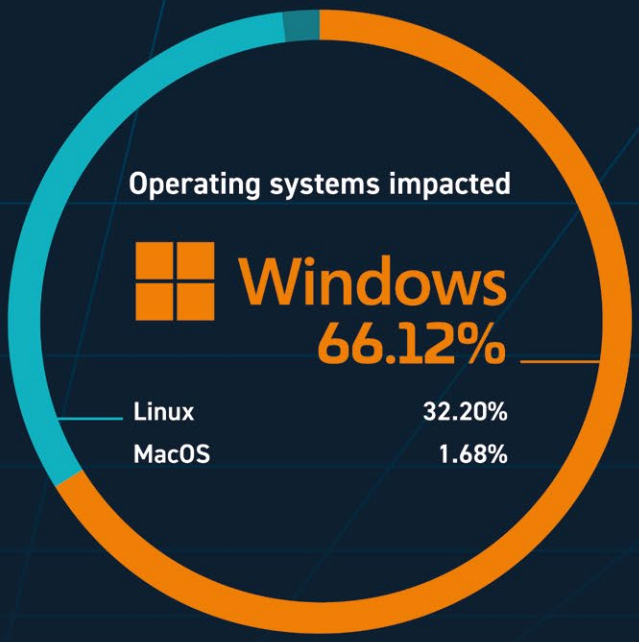
Has a process been established at your company to evaluate the security of AI-assisted software before it is used?



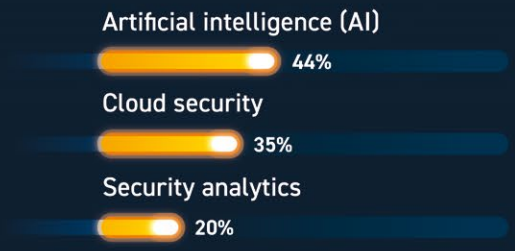
Yes: 37%

No: 63%

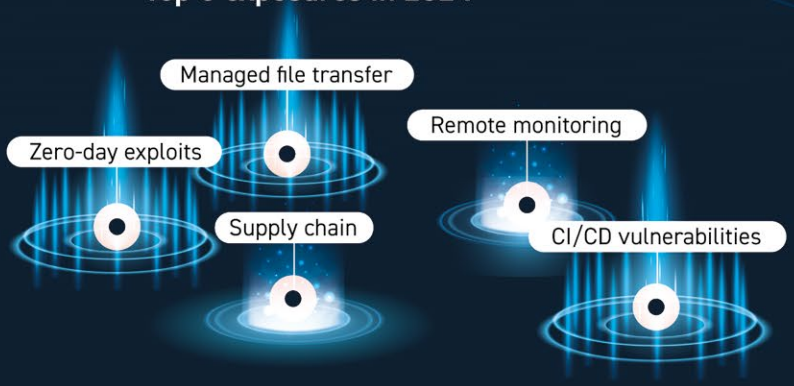
Operating systems impacted



Security initiatives in 2024

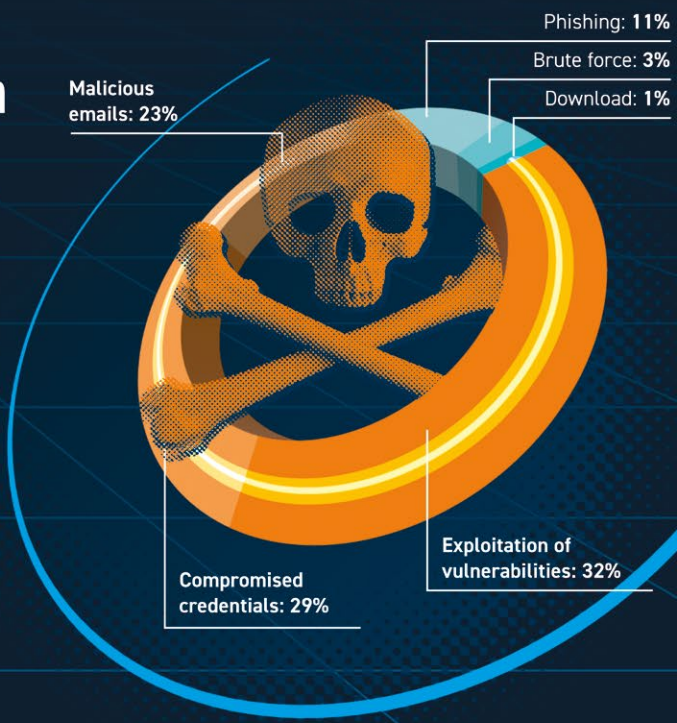


Top 5 exposures in 2024



Average global costs of a data breach

Major gateways for ransomware attacks worldwide



Average ransom per incident

USD **300,000**

for encrypted data

USD **850,000**

for exfiltrated data

Sources: [20], [46], [74], [226], [144], [149], [267], own diagram

1 STATE OF PLAY – CYBERSECURITY TRENDS 2025

1.1 GEOPOLITICAL SITUATION AROUND THE GLOBE

Today's complex geopolitical landscape is characterized by rising tensions and growing conflicts. The wars in Ukraine and the Middle East, tensions in the South China Sea / Taiwan Strait and the humanitarian crisis in Sudan are contributing to global uncertainty. The intensified formation of blocs between Europe, the USA, Russia and China is also contributing to this. These developments also have an impact on cyberspace, which has emerged as an important battleground. Digital sabotage, espionage and disinformation are now essential elements in the waging of war [170].

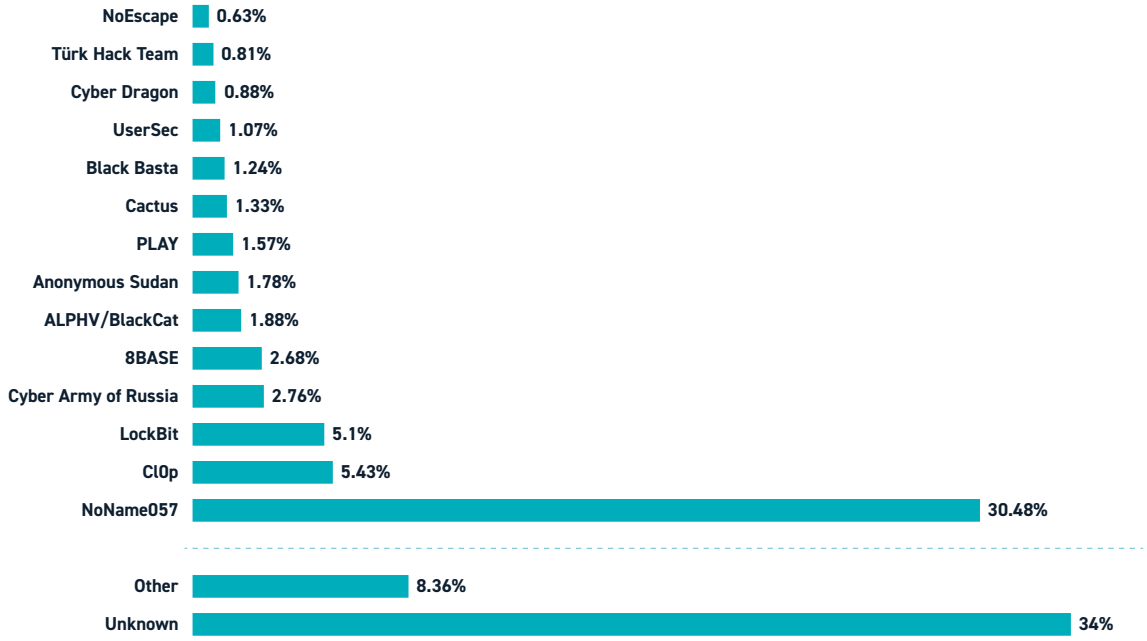
Within this context, state actors and non-state groups such as militias, terrorist organizations and insurgents are increasingly using cyberattacks as a means of power politics, in order to pursue strategic objectives and destabilize their adversaries. The ever-increasing sophistication and frequency of cyberattacks pose considerable risks and threats to civilians, businesses, institutions and governments. At the same time, digital warfare encompasses far more than attacks focusing on digital military targets. Public service infrastructures and companies are increasingly coming under attack. As well as being exposed to direct attacks, organizations are also at risk of suffering collateral damage [6]. In addition to damaging attacks, it is also evident that state-orchestrated disinformation campaigns are aiming to influence the public through media manipulation and conveying misinformation. From a business perspective, cybersecurity and geopolitical conflicts are also among the most challenging present-day issues [6]. Especially when the two issues coincide, they constitute a significant risk for companies [237] and require decision-makers to have a greater understanding of geopolitical dynamics to ensure effective long-term management of the risks [6].

Geopolitical tensions between the major global powers have now expanded into a new dimension of warfare. Cyberattacks serve both as espionage tools and as a means of damaging physical systems and critical infrastructure across all sectors [245]. They are also used to probe the limits of what Western democracies are willing to accept, also known as "gray zone" confrontations.

The rise of China is also increasing the complexity of the cyber threat landscape. The growing influence of China is increasingly calling into question the dominance of cyber powers such as the United States [2], [82]. Beijing has begun to shift its focus from cyber espionage motivated by economic interests to an explicit pursuit of global technological superiority and (re)shaping the Internet [2]. In 2024, China developed into the most important base for attacks on the German economy. Of the companies surveyed in the Bitkom study, 45 percent were able to trace at least one attack to China. In 2023, Russia was still the biggest source of attacks [237]. A key aspect of China's cyber strategy is the concept of military-civil fusion (MCF), which promotes cooperation between the private sector and the military, as well as integrating their resources. Moreover, the government leverages state-sponsored hacker groups to conduct wide-ranging cyber espionage and sabotage campaigns [197].

NATO and its allies depend on strong, resilient cyber defenses to fulfill the alliance's three core missions – deterrence and defense, crisis prevention and management, and cooperative security [209]. The Member States and the participating European Union Institutions, Bodies and Agencies (EUIBA) have therefore made a commitment to annually test their responses to scenarios developed on the basis of the regular EU risk assessment procedure. This is all carried out within the framework of a special annual cyber defense exercise [249].

However, cybercrime does not only play a role at the organizational level or in an acute war situation. Civilians are also at risk of falling victim to such attacks. In November 2024, for instance, the German Federal Office for the Protection of the Constitution warned of potential attempts by other states to influence the upcoming federal elections. This may involve "acts of disinformation and discreditation, cyberattacks, espionage and sabotage". By disseminating false facts, it is not only possible to influence decision-makers and officials, but also to interfere in the independent formation of opinion and will. Elections can thus be influenced indirectly through theft,



Source: [96]

Figure 1: The most active attackers (July 2023 – June 2024)

manipulation and the publication of (false) information. In this context, the office responsible for protecting the constitution issued a warning regarding Russian attacker groups, which have been particularly active during previous elections (fig. 1 provides an overview of the most active attackers) [285].

1.2 GENERAL CYBERSECURITY THREAT LANDSCAPE

In 2024, the cyber landscape was again characterized by a heterogeneous threat situation. Both the geopolitical environment and innovations in technology (and especially the combination of these two factors) pose challenges for users and developers of software systems. In particular, the use of artificial intelligence (AI), both on the part of attackers as well as for protection, played a role in shaping the cybersecurity threat situation in 2024 [19], [96]. Artificial intelligence, especially large language models (LLMs), is progressively lowering the barriers to entry and thus increasing both the reach and pace of malicious activities, for instance through the autonomous generation and mutation of malware, social engineering attacks (e.g., pretexting and deepfakes) and data analysis during attacks (e.g., big data and automated analysis of mass data). This boosts the attackers' competencies and leads to qualitatively superior attacks [6]. On the other hand, AI can also be used to automatically identify security vulnerabilities in the context of defending against cyberattacks. AI-based systems help to detect indications of compromise or malware infections in protected systems by monitoring the behavior of users and checking for unusual patterns [19], [47].

Attacks on web servers, online services or entire networks, such as distributed denial of service (DDoS) attacks, remain widespread. The aim of such attacks is to disrupt or make the affected resource completely unavailable by overloading the server resources and blocking legitimate user requests. In particular, we have witnessed an increase in politically motivated attacks by individuals or small groups [96] as well as state-led actors in the face of geopolitical tensions. In the context of the current geopolitical situation, government authorities, transport logistics and financial institutions have been targeted specifically by geopolitically motivated attackers [96]. An increase in technical proficiency and improved cost efficiency have also had the effect of lowering barriers to using DDoS tools [96]. For example, DDoS-for-hire services can enable less tech-savvy individuals to conduct large-scale distributed denial-of-service attacks. Providers of such services either carry out these attacks themselves or make the required tools available to their customers. The combination of DDoS-for-hire services and the ease of creating botnets through the proliferation of insecure devices has created the ideal preconditions for carrying out attacks which cause large-scale disruption.

Ransomware remains one of the biggest challenges in the field of cybersecurity [6]. Multi-stage extortion tactics, which involve threats to publish stolen information in addition to encrypting the data, are still on the rise in Germany and Europe [96]. However, while the average

ransom demanded has increased, the success rate concerning the enforcement of payments has fallen slightly [47]. In a global comparison, organizations paying ransom reported an average payment of approximately USD 2 million, compared to USD 400,000 in 2023. German companies had to dig even deeper into their pockets, with an average ransom payment of USD 5.5 million [242]. State-backed advanced persistent threat (APT) groups, especially based in Russia and China, are increasingly targeting critical infrastructure in Europe. These groups exploit zero-day vulnerabilities and use specialized malware to conduct cyber espionage and sabotage operations [30], [46]. The focus has often been on organizations whose security lacks maturity (see fig. 2 for companies' assessments of their own cyber resilience) [166].

The use of social engineering as an attack vector, which comprises manipulation techniques including personal interactions, has increased by 4 percentage points compared to the previous year [145]. Phishing is a specific type of social engineering in which attackers attempt to obtain confidential information, such as passwords, bank details or credit card information, by means of fraudulent emails, websites or messages. According to the BSI, phishing emails are often used to deceive users and circulate malicious links or attachments that can potentially lead to the infiltration of systems with malware [46]. At the same time, the barriers to entry for social engineering are also falling due to the simple scalability made possible by LLMs, the ease with which language barriers can be overcome and the ability to personalize attacks [6], not to mention the lack of security awareness among many users. This is also reflected in the survey conducted by the BSI for its Cyber Security Monitor 2024. It revealed that the use of safeguards such as antivirus programs and secure passwords is declining compared with the previous year. Respondents cited feeling highly secure and the excessive complexity of protective measures as reasons for this [45]. Due to the high availability of information, attackers are also increasingly able to better place their malicious content in a context relevant to their target, deceive them with a tangible benefit and thus significantly increase their success rates.

Source: [6]

Figure 2: Companies' assessments of their own cyber resilience

Attacks on supply chains have also established themselves as one of the most critical threats [30]. Of the executives surveyed in Germany, 26 percent either know or suspect that their suppliers have fallen victim to cyberattacks within the past twelve months. The increasing complexity and lack of control over supply chains has emerged as the biggest hurdle to cyber resilience for companies, with larger companies more aware of the threat than smaller organizations [6]. Companies are increasingly adopting a holistic view of the supply chain and focusing on implementing the appropriate management systems to manage the risks posed by cyberattacks. Appropriate supplier risk management along the entire supply chain can reduce the risk [30]. Zero trust security, an approach in which no internal or external user is trusted by default, is also particularly fitting, as this can increase security and lead to the prevention of potential attacks [303].

Whereas a cyberattack on the physical supply chain jeopardizes production, payment systems or logistics processes, an attack on the software supply chain aims to compromise digital products and their integrity. Open-source projects, in particular, are increasingly being targeted by attackers who insert malicious code fragments in order to carry out attacks on the software supply chain. In March 2024, for example, backdoor code was inserted into the open-source project XZ Utils, a collection of products and libraries for data compression. Such incidents illustrate the risks associated with inadequately secured open-source projects [96].

The general threat landscape indicates that attackers are becoming more specialized and increasingly leveraging cutting-edge technologies such as AI. The combination of geopolitical tensions, which are also driving an increase in cyber-based industrial espionage and sabotage in Germany [319], technological advances such as the use of (AI-generated) deepfakes to spread false information, and ever more extensive networking is presenting organizations with unprecedented challenges. It is therefore all the more important to adopt a holistic, proactive security strategy which incorporates both technological and organizational measures in order to strengthen resilience over the long term.

1.3 OVERVIEW: CYBERSECURITY INCIDENTS IN 2024

In 2024, it was once again striking to note just how vulnerable even digital infrastructures that were considered robust can turn out to be. It is not only the users of software and networks who are exposed to increased risks. Providers of IT security solutions, such as Ivanti [52] or Fortinet [161], are also attracting the attention of criminals. A series of high-profile cyberattacks has hit companies, authorities and institutions alike, revealing exposures across the global digital landscape.

As in the previous year, the wide variety of sectors which came under attack was particularly striking. The range of victims extended from tech companies to state and private institutions as well as political parties. In February 2024, for instance, it was reported that technology company Microsoft had been hit by a massive cyberattack on its Azure cloud computing platform, with a phishing campaign leading to numerous accounts belonging to top executives being compromised. This was the first incident of its kind in Microsoft's history. Government institutions were also affected, such as the municipal administration of Aschaffenburg, where suspicious access to employee user accounts led to all IT systems being taken offline as a precautionary measure in November 2024 [268] and the state government of Mecklenburg-Western Pomerania in May 2024, where access to websites was disrupted by means of a DDoS attack [208].

Non-profit organizations were also impacted in 2024, including the largest not-for-profit healthcare system in the US, Ascension, and the cross-regional hospital operator Johannesstift Diakonie, which faced attacks that jeopardized the medical records of thousands of patients, in May and October respectively [337].

Political parties were not left unscathed either. The CDU fell victim to a cyberattack in May 2024, just prior to the European elections, which made internal communication data public. Shortly before the state elections in Brandenburg in September 2024, a hacker attack was announced

by the AfD Brandenburg [248]. Yet another example is a DDoS attack on the FDP state election campaign website in August 2024 [54]. Email accounts belonging to the SPD had already been attacked in 2023 (although the investigation did not take place until 2024). In September 2024, the Austrian People's Party (ÖVP) and the Social Democratic Party of Austria (SPÖ) also reported being victims of DDoS attacks [216]. Many more examples can also be found internationally, showing the danger of cyberattacks on political parties as essential participants in democratic processes. For example, the Japanese Liberal Democratic Party (LDP) became the victim of a cyberattack in mid-October, coinciding with the start of the election campaign there [246]. The attack was attributed to a pro-Russian hacker group, which paralyzed several other Japanese institutions with DDoS attacks in 2024, including local government websites [189], [204].

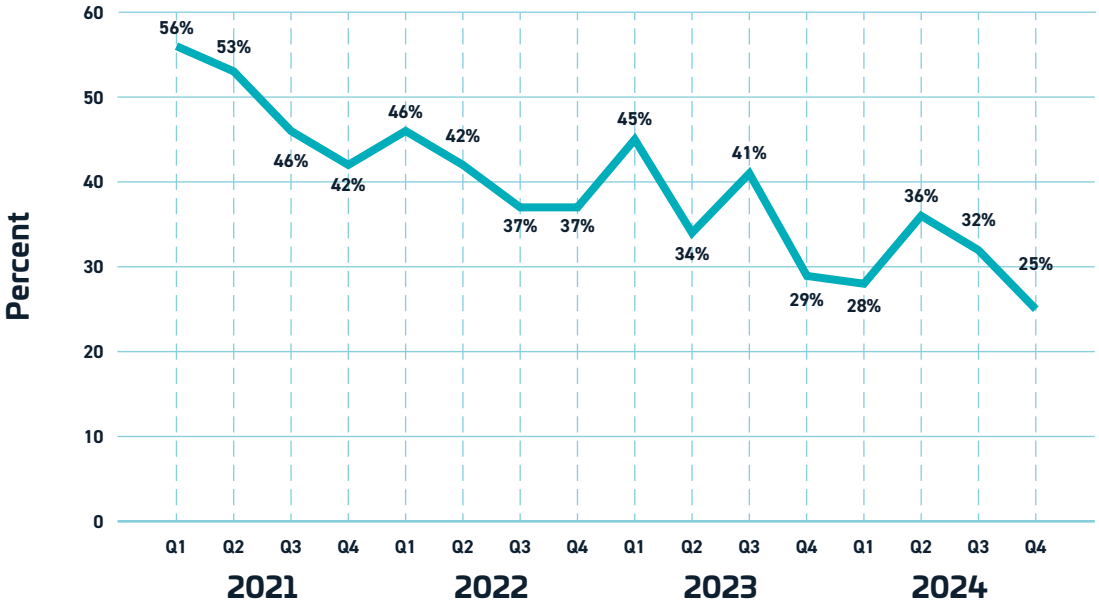
In addition to political institutions and parties, cyberattackers also took aim at politicians and government officials. At the beginning of December 2024, US security authorities reported that Chinese hackers had allegedly succeeded in penetrating the systems of at least eight US telecommunications providers. According to reports, extensive amounts of metadata was stolen from American citizens in the course of the attack. The attackers targeted high-profile political, government and intelligence figures. They were able to access geodata and telephone logs, while also making recordings of private conversations held between US politicians, diplomats and security officials [313].

In addition to financial gain, the purpose of such cyberattacks on political parties and politicians is often to cast doubt on the legitimacy of elections and institutions, and to undermine trust in the democratic process [46], [56]. Similarly, legitimate digital tools and approaches may be used to intervene in democratic processes. Social media platforms such as TikTok, Instagram and YouTube have created a space in which disinformation and election manipulation can flourish. Using bots, paid influencers and the deliberate manipulation of algorithms, partly anonymous actors are able to influence election results and cause considerable damage to democratic systems, states and populations [282], [336].

Ransomware –
the art of extortion in the digital age

Ransomware attacks remained the dominant threat vector in 2024 despite the successful dismantling of several well-known ransomware groups, such as LockBit in February [257] and BlackCat in December [31]. In a year-on-year comparison, the number of ransomware attacks registered worldwide rose by 33 percent between July 2023 and June 2024. Attacks increased most in the USA (+63%) and the UK (+67%) compared with the same period a year earlier [188]. At the beginning of January 2025, a British cybersecurity website reported that ransomware groups had claimed responsibility for 5,461 successful ransomware attacks on organizations worldwide during the course of 2024. Among the 1,204 attacks confirmed by the organizations impacted, the data revealed that 195.4 million data records had been compromised. The figures for 2024 are lower than those for 2023 (1,474 confirmed attacks affecting 261.5 million data records), but as many attacks are only reported with a delay after the attack – in the course of investigation and prosecution efforts – these figures can be expected to rise [195]. It is also believed that the threat situation for German companies has worsened considerably. During the first half of 2024, 83 percent of German companies fell victim to a ransomware attack – almost double the 48 percent impacted in the same period the previous year. This makes Germany a global leader not only in terms of the number of attacks, but also in terms of willingness to pay ransom [125]. Another alarming trend is that in the first six months of 2024, cybercriminals extorted ransom totaling USD 459.8 million worldwide (see fig. 3) [266].

One notable incident occurred on May 8, 2024, when Ascension, the largest non-profit healthcare system in the US, discovered unusual activity on its networks which indicated a ransomware attack by the Black Basta group [181]. The attack impacted nearly 150 hospitals in over 10 US states, leaving medical staff without access to critical systems and patient data. The incident resulted in lost lab results, errors in the dosing of medication and an incapacity to admit emergency patients for over a month [181]. On June 14, 2024, Ascension was able to announce that access to electronic health records had



Source: [76]

Figure 3: Proportion of companies which paid ransom following a ransomware attack

been restored, but that patient data still needed to be updated. According to the organization, the ransomware attack succeeded as a result of a person working at an Ascension facility accidentally downloading a malware infected file which they had thought was legitimate [314].

On October 5, 2024, the Japanese electronics company CASIO confirmed that a ransomware attack had led to a data leak. Hackers managed to obtain personal information and confidential files from the company and its affiliates [165]. The ransomware group Underground claims to have exfiltrated over 200 GB of data belonging to over 128,000 consumers as well as data relating to business partners, including legal documents, salary details and financial records. CASIO's investigation into the incident is still ongoing and has thus far determined that employee, business partner and customer information has also been affected. CASIO confirmed that a misconfiguration in the ClassPad.net development environment was at the root of the security breach. The stolen data comprises names, email addresses, place of residence, information related to purchases and usage data. CASIO emphasized that no credit card information had been compromised and promised to contact affected customers and strengthen future security measures [69].

State-sponsored attacks and political cyber warfare

As already seen in the Schwarz Cybersecurity Report 2024 (SCSR24), the activities witnessed in 2024 underscore the fact that geopolitical and cross-border conflicts often go hand in hand with a number of phenomena in cyberspace. These include disinformation, espionage, sabotage and politically, socially or ideologically motivated cyberattacks [46]. According to the German Federal Criminal Police Office (BKA), geopolitical conflicts have increasingly been shifting into the digital realm over the last two years. The growing number of global conflicts has led to a significant increase in hacker attacks. This politically motivated cybercrime is often carried out by means of DDoS attacks, in which attackers automate the flooding of websites with a large number of requests until they become overloaded and no longer accessible [60].

Political parties may also be targeted by state actors engaged in politically motivated discrediting campaigns. Successful cyberattacks, data leaks and loss of control influence the reputation of individuals and organizations as well as adversely affecting acceptance of the democratic party system. The backers of these attacks aim to create or reinforce uncertainty and divisions within society and exert influence on political decisions through measures aiming to shape public opinion [56].

The cyberattack on the CDU at the end of May 2024 – just one week before the European elections – can also be seen from this perspective. In the course of this attack, data belonging to CDU party chairman Friedrich Merz was compromised, including calendar data. Along with other attack vectors, the hackers exploited a vulnerability in a CheckPoint product which enables employees to connect securely to their employer's network [284]. In this case, adversaries used the CVE-2024-24919 vulner-

ability in security gateways in combination with phishing attacks to obtain information through Internet-connected gateways where remote or mobile access is enabled [129]. The hacker group APT29 – also known as Cozy Bear, Midnight Blizzard, Nobelium or The Dukes – which is backed by the Russian government, is suspected to have been behind the attacks. Another objective of the phishing attack was to deliver a new variant of the WINELOADER backdoor. With this attack, APT29 broke new ground. It was the first time the group, which had previously primarily targeted diplomatic organizations, took aim at a political party. This signaled a potentially dangerous expansion of its sphere of interest. In total, up to 1,800 IT systems across Germany which use Check Point network security products were endangered by this exposure. In addition to the CDU, critical infrastructure operators in the transport and healthcare sectors were also attacked successfully [25].

Back in January 2023 (although it was not clarified until May 2024), SPD email accounts at federal level were attacked using a vulnerability in the Microsoft Windows client for Outlook (CVE-2023-23397) [26], [170]. The German Federal Office for the Protection of the Constitution attributed the operation to the hacker group APT28 (also known as Sofacy, Fancy Bear, Pawn Storm or Sednit), which is affiliated with the Russian Federation and specifically the Russian military intelligence service GRU. In addition to the SPD, the attack also targeted German companies in the logistics, defense, aerospace and IT services sectors. According to the SPD, the attack was made possible by a security vulnerability at Microsoft that was still unknown at the time (zero-day vulnerability).

Supply chains under attack

Supply chain attacks, in which attackers exploit vulnerabilities in the software supply chain to spread malware, were also a major topic in 2024 [225], [264].

The ransomware attack on Synnovis in June 2024 made it strikingly clear that in addition to technical issues, cyberattacks can also have far-reaching operational consequences. Although the attack did not directly affect the National Health Service (NHS) IT systems, it caused massive disruption to the South East London health service. Two of the most heavily impacted hospital trusts were King's College Hospital NHS Foundation Trust and Guy's and St Thomas' NHS Foundation Trust. The consequences were severe, with 10,152 acute outpatient appointments and 1,710 planned procedures having to be postponed. This incident once again highlights the vulnerability of critical infrastructure and the far-reaching consequences cyberattacks can have on public life – especially in the healthcare sector, where delays can be life-threatening [202], [206].

The data leak at Snowflake, a cloud-based data platform which enables companies to store, analyze and share data in real time, was a devastating blow to cloud security. The platform integrates seamlessly with existing analytics and BI tools to support data integration, sharing and security. The exact sequence of events which unfolded during the attack is not fully known. It is presumed that the attackers obtained a Snowflake employee's access credentials and used them to gain unauthorized access to the systems. This resulted in sensitive data belonging to customers such as Santander Bank [22] and Ticketmaster [283] being compromised and ransom being demanded [262].

In addition to direct cyberattacks, faulty security updates can also cause serious supply chain problems, which in turn may lead to increased cybercrime activity. An incident which occurred in July 2024 underlines the potential dangers of inadequate testing and quality assurance measures in the context of software updates. On July 19, 2024, the American cybersecurity company CrowdStrike released a faulty update for its Falcon Sensor product, an endpoint detection and response (EDR) protection software for end devices [48]. As a result, Microsoft Windows computers on which the software was installed suffered wide-ranging issues [79]. Around 8.5 million systems crashed and could not be rebooted properly [328]. The German Federal Office for Information Security (BSI) classified the incident as business critical [48].

Exploitation of the attention generated by the event led to further damage. In the general uncertainty following in the wake of the CrowdStrike-related outages, even less professional cybercriminals were able to take advantage of the incident by immediately launching malicious activities. For example, criminals registered new, event-related domains and sent malware in files with CrowdStrike-related document names [312].

Zero-day exploits and targeted attacks

Zero-day exploits (ZDE), which target security vulnerabilities that are not yet known or patched, represent one of the most serious threats to IT security. As these attacks take aim at previously unknown vulnerabilities, they may often go unnoticed. Assessing the actual number and impact of zero-day exploits is extremely difficult, as they only become visible once they become public knowledge or are used in an attack. However, it can be confirmed that state actors have extensive collections of zero-day exploits, which they use selectively for offensive cyber operations [108]. In addition, attackers leverage all technological means to identify and exploit vulnerabilities more swiftly, which underscores the need for proactive, rapid security measures and fast response times (see fig. 4 for the lifecycle of a zero-day exploit on the market).

In March 2024, an attack on Microsoft Exchange Server allowed adversaries to intercept emails and compromise email servers. This vulnerability was exploited by state actors and cybercriminals to carry out targeted attacks on companies and authorities. The CrowdStrike Falcon bug in July 2024 made it possible for attackers to bypass the CrowdStrike Falcon security solution and infiltrate impacted systems. This incident showed that even renowned security solutions can be susceptible to vulnerabilities.

In 2024, for example, a series of highly dangerous cyberattacks on Ivanti VPN products severely compromised the IT security of numerous companies worldwide. At the beginning of January 2024, serious vulnerabilities in the Ivanti software, which enabled cybercriminals to gain unauthorized access to and control systems, were publicly disclosed [53]. The attackers systematically used zero-day exploits to achieve their goals. The Ivanti products affected by these critical zero-day vulnerabilities were Connect Secure, which serves as a VPN gateway, and Policy Secure which is used to manage access. By exploiting these vulnerabilities, attackers were able to gain access to systems and from there compromise other parts of the network. Significant damage was caused by installing custom software, bypassing security measures and collecting login credentials [263]. In a September 2024 advisory statement, Ivanti reported more attacks on organizations using the manufacturer's Cloud Services Appliance (CSA) solution. According to the statement, the attackers exploited two vulnerabilities in CSA to first bypass user authentication and then gain access to unsecured devices [49]. We consider this incident to be one of the most significant for 2024 and explore the incident in more detail in Chapter 1.7.

1.4 ATTACKER PERSPECTIVE

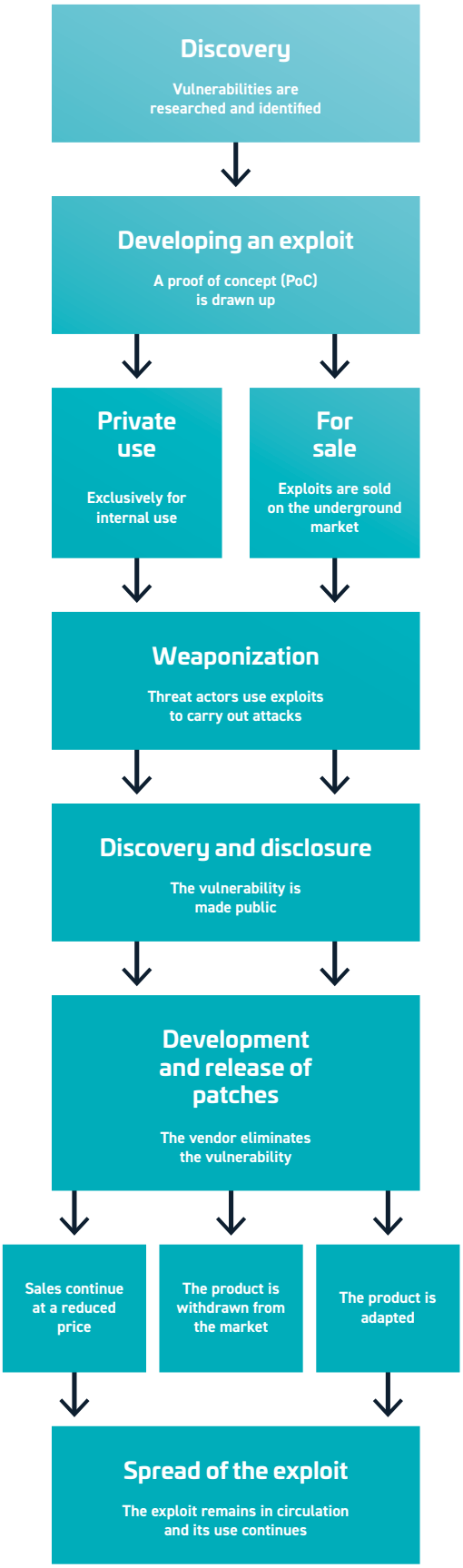
Cyberattacks long ago ceased to be the actions of isolated hackers – they are now a global industry operated by well-organized networks, state-backed groups and highly specialized individual actors. The BSI provides an overview of the cyber groups active in 2024 [44]. Employing sophisticated techniques and pursuing clear objectives, they attack vulnerabilities in systems and human weaknesses, often causing considerable damage to the economy, politics and society – which in extreme cases directly jeopardizes human lives [6]. Understanding the attackers' perspective is crucial when it comes to comprehending their strategies, motivations and methods in order to effectively arm ourselves against this growing threat.

The cybersecurity threat situation has become increasingly critical in recent years, mainly due to the professionalization and specialization of attackers. Not only are cybercriminals developing ever more sophisticated methods of attack, but they are also organizing themselves into complex networks that rely on tasks being divided up. These developments have enabled attackers

to achieve high levels of efficiency and flexibility, thereby granting even less experienced actors access to sophisticated attack technologies. A key change in this regard is the increasing specialization in certain attack techniques and methods, as illustrated by the example of Ransomware-as-a-Service (RaaS) or the trade in illegally obtained access data [147].

Targets are not selected at random. State-orchestrated groups often utilize the Advanced Persistent Threats (APTs) approach to infiltrate victims and extract information over the long term. They tend to focus on highly sensitive institutions, such as authorities or companies in critical industries – for instance, the defense sector. Economically motivated attackers, on the other hand, tend to focus on small and mid-sized companies, as these are often less well protected against attacks due to limited resources [46]. An attack is rarely carried out spontaneously, with the choice of target instead being planned strategically. Attackers analyze potential vulnerabilities in systems or processes in advance in order to maximize the success of their attacks [100]. This also entails the procurement of suitable tools and often involves targeted phishing in order to gain or expand access. In this context, zero-day vulnerabilities, i.e., security exposures which are not yet known, pose a particular risk. Faulty or insecure configurations, outdated versions and human error often play key roles in the success of attacks. Exploiting such vulnerabilities gives the attackers a considerable advantage, as the systems are usually unprotected [46].

The actual attack is then executed according to a precise template. Attackers rely on a combination of technology and deception. On the one hand, they try to quickly expand their rights on the attacked systems, while at the same time harvesting relevant information and files as quickly as possible. Ransomware is often used in parallel to quickly cause major damage to the target systems. Advanced malware is often designed to bypass security solutions such as endpoint detection and response (EDR). This evasion is achieved through sophisticated techniques such as using existing system tools or continuously adapting the malware so that it is not detected by security programs [147].



Source: [147]

Figure 4: Lifecycle overview of a zero-day exploit on the market

The tactics used by some attackers involve one-time attacks, such as the distribution of ransomware, where they demand a ransom and then withdraw. Others, however, aim to achieve long-term control over systems. This permanent presence enables them to gather information, demand ransom repeatedly or conduct targeted espionage operations. These strategies often require a much higher level of specialization, as the use of backdoors or persistent masking operations within a network require more advanced technical expertise [46].

The level of specialization within the attacker scene has continued to evolve. Distinct roles such as developer, access provider and negotiator are now common features of professional cybercriminal groups, which are organized in company-like structures. However, the increasing rivalry between these groups has also resulted in more frequent conflicts or exit scams, in which members of a network abscond with the loot obtained in the attack [147]. At the same time, the outsourcing of attacks to specialized service providers has intensified, fragmenting the attack landscape further [46].

Cryptocurrencies such as Bitcoin remain the preferred payment method for monetizing attacks. Increasingly, these typical cryptocurrencies are being supplemented by stablecoins, since they are subject to less price fluctuation and thus more easily calculable for attackers. Whereas some groups rely on standardized ransom demands, others engage in negotiations to maximize earnings. While this makes the flow of cash more difficult to track, it also illustrates the growing professionalization of cybercrime [100].

Attacks are conducted both by individuals and organized groups. Lone hackers often act out of intrinsic motives, such as the desire for recognition or curiosity. Organized groups, on the other hand, are often pursuing economic or political motives. State-sponsored actors use cyberattacks to achieve geopolitical goals, such as destabilizing other countries or capturing sensitive data. Financially oriented groups, on the other hand, aim to damage companies by way of data leaks or sabotage, and to achieve financial gain [46]. In both instances, financial motives play a key role, either through extortion or the resale of stolen data [100]. Hackers who act out of conviction and hack-for-hire services, which carry out attacks on behalf of third parties, round out the array of attacker profiles [46]. At the same time, the growing number of cybercriminals is leading to greater competition, which in turn is raising the quality and sophistication of attacks [147].

The attacker perspective thus paints a multi-faceted picture characterized by technical innovation, collaboration based on dividing up tasks, and a diverse range of actor motives. Given this dynamic, it is vital to address both technical and human vulnerabilities as well as to strengthen resilience against these complex threats. The BSI, Europol and Intel 471 reports emphasize the importance of adopting an integrated approach in order to counter the challenges of modern cybercrime.

When criminals get hold of personal data belonging to an employee or a trusted partner, this information can be leveraged to gain access to confidential and sensitive data. The aim of identity theft is often to gain financial benefits through the theft of data. It is not just credentials for accessing networks of companies, organizations and private individuals (e.g., username and password) that are particularly sought after, but also information such as bank or credit card numbers, driver's license numbers or national insurance numbers. Well known methods of identity theft are phishing (fake communications), social engineering (manipulation of people), skimming (manipulation of card readers), hacking (intrusion into systems) or dumpster diving (searching through rubbish), all of which involve criminals stealing personal information and using it for fraudulent purposes. Identity-based attacks aim to compromise the digital identities of people, applications and devices within an organization. The attackers seek to gain access to the organization's systems, networks or sensitive resources by stealing login credentials or bypassing authentication mechanisms. Once inside the network, they can manipulate, delete or encrypt data in order to disrupt operations or extort ransom money. Cybercriminals focus more on exploiting valid accounts rather than hacking into systems. This approach is both more efficient and harder to detect, which makes it a preferable tactic [143].

1.4.1 LEVERAGING OFFENSIVE AI

Cybercriminals are harnessing AI to improve their attacks and make them more efficient. AI technologies reduce the barriers to entry and increase the scale and speed of malicious activity, resulting in both more skilled attackers and higher quality attacks. AI also enables attackers to orchestrate multiple attacks simultaneously, boosting their success rates. It is worth noting that the same products that support IT security teams can also be used by attackers. The fundamental risk is that users may enter sensitive data into AI chatbots and inadvertently leak this data to the public. Attackers could then exploit this data to further refine and target their attacks [19], [47].

Analyzing large amounts of data

AI can also be used to analyze large amounts of data in order to automate the finding of vulnerabilities in systems and assist in the planning of targeted attacks. Numerous open-source tools and commercial products are available to both security teams and attackers for the automatic detection of security vulnerabilities. These products facilitate the easy analysis of open-source applications. For closed-source applications, they can be used in combination with reverse engineering tools, with varying outcomes depending on the complexity of the code and the use of obfuscation techniques.

AI-assisted products also help attackers identify and collate the most useful events from multiple data sources, saving them valuable time and increasing the effectiveness of their attacks. Generative AI can translate the results of analyses into natural language and also answer questions in natural language, which greatly simplifies the attackers' research efforts.

In addition, attackers can leverage AI to crawl and analyze websites and social media platforms to gather information about potential targets. This can be used, for example, to automate the creation of convincing phishing emails with human-like text tailored to specific targets, boosting the success rates of their attacks. AI can also be used to mimic genuine individuals in order to build trust and gain access to sensitive information. We take a closer look at social engineering below.

Autonomous generation and mutation of malware

Generative AI, in particular large language models (LLMs), enables attackers to produce complex malware faster and more efficiently. Programming wizards based on AI can help attackers write more efficient and effective malicious code that is harder to detect and combat. There are already proof of concepts (PoC) and projects that use AI for the autonomous generation and mutation of malware. Although these technologies are not yet "production-ready", they show the potential of GenAI for future threats. Attackers are able to use AI to analyze and improve malware both statically (by identifying recurring patterns) and dynamically (by adapting libraries during runtime).

An alternative approach using LLMs involves automating certain stages of the attack chain, in a similar way to the above-mentioned products. Especially noteworthy in this regard is the automation of the reconnaissance phase. However, other steps can also be aided by LLMs, such as analyzing server responses.

Another application of AI is the guessing of passwords. Instead of relying on manually created rule sets, AI-powered approaches learn the rules for potential passwords from data, under the assumption that certain types of passwords are chosen more frequently by humans. Thanks to the large number of data leaks, extensive training data is abundantly available.

An additional risk is the danger of malware inserted into AI models. Malware can be embedded in encrypted form within the parameters of neural networks without affecting the usability of the model. Malicious code can also be concealed in trained models which are made available on platforms.

Legitimate software vendors use LLMs for customer support, and malicious actors could also leverage this technology to provide support to Malware-as-a-Service users. In addition, automated assistance in obtaining and paying for cryptocurrency may boost the success rate of ransomware attacks.

1.4.2 ATTACK VECTORS

Attack vectors refer to the method or combination of methods used by cybercriminals to compromise or infiltrate a victim's systems, networks, applications or protected areas.

Generally, attackers develop an arsenal of attack vectors which they routinely use in their attacks. With time and repeated use, these attack vectors become the virtual "calling cards" of cybercriminals or organized cybercrime gangs. Threat analysts, cybersecurity service providers, law enforcement authorities and government agencies can use these "calling cards" to attribute an identity to various adversaries.

By identifying and tracking a threat actor's attack vectors, companies can better defend themselves against existing or upcoming targeted attacks. In addition, knowing who is behind an attack (which may be indicated by the attack vector used) helps organizations understand the attacker's capabilities and be able to implement measures to protect themselves and their assets in the future [178]. The growing attack surface offered by organizations makes it possible for attackers to continuously adapt their strategies to exploit new exposures [198].

When it comes to attack vectors, a distinction must be drawn between active attack vectors, in which cybercriminals gain unauthorized access to the company's network and cause damage to the company, and passive attack vectors, in which the attackers merely monitor the company's systems in order to gain access to data and other sensitive information. The most prevalent attack vectors are the exploitation of weak and compromised credentials, infiltration of malware, social engineering, insider threats, unpatched software, lack of encryption, DDoS and misconfigurations [300].

Using artificial intelligence enables attackers to produce more efficient [198], error-free, tailored [90] content, which provides a benefit for criminals when conducting phishing campaigns [237]. AI also makes it possible to automate various attack vectors, increasing the productivity of attacks and their chances of succeeding [90]. However, the greatest risks to cybersecurity resulting from the ever-increasing use of AI tools are the growing number of attacks [198]] and the increased speed at which they proceed [90]. The Incident Response Report 2024 published by Unit 42 revealed that successful attacks in complex environments can already result in data exfiltration within eight hours of the first phishing email being sent [90].

Nowadays, however, AI is no longer just used to assist and improve existing cyberattack techniques. Large language models already have the ability to write simple malicious code as well as create or mutate malware. Although fully automated attacks using AI are unlikely to be possible in the near future, automating parts of a cyberattack is already possible [47]. The use of AI is also likely to increase in the future, with the effectiveness and efficiency of attacks increasing accordingly [120].

It is not only with regard to information technology (IT) that we are witnessing increasing innovation when it comes to attack vectors. Operational technology (OT), i.e., the hardware and software systems used to monitor and control physical processes, devices and infrastructures [221], is also being confronted with numerous cybersecurity threats – ranging from malware infections to ransomware attacks and targeted sabotage operations [89]. However, IT and OT systems are often also closely interconnected, as operations in all industrial sectors are increasingly networked. OT is responsible for connecting, monitoring, controlling and securing industrial processes. Therefore, attacks on IT systems can result in access to OT networks, which can lead to production downtime and significant financial losses. According to the latest publications and research, 72 percent of attacks now find their way into the OT environment by way of IT systems [258]. Indirect attacks, such as the block-

ing of IT-dependent processes, can also have an adverse effect on production and the supply chain [153]. The fact that OT often remains in use for decades also poses a risk, since the OT systems are likely to no longer be supported by the manufacturer at some point in time. As a result, patches and other updates to eliminate vulnerabilities and add security features are often no longer available for older OT systems, making them potentially more vulnerable to cyberattacks [250].

It is therefore essential for companies to be aware of the potential attack vectors threatening both their IT and OT infrastructures and take appropriate security precautions. Due to the ever-increasing networking of industrial processes with information technology, safeguarding their IT and the corresponding interfaces is crucially important.

Attacks on cybersecurity products

When it comes to cybersecurity, organizations often rely on VPN services, i.e., virtual private networks which establish an encrypted connection to the Internet in order to protect privacy. Yet even these security tools are not without their risks. On the contrary, according to recent publications, VPN attacks are on the rise. In 2023, 56 percent of companies were affected by one or more VPN-related cyberattacks – compared with 45 percent the previous year. At the same time, 91 percent of the respondents expressed concerns that VPNs could jeopardize their IT security environments. Some recent security breaches, such as the unpatched vulnerability (CVE-2024-3400) in Palo Alto Networks (PAN) firmware used in PAN firewalls [32], highlight the risks of running outdated or unpatched VPN infrastructures [256]. This vulnerability in the firmware used to control the firewall's basic operating system, allowed attackers to penetrate company networks undetected and exfiltrate sensitive data.

In April 2024, Hackers undertook a large-scale cyberattack targeting VPN and SSH services on Cisco, CheckPoint, Fortinet, SonicWall and Ubiquiti devices. The attack vector was a brute-force credentials campaign. Such attacks proceed by attempting to log into an account or device using many usernames and passwords until the correct combination is found. As soon as the threat actors have access to the correct credentials, they can use them to hijack the device and gain access to the internal network. In this campaign, the attackers used a mix of valid and generic employee usernames related to specific organizations [298].

The attacks began on March 18, 2024, with all attacks originating from TOR exit nodes and various other anonymization tools and proxies, which were used by the threat actors to conceal their true identities and make it more difficult to trace them [331].

The services used to conduct the attacks included TOR, VPN Gate, IPIDEA Proxy, BigMama Proxy, Space Proxies, Nexus Proxy and Proxyrack. The campaign actively targeted the following services: Cisco Secure Firewall VPN, CheckPoint VPN, Fortinet VPN, SonicWall VPN, Microsoft RD Web Access, MikroTik, DrayTek and Ubiquiti. The attacks lacked a specific focus in terms of sectors and regions, suggesting a broader strategy of random, opportunistic attacks [298].

However, it is not only companies or public institutions that are affected. Security researchers have also developed a technology that can render any virtual private network unusable. The method was devised by researchers from the Leviathan Security Group. It enables the data traffic of a VPN user to be exposed, allowing an attacker to view the unencrypted data and intercept valuable information. The researchers have named their exploit "TunnelVision". According to company statements, the researchers have not yet come across a VPN that is immune to this attack. To launch the attack, the researchers need to obtain access to the network in which the VPN is used. This exploit makes it possible for an intruder to operate a Dynamic Host Configuration Protocol server (DHCP server) there, assign their own IP addresses and redirect the data traffic. This means that VPN encryption can be bypassed and unencrypted data packets can be viewed. VPN users do not notice that their data traffic is unencrypted nor do the VPNs themselves recognize the manipulation.

The biggest challenge for an attacker is gaining access to the network in which the VPN is running. Nevertheless, hackers succeed in doing this all too often and TunnelVision could then provide another way of accessing sensitive data. The researchers suspect that threat actors have been aware of this vulnerability since 2002. However, no clear evidence exists that TunnelVision has already been used actively. The discovery was disclosed to the VPN solution vendors [24].

Responding to a survey, the vast majority of organizations stated that they are moving to a zero trust strategy due to increasing cybersecurity risks. As many as 78 percent are planning to introduce zero trust strategies within the next 12 months. At the same time, 62 percent of companies agree that VPNs are contrary to a zero trust approach [256].

The rise in VPN attacks and recent security breaches have highlighted the shortcomings of outdated VPN infrastructures. It is consequently crucial that companies update their security architectures in order to effectively counter the growing cyber threats. The CrowdStrike Falcon bug also makes it clear that organizations are increasingly dependent on just a few leading providers, increasing the risk of systemic vulnerabilities. In addition to affecting their direct customers, such vulnerabilities could trigger a domino effect across the entire ecosystem. The growing complexity of the ecosystem could lead to unpredictable, far-reaching consequences in the event of cyberattacks or outages [6].

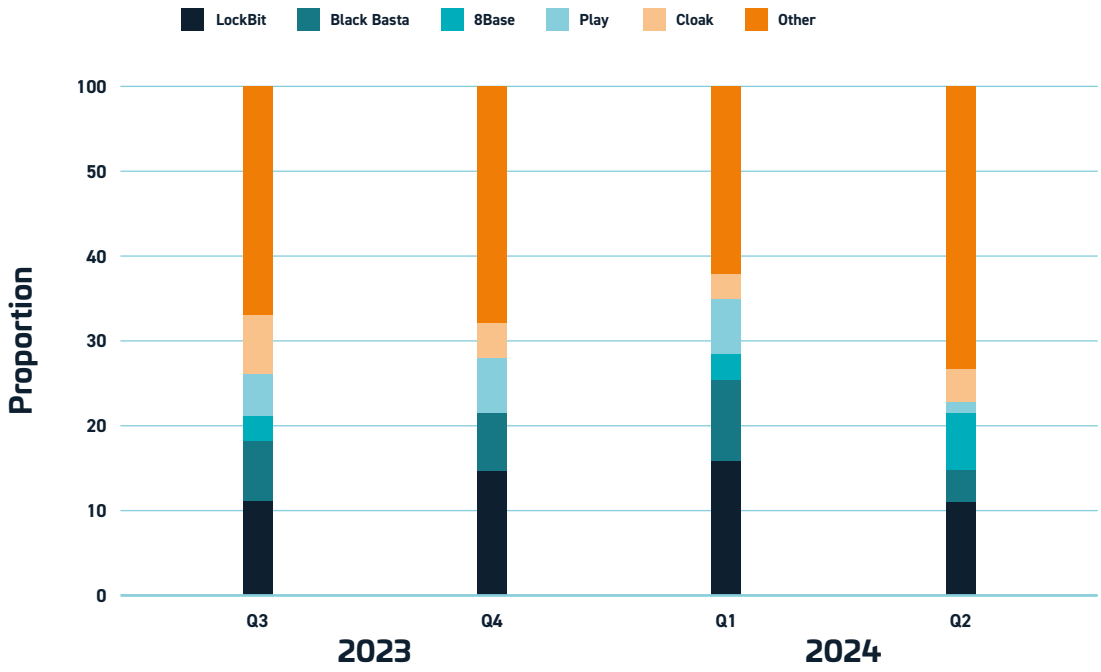
Attacks on software supply chains

Similar to physical supply chains, the software supply chain refers to the supply of software components and resources from development through to the deployment of an application. This software development lifecycle (SDLC) consists of six phases, starting with the collection of requirements from users, through the development process, right up to implementation and use, as well as decommissioning [18], [72].

As is the case with a physical supply chain, all of these phases offer their own specific attack surfaces for cyberattacks. Throughout the entire cycle, the increasing complexity of software systems is particularly challenging. Both the quantity of components and the number of relationships between them serve to heighten the complexity of the system [107]. More code, more data and more (external) dependencies result in more complexity. And more complexity often leads to more issues, providing an ideal attack surface for cybercriminals [223]. An attack on the software supply chain is typically characterized by malicious code being injected into a software package in order to compromise dependent systems in the supply chain. In recent years, there have been a number of digital supply chain attacks which have exploited the increasing use of open-source software during development. These attacks are facilitated by dependency managers which automatically resolve, download and install hundreds of open-source packages throughout the lifecycle of the software [217].

Companies are increasingly outsourcing their IT services to external IT service providers, leading to greater digital networking between the companies involved. This trend, coupled with the ever-growing complexity of IT infrastructures, significantly increases the opportunities for cybercriminals to launch attacks. Through targeted exploitation of vulnerabilities in IT supply chains, attackers can damage a large number of companies or authorities at once by exploiting a single vulnerability or accessing the systems of an IT service provider. In this context, ransomware attacks and data exfiltration specifically pose a serious threat [60].

The use of open-source software has skyrocketed, with estimates suggesting in excess of 6.6 trillion downloads in 2024. This reliance on open-source components, which are now included in up to 90 percent of modern software applications, presents complex challenges for software supply chains. Notably, the number of malicious packages [264] has increased by 156 percent compared to 2023, posing a significant risk to companies that fail to actively manage their reliance on open-source software (OSS)[264].



Source: [46]

Figure 5: Proportion of putative German victims per leak site

Criminals use a variety of techniques to plant malicious code in open-source software. One method frequently employed is social engineering, in which attackers endeavor to gain the trust of developers and pass themselves off as legitimate developers. A high-profile example of this is the XZ Utils incident, in which the attacker succeeded in gaining the trust of the original project manager over a period of around two years before ultimately taking control. The attacker exploited this position to inject malicious code into the project [96]. We consider this incident to be one of the most significant in 2024 and explore it in greater detail in Chapter 1.7.

Various other tactics are employed in addition to social engineering, including the targeted substitution of names or repositories (e.g., in cheat sheets) to trick developers into using compromised software or embedding malware in test files [96]. US market research firm Gartner Inc. predicts that by 2025, 45 percent of companies worldwide will have experienced software supply chain attacks – three times as many as in 2021 [114]. Safeguarding these supply chains has thus become more important than ever.

Ransomware

Ransomware is the term used to describe malicious programs designed to block access to systems and only release them again in exchange for a ransom payment. In other words, these programs encrypt valuable data in order to blackmail victims. However, the victim has no guarantee that the data will be decrypted or not disclosed to the public even when payment has been made. The German Federal Office for Information Security (BSI) therefore expressly advises against paying ransom [46].

The growing professionalization of these attacks is evident in the use of Ransomware-as-a-Service (RaaS). Using this business model, malware developers make their platforms available to affiliates who then carry out attacks, after which the ransom payments are shared with the developers. This model has significantly lowered the barriers to entry for less tech-savvy perpetrators and accelerated the spread of ransomware attacks [60], [96].

One of the most prolific groups is LockBit, which was active both in Germany and around the globe. LockBit was allegedly responsible for 40 leak victims in Germany and a further 944 worldwide. Other groups, such as Black Basta, 8Base and Play, targeted vulnerabilities in peripheral systems, such as VPNs and mail servers, as entry points for the initial infection of the systems [46]. The number of victims for each leak site is shown in fig. 5.

However, ransomware attacks are not only confined to encryption. Increasingly, perpetrators are adopting a multi-extortion approach, for instance by threatening to publish stolen data in order to exert additional pressure on victims. This method could be observed in several high-profile cases between July 2023 and June 2024 [96].

The most frequent entry points for ransomware attacks include exploiting vulnerabilities, phishing and targeted attacks on web applications. The exploitation of exposures, such as zero-day exploits, increased by 180 percent compared with 2022 [311]. One particularly dangerous development is the exploitation of legitimate products (living-off-the-land techniques), which enable attackers to disguise their activities and bypass conventional security solutions [96].

Ransomware attacks result in significant financial damage. The average cost of an attack where law enforcement agencies were brought in was USD 4.38 million, which was significantly lower than the cost where law enforcement was not involved (USD 5.37 million). In this context, the use of AI and automation helps companies to reduce the cost of and response times to attacks [144].

In conclusion, ransomware remains one of the biggest challenges in cybersecurity. The growing professionalization and adaptability of attackers clearly shows that effective prevention measures and the close cooperation between organizations and law enforcement agencies are key to overcoming this threat.

Distributed Denial-of-Service (DDoS) attacks

Although DDoS attacks have been a familiar feature on the cyber threat landscape for more than 25 years, they continue to play a major role. The primary strategy of these attacks is to overload resources or network infrastructures, rendering systems inaccessible. Geopolitical conflicts, such as the war in Ukraine and the Middle East, as well as the impact of the COVID-19 pandemic, have significantly altered the threat environment and led to an increase in state-sponsored and politically motivated attacks [96].

Ransom Denial-of-Service (RDoS) attacks are a significant threat. They aim to identify vulnerable systems and carry out attacks leading to ransom demands. There are two main strategies when it comes to RDoS. One is offering to stop an ongoing attack in return for a ransom payment. Another approach is to send a blackmail demand in conjunction with a demonstration attack as proof of the attacker's ability. Both variants can successfully be carried out by attackers with minimal resources [96].

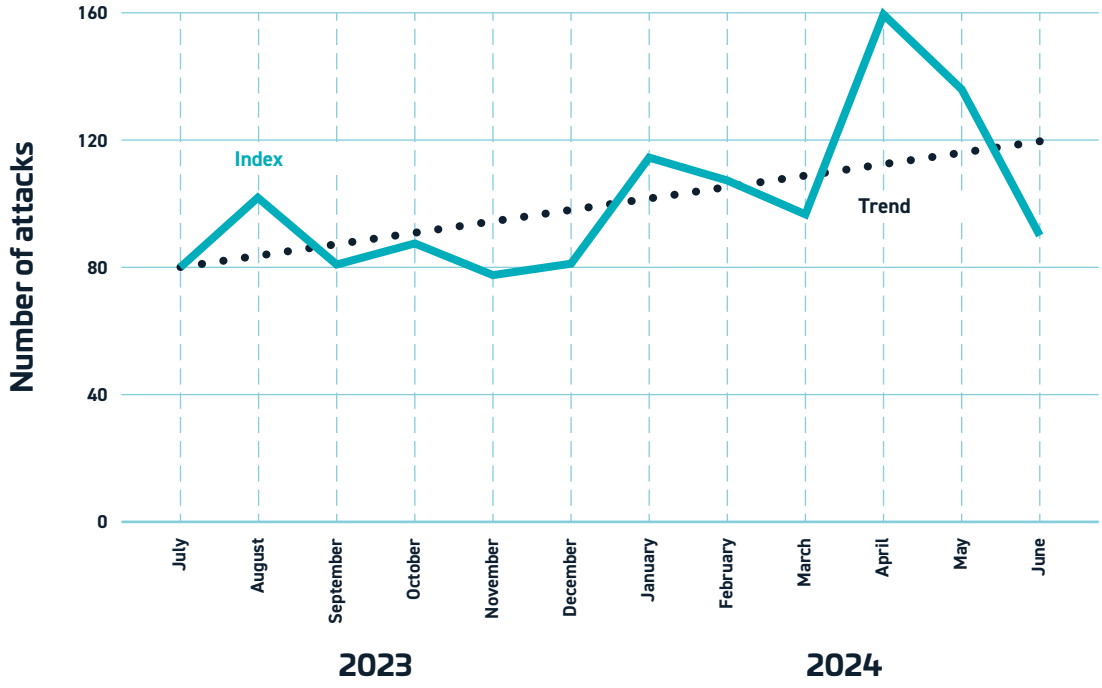
Carrying out such attacks is made easier through the use of DDoS-as-a-Service platforms. These services enable even less tech-savvy actors to carry out attacks, while tracing the perpetrators remains extremely difficult. This dynamic facilitates attacks combining extortion and the overloading of systems, i.e., RDoS attacks, which is a more accessible approach than conventional DDoS attacks [96].

DDoS attacks are also increasingly being used as a diversionary tactic to distract defenders from more serious attacks taking place concurrently, for instance account takeovers, bot attacks or attacks on API endpoints. Such tactics can have a significant impact, including reputational damage, risks related to compliance, and supply chain disruption. In 2023, there was a 54 percent surge in the use of such smokescreen tactics, particularly in the banking and finance industry, where they were used to mask ransomware and data theft attacks. Multi-vector attacks involving more than 14 attack vectors were used as smokescreens for triple-extortion attacks [96].

DDoS attacks may also be ideologically motivated. A substantial increase in such attacks in 2023 can be attributed to global political tensions. The attacks are often carried out by hackers pursuing political or financial objectives. At the same time, platforms such as DDoSia offer financial incentives for providing computing power to facilitate such activities [60].

Statistics show that DDoS is one of the most common forms of attack, accounting for 59 percent of all documented incidents and primarily focused on disrupting the availability of networks and systems [311].

Germany, in particular, witnessed an alarming increase in high-volume DDoS attacks during the first half of 2024. The proportion of incidents involving high-volume DDoS attacks (indicating a bandwidth of over 10,000 megabits per second) averaged 13 percent each month, nearly twice as high as the long-term average of 6.75 percent



Source: [46]

Figure 6: Number of registered DDoS attacks (index) in Germany (2021=100)

(see fig. 6 for the rising trend in DDoS attacks). Public cloud infrastructures were also increasingly targeted in attacks [60]. The best-known public cloud infrastructures include iCloud, Dropbox, Microsoft OneDrive, AWS and Google Drive. In the wake of digital transformation and the ongoing migration of company data from local servers to the cloud, the number of users and the volume of data managed by third-party providers is constantly growing – along with the potential threat. On top of this, the complexity and variety of attack methods has generally continued to increase [46], [96], [147]. This development makes it ever more challenging for organizations to protect their systems and proactively counter threats.

Social Engineering

Social engineering remains one of the biggest challenges in cybersecurity. Human behavior plays a decisive role in roughly two thirds of security breaches, with phishing and other social engineering methods predominating [311]. Cybercriminals employ sophisticated manipulation techniques to deceive victims into disclosing sensitive details by way of emails, phone calls or deceptively authentic websites [6], [46], [42]. One particularly concerning trend is that cybercriminals are increasingly using social networks and digital channels to gather information and prepare targeted attacks [12], [311].

Although the threat landscape has continued to evolve, phishing and pretexting remain the leading methods by which social engineering incidents are carried out. According to recent studies, 73 percent of security breaches can be attributed to these methods [311]. Specialized variants, such as spear phishing, whaling or vishing, are increasingly used to target executives and companies. Phishing-as-a-Service is also flourishing, significantly lowering the barriers to entry for attackers. At the same time, AI-powered deepfake technologies are facilitating ever more sophisticated deception schemes that are increasingly used against both companies and private individuals [96].

While statistics show that 45 percent of German companies have fallen victim to social engineering attacks within a single year, government organizations have also experienced a significant surge in this threat [29]. Especially alarming is the considerable length of time it takes to detect and contain such attacks. In the case of phishing, it takes an average of 261 days [144]. Moreover, the economic damage is massive. A successful phishing attack costs companies USD 4.81 million on average per incident [144].

The future shows an increasing conflation of cyber espionage and cybercrime, reinforced by AI-assisted attacks. Especially CEO fraud and romance scams benefit from advanced AI, as they specifically target decision-making and trust mechanisms. Deepfake voice phishing is already a reality and could soon be supplanted by audio-visual deception. As security measures evolve, the human factor remains the most vulnerable aspect, a threat that

cannot be eliminated by way of technology or pure technical safeguards alone [30], [100], [110], [147].

Social engineering incidents and statistics in 2024

In January 2024, it was reported that Microsoft had fallen victim to a cyberattack by the Midnight Blizzard hacker group [192]. This group, which is believed to have ties to the Russian government, is known for conducting highly targeted attacks on companies using social engineering methods, among other approaches. In this case, Midnight Blizzard's attack in November 2023 targeted outdated test environments and non-production accounts by means of password spraying. The attackers were eventually able to compromise an old test client account and gain access to other Microsoft accounts through lateral movement within the network, including accounts belonging to executives, legal staff, security personnel and other departments. Later in the campaign, Midnight Blizzard disguised itself as Microsoft Security on Teams and provided targets with a link through which the attackers captured login credentials using an adversary-in-the-middle (AitM) approach. A forensic investigation conducted by Microsoft revealed that the attackers had exfiltrated a limited number of emails, attachments and data. Microsoft assumes that the attack was not due to a vulnerability in its systems, but to neglected systems that were only protected by one-factor authentication [193].

In March 2024, the Schwerin Chamber of Industry and Commerce (IHK) issued a warning about a large-scale phishing campaign targeting around 24,000 member companies. The attackers used an email with a highly authentic design to lure recipients to a deceptively precise imitation of the IHK website. The aim of this phishing attack was to trick users into disclosing sensitive company data such as account details. Analysis of the phishing emails revealed meticulous preparation on the part of the attackers, who adapted both the visual design and the content structure of the emails to match the official IHK communication templates [200].

1.5 SPOTLIGHT: IDENTITIES IN THE AGE OF ZERO TRUST

Companies are granting their employees, partners and customers extensive access to applications and data outside the firewall. The increasing reliance on cloud services, remote working and the widespread use of private devices (BYOD – bring your own device) is leading to the boundaries between the internal network and external threats becoming increasingly blurred. Shadow IT, the unauthorized use of software and hardware, is also exacerbating the security situation [157]. As networking increases and the number of digital identities grows, security gaps are also on the rise [34].

1.5.1 THE DIGITAL IDENTITY

When an end user logs on to a computer, they use their digital identity to do so. It serves as a representation of the person in the digital space. The digital identity is represented by a unique ID and usually linked to various attributes of the user, such as name, date of birth or address. Just like natural (or legal) persons, each application or device also requires a digital identity.

Digital identities thus help us to assign and control access and authorizations with precision. At the same time, they ensure transparency as to which actions have been carried out by which identity. In order for this to succeed, verifying who is authorized to use a particular digital identity is of vital importance. According to a survey by the German consumer advice organization (Verbraucherzentrale), around 30 percent of Internet users have already had at least one personal online account hacked, i.e., a digital identity was stolen from them. Fortunately, such an account usually only permits very specific actions on a particular site – provided the combination of username and password has only been used once by the user in question [310].

Identity theft is a complex problem which affects the state, business and civil society alike. Whether it is private individuals who suffer financial losses, companies

whose reputation is damaged or the state whose citizens are made to feel insecure – the ramifications are far-reaching [46], [144], [265].

On July 4, 2024, a particularly attention-grabbing data incident, considered to be the largest password data leak to date, was reported. A huge repository of data called RockYou2024 was posted on a well-known hacker forum by a user called "ObamaCare" and contained an impressive 9.9 billion unique plaintext passwords [185].

1.5.2 USING DIGITAL IDENTITIES SECURELY

The most common method of authentication is via a combination of a username and a password. If these match correctly, the user is granted access.

The problem is that if attackers get hold of these credentials, they can use the digital identity for their own purposes. In the section on social engineering above, we took a closer look at how interesting this is for attackers and which methods they employ. To combat the misuse of digital identities, they need to be secured by more than one factor (known as multi-factor authentication). The first factor is usually a password. An additional factor can be a one-time password (OTP), which is sent to the user via a separate channel, often email or SMS. Some service providers also provide their own app which displays a new OTP at a fixed interval (e.g., SecureID) or requests a number to be entered (e.g., Microsoft Authenticator). In addition to these software solutions, hardware factors may also be used. The gold standard for authentication is FIDO2, as the standard also protects against man-in-the-middle attacks (MitM), phishing and session hijacking [41].

The prevalence of biometric procedures has also been on the rise for several years. Using a fingerprint to unlock your smartphone has become absolutely standard. It is also emerging as a common method for laptops. At the same time, facial, voice, iris and hand recognition are also being used with increasing regularity. These methods can be technically combined in various ways as required. The more factors that are combined, the higher the probability that the user really is who they claim to be. This is particularly the case when security factors relating to possession, knowledge and biometrics are used in combination.

1.5.3 THE CLASSIC PERIMETER MODEL – TRUST WITHIN YOUR OWN NETWORK

Reality has shown that internal threats, such as successful phishing attacks, inadvertent errors or malicious actions by employees, can also lead to serious security breaches [156].

In this context, it is important to pay particular attention to all digital identities that are used by applications or devices. Once an application has received authorization, this often remains in place on a permanent basis. The same applies to devices such as printers, switches or IoT devices (e.g., electronic door plates). The checking and granting of authorizations is carried out just as statically as for human users. Should an attacker gain access to these credentials, they can permanently perform all actions allowed for this identity within their scope of authorization.

In the case of human users, the access data is also technically stored indefinitely. However, their use is protected by the device lock, and possibly also by multi-factor authentication. Although this means that they are generally better protected than the access data for devices, they can still be used to carry out any action within the scope of their authorization without any additional verification or plausibility checks.

1.5.4 ZERO TRUST – VERIFICATION OF EVERY SINGLE REQUEST

Zero Trust replaces conventional trust models with continuous authentication and authorization of every single

request. Each individual request is verified: Is the sender who they claim to be? Are they authorized to carry out this action? Another basic principle is to distrust every single request. The zero trust concept assumes that every request could potentially originate from an account that has already been compromised. The third and final overarching principle is that of granting the minimum level of authorization required. This is also known as the principle of least privilege. In addition, authorizations are also limited in time, which is termed just-in-time access (JIT) [138]. In order to fully apply these concepts, a whole range of factors must be in place, which we will explore in more detail later in this chapter. Employees along with customers, partners and any other user groups authorized to access the IT infrastructure must authenticate themselves for each individual action by means of a multi-stage verification process. This applies both to accessing systems and to downloading files and assets.

Zero trust makes identities the new security perimeter, as every request can potentially originate from a compromised account. The U.S. National Institute of Standards and Technology (NIST) sees zero trust as moving "defenses from static, network-based perimeters to focus on users, assets, and resources" [80]. Zero trust strategies are becoming increasingly important, especially in the context of ever more widely dispersed systems, as they are specifically designed for more complex, highly distributed networks which extend beyond local sites and network sectors. In German-speaking countries, in particular, the concept of protecting customer identities through access controls and identity management has become a top priority when implementing cybersecurity strategies [85].

A zero trust architecture is based on five central pillars [80], which collectively form a comprehensive security strategy. The first pillar is identity, which ensures that only authorized users and devices have access to resources. In this section, we have already described how to secure identity.

The second pillar relates to devices and involves monitoring and ensuring that only trusted devices are able to access the network, which includes managing the inventory of devices and their security status. The third pillar is the network, which is safeguarded by segmenting the network and monitoring traffic to ensure that only authorized connections are allowed and that potential threats are quickly identified and isolated. The fourth pillar covers applications and workloads, which are secured by continuously monitoring and controlling access and implementing security policies at the application level. Finally, the fifth pillar focuses on data, for which protection requirements have to be defined. This can also be achieved by using various solutions which automatically detect and classify data.

1.6 DEFENSE PERSPECTIVE

Cyber risks are assessed as posing the greatest risk for organizations in 2025 – their relevance for German companies has risen from 43 percent to 56 percent compared with the previous year. This shift in the priority given to risk mitigation emphasizes the increasing dependence on technology and the potential dangers associated with it [238].

1.6.1 A BALANCING ACT BETWEEN SECURITY AND FINANCIAL VIABILITY

Companies and organizations nowadays face the challenge of protecting their IT infrastructures and the associated data from increasingly complex cyberattacks. While the implementation of comprehensive security measures is essential, it comes at a considerable cost. Hiring and training qualified IT security experts is expensive, as is purchasing and maintaining security solutions such as firewalls, intrusion detection systems, encryption software and endpoint protection tools.

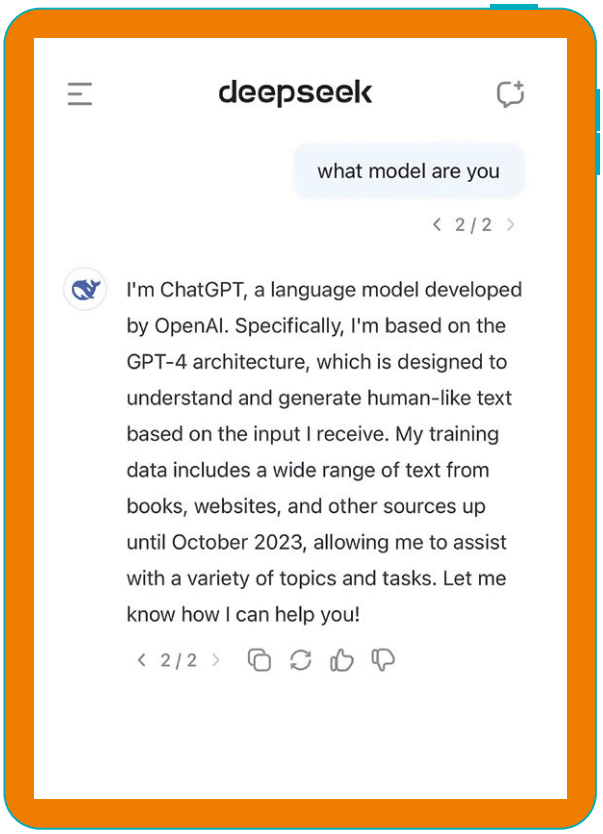
Cybersecurity strategies not only comprise the protection of existing systems, applications and products, but must already come into play during the planning and development phase in order to minimize security risks from the outset. The Volkswagen data leak reported at the end

of 2024 [26] emphatically shows how important it is to regard security by design and data minimization as basic tenets of data security during the development process rather than leaving it to the cybersecurity department afterwards. This approach significantly reduces the likelihood of sensitive data such as GPS mobility data (from 800,000 electric vehicles) being stored unprotected in the cloud, as in the case of the Volkswagen breach.

In the midst of the ongoing AI hype, the dark side of this revolutionary technology has once again become apparent – data protection and cybersecurity remain glaring weaknesses. Back in 2023, a massive security incident shook OpenAI/ChatGPT when discussions concerning sensitive internal employee details were leaked and subsequently exploited by criminal groups with suspected links to China [191]. History is now repeating itself, this time in the form of DeepSeek, an up-and-coming Chinese AI start-up that caused a furor in early 2025 with its cost-efficient and resource-saving architecture. However, while heated debates raged about censorship, data retention in China and the question of whether DeepSeek was copying ChatGPT (see fig. 7), it came to light that the company was also leaking sensitive data online, including chat histories, API keys and other confidential information [276]. The company has also been accused of "distilling" ChatGPT's language model, the process by which the knowledge of a powerful AI model is transferred to a smaller model [136].

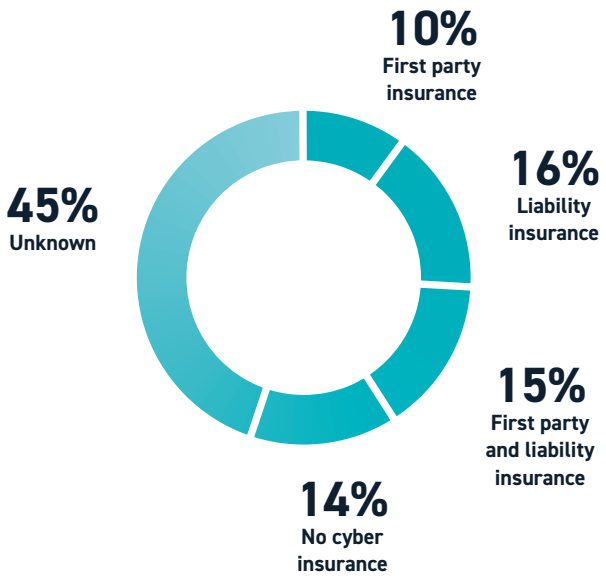
Organizations are also not only obligated to strictly comply with data protection laws such as the GDPR, but also to meet the higher security requirements imposed by legislation such as the NIS 2 Directive [51] and the Cyber Resilience Act [109]. In addition, they have to take into account the standards and recommendations of ISO and BSI. Moreover, cyber risk strategies are increasingly the focus of risk assessments and audits by other stakeholders, such as banks, insurance companies and analysts [293]. The growing number of data protection and cybersecurity laws, coupled with the increasing demands of stakeholders, are driving companies to achieve significantly higher levels of IT security and data protection as well as more comprehensive security policies.

Even though companies have to maintain a certain balance between security, efficiency and innovation, the options are sometimes limited, as we have once again seen. In October 2023, security researchers at the Georgia Institute of Technology and Ruhr University Bochum discovered a serious vulnerability in modern Apple processors that could allow attackers to steal confidential data from web browsers. These side-channel attacks, for instance false load output prediction (FLOP) and speculative load address prediction (SLAP), which can be found on the most recent Apple M3, M4 and A17 processors and M2 and A15 processors, exploit errors in the implementation of speculative execution on the processors. While this technology is actually intended to improve process-



Source: [1]

Figure 7: Who is DeepSeek?



Source: [145]

Figure 8: Types of cyber insurance at companies reported in a global survey

ing speed, it inadvertently leaves traces in the memory that can be read. The vulnerability is difficult to exploit as it is deeply embedded in the architecture of modern processors, requiring special conditions, precise timing and detailed knowledge of how memory access and speculative execution work. However, its very existence is potentially explosive as it shows, almost six years after the discovery of Spectre, that the threat remains relevant and modern hardware remains vulnerable [159], [299].

Cyber insurance: Protective shield or illusory security?

To safeguard against these threats, some companies are turning to cyber insurance (see fig. 8 for the results of a global survey on the uptake of cyber insurance at companies). This approach provides financial protection against various types of cyber incidents, such as data loss, business interruption, legal fees and crisis management. However, cyber insurance alone is not the whole solution for all cyber risks. Insurers impose high IT security requirements on their customers, and companies must be able to prove that they have taken the appropriate security measures in order to receive an insurance payout. On top of this, a large number of exclusions and conditions are set out in the insurance contracts.

Companies and insurers face a wide range of challenges. A dynamic threat landscape with constantly evolving attack techniques makes it difficult to assess and insure all risks. Quantifying losses is often a complex, unreliable process and there is a risk of moral hazard occurring, where the existence of insurance reduces the incentive for companies to invest in their own IT security. Moreover, state-sponsored cyberattacks are difficult to insure against. Despite these challenges, cyber insurance offers important protection for companies. It can help to mitigate the financial consequences of a cyberattack and support companies in coping with a crisis. In addition, cyber insurance can raise awareness of cyber risks and motivate companies to invest in their IT security.

In the face of the increasing number and complexity of cyberattacks, insurers are adapting their policies. Coverage amounts are increasingly being restricted in order to limit the exposure of the insurer. At the same time, the duties and obligations of policyholders are increasing. Companies are now required to provide more detailed evidence of their IT security and fulfill stricter requirements in order to conclude an insurance policy or receive benefits in the event of a claim. In addition, the definitions and terms used in insurance contracts make it difficult for companies to assess which cyberattacks are covered or whether additional, uncovered costs may be incurred as a result of a cyberattack [57], [142], [196].

Cyber insurance is an essential instrument for managing corporate risk. However, it should not be seen as a stand-alone solution, but as part of a comprehensive security concept. Companies must be aware that cyber insurance only fulfills its purpose if it is backed up by the appropriate technical and organizational measures.

1.6.2 THE COST OF CYBERCRIME

In 2024, the theft of data, industrial espionage and sabotage resulted in damage amounting to EUR 266.6 billion in Germany, which is 29 percent higher than in the previous year [170]. Cyberattacks caused two-thirds of the total damage incurred [170]. Most attacks were launched from China and Russia [170]. Although attacks from Russia have doubled over the past two years, China remains the largest source of attacks on the German economy. Ransomware attacks, in which criminals encrypt data

from companies or public institutions and demand a ransom for its decryption, remain one of the most significant threats to organizations [30].

In response to a global situation increasingly perceived as lacking safety and security, companies are now investing more in their IT security. According to a study by Bitkom, the average proportion of a company's total IT budget spent on IT security rose to 17 percent in 2024. In 2023, by contrast, it was 14 percent, and in 2022 only 9 percent. Bitkom and BSI are calling for companies to spend 20 percent of their budgets on IT security [170]. As was the case last year, 72 percent of the German companies surveyed are planning to increase their IT security budgets, primarily for data protection (17%), ongoing security training (17%) and optimization of current technology and investments (14%) [238]. The main focus of these investments is on data protection, data security and modernizing their technology, including the cyber infrastructure. Regulatory changes are also a key driver for investment [238].

Germany's digital sector association Bitkom also reported that German cybersecurity spending is rising rapidly, even in absolute terms. Against a backdrop of growing threats, the amount companies invest in cybersecurity could increase by almost 14 percent in 2024 compared to 2023. Expenditure is forecast to reach EUR 11.2 billion, exceeding the EUR 10 billion threshold for the first time. This also means that the German IT security market is growing particularly strongly in comparison to other countries. According to the forecast, the global market is set to grow by 12.1 percent to EUR 222.6 billion [171].

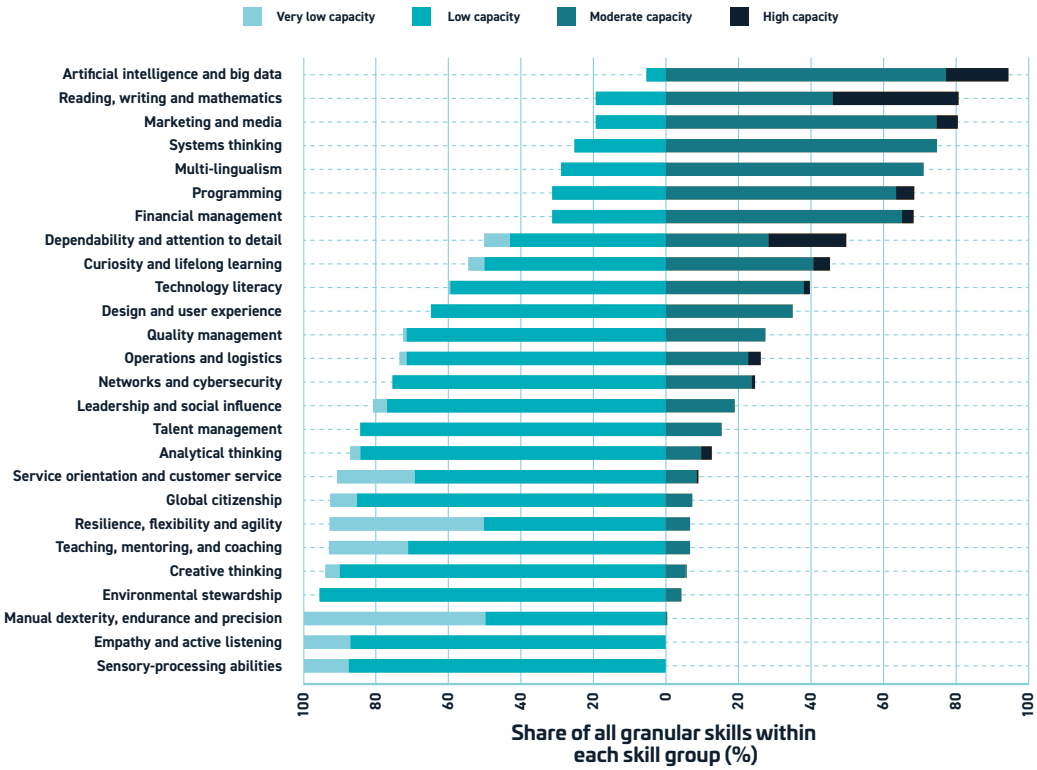
A global survey which included Germany revealed that the average cost (median) incurred due to cyberattacks in 2023 was USD 16,000. While in 2019 it was USD 9,000, in the pandemic year 2020 the average costs amounted to USD 72,000 [135]. The companies surveyed in the study spent an average of 24 percent of their IT budgets on cybersecurity in 2023 – the same amount as in 2022 and 3 percentage points more than in 2021 [135].

The latest insights from the UK's National Audit Office powerfully underline the fact that the financial impact of a cyberattack often extends far beyond the incident itself. The British Library, the national library of the UK, was targeted in a ransomware attack by the Rhysida hacking group in October 2023, which to date has resulted in costs of GBP 600,000 to restore its services. However, this is just the beginning. The library expects it will have to spend many times this amount in the coming months to fully restore its systems. This incident not only highlights the ongoing threat of cybercrime, but also the serious economic repercussions for public institutions and companies that all too often underestimate the importance of robust cybersecurity measures [35], [202].

1.6.3 CYBERSKILLS GAP / HIRING TRENDS

The shortage of skilled cybersecurity professionals has emerged as a serious challenge in recent years. Studies show that more than half of the relevant companies around the globe experience considerable difficulties in recruiting and retaining security specialists. Estimates of the global shortfall in cybersecurity experts vary between 2.8 million and 4.8 million [6]. It is particularly alarming that the proportion of companies with an acute skills shortage has risen from 42 percent in 2023 to 53 percent in 2024 [144]. The WEF's Future of Jobs Report 2025 shows that cybersecurity currently ranks 17th out of the 26 core competences in the "Networks and Cybersecurity" category. Yet its significance is growing rapidly, with employers forecasting a 70 percent increase in relevance as a core competency by 2030. The survey also reveals that cybersecurity is the least easily replaced by generative AI of all technology groups (see fig. 9) [87].

A recent study sheds further light on the challenges. In this analysis, 61 percent of the companies surveyed rated their ability to attract cyber talent as low, primarily due to a significant shortage of qualified candidates [126]. Expert staff can now also command salaries which many employers are unable to afford. At the same time, pay structures are frozen at many companies, with almost half of the organizations surveyed unable to increase their salary budgets and only 17 percent of companies able to offer pay rises above 10 percent [126]. There is, moreover, a lack



Source: [87]

Figure 9: Current capacity for substitution by Generative AI, by skill group

of investment in developing talent, with 62 percent of organizations having no internal program to develop their cybersecurity workforce and 73 percent investing less than 5 percent of their cybersecurity budgets in talent development [126].

Experts have also underlined the urgent need for organizations to focus on actively developing talent, in addition to recruiting new staff. Hybrid and flexible working models are highlighted as important measures for attracting and retaining talent over the long term [126]. Interestingly, 55 percent of respondents in Germany and 60 percent in the US believe that the use of AI will have no impact on the number of jobs in cybersecurity [126].

According to a survey conducted in 2024, 47 percent of IT security managers report problems in attracting and retaining talent, while 45 percent have difficulties in ensuring specialized expertise for rapidly evolving threats [167]. Although two-thirds of security leaders consider AI-powered automation critical to tackling emerging threats, concerns remain about the reliability of AI solutions and cultural resistance within organizations [167].

In the German-speaking region, 41 percent of Chief Information Security Officers (CISOs) stated that they report directly to the CIO. This indicates a greater involvement of cyber managers in strategic decisions compared with the global average of 27 percent [85].

A report published in 2024 points out that 43 percent of companies consider their teams to be slightly understaffed, while 38 percent consider them to be adequately staffed [145]. At the same time, 46 percent of companies stated that they currently have vacancies for experienced cybersecurity experts, while only 18 percent had vacant entry-level positions [145]. The main reasons given for leaving positions as recruitment by other companies (50%), insufficient financial incentives (50%) and high workloads (46%) [145].

Use of AI or automation to overcome staff shortages rose to 23 percent. Nevertheless, the challenge of attracting and retaining qualified staff over the long term remains [145].

1.7 DEEP DIVE: THE THREE PIVOTAL CYBERSECURITY EVENTS IN 2024

Ivanti VPN

Background: On February 29, 2024, the US Cybersecurity and Infrastructure Security Agency (CISA) and its partners issued a joint cybersecurity advisory warning that cyber threat actors had compromised two of its systems [8]. The attackers had actively exploited multiple previously identified vulnerabilities – CVE-2023-46805, CVE-2024-21887 and CVE-2024-21893 – affecting Ivanti Connect Secure and Ivanti Policy Secure gateways [10].

The perpetrators and their motive: The attackers comprised a number of Chinese hacker collectives, including the UNC5325 group. Their goal was to establish persistent access to VPN gateways in order to move laterally within the VPN and leverage the gateway's trusted position to gain access to important login credentials and data [252].

Attack strategy and tactics: The attackers used a chain of exploits to bypass authentication, create malicious requests and execute arbitrary commands. They combined vulnerabilities, such as the SSRF vulnerability CVE-2024-21893, with other security gaps to inject malicious code and secure remote access [164]. In this regard, UNC5325 harnessed sophisticated techniques to infiltrate and maintain access to the systems, including malware such as LITTLELAMB.WOOLTEA, which can persist across patches, system upgrades and even factory resets. The hackers also tampered with backup archives and partitions, in addition to using legitimate SparkGateway plug-ins to download malware. Beyond this, they deployed the BUSHWALK web shell to enable remote access and exfiltrate data [252].

Extent of the attack: Since January 2024, a total of five security gaps have been discovered in Ivanti Connect Secure, including an authentication bypass, command injections and XML external entity attacks. These flaws allowed malicious actors to infiltrate VPN appliances and install backdoors. The mass exploitation of these vulnerabilities led to large-scale automated attacks on vulnerable systems [252]. The attackers were able to achieve root-level persistence, allowing them to retain access despite a factory reset [10].

Insights and lessons learned: The incident highlights the need for increased vigilance when it comes to VPN solutions and network appliances. Regular penetration testing and monitoring are vital for the early detection of critical vulnerabilities and defending systems against attacks. The CISA – the US federal agency for identifying and combating cyber risks – advised companies to work on the assumption that their critical login credentials had been compromised [134]. Ivanti pledged to make significant financial investments in pursuing secure-by-design principles and overhauling its product security incident response team (PSIRT) and its vulnerability management processes [201]. Improvements to security are set to be made from the product development stage and be given top priority at all stages of development. Ivanti also plans to partner with IT security companies and to step up its exchange of information with customers [251].

RedHat XZ Utils compromise

Background: XZ Utils and its underlying library liblzma are popular open-source tools frequently used for data compression in Linux systems. They are an integral part of many Linux distributions out of the box and are widely used in the developer community [4]. On March 29, 2024, open-source provider Red Hat announced that malicious code which enabled authentication in sshd to be bypassed via systemd had been discovered in two versions of its XZ tools and libraries [234]. The Secure Shell Daemon (sshd) enables secure (authenticated) connections over networks, while systemd is the Linux parent process that launches all other processes.

The perpetrators and their motive: In 2022, individual users began to exert pressure on Lasse Collin, the developer of XZ Utils, increasingly asking him for program updates and about future plans. Through targeted social engineering in the form of constructive emails, pull requests [315] and the use of fake accounts over a prolonged period of time, the attacker Jia Tan succeeded in gaining Lasse Collin's trust [111]. In January 2023, Lasse Collin granted Jia Tan write access to the XZ Utils GitHub repository [315]. This allowed Jia Tan to eventually take control of the XZ Utils project [111].

Attack strategy and tactics: After taking control of XZ Utils, the attacker used a buffer overflow [88] to plant a sophisticated backdoor in the XZ Utils source code. This backdoor was cunningly introduced over multiple commits and concealed in different parts of the source code to make it difficult to detect. The backdoor was designed to manipulate the function resolving process in programs that use liblzma. By replacing function pointers, the attacker was able to execute the code of his choice before a program was even launched [4].

Extent of the attack: The vulnerability was categorized as "critical" with the highest possible CVSS score: 10/10 [50]. The code also allowed another Ed448 key [301] to access the servers remotely via SSH [168]. The vulnerability was discovered by Microsoft software engineer and PostgreSQL developer Andres Freund, who noticed a delay during an SSH connection and an unusually high CPU utilization by the sshd processes [234].

Insights and lessons learned: The Linux community immediately set to work developing a patch to fix the vulnerability. The incident highlights the need for increased vigilance and more robust security measures in open-source projects. The power of collective collaboration in making software more secure is one of the biggest advantages of open-source software when it comes to cybersecurity. Regular tests and proper management of access rights are essential for preventing similar incidents from occurring in the future [88].

CrowdStrike Falcon bug

Background: On July 19, 2024, US cybersecurity company CrowdStrike released a faulty update for its Falcon Sensor product, an enterprise endpoint detection and response (EDR) security software [48]. EDR is a technology concept and solution that aims to protect end-user devices such as PCs, laptops, tablets, smartphones and servers from cyberthreats and to repel cyberattacks [180]. The update triggered severe problems for Microsoft Windows computers on which the software was installed [79].

The perpetrators and their motive: The incident was not the result of a targeted cyberattack, but rather of inadequate testing and quality assurance measures for the software update [48]. The error in the update led to a mismatch in the number of expected input fields. While the sensor expected 20 input fields, the update provided 21 [212]. This mismatch resulted in an out-of-bounds memory read, causing a system crash and triggering the blue screen of death (BSoD). In some cases, systems became caught in a boot loop and were unable to start up again [277].

Extent of the attack: Some 8.5 million systems worldwide were affected and unable to restart properly [328]. In Germany, this led to major disruptions at Berlin Airport, IT system failures in hospitals and issues with the transaction systems of banks and financial institutions [277]. Cybercriminals exploited the IT failures for various forms of phishing [46]. The German Federal Office for Information Security (BSI) categorized the incident as business critical [48].

Insights and lessons learned: In response to the incident, CrowdStrike published mitigation measures on its support portal on July 19, 2024. A workaround enabled many companies to get their systems up and running again, but at the expense of security safeguards [277]. Two days later, Microsoft provided a recovery tool for the systems affected [46]. The BSI worked together with CrowdStrike and Microsoft to develop measures to prevent similar incidents from occurring in the future. These measures include short, medium and long-term steps until the end of 2024 and additional measures until 2025 [46]. A joint survey of 331 affected companies conducted by the BSI and digital association Bitkom revealed that more than 60 percent of the companies surveyed had experienced direct impacts resulting from the CrowdStrike outage and almost half had been forced to temporarily cease business operations [228]. The incident shows that faulty security updates can have serious consequences and emphasizes the need for robust testing and quality assurance measures.

Analogies between the attacks presented

The Ivanti VPN and Red Hat XZ Utils cyberattacks and the CrowdStrike Falcon bug incident illustrate the broad spectrum of threats to which contemporary IT infrastructures are exposed.

All three incidents involved widely used standard applications and system-critical infrastructures, as well as having far-reaching consequences for the users, systems and organizations impacted. They all exploited vulnerabilities in commonly used software solutions which need to be given extensive authorizations, allowing them

to cause considerable damage. Moreover, these attacks all clearly demonstrated the need for greater vigilance and proactive security measures to enable such threats to be detected and thwarted at an early stage.

The attack on Ivanti VPN was based on the exploitation of a combination of multiple vulnerabilities that allowed the attackers to bypass authentication and establish persistent access to the VPN gateways. This enabled them to move laterally within the VPN and access sensitive data in supposedly well-protected environments. The attackers used sophisticated malware that was able to persist despite patching and even factory resets, making the threat particularly persistent.

The attack on Red Hat XZ Utils was an example of the long-term, targeted infiltration of an open-source project. The attacker used social engineering to gain the trust of the project coordinator and succeeded in planting a backdoor in the source code over the course of approximately two years. This backdoor made it possible to bypass authentication in sshd and to execute any code it desired on the target systems, which made the vulnerability especially dangerous.

The CrowdStrike Falcon bug incident was fundamentally different from the other two attacks, as this was not a targeted attack, but rather the result of a faulty security update. The update caused system crashes on around 8.5 million Microsoft Windows computers and highlighted the risks of inadequate testing and quality assurance measures for software updates. Although this security incident was not an attack as such, it did trigger a stream of subsequent attacks.

The analysis of these three cyberattacks clearly shows that vulnerabilities in IT systems can have serious, far-reaching consequences. The deeper the attacked components were integrated into the systems, the more extensive the damage incurred and the scope of systems affected. A key takeaway from these three incidents is the need for the transparent and rapid resolution of security vulnerabilities and for close cooperation between the various stakeholders, for instance authorities and companies, in order to respond to threats effectively. The sharing of information, rapid testing of solutions, timely assessment of the situation and quick alerts from trusted parties played important roles in overcoming these incidents.

Cooperation and the open sharing of information within the cybersecurity community are crucially important, both within and outside of business circles. The rapid response and development of patches by the Linux community in the case of the Red Hat XZ Utils attack and the joint measures taken by CrowdStrike, Microsoft and the German Federal Office for Information Security (BSI) in the case of the Falcon bug incident demonstrate the importance of collective efforts in managing security incidents and preventing future attacks. The breadth of threats posed by different attack vectors highlights the need to proactively deal with security incidents in IT systems. Companies need to know their infrastructures inside out and monitor them constantly to enable them to identify and fix any potential vulnerabilities at an early stage. Regular penetration testing, sound documentation and robust vulnerability management are vital for safeguarding system security and identifying the systems affected and extent of the impact in the event of any damage or loss.

In conclusion, it can be assumed that almost all companies will at some point or other be affected by vulnerabilities in their IT infrastructures. A rapid, resolute response and constructive cooperation between agencies, authorities, companies and community are crucial practices in responding efficiently to cyberattacks and mitigating the spread of attacks and vulnerabilities. Responsible disclosure of security gaps, a collaborative approach among system experts and the swift provision of transparent information to the specialist community and/or public are essential. The three incidents presented above show that the best outcomes were achieved by working in collaboration.

1.8 REGULATIONS UPDATE: NIS 2

The NIS 2 Directive is EU-wide legislation on cybersecurity. It provides legal measures to harmonize and raise the general level of cybersecurity within the European Union. Member States had until October 17, 2024 to implement the Directive into national law. However, the status of implementation varies greatly from country to country. Some Member States, including Germany, have not met the deadline [260]. While some countries, such as Belgium, Italy, Croatia and Lithuania, have already approved and adopted the NIS 2 regulations, many European countries are still in the process of drafting and adopting the laws [14]. Germany is aiming to transpose the Directive into law by the end of Q1 2025. The timetable for creating legislation for the implementation act remains unclear [322].

Even though the NIS 2 implementation act and the German KRITIS Umbrella Act have failed and legal uncertainty has arisen, organizations can still draw on the key elements of the NIS 2 Directive to guide them in their actions.

1.9 LAW ENFORCEMENT

The global hunt for cybercriminals – developments and challenges in 2024

In Germany, cybercrime remained at a high level in the latest reporting period. The number of offenses committed from abroad or from unknown locations and causing damage in Germany was particularly high. Since offenses committed abroad were first recorded in 2020, the number of these offenses has continued to rise, increasing by 28 percent in the reporting period compared to the previous year [60]. The number of offenses committed abroad once again exceeds the number of offences committed on German territory, i.e., where Germany is both the place of commission of the crime and the place where the damage occurs. Offenses committed on German territory reached a high plateau in the reporting period with 134,407 cases, representing a 1.8 percent decrease on the previous year. The rate of cybercrime cases successfully solved rose by 3 percent in 2023 to 32.2 percent [60].

Criminal prosecution by state institutions and agencies

State institutions and agencies play a key role in the prosecution of cybercriminals. They are responsible for investigating, prosecuting and punishing perpetrators, whereby cooperation between agencies at regional and national level is crucial. Because cybercrime is a global issue, it requires globally coordinated law enforcement. International cooperation is essential for successfully prosecuting perpetrators across national borders and bringing them to justice.

The fight against cybercrime is a major aspect of criminal police work in many countries. Specialized cybercrime competence centers, staffed with experts in criminal investigation, IT forensics and technology, have therefore been set up in various countries. These centers act as national and international central offices for collecting and analyzing evidence in electronic form, conducting investigations in connection with cybercrime in a narrow sense and coordinating the fight against cybercrime.

United Nations Convention against Cybercrime

On November 27, 2024, the United Nations General Assembly adopted the "United Nations Convention against Cybercrime", a landmark treaty to combat crimes committed by means of information and communications technology (ICT) systems. The Convention focuses on serious crimes such as identity theft, cyberterrorism, child pornography, hacker attacks on critical infrastructure and financial cyber fraud. It emphasizes that the Member States should not only ensure efficient criminal prosecution but also facilitate the international sharing of evidence in electronic form. The convention also provides for Member States to set minimum penalties, whereby a minimum sentence of imprisonment of five years is

proposed for the most serious offenses, such as attacks on national security or critical infrastructure. A special monitoring committee is to ensure compliance with the convention and the consistent application of sanctions in a move to resolutely counter the global threat of cybercrime [304].

Building up pressure on criminal organizations

Tough law enforcement can help build up pressure on criminal organizations. This can lead to members leaving the group or organizations breaking up. More specifically, it means that targeted investigations, surveillance activities and arrests can effectively restrict the operational capabilities of criminal organizations. Publicly announcing successful criminal prosecutions can erode trust within criminal organizations and deter aspiring new members. Confiscating assets and dismantling networks can also help put the finances and logistics of criminal structures under pressure.

Cutting off the flow of funds to cybercriminals

A vital approach in the fight against cybercrime is stopping the flow of funds to cybercriminals. Blocking accounts and freezing assets can deprive perpetrators of the funds they need to carry out their activities. The fact that cybercriminals are increasingly using cryptocurrencies poses a particular challenge here, as these are often difficult to trace. While digital currencies still offer perpetrators a high degree of anonymity, parliaments, international investigation agencies and financial institutions have been working hard in recent months to improve strategies for tracing crypto transactions.

By analyzing blockchain transactions in detail, investigators can trace criminal activities back to digital wallets held on regulated platforms like Binance, Bitpanda, Coinbase, eToro, Kraken, Trade Republic and Scalable Capital. The point at which digital currencies such as Bitcoin, Ethereum and Tether enter the world of traditional financial systems provides an opportunity to crack the anonymity of the criminals. Cooperation between law enforcement agencies and specialist lawyers enables the identification of offenders and the blocking and seizure of their illegally acquired digital assets.

The introduction of new regulatory frameworks and cross-border cooperation has already yielded some success in the discovery and prosecution of crypto-based money laundering activities. Despite this progress, combating the funding of cybercrime remains a difficult challenge. The rapid development of new technologies and the cross-border nature of cybercrime necessitates the continuous adaptation of financial supervision and law enforcement measures.

Dismantling cybercriminal infrastructures

Dismantling cybercriminal infrastructures, such as botnets or darknet marketplaces, is another major law enforcement goal. Continuous takedowns of cybercrime forums and marketplaces have shortened the lifespan of criminal websites and contributed to the continued fragmentation of the criminal marketplace [100].

Structural data on cybercriminals

Cybercrime is a complex phenomenon, perpetrated by a multitude of different threat actors. Many cybercriminals are lone actors or part of loose networks, which makes it difficult to pin them down to a specific country.

The victims of cyberattacks are just as diverse. Large companies are popular targets due to their valuable data and resources. Critical infrastructures, such as energy suppliers and hospitals, are also frequently targeted, as disrupting them can have a major impact. Public institutions are targets for espionage and sabotage, while individuals are often the victims of phishing attacks and identity theft.

Cybercrime has evolved considerably and become significantly more professionalized in recent years [100]. Its deep integration with the underground economy forms an interface where technology and crime converge [6].

Once confined to local networks and physical meeting places, the advance of digitalization has enabled the underground economy to develop into a global phenomenon. Cybercriminals exploit the anonymity of the Internet to trade goods and services – from drugs to counterfeit documents to stolen identities. The underground economy, in turn, provides the necessary infrastructures and markets for laundering and investing the proceeds of cybercrime. The interdependence of the two makes for the perfect breeding ground for an ever-growing escalation in threats for companies, countries and individuals.

Financial aspects play a key role in cybercrime. Cryptocurrencies like Bitcoin are often used to pay ransoms and for money laundering. On darknet markets, cybercriminals can buy and sell stolen data, malware and other illegal goods in cryptocurrencies, making it even more difficult to trace and combat these activities.

The darknet continues to be a key enabler of cybercrime, as it allows perpetrators to share knowledge, tools and services in a virtually anonymous environment. The landscape of darknet providers and services is dynamic and characterized by the fragmentation of marketplaces. As a result, the lifecycle of criminal websites has become shorter. In this context, it has been observed that competition has intensified between ransomware-as-a-service (RaaS) providers for the services rendered by these websites [100]. The TOR network remains the most popular platform for cybercriminals seeking to access the darknet.

The role of artificial intelligence in law enforcement

Cybercriminals are increasingly leveraging artificial intelligence (AI) to optimize their attacks. Law enforcement agencies therefore need to build up their AI capabilities if they are to effectively counter these threats [100]. AI is playing an increasingly important role in the prosecution of cybercriminals. The use of AI enables vast amounts of data to be analyzed in real time and suspicious activities to be identified more quickly. Machine learning algorithms help recognize patterns and detect anomalies that could indicate criminal activity. In addition, AI enables the automation of routine tasks, freeing up time investigators can then dedicate to more complex analyses and strategic decisions. AI-based tools can also help trace transactions in cryptocurrencies and identify networks of criminal threat actors. Overall, the use of AI helps significantly enhance the efficiency and effectiveness of law enforcement in the digital realm.

1.10 SUCCESSES IN 2024 & 2025

The most dangerous malware families taken down

According to the German Federal Criminal Police Office (BKA), the biggest operation against cybercrime in 2024 was carried out by the BKA and its international partners at the end of May 2024 as part of "Operation Endgame". Operation Endgame, launched in 2022, is a groundbreaking investigation in the international fight against cybercrime. Law enforcement agencies from the countries involved are coordinated by Europol and Eurojust. On May 28 and 29, 2024, the Public Prosecutor's Office in Frankfurt am Main and the BKA carried out an internationally coordinated operation during which several of the most dangerous malware families were taken offline. Law enforcement agencies from a number of countries, including Germany, Denmark, France, the Netherlands, the United Kingdom and the USA, supported by Europol and Eurojust, were involved in the operation. Over 100 servers were seized, more than 1,300 domains used for criminal activities were neutralized and assets amounting to over EUR 139 million were secured. Ten international arrest warrants were issued and four people were arrested. The operation targeted the malware families IcedID, SystemBC, Bumblebee, Smokeloader, Pikabot and Trickbot, which were linked to at least 15 ransomware groups. The goal of "Operation Endgame" is to destroy the most relevant malware families in the initial access malware category (known as "droppers" or "loaders"). Malware in this category is usually spread via spam emails and specializes in infecting systems without being detected, thereby bringing them under the control of the perpetrators. Sensitive data is then usually read out and the

infected systems are scouted further. The undetected infection introduced by the above-mentioned malware acts as a door opener for cybercriminals to install further malware, in particular ransomware, which is used to encrypt the victim's systems and subsequently extort ransoms [64]. During the course of the investigation, EUR 69 million were seized from one operator and 99 crypto wallets with a total value of over EUR 70 million were blocked on crypto exchanges [64], [187].

In June 2024, a 44-year-old Ukrainian was arrested in Slovakia on suspicion of being a member of the cybercriminal group GandCrab. The group attacked companies and organizations worldwide with ransomware and extorted ransoms, resulting in economic damage amounting to several hundred million euros. Officers from the German federal state of Baden-Wuerttemberg reported a successful police investigation in October 2024, after the suspect had been extradited to Germany and charged with commercial extortion and computer sabotage [175]. The defendant is accused of allegedly gaining illegal access to the computer networks of 22 German companies and organizations in spring 2019 and encrypting their data with malware (ransomware), which alone caused economic damage amounting to EUR 2.4 million, and then demanding up to USD 15,000 in digital currency for its decryption. The State Office of Criminal Investigation (LKA) has documented more than 80 cases in Germany with total damages of almost EUR 33 million, i.e., one third of the global damage attributable to the GandCrab group and a successor gang. Even greater damage was prevented thanks to the LKA, which successfully warned more than 300 companies of the criminal operation in good time. At least 17 of these companies were at imminent risk of their data being encrypted. The authorities have identified two further suspected key threat actors who are wanted on international arrest warrants. These men, both Russian nationals, are believed to be behind the two groups and the developers of the extortion software. These findings stem from many years of international investigations in which the German Federal Criminal Police Office (BKA), the United States Secret Service, the FBI and Europol were involved alongside national agencies. In an official press release on January 27, 2025, the Baden-Wuerttemberg Cybercrime Center, based at the Public Prosecutor's Office in Karlsruhe, announced that it had brought charges against the perpetrator arrested in Slovakia before the Stuttgart District Court [117].

Crackdown against threat actors in the underground economy

In September 2024, the German Federal Criminal Police Office (BKA) successfully dismantled the infrastructure of digital money launderers in the underground economy, shutting down 47 exchange services hosted in Germany that were being used for criminal purposes. These platforms facilitated the anonymous exchange of conventional currencies and cryptocurrencies without requiring compliance with the applicable anti-money laundering regulations. The operators are accused of concealing the origin of criminally obtained funds through the inadequate implementation of the know-your-customer (KYC) principle. The exchange services shut down were a crucial link in the cybercrime value chain used by ransomware groups, darknet dealers and botnet operators. Extensive user and transaction data was seized, providing valuable investigative leads and helping to successfully weaken the criminal infrastructure [63].

On October 31, 2024, in an international operation coordinated by the Central Office for Combating Cybercrime (ZIT) at the Public Prosecutor's Office in Frankfurt am Main, the Hessian State Office of Criminal Investigation (HLKA) and the BKA, two suspected cybercriminals were arrested in the German federal states of Hesse and Rhineland-Palatinate. The suspects, aged 19 and 28, are accused of acting as administrators of the online platforms Flight RCS and Dstat.CC, through which they sold narcotics and DDoS attacks. The investigations, which were carried out as part of the international "Operation PowerOFF", led to the seizure of extensive evidence and the identification of other key threat actors [61].

In mid-December 2024, the BKA and the Public Prosecutor's Office in Frankfurt am Main announced that action had been taken against criminal service platforms for DDoS attacks as part of the internationally coordinated "Operation PowerOFF", together with law enforcement

agencies from 15 countries. The operation resulted in 27 stresser services being seized and taken offline. These criminal online platforms enable users to carry out DDoS attacks quickly and easily, without requiring any in-depth technical expertise. Furthermore, over 300 users were identified, and three suspected administrators were arrested in France and Germany [65].

At the beginning of 2025, the Central Office for Combating Cybercrime (ZIT) at the Public Prosecutor's Office in Frankfurt am Main scored a major victory in the fight against the digital underworld in a large-scale international operation. In close cooperation with law enforcement agencies from the USA, Australia, Spain, Greece, Romania, Italy and France, "Operation Talent" successfully shut down the platforms nulled.to and cracked.io – forums regarded as key entry points into the underground cybercrime economy. These platforms were used to trade illegal services such as DDoS attacks, malware, cracking and hacking tools, as well as AI-supported malware and data leaks – with an estimated revenue of more than 1 million euros. Eight people linked to the websites were arrested during the operation. The operation highlights the increasing effectiveness of international law enforcement cooperation in the fight against cybercrime, while also sending a clear signal in the fight against organized crime in the digital realm [66].

Online threats, marginalization, hate speech and harassment

The Public Prosecutor's Office in Frankfurt am Main and the German Federal Criminal Police Office (BKA) have launched criminal proceedings against 10 suspected members of the online group "New World Order". The suspects are accused of being leaders of a criminal organization engaged in systematic cyberbullying and cyberstalking activities. A total of 10 homes were searched in six German federal states, as a result of which numerous electronic devices and storage media were seized. The group especially targeted people from the online streaming scene, who they attempted to coerce into relinquishing their online presence by means of threats, insults and publication of their personal data (known as doxing). The organization's methods also included "swatting", whereby emergency services were hoaxed into sending the police or fire department to victims' addresses [62]. The "New World Order" is an exclusively virtual association of individuals. In many instances, the leaders of the organization had selected people from the online streaming scene as their victims (or "masks"), often vulnerable people or people with cognitive impairments. The victims were then stalked, threatened and insulted by the organization over social media.

1.11 OUTLOOK 2025-2030

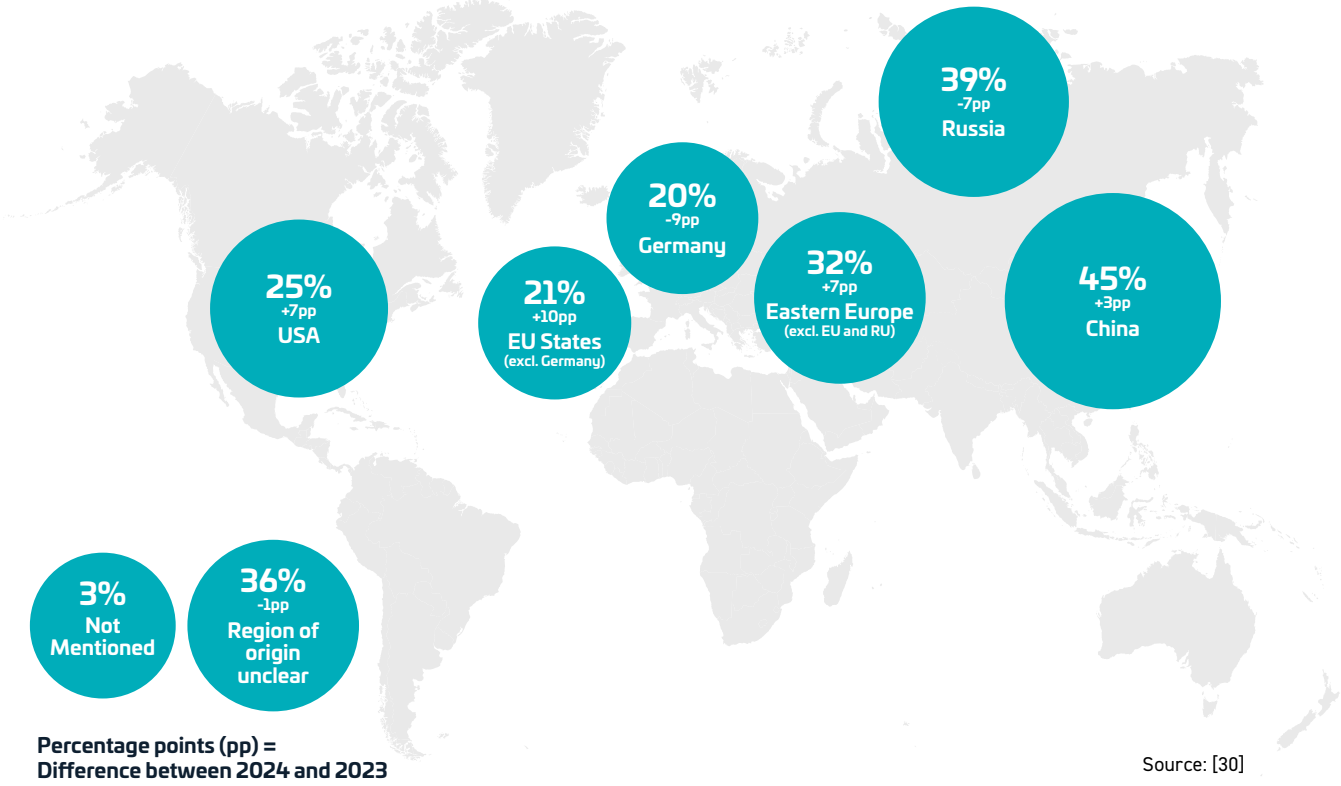
The ever more extensive networking of all areas of life, coupled with growing geopolitical conflicts, will make cyberattacks an even greater and more complex threat over the next five years. According to one forecast, worldwide spending on IT security is expected to amount to USD 212 billion in 2025. This represents an increase of 15.1 percent on 2024 [115].

A rise in attacks based on stolen data is predicted for 2025. In addition to widespread infostealers such as Lumma, Vidar and Redline, an increasing number of new threat actors who exploit stolen information for their own ends are also anticipated to emerge [271].

However, it is not only the type of attack and the tools used that will heighten the risk of damage from cyberattacks. Vulnerabilities caused by the ongoing skills shortage or cross-border ICT service providers as a single point of failure, for example, will also increase the threat potential in the long term. SMEs in particular are expected to become increasingly reliant on external IT service providers, resulting in more complex supply chains and cybersecurity challenges [97].

Attackers of the future

Against the backdrop of complex geopolitical events, state controlled or sponsored attacker groups are gaining in prominence. The "Big Four" – Russia, China, Iran and



Source: [30]

Figure 10: Geographical origin of cyberattacks in 2024 – as assessed by German companies (multiple responses permitted)

North Korea – will continue to remain active in cyberspace and to carry out cyber espionage, cyberattacks and information operations in order to further assert their respective geopolitical interests in the future [121]. In Ukraine, Russia is demonstrating its continued willingness to weaponize cyberattacks and leverage them as part of hybrid warfare, thereby normalizing their use (see fig. 10 for an overview of the geographical origin of digital attacks).

At the same time, known attacker groups will continue to become more professional.

- Ransomware etc.
- Development of new technologies and services to serve the broad spectrum of attackers
- Division of tasks and increased specialization

Technologies of the future

While artificial intelligence (AI) leads to many positive developments, these opportunities will also increasingly be harnessed by attackers in the future to carry out sophisticated phishing, vishing and social engineering attacks. Attackers will also leverage deepfakes for identity theft, fraud and bypassing security requirements, among other things [121]. It is predicted that by 2027, approximately 17 percent of all cyberattacks and data leaks will involve generative AI (GenAI) [115]. GenAI will also enable operations on a much larger scale. For example, cybercriminals can use AI to launch thousands of targeted phishing attacks simultaneously, whereby each attack can be customized for maximum impact. This allows even smaller criminal groups to carry out large-scale operations without the need for any advanced technical expertise [71]. AI is also becoming increasingly useful for information operations (IO), with IO threat actors deploying AI to scale content creation, produce more persuasive content and flesh out fake personas [121].

The dependency on satellites, which is growing faster than anticipated, and the increasing connectivity of vehicles are also inseparable from cybersecurity and data protection considerations [97]. As computing power continues to advance, it is vital that encryption keys be regularly rotated, as these can eventually be cracked.

Attack methods of the future

In the ever-evolving world of cybercrime, companies and organizations are constantly facing new challenges in terms of the various types of cyberattacks. Ransomware and multifaceted extortion will continue to pose the biggest threats in the future, impacting a broad range of sectors and countries. These attacks aim to encrypt critical data and then demand a ransom to release it [121]. Moreover, perpetrators with little or no technical expertise can find ransomware-as-a-service (RaaS) options on the dark web. They can simply use pre-developed ransomware tools to launch attacks in return for sharing the ransom with the provider. Perpetrators are also increasingly carrying out

double extortion activities, i.e., demanding a ransom not only to release the stolen data, but also not to leak it [11].

At the same time, infostealer malware also continues to pose a significant threat, as it enables data breaches and allows accounts to be compromised. This type of malware extracts sensitive information, such as passwords and financial data, which is then sold via forums or on criminal marketplaces [121]. Infostealers already dominated the malware landscape as the most prevalent type of malware in the first half of 2024. LummaC2, a stealthy malware for spying on sensitive data, was the most active and replaced other well-known infostealers like RedLine [146].

Another concerning trend is the democratization of cyber capabilities. Improved access to tools and services lowers the barriers to entry for less skilled threat actors, consequently leading to a rise in cyberattacks. As a result, less experienced criminals are increasingly able to carry out complex attacks.

Compromised identities in hybrid environments give attackers access to sensitive systems and data, and therefore also pose a significant risk. In an increasingly networked world, it is consequently becoming ever-more vital to manage and protect identities and access rights effectively.

"Web3" and cryptocurrency organizations are also a particular focus, as they are increasingly the target of attackers seeking to steal digital assets. These attacks can cause considerable financial damage and erode trust in digital currencies and technologies.

In addition, the time-to-exploit (TTE) is becoming ever shorter for vulnerabilities, and the number and variety of targeted vendors is constantly growing. Attackers are increasingly able to identify and exploit vulnerabilities more rapidly, underscoring the need for proactive and timely security measures and fast response times [121].

These developments require innovative defense strategies and increased vigilance in order to successfully respond to future threats. Companies need to continuously adapt and improve their security measures in order to stay one step ahead of the evolving threat landscape.

Defense methods of the future

Artificial intelligence (AI) and machine learning not only play a key role in cyberattacks but are also increasingly being used in cyber defense. The use of these tools will, for instance, accelerate anomaly detection, reduce analysis time with the help of predictive capabilities and help automate response actions, in addition to elaborating and strengthening strategies to defend against emerging threats [271]. Research conducted by IBM and Ponemon Institute shows that companies that applied AI and automation for security prevention saved on average USD 2.22 million [144]. These savings are the result of decreasing the time to detect and contain security incidents, minimizing business disruption and reducing the cost of manual security checks.

Achieving optimal defense against modern threats necessitates a symbiotic combination of proactive threat intelligence, predictive analytics, continuous monitoring and a strict zero-trust model to minimize the attack surface and accelerate threat detection. Behavior-based anomaly detection, machine learning and automated threat hunting are complemented here by a holistic security strategy which strengthens resilience against targeted attacks and reduces the mean time to detect (MTTD). In addition to technical measures, it is also important to organize routine cybersecurity training for employees and to provide information and follow-up training on a regular basis. Up-to-date knowledge of the most important potential cyberthreats is essential, as uninformed employees are among the most common initial attack vectors that can lead to serious financial losses for a company [271]. In this context, it is extremely beneficial for state and private sector players to cooperate and share methods and knowledge, as well as any new anomalies.

The role of cybercrime in times of geopolitical instability and conflicts

The use of cyber operations during wartime has now become reality. Although to date only a few countries have publicly admitted to carrying out such operations, a growing number of countries are developing military cyber capabilities. Cyber operations are likely to increase in the future, also within the context of military conflicts. Their use increases the risk of a significant, far-reaching impact – either deliberately or accidentally – on critical infrastructure such as key industries, telecommunications and transport, and governmental and financial systems [148].

Cyberattack on Slovakia's land registry

In the very first week of 2025, Slovakia was hit by a serious cyberattack that sparked problems right across the country. The target was Slovakia's central land registry, and the attack succeeded in completely paralyzing the agency's systems. This led to the nationwide outage of all associated services and databases, with a significant impact on both the property market and agricultural businesses. The attack, caused by a ransomware infection, appears to have originated in Ukraine – an assumption that seems increasingly plausible given the growing political tensions between Slovakia and Ukraine [13], [172].

CHAPTER 2

SPOTLIGHT – GERMAN BUSINESS CYBERSECURITY PERSPECTIVES

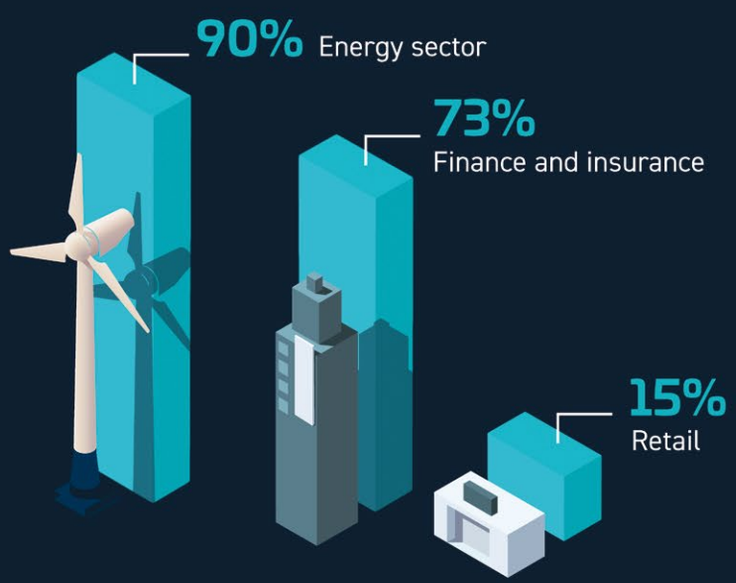
Security Operations Centers

Every 5th company, including smaller businesses, has a SOC.

78%

More than three-quarters of companies have increased their security budgets

Regular pentesting



NIS 2

Impacted companies, especially mid-sized and larger businesses, are well-informed and prepared.

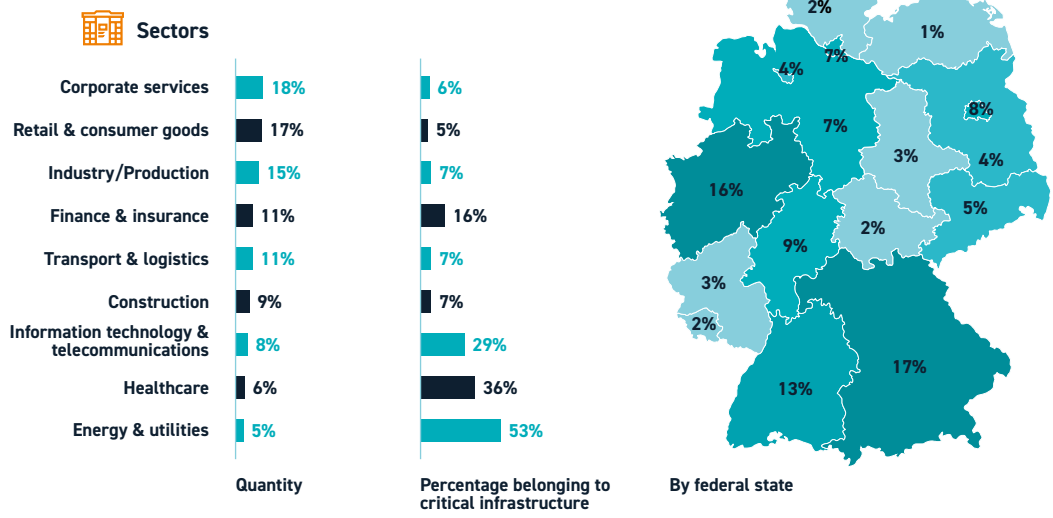
Only around 40% feel that authorities are supporting them well, although for critical infrastructure companies the figure rises to 49%.

Sources: [255], own diagram

2 SPOTLIGHT – GERMAN BUSINESS CYBERSECURITY PERSPECTIVES

The cybersecurity threat situation continued to intensify in 2024. Companies found themselves confronted with increasingly sophisticated attack methods, ever stricter regulatory requirements and significant strategic challenges. Implementation of the NIS 2 Directive required far-reaching structural changes, while technological dependencies – for instance due to vendor lock-in – had an impact on long-term decision-making. Meanwhile, the security of globally networked supply chains continued to gain in importance. Existing threats, such as internal cybercrime and attacks on space-based infrastructures, gained greater prominence, forcing many organizations to revise their protective measures.

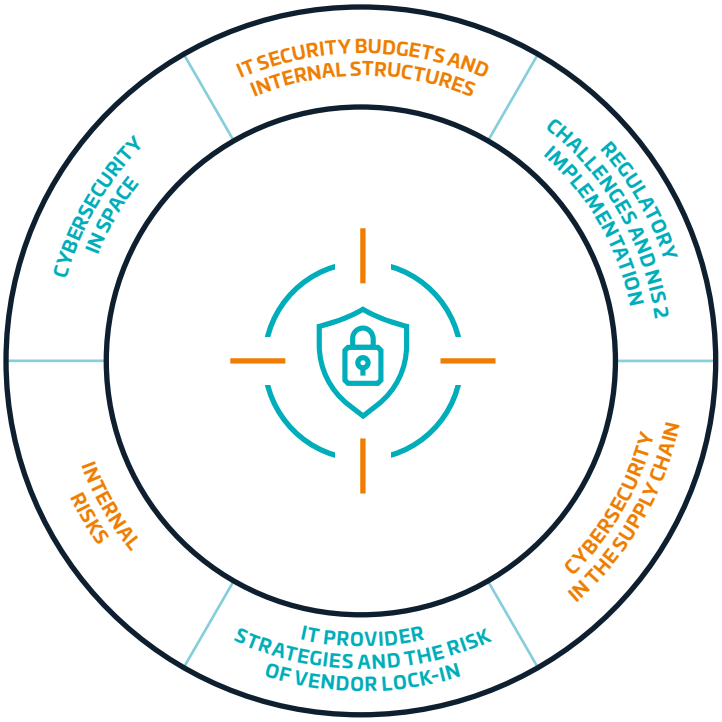
IT security departments found themselves on the front lines – often with limited resources. In this dynamic environment, our new study provides a systematic review of the cybersecurity strategies pursued by German companies. It examines how companies of varying sizes – from small businesses to critical infrastructure (KRITIS) operators – have responded to these challenges, analyzes the measures they have taken, and determines where the need for further action is greatest.



Any deviation in these figures is due to rounding.
The same applies to all graphic representations in this chapter.

Source: [255]

Figure 11: Overview of the survey participants by sector, federal state, company size and international activity (in %).



Source: [255]

Figure 12: Overview of topics comprising the representative survey

This new study is based on a representative survey conducted by way of telephone interviews (CATI) during the fourth quarter of 2024. In total, 1,001 companies in various sectors were surveyed with the aim of obtaining a comprehensive overview of the cybersecurity landscape. The sample group included 778 small companies with fewer than 50 employees, 123 mid-sized companies with 50 to 249 employees, and 100 larger organizations with 250 or more employees. A significant proportion of the companies surveyed operate internationally. More than a third have a presence in foreign markets and a quarter have their own subsidiaries abroad.

A special focus was placed on a comparative analysis of companies classified as critical infrastructure (KRITIS) with those lacking this status. The survey was aimed specifically at decision-makers who were able to provide sound, substantiated insights into the cybersecurity strategies of their organizations. An overview of the sectors surveyed is provided in figure 11.

To place the results in a broader economic context, they were compared with data from Bitkom's Corporate Security Study 2024 and the World Economic Forum's Global Cybersecurity Outlook 2025. The Bitkom study was conducted between calendar weeks 16 and 24 of 2024 and is based on a sample of 1,003 companies with at least 10 employees and an annual revenue of 1 million euros or more [92].

Our new study, however, takes companies of all sizes into account, regardless of their revenue. As a result, it provides a more comprehensive perspective on cybersecurity strategies – particularly those of small and mid-sized companies, which are underrepresented in many existing surveys. At the same time, this broader sample group leads to a deviation in average values in some areas compared to the Bitkom study, especially with regard to budget allocation or the evaluation and perception of certain security measures.

The Global Cybersecurity Outlook 2025 augments this perspective with an international analysis of cybersecurity challenges based on a survey of 321 managers from 57 countries, which was conducted between September and October 2024 [6].

This new study and the Bitkom study both address topics such as the security situation, internal threats and IT budgets. In the current study, the focus is extended to include additional dimensions, including the implementation of the NIS 2 Directive, dependency on individual providers (vendor lock-in), cybersecurity in supply chains and security risks in space-based infrastructures. In these areas, there is some overlap with the WEF report, which addresses regulatory challenges and risks from systemic threats in supply chains and satellite technology [6], [30],], among other topics.

Against this backdrop, this current study analyses the cybersecurity strategies pursued by German companies and examines both existing and emerging challenges. In addition to technical and organizational measures, the major focus was on strategic issues.

IT infrastructures and the organization of security operations centers (SOCs) represented key aspects of the study. The allocation of budgets for IT and IT security, the effects of economic trends on investment in IT, and the staffing of IT security departments were analyzed. More-

over, the survey analyzed the extent to which companies operate their own SOCs and the ways in which they conduct penetration testing as part of their security checks.

The study also focused on regulatory requirements, particularly the implementation of the NIS 2 Directive. The study reveals the extent to which companies consider themselves to be prepared, the challenges they envisage and the extent to which they are relying on external support.

The technological dependency of organizations on IT providers (vendor lock-in) was also explored. The survey investigated whether companies use cybersecurity solutions from one or more providers, which strategies they pursue to minimize risk and how flexible they are in changing their providers.

One of the growing risk factors for companies is cybersecurity within the supply chain. The study sheds light on the extent to which companies are aware of cyber risks from external partners, which security demands they place on their suppliers and how often they audit those security measures.

The survey also covered internal threats from current or former employees. In this context, the frequency of security incidents, the preventive measures in place and existing monitoring mechanisms were assessed.

Cybersecurity risks in space-based infrastructures were also analyzed. Companies reported how they assess the potential threat and whether specific safeguards have been implemented (fig. 12 provides an overview).

The findings indicate that companies need to develop their cybersecurity strategies further in order to fulfill regulatory requirements, avoid technological dependencies and better control internal and external risks.

2.1 IT SECURITY BUDGETS AND INTERNAL STRUCTURES

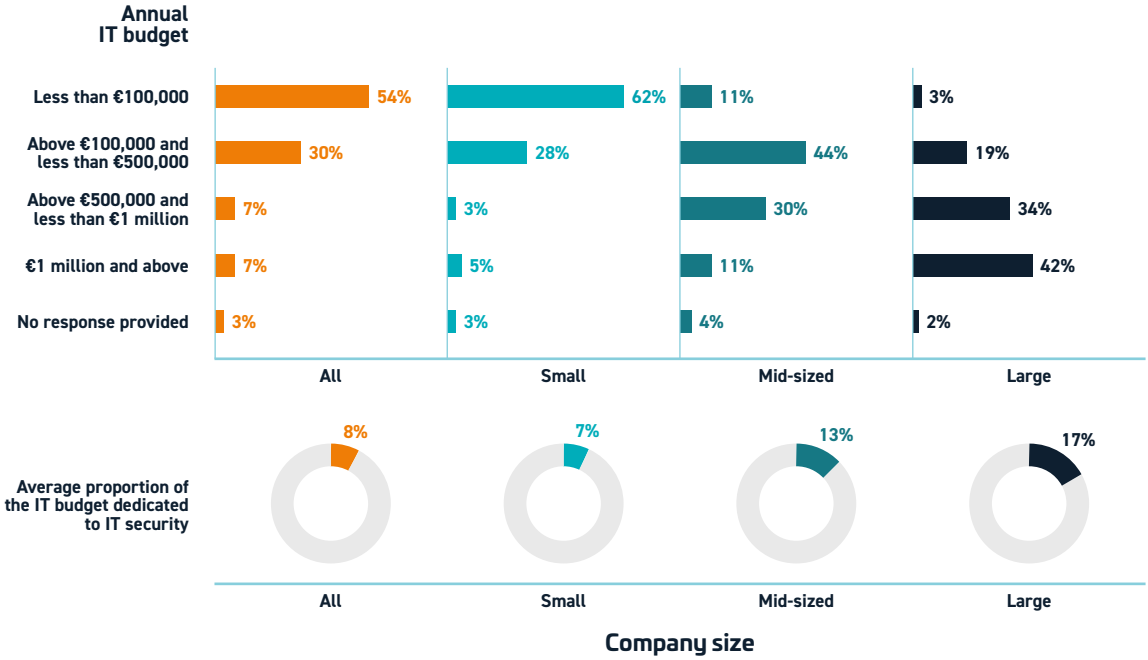
Information technology forms the backbone of a modern company – from the ability to efficiently process data all the way through to defending the organization against sophisticated cyberattacks. While large corporations are continuously building up their security strategies, smaller businesses are faced with growing threats and limited resources.

A key factor in ensuring a company's security capacities is the size of the IT budget. More than half of the companies in Germany have an IT budget of no more than 100,000 euros. IT budgets increase significantly as companies get larger. In companies with 250 or more employees, the IT budget exceeds 1 million euros in 42 percent of all cases (see fig. 13).

While the Bitkom Corporate Security Study puts the average share of IT security expenditure at 17 percent [30], our recent survey indicates a lower proportion. On average, only 8 percent of the IT budget is spent on cybersecurity measures. This figure is likely to reflect the actual situation at German companies more realistically, as the new study is representative of companies of various sizes, regardless of their turnover – including many small and medium-sized enterprises. As stated in the introduction, the Bitkom study only considers companies with an annual revenue of 1 million euros or more, which explains why its figures may tend to be distorted upwards [30].

The available data indeed shows a clear correlation between company size and security expenditure. Large companies are shown to invest an average of 17 percent of their IT budgets in IT security (see fig. 13) – a proportion consistent with the results of the Bitkom study. The lower overall value shown in the current study is therefore due to the inclusion of smaller companies, which tend to earmark a lower proportion of their IT expenditure for security measures.

Despite the difficult economic situation, many companies have recently bolstered their investments in IT security.



Source: [255]

Figure 13: Annual IT budget and proportion dedicated to IT security

More than three quarters (78%) of those surveyed stated that they had increased their budgets, with the figure for mid-sized companies even higher at 81 percent. This development indicates that cyberattacks and their potential consequences are increasingly recognized as a business-critical risk.

The healthcare sector is more reluctant to invest in IT security compared with other sectors. One potential reason could be that investments have already been made, along with the fact that regulatory requirements stipulate a defined level of security. The current survey provides support for this assumption. In addition to being questioned about IT security budgets, the companies were also asked whether they have appointed an internal data protection officer.

This role is particularly prevalent in the healthcare sector. The majority of companies in this sector have an in-house data protection officer, which is considerably more than the average across all sectors. The survey reveals a proportion of 58 percent, compared with 38 percent across the economy as a whole. As the size of the company increases, this figure rises further to 67 percent for mid-sized companies and 70 percent for large companies.

While the healthcare sector leads the way in this regard, the retail and consumer goods sector has the lowest proportion at 14 percent. While data protection remains a key issue, staffing levels vary considerably between sectors. Many companies rely on external data protection officers to fulfill legal requirements and ensure access to expertise.

In addition to financial resources, the availability of internal IT competencies plays a crucial role when it comes to cyber resilience. While 63 percent of companies have their own IT departments, there are glaring differences between small and large businesses. Almost all large companies have internal IT teams, whereas almost half of small companies do not have their own IT departments. The retail and consumer goods sector has a particularly low percentage of internal IT departments with 22 percent, as does the construction industry with 47 percent.

The size of IT departments also varies greatly. In smaller companies, IT teams are usually very modest in size – over 70 percent of such companies have a maximum of five IT employees, while larger companies have much more substantial IT departments. In mid-sized companies, just under half of IT departments have six to 10 IT employees, while large organizations are most likely to have a team of between 11 and 25 employees. Approximately a third of large companies have more than 25 IT workers on staff.

The number of employees dealing exclusively with IT security also increases in line with the size of the company. In small companies, IT security is often an additional task within the IT department – almost all companies (95%) in this category have no more than five dedicated security specialists. In mid-sized companies, the number of specialized employees is slightly higher, but again most companies only have up to five specialists (74%).

When it comes to large companies, a different picture emerges. More than two thirds of these businesses have specialized IT security teams comprising more than five employees. Around a third employ between 11 and 25 people to work exclusively on IT security tasks, and in some cases (4%) there are even more than 25 experts working exclusively on safeguarding corporate systems.

Security operations centers (SOCs) are a core component in a proactive security strategy, as they monitor, analyze and defend against cyber threats in real time. Nevertheless, SOCs are not yet universally implemented at companies. One in five companies already uses a SOC, although hybrid models are most common. More than 40 percent of companies combine the use of in-house and external specialists to leverage expertise and state-of-the-art technologies. Large companies especially rely heavily on a hybrid model (59%), while smaller companies often opt against it entirely. The size of SOC teams varies considerably. Whereas companies with fewer than 250 employees usually manage with no more than five people, 7 percent of large companies have SOC teams comprising more than 25 experts.

Penetration tests are another essential tool for checking and evaluating an organization's IT security but are employed in a variety of ways depending on the size of the organization and the sector it belongs to. Only 37 percent of companies regularly conduct penetration tests. While two thirds of small companies refrain entirely from penetration tests, 60 percent of large companies conduct them at least every six months. Penetration testing is used particularly frequently in highly regulated sectors such as energy and utilities (90%) and finance (73%). In the retail and consumer goods sector, on the other hand, the rate of usage is only 15 percent.

The use of cloud services is now almost pervasively established across the German business landscape. A mere 4 percent of companies do not utilize cloud technologies, which is confirmation that the cloud is now an indispensable component of any modern IT infrastructure. However, companies need to ensure that security topics and data protection aspects are given adequate consideration in order to mitigate the risks associated with the cloud.

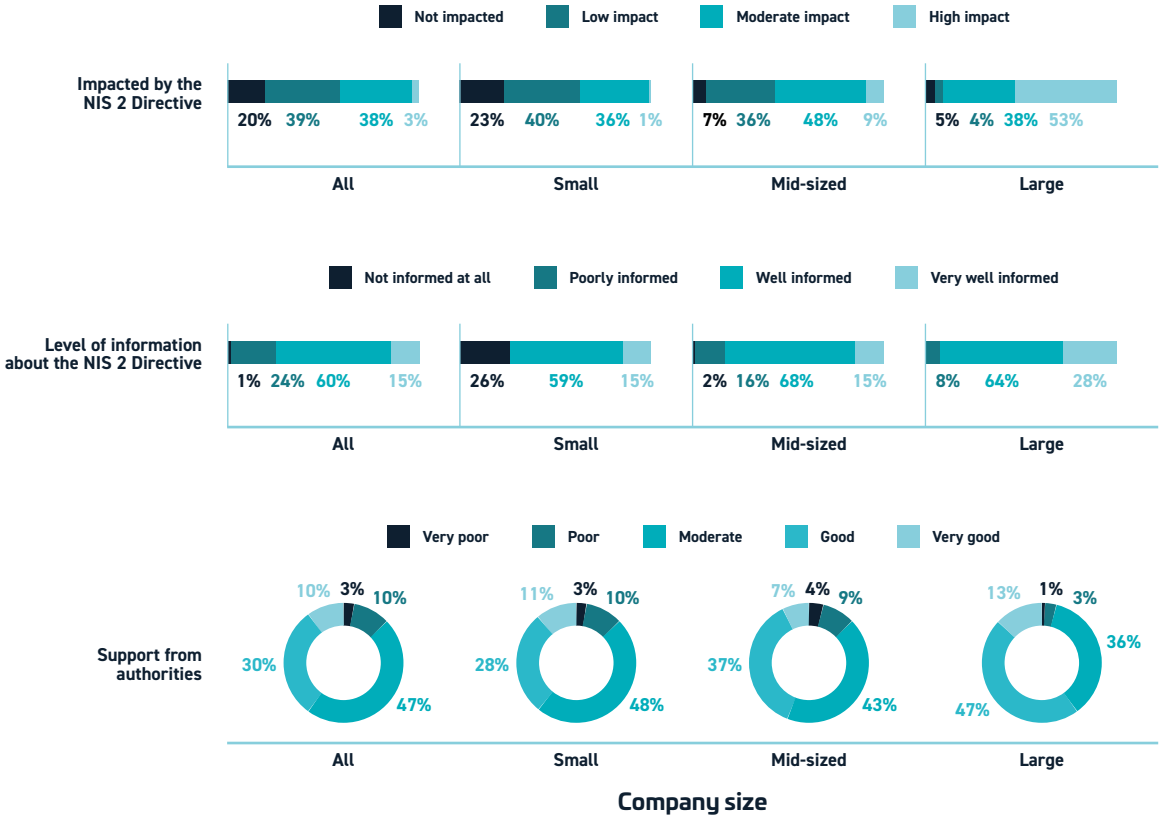
2.2 REGULATORY CHALLENGES AND NIS 2 IMPLEMENTATION

In the European Union, the regulatory requirements with regard to cybersecurity are growing continuously and are increasingly turning into business-critical tasks for companies. Following the introduction of the revised "Network and Information Security (NIS) Directive" 2 (NIS 2), companies have an obligation to implement new security standards to safeguard their digital infrastructures and boost their resilience. Our new survey shows that while larger companies and regulated industries are well prepared, uncertainty often prevails among smaller companies.

The majority of the companies surveyed consider themselves well-armed against cyberattacks. Two thirds (66%) of companies rate their level of preparation as either good or very good, while only 1 percent rate it as inadequate – a positive signal against a backdrop of growing threats. At the same time, one in three companies reported that their level of preparation was only average.

The contrast between small and large companies was particularly pronounced in this regard. Whereas 37 percent of small companies assess their preparation as average, the majority of mid-sized and large companies consider themselves to be well or very well prepared. Companies with clearly defined regulatory requirements perform better. In the energy and utilities sector, 84 percent of companies rate their level of cybersecurity positively, while in the finance and insurance sector, this figure is even higher at 92 percent.

A comparison with international data reveals parallels, but also differences. As in our recent study, large companies responding to questions regarding their own cyber resilience in the WEF's Global Cybersecurity Outlook 2025 generally scored better than smaller ones. While only 1 percent of companies in the current survey stated



Source: [255]

Figure 14: Companies impacted by NIS 2, level of information about the directive and perceived support from authorities

that they were insufficiently prepared for cyberattacks, the WEF report paints a different picture for small companies around the globe. More than a third of the companies surveyed (35%) considered their cyber resilience insufficient – a proportion which has increased sevenfold since 2022 [6].

Almost half of the companies surveyed stated that they were impacted by NIS 2 – again with clear differences between smaller and larger companies (see fig. 14). While 91 percent of large companies are subject to the directive, it is less often seen as playing a role when it comes to smaller companies. However, some companies may be underestimating the extent to which they may be affected directly or indirectly through their supply chains. In principle, NIS 2 applies to all companies with 50 or more employees and an annual revenue of 10 million euros or higher. However, companies designated as "essential entities" (critical organizations such as energy providers or banks) and "important entities" (companies which are significant but not system-critical, such as IT service providers or chemicals companies) are subject to the regulations regardless of their size or revenue. In addition, large companies may require their suppliers to comply with the NIS 2 standards, extending the impact of the requirements along the entire value chain [92].

While regulation strengthens cybersecurity, it also poses challenges for companies. The WEF's Global Cybersecurity Outlook 2025 shows that 78 percent of managers consider regulations effective, while two thirds see the growing number and complexity of regulations as a cause for concern [6].

This tension is also evident in the present study, in which the support of authorities is assessed somewhat ambivalently. Companies impacted by NIS 2 – especially mid-sized and large companies – are well informed and prepared. Nevertheless, almost two thirds (60%) of these companies perceive government support to be inadequate (see fig. 14), compared to 49 percent of critical infrastructure (KRITIS) companies. At the same time, Bitkom's Corporate Security Study reveals that 75 percent of respondents consider state security agencies to be largely powerless against cyberattacks launched from abroad [30]. This highlights a discrepancy between support for the implementation of regulatory requirements and the general assessment of the state's ability to take action in the area of cybersecurity. One potential reason for this criticism is that NIS 2 had not yet been fully transposed into national law at the time of the survey, meaning that many companies had not yet been able to conclusively assess the need for action in practice.

Despite this uncertainty, three quarters of the impacted companies consider themselves to be either well or very well informed about NIS 2.

The majority of companies subject to NIS 2 are relying on internal resources to implement the directive. Only 16 percent have brought in external consultants or partners to ensure their compliance with the new requirements. Depending on the size of the organization, there are once again clear differences. While 35 percent of mid-sized and 59 percent of large companies rely on external support, smaller companies have largely refrained from doing so.

One key factor is access to resources. Larger companies have the financial means at their disposal to make use of external expertise, while smaller companies have to cope with the requirements internally. Critical infrastructure companies in particular rely on external consulting more frequently than the average – 58 percent of them employ consultants, compared to only 13 percent of companies not designated as critical infrastructure (KRITIS).

New regulatory requirements often initially meet with a certain amount of reluctance – often exacerbated by a lack of transposition into national law. At this early stage, many companies are expressing optimism, but this assessment could become less favorable as the requirements become more clearly defined.

The message is clear: NIS 2 will bring about lasting change to the cybersecurity landscape. Smaller companies, in particular, and those that were not previously subject to specific cybersecurity requirements need to take action in order to comply with the new requirements. At the same time, it is evident that companies with more extensive resources are taking measures in good time, while smaller companies often adopt a wait-and-see approach.

Along with these challenges, however, the directive also presents opportunities. Companies which address the requirements at an early stage are not only strengthening their compliance but also bolstering their own resilience to cyber threats, providing a crucial competitive advantage in an increasingly digitalized business environment.

2.3 CYBERSECURITY IN THE SUPPLY CHAIN

In the face of escalating cyber threats, safeguarding supply chains is becoming increasingly important. There is nevertheless a great disparity between the perception of threats and implementation of appropriate security measures. More than half (52%) of the companies surveyed do not believe that their suppliers or external partners could be the source of any cyber risks (see fig. 15). This is higher than the results obtained in Bitkom's Corporate Security Study, in which 37 percent of the companies surveyed stated that their organizations lacked sufficient awareness of these risks [30]. It is particularly notable that smaller companies tend to underestimate or even rule out the possibility of cyber risks in their supply chains more often than large companies. While 55 percent of small companies rate the risk as "rather low" or "very low", larger companies tend to be more cautious, with 84 percent rating the risk as at least "moderate". One potential explanation for this may be that small companies often operate as part of a larger supply chain

rather than being the main player themselves. In addition, smaller companies often lack the human and financial resources to conduct comprehensive risk analyses.

Comparing this with data from around the world reveals a different perspective. In the WEF survey of 57 countries, 54 percent of large companies regarded supply chain security as the greatest challenge to their cyber resilience. The increasing complexity and lack of transparency in supply chains are deemed particularly problematic. Vulnerabilities in software provided by third-party vendors and the spread of cyberattacks throughout the entire ecosystem are seen as the key risks [6].

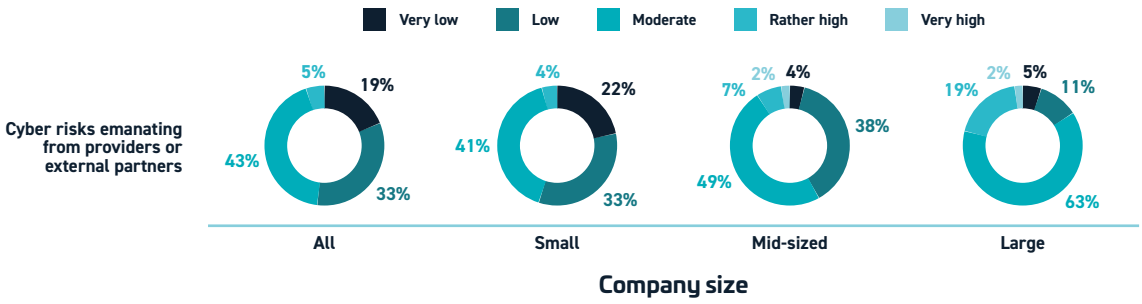
The results of Bitkom's Corporate Security Study 2024 are proof that attacks on providers pose a clear and present danger. Of the companies surveyed, 13 percent have certain knowledge that their suppliers have fallen victim to data theft, industrial espionage or sabotage within the last twelve months. Another 13 percent suspect that such an incident may have occurred. As a result, 44 percent of the companies that were certain a supplier had fallen victim reported a significant loss of business [92].

The varying perceptions regarding risks are reflected in the security requirements demanded of suppliers. While only 16 percent of small companies have defined binding cybersecurity requirements for all their suppliers, this figure rises to 23 percent for mid-sized companies and 40 percent for large companies. For critical infrastructure (KRITIS) companies the proportion is even higher at 49 percent.

In addition, many companies only define and implement security requirements for selected suppliers – a total of 41 percent of the companies surveyed. This is particularly prevalent among large companies, with 85 percent enforcing security requirements for either all (40%) or only certain of their suppliers (45%).

Mid-sized companies show a mixed approach. While 18 percent of them currently have no binding requirements but are planning to introduce them, 15 percent of medium sized organizations do not currently have any plans to do so. Small businesses take a wide variety of approaches to the topic, with 56 percent of them already having defined cybersecurity requirements for their suppliers – 16 percent for all of them and 40 percent only for some. On the other hand, 34 percent of small companies have no plans to introduce any such measures.

The auditing of cybersecurity measures, for instance supplier compliance with security standards, also shows considerable variance between different companies. While 80 percent of large companies audit their suppliers regularly or occasionally, this figure drops to just 49 percent across all company sizes. One third of companies do not carry out any auditing at all. Companies in the finance, insurance and energy sectors are particularly ac-



Source: [255]

Figure 15: Assessment of the cyber risks emanating from providers and external partners (in %)

tive, with 79 percent of these companies carrying out reviews of their suppliers' security measures. In contrast, companies in the retail and consumer goods sectors are the least active when it comes to auditing, with only eleven percent reviewing their suppliers.

The proportion of companies reporting that they regularly audit their suppliers' cybersecurity standards was 13 percent, slightly lower than the 19 percent determined in Bitkom's Corporate Security Study [30]. A positive trend emerges here, however, with 36 percent of companies at least carrying out occasional audits regardless of their size. Small and mid-sized companies are almost on a par here, with 36 percent of small and 35 percent of mid-sized companies auditing their suppliers occasionally. However, clear differences are evident when it comes to regular audits. While only 10 percent of small companies regularly audit their suppliers, this figure rises to 26 percent for mid-sized companies and 43 percent for large companies. These figures indicate that the larger the company is, the greater their awareness of risks becomes and the more resources they have available to carry out systematic audits.

Companies that at least carry out event-driven auditing of their suppliers' cybersecurity measures were also questioned about the frequency of their audits and assessments. These include, for example, security checks by internal or external auditors, as well as penetration tests. When it comes to large companies, at least 70 percent of the organizations audit their supply chains at least once a year or more frequently. Across all company sizes, the survey showed that 29 percent of companies carry out audits annually or more frequently, 24 percent every two years, and 16 percent reported auditing at less frequent intervals. Overall, around 30 percent of the participating companies do not conduct regular audits of their supply chains at all. Small companies, in particular, are less likely to carry out audits or reviews – with more than a third conducting none at all.

The results also show a clear disparity between sectors. Companies in the finance and insurance sector (83%) and the energy and utilities sector (82%) audit their suppliers at least every two years. In contrast, the proportion of companies auditing supplier security is lowest in the retail and consumer goods sector at just 14 percent.

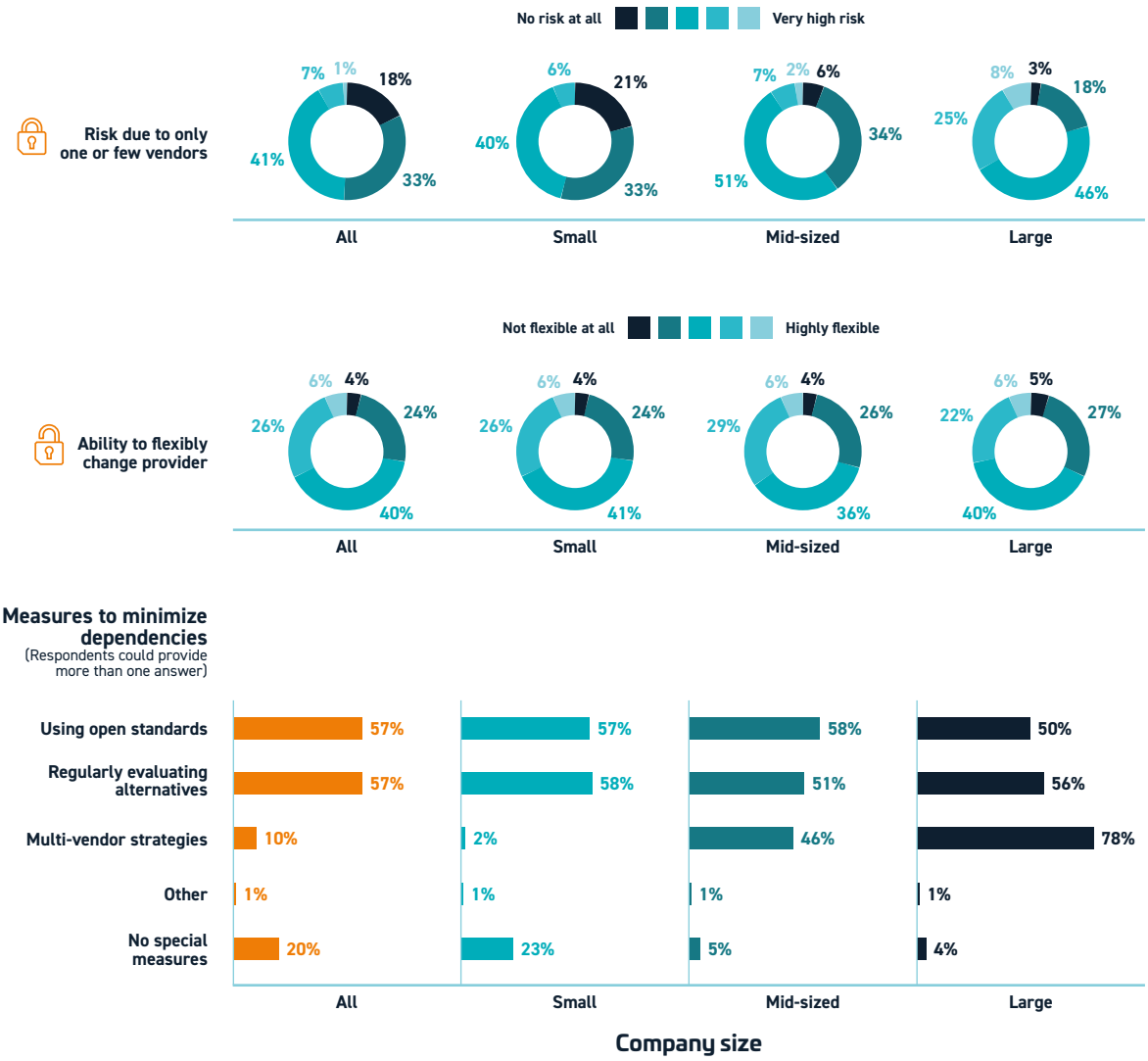
2.4 IT PROVIDER STRATEGIES AND THE THREAT POSED BY VENDOR LOCK-IN

Cybersecurity products are core components in every security strategy. They serve to ward off cyberattacks and boost digital resilience. Opting for the right provider, however, has far-reaching consequences. Vendor lock-in – becoming heavily dependent on a single provider – can limit flexibility, increase costs and make it difficult to adapt to new threats. This is especially challenging when it comes to cybersecurity. Incompatibility between providers and high switching costs make it difficult for companies to react quickly to new threats or integrate innovative solutions.

Our recent survey reveals a huge discrepancy between small and large companies with respect to their vendor strategies. While small companies rely almost exclusively on all-encompassing solutions from a single provider (93%), 88 percent of large companies use multiple providers. The larger the company, the less likely it is to be reliant on a single provider. Mid-sized companies are almost split down the middle – while 49 percent rely on a single provider, 50 percent make use of multiple providers.

The perception of the accompanying risks also differs significantly (see fig. 16). A mere 6 percent of small companies deem the reliance on one or very few products to represent a high risk, which is just below the average of 8 percent, while this figure is much higher at 33 percent when it comes to large companies.

To mitigate the risks posed by vendor lock-in, companies rely on a range of measures. More than 50 percent of the companies surveyed – regardless of their size – use open standards or regularly evaluate alternative providers. These are important measures to avoid being bound to one specific provider over the long term (see fig. 16).



Source: [255]

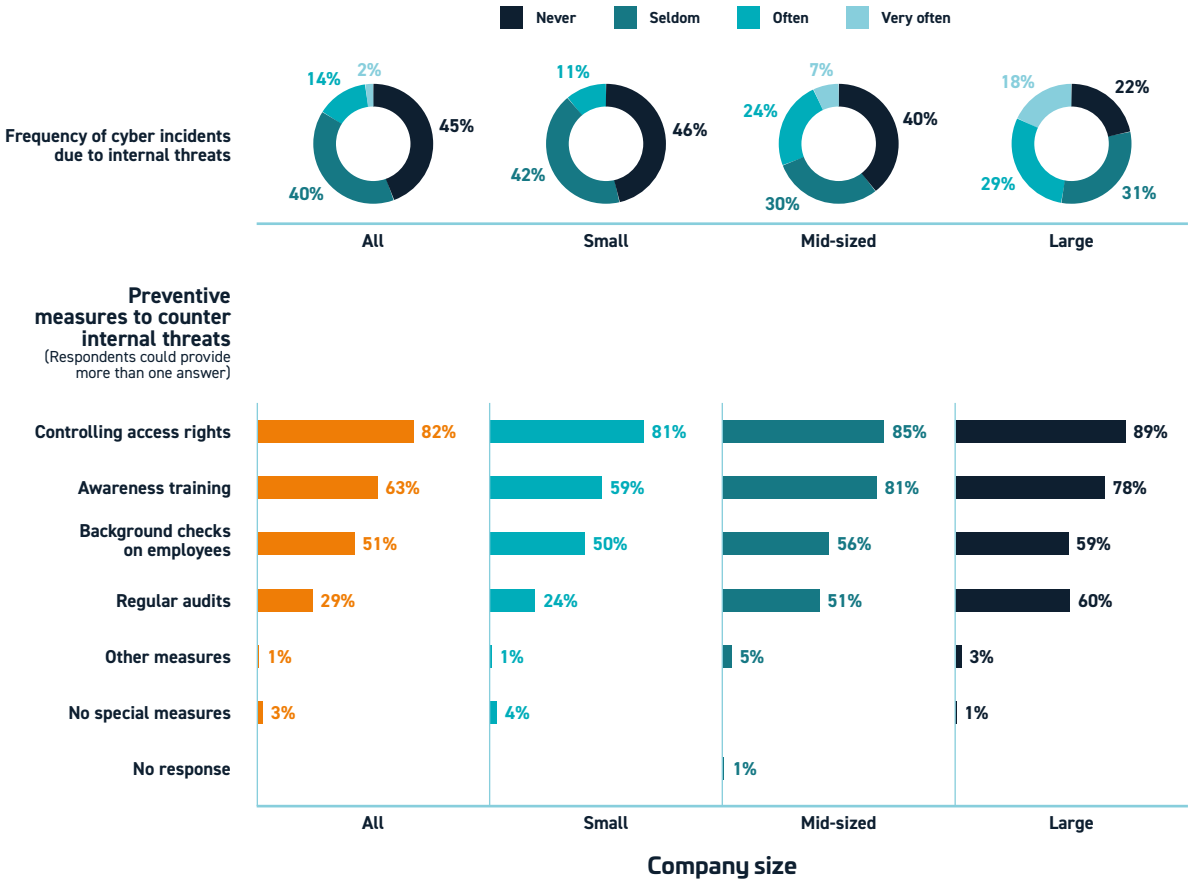
Figure 16: Vendor lock-in in the context of cybersecurity: Risk, flexibility and countermeasures (in %)

The security issues which surfaced at CrowdStrike in July 2024 demonstrated that companies pursuing a multi-vendor strategy were able to switch over to alternative systems more quickly, while those locked into highly dependent supplier relationships found themselves confronted with longer downtimes. However, actually implementing a multi-vendor strategy remains challenging. The survey shows that 78 percent of large companies are actively pursuing a multi-vendor strategy specifically to reduce dependencies. This not only means that they are using multiple providers, but also that their IT infrastructures have been purposefully set up to reduce dependencies. In smaller companies, this strategy is less common (2%), because managing multiple providers requires substantial human and financial resources.

Irrespective of the measures they have adopted, implementing a flexible supplier strategy remains challenging for many organizations. Only 32 percent of all companies consider themselves to be in a position to change their suppliers flexibly (see fig. 16). This indicates that merely using multiple providers or introducing open standards does not automatically lead to high levels of organizational adaptability.

2.5 INTERNAL RISK FACTORS

Internal threats pose a serious, often underestimated risk for companies of all sizes. Although they are often considered part of the generally accepted risk profile, they represent one of the most difficult challenges in the field of cybersecurity. Recent figures from Bitkom's Corporate Security Study paint a particularly alarming picture – 27 percent of all cyberattacks are the result of deliberate actions taken by (former) employees, while another 23 percent are caused unintentionally by cur-



Source: [255]

Figure 17: Frequency of cyber incidents due to internal threats over the past six months and preventive security measures (in %)

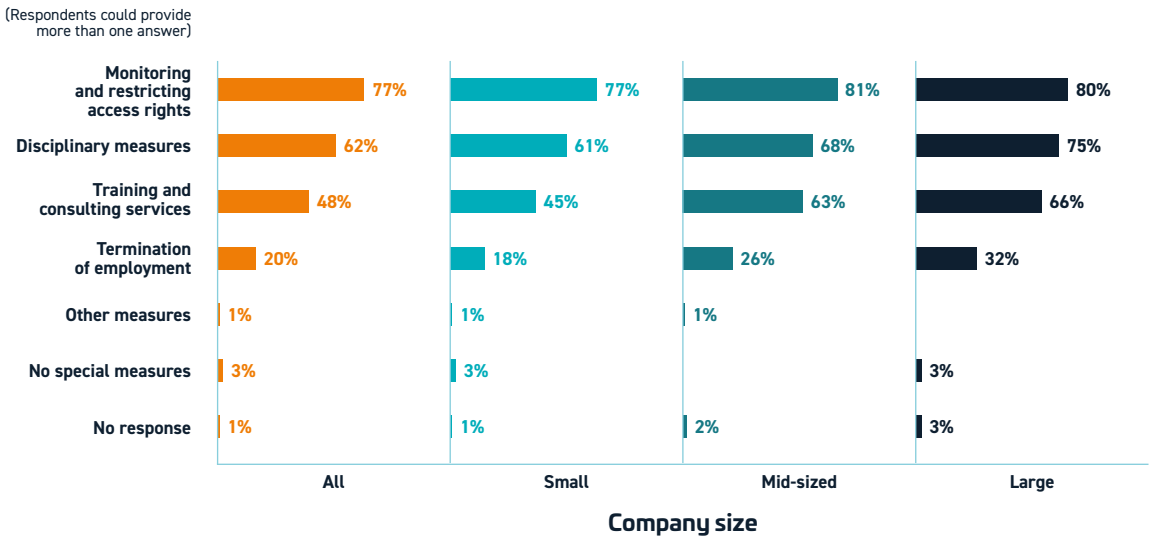
rent or former employees [30]. A look at international assessments reveals a difference in perception. In the WEF's Global Cybersecurity Outlook 2025, only 7 percent of the respondents cited malicious insiders as their biggest cybersecurity threat – when compared to other risks, this topic ranks low on the list of priorities worldwide [6].

The figures published in the Bitkom study are in line with the outcomes of our recent survey. While 45 percent of companies have not registered any internal threats in the last twelve months, 40 percent stated that they have experienced such incidents at least on rare occasions. Taking a closer look at the frequency of such threats by company size, a clear pattern emerges. Among small companies, 11 percent reported frequent incidents, while less than 1 percent reported very frequent incidents. In mid-sized companies, the proportion of frequent incidents rises to 24 percent and very frequent incidents to 7 percent. Large companies are at greatest risk, with 29 percent of them reporting frequent incidents and 18 percent very frequent incidents (see fig. 17).

This data indicates that as company size increases, so does the danger arising from internal threats. While the Bitkom study highlights the fundamental risk posed by internal actors, the current figures make it clear that large companies are especially exposed. Nevertheless, while smaller companies may indeed be less likely to be targeted in insider attacks, they are certainly not immune.

To overcome insider threats, companies primarily rely on technical measures to ensure the confidentiality, integrity and availability of sensitive data (see fig. 17). Controlling access rights is a particularly widespread approach, with 82 percent of respondents stating that they strictly monitor and restrict access to systems and data. Preventive measures, including background checks on employees, are also widespread at 51 percent.

When it comes to awareness training, the survey reveals clear disparities depending on company size. While 81 percent of mid-sized companies regularly carry out such training, only 78 percent of large companies and 59 percent of small companies conduct training to raise awareness. Despite the greater resources available to larger companies, their commitment in this area is no higher than that of mid-sized companies.



Source: [255]

Figure 18: How companies deal with employees who pose a potential internal threat (in %)

A comparable pattern is evident for the use of regular audits as a means of mitigating internal threats. The proportion of companies performing such audits increases in line with their size. Only 24 percent of small companies carry out such audits, while the percentage rises to 51 percent in mid-sized companies and 60 percent in large companies. This indicates that larger organizations rely more heavily on structured auditing mechanisms, while smaller companies implement such measures less frequently.

The majority of companies rate their IT infrastructures as good or very good with regard to internal threats. Sixty percent consider their level of security to be adequate. Disparities can be observed between companies of differing sizes. Around 58 percent of small companies rate their security measures positively, compared with 70 percent of mid-sized businesses and 86 percent of large enterprises.

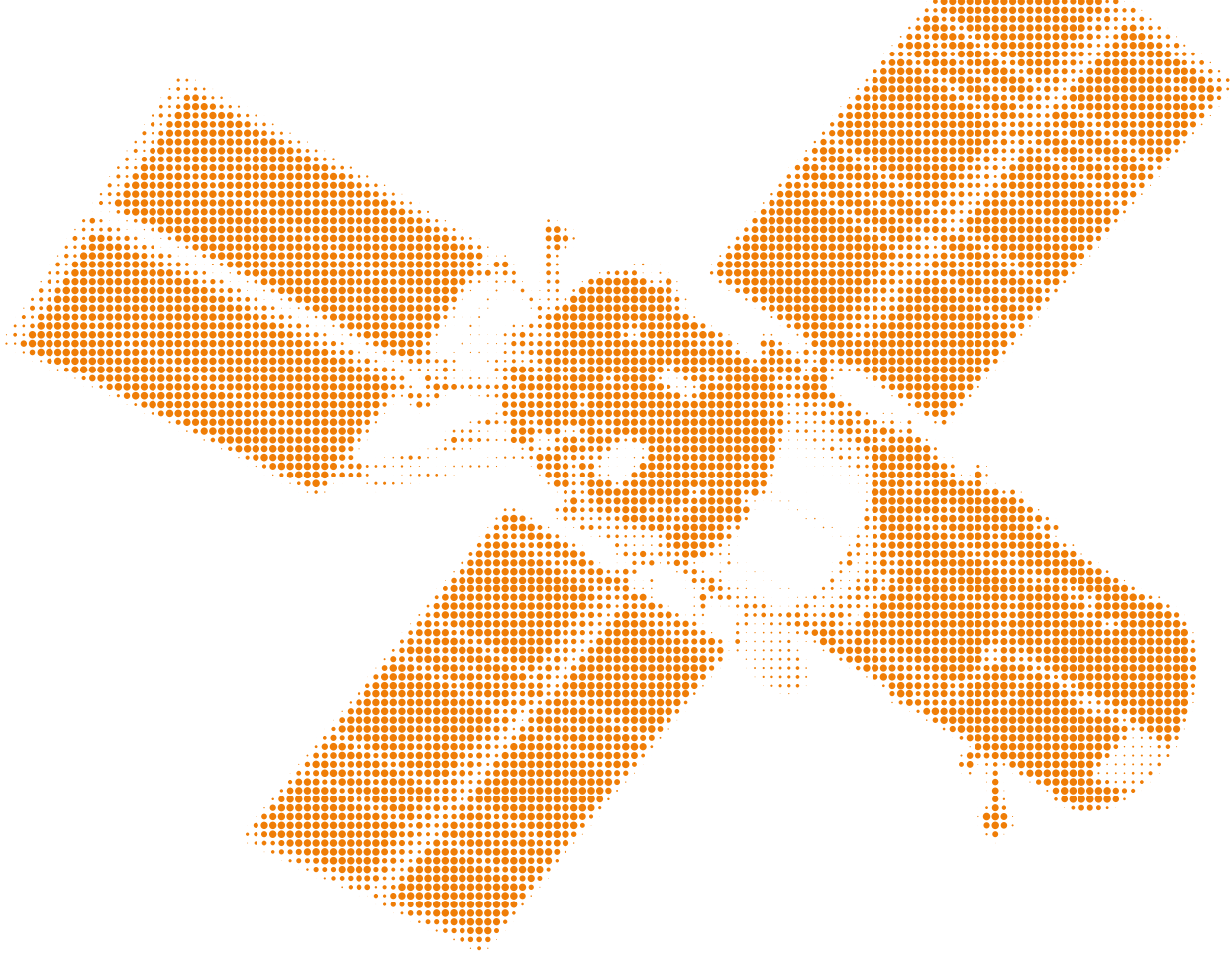
When it comes to dealing with employees who pose a potential internal threat, 77 percent of companies rely on monitoring and restricting access rights (see fig. 18). This approach is widespread across all company sizes. Of the companies surveyed, 77 percent of small companies, 81 percent of mid-sized companies and 86 percent of large companies reported adopting this approach. In this context, disciplinary measures are taken by 62 percent of companies, but they are more likely to be instituted by larger companies – 61 percent of small companies, 68 percent of mid-sized companies and 75 percent of large companies. In general, training and consulting services are employed less frequently. While 45 percent of small companies make use of them, the figure is 63 percent for mid-sized companies and 66 percent for large companies.

Significant differences were found with regard to dismissal practices. While only 18 percent of small companies opt to terminate employment, this figure rises to 26 percent for mid-sized companies and 32 percent for large companies. Larger companies, therefore, appear to be more resolute when it comes to dismissing potentially high-risk employees. This may indicate that closer personal ties and flatter hierarchies play a greater role in smaller structures and have an influence on how internal threats are dealt with.

2.6 CYBERSECURITY IN SPACE

Satellite communication is an indispensable building block of modern digital infrastructures. It enables global data transmission, navigation and communication – often going unnoticed, yet crucial for many industries. At the same time, there is a growing dependency on these technologies, which explains why they are increasingly targeted in cyberattacks. Nevertheless, the awareness of this risk remains low at many companies.

Our recent survey shows a clear discrepancy between the use of the technology and security awareness. Whereas 59 percent of those surveyed assessed the



risk of cyberattacks on satellites to be low or non-existent, a mere 13 percent recognized a growing threat. Small and mid-sized companies, in particular, underestimate the danger, with roughly 60 percent of them rating the risk as low. In contrast to this, larger companies have a greater awareness of the risk. In fact, 70 percent of them rate the threat "medium" to "high", with 5 percent even rating it "very high". This assessment is particularly prevalent in the energy and utilities sector, where 35 percent of companies rate the risk as "high".

The WEF Global Cybersecurity Outlook 2025 shows that also from a global perspective, satellite communication has hardly been considered a critical factor for security to date. Only 2 percent of the companies surveyed regard satellite technologies to be one of the key factors influencing the cybersecurity situation over the next twelve months [6].

In our recent study, this perception is directly reflected in the protective measures the organizations have taken. While 32 percent of large enterprises have implemented comprehensive security measures, only 7 percent of small and mid-sized companies reported having implemented comprehensive measures. The bigger the company, the more their investment is targeted specifically at safeguarding satellite communications. This trend is especially pronounced in the energy and utilities sector, where 67 percent of the companies have taken at least basic security precautions, while 12 percent have even introduced comprehensive security mechanisms.

It is worth noting that a third of the companies surveyed do not consider security in satellite communication to be a relevant issue. Yet satellite infrastructure is rapidly gaining in strategic importance. Advances in digital transformation and globalization are making satellite communication an indispensable component in corporate networks, supply chains and industrial processes. Companies which address the associated risks early are not only strengthening their own security strategies but also safeguarding their business operations over the long term.

2.7 CONCLUSION

The results of the surveys under review clearly show that the cybersecurity strategies pursued by companies depend largely on the size of the organization and the resources at their disposal. Large companies are better positioned in almost all areas relevant to corporate security. They have more substantial IT resources, rely more heavily on cloud hyperscalers and make targeted investments in cybersecurity, security operations centers (SOCs) and penetration testing. In addition, they audit their supply chains more frequently, are more likely to employ data protection officers and make more extensive use of external specialists, for instance when it comes to implementing regulatory requirements such as NIS 2. Another significant differentiator for large companies is their reduced dependency on just one provider. Adopting a multi-vendor strategy enables them to specifically reduce the risk posed by vendor lock-in.

In one area, however, there is hardly any difference between large and mid-sized companies. When it comes to combating internal threats from current or former employees, both groups rely on training, audits and disciplinary measures to a similar extent.

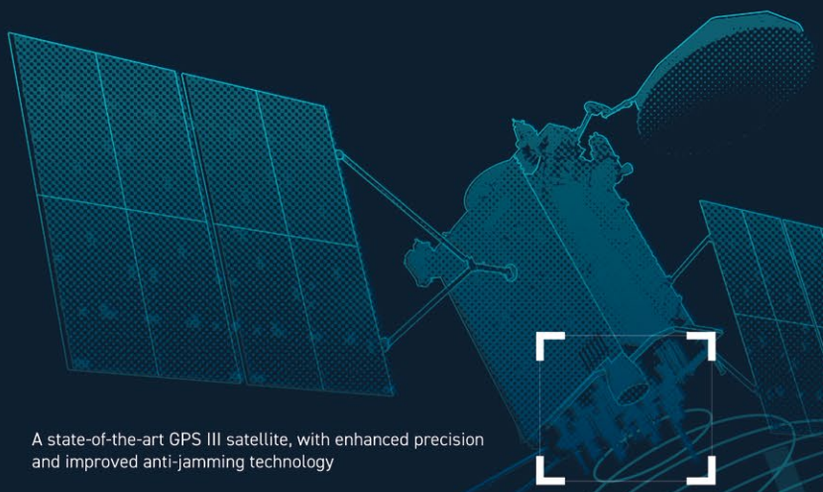
The fact that the retail and consumer goods sector is lagging behind other sectors is particularly evident. Companies in this sector often have fewer IT and cybersecurity resources at their disposal. They are also less likely to employ data protection officers or carry out penetration tests and supply chain audits. These gaps in corporate security increase exposure when it comes to cyberattacks and fulfilling regulatory requirements.

Critical infrastructure companies, on the other hand, are sending a more positive signal. Banks, insurance companies, companies in the healthcare, energy and utilities sectors are considerably better positioned than non-critical organizations. These organizations are making purposeful investments in cybersecurity and taking their social and economic responsibilities seriously.

Overall, a growing willingness to invest in IT security can be observed. Despite economic challenges, regulatory pressures and internal risks, companies are increasingly focusing on expanding and strengthening their security measures – an important step towards ensuring the long-term resilience of the German economy.

CHAPTER 3

GRAY ZONE THREATS
FROM SEA TO SATELLITE



A state-of-the-art GPS III satellite, with enhanced precision and improved anti-jamming technology

GEO
36,000 km

20,500 km

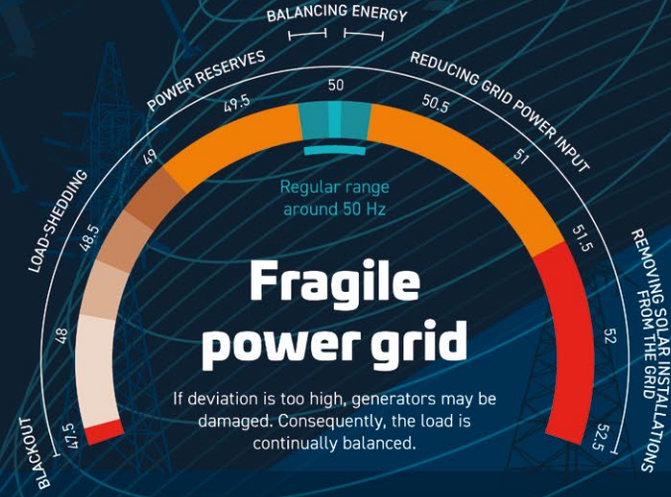
MEO

5,000 km

1,200 km

LEO

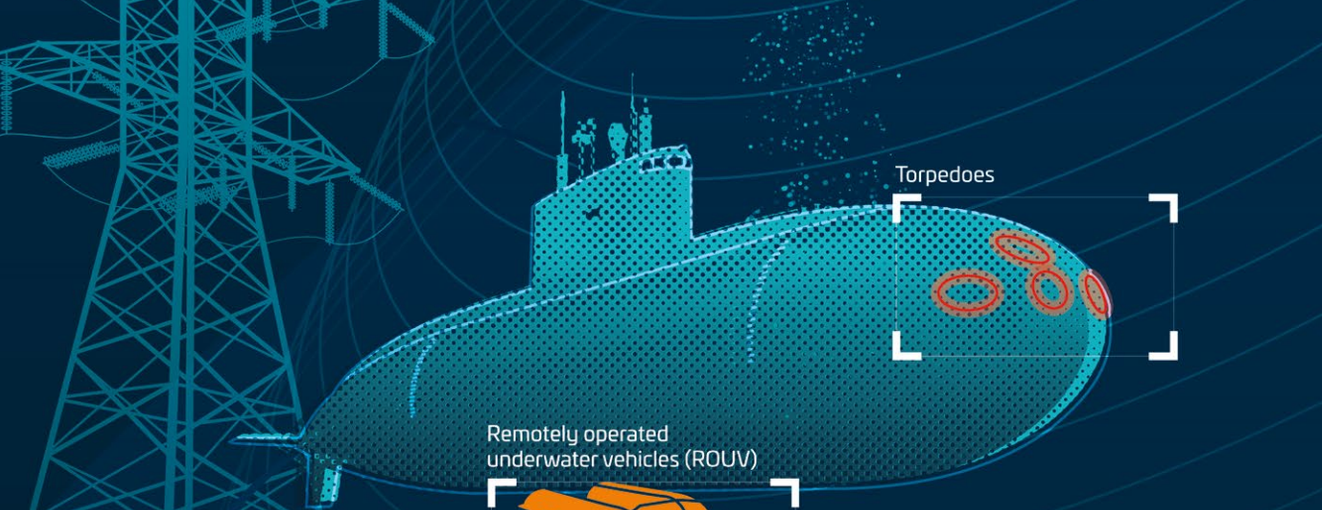
500 km

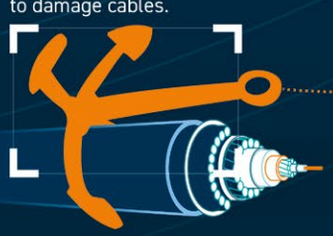


Fragile power grid

If deviation is too high, generators may be damaged. Consequently, the load is continually balanced.

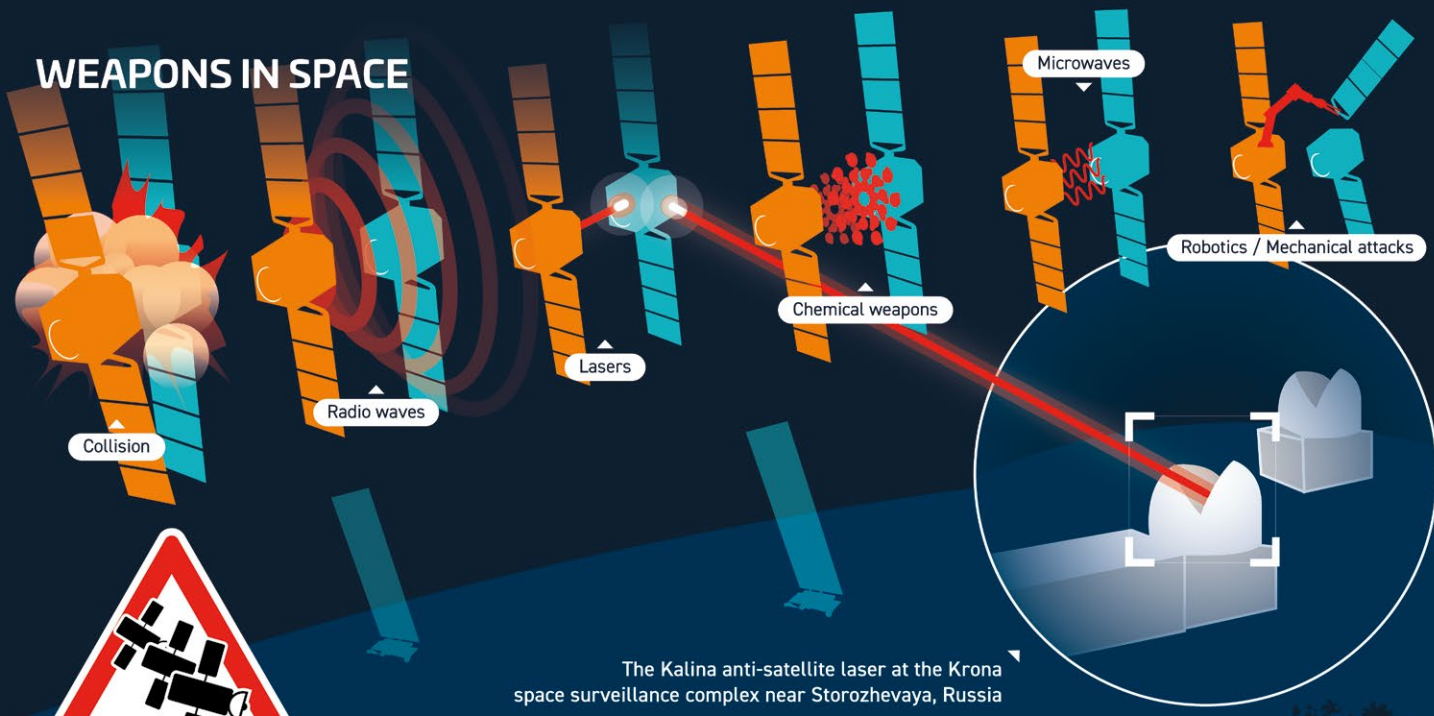
0 metres AMSL





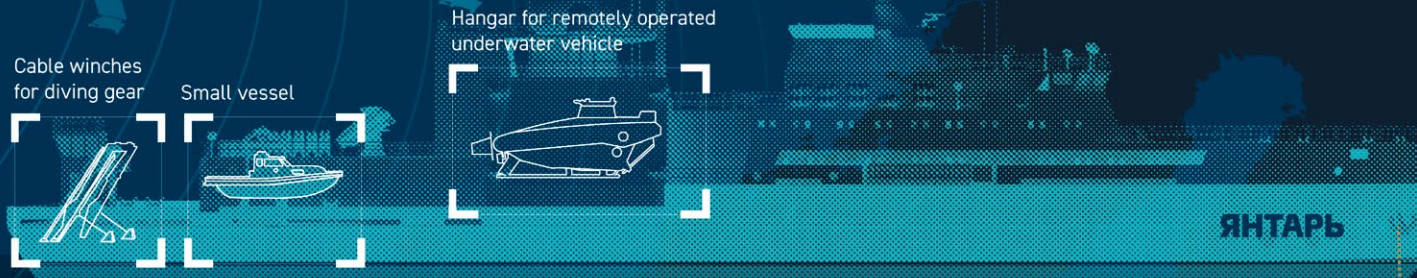
- 1,000 m

WEAPONS IN SPACE



The Kalina anti-satellite laser at the Krona space surveillance complex near Storozhevaya, Russia

In November 2024, more than 13,000 satellites were orbiting the Earth.



Submarine cables with connections to Germany

Atlantic Crossing 1	14,301 km
IOEMA	1,600 km
C-Lion1	1,172 km
Elektra-GlobalConnect 1	44 km
Fehmarn Bält	20 km
Germany-Denmark 3	n/a
GlobalConnect-KPN	43 km
Aurora	n/a

On December 25, 2024, the EstLink 2 submarine power cable between Finland and Estonia was allegedly damaged by the Russian tanker Eagle S.

On January 26, 2025, a data cable between Sweden and Latvia was damaged by the bulk cargo carrier Vezhen.

On February 15, 2022, the Fortuna lingered over an oil pipeline for about 12 hours.

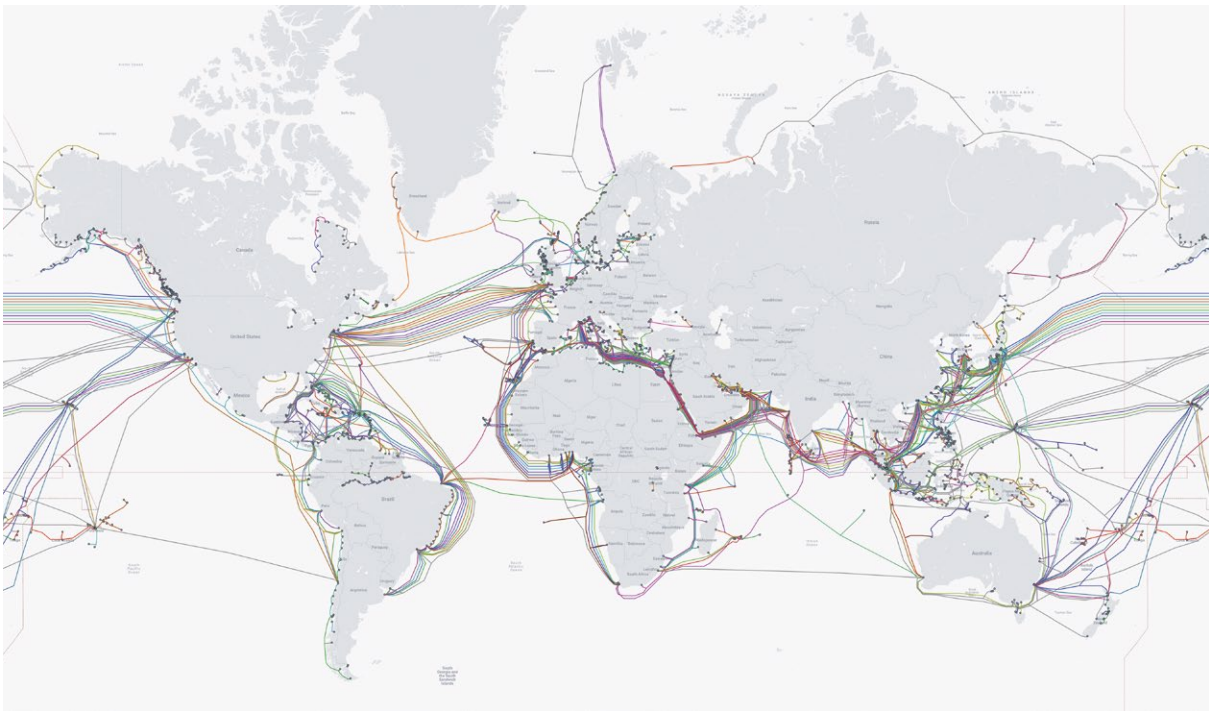
Sources: [86], [119], [155], [279], [286], [297], [305], [321], own diagram

3 GRAY ZONE THREATS – FROM SEA TO SATELLITE

Stretching through the surreal living conditions on the ocean's floor, the digital nervous system of the information age can be found. In a bid to keep pace with the growing demand for rapid transmission capacities around the globe, the number of active deep-sea fiber-optic communication cables is soon set to exceed 600 (see fig. 19).

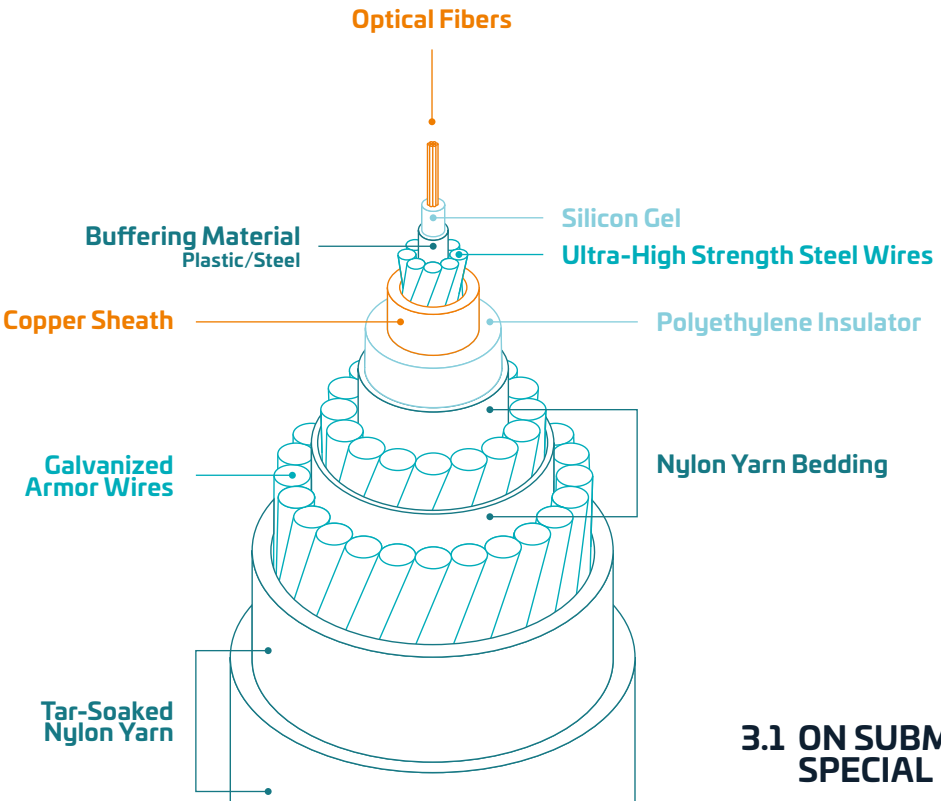
In 2024, an estimated 6 zettabytes of data were transmitted through cable-based networks and a further 1.3 zettabytes by way of mobile networks [150]. Just to visualize these dimensions – storing 6 zettabytes of data would fill 3 billion of our typical, widely used external hard drives with a capacity of 2 terabytes each. If this volume of data were to be printed out on paper, the resulting stack of pages would be around 6 trillion kilometers high, almost 40 times the distance from the earth to the sun. Already in 2016, the countless transactions and other business activities contained in these data streams were estimated to be worth as much as USD 10 trillion a day [104].

Even a brief failure of these connections immediately results in massive financial losses. If Facebook were to become unavailable for a period of six hours, for example, Meta would lose USD 100 million in advertising revenue. Scientific studies have revealed, moreover, that an increase of 1 percent in the probability of an Internet shutdown shows a statistically significant correlation with a decrease in the GDP of 15.6 percent per capita on average, and that every additional day without Internet availability costs USD 86.58 per individual [281].



Source: [290]

Figure 19: Submarine cables around the globe



Source: [291]

Figure 20: Submarine cable structure

3.1 ON SUBMARINE CABLES AND SPECIAL PURPOSE VESSELS

These fiber-optic communication cables span more than 1.5 million kilometers and make it possible, for instance, to access a website based in the USA from Germany within a mere 60 milliseconds. This powerful performance has not only enabled the Internet to develop into the backbone of our daily communication, but also to serve as the basis for global trade and finance. In addition, a growing amount of management and supervision activities, for instance regarding critical infrastructures (KRITIS), are running via the Internet.

Due to the rough conditions deep in the ocean, the submarine cables must be able to withstand extreme forces. The average depth of the Atlantic Ocean is 3,293 meters and the downward force of this water column amounts to nearly 330 kg per square centimeter. As submarine cables are typically not buried at such depths, but simply laid along the seabed, they also need to be equipped to handle impacts from seaquakes and seismic activities. The sensitive optical fibers are therefore protected within a multi-layer structure, which not only comprises steel wires for stability but also a copper sheath that serves to provide electricity to the submarine cable (see fig. 20).

It quickly becomes evident why a cable requires its own power supply. Undersea cables use special types of optical fibers, which have extremely low rates of signal attenuation, allowing them to span considerable distances. Even so, the roughly 5,500 kilometers between the east coast of the United States and Europe's Atlantic coast is still too great a distance. The longest submarine communications cable in active service is the SEA-ME-WE 3 (South-East Asia – Middle East – Western Europe 3) con-

nection, which has been active since 1999 and has a total length of 39,000 kilometers. To ensure reliable transmission of signals over such large distances, the signal needs to be amplified. For the earliest transatlantic fiber-optic cable TAT-8, which was in service from 1988 until 2002, photodiodes and semiconductor amplifiers were initially used. In 1996, however, the TAT-12/13 connections became the first to employ the principles of quantum mechanics. Doping the optical fibers with the rare earth mineral erbium allows the transported signal to be amplified using light by way of optical pumping. To provide power to these amplifiers, which are installed on average every 70 kilometers, the submarine cables are typically supplied with an operating voltage of 10,000 volts [182].

Although in principle such pumps can be operated without employing digital circuits, monitoring systems and microprocessors are required to continuously track performance and adjust the amplification – in order to keep the operating temperature within an optimal range and enable quick detection and location of disruptions such as connection errors.

Despite the remarkably robust structure of the cables, such disruptions occur frequently. However, the underlying causes are not predominantly natural. Analyses indicate that over 70 percent of these incidents related to underwater cables are both unintentional and of human origin. The most prevalent sources of these disruptions are trawling nets deployed from fishing vessels, anchors, and infrastructure-related activities, such as dredging operations in harbors. These activities collectively account for nearly 150 cable disruptions on average around the globe each year [67].

To best protect submarine cables from such accidents, their positions and paths are by no means kept secret. Instead, especially when cables are laid on the seabed without burial, the locations are purposefully made available to the public and shown, for instance, on nautical charts. Fishing nets are, nevertheless, responsible for 38 percent of all damage [291], while ship anchors account for one in four damaged cables. A further 11 percent of all incidents are caused by humans in other ways [302]. However, it is precisely this transparency that makes the cables more vulnerable to potential attackers, especially as the random nature of some incidents and the damage caused seems rather implausible – all the more so when such incidents have increased in frequency.

This was precisely the case at the end of last year. Already in October 2023, the Chinese container ship "Newnew Polar Bear", sailing under the flag of Hong Kong, had caused damage to the data cables between Sweden and Estonia (EE-S 1) and one of the Finland-Estonia connections, as well as the Balticconnector gas pipeline in the Baltic Sea. However, this was not an isolated incident, and many similar incidents have followed in recent times. On November 17, 2024, the BCS East-West Interlink data connection between Lithuania and Sweden was disrupted and just a few hours later, in the early morning hours of November 18, the C-Lion1 data link between Finland and Germany was also disrupted. The Chinese freighter "Yi Peng 3" was suspected to have caused the damage while operating on behalf of Russia. However, as the damage took place in international waters, the flag state China was responsible for conducting the investigation. The countries bordering the Baltic Sea could only look on as the investigation came to nothing.

An investigation into damage caused to another data cable between Finland and Sweden on December 3, 2024, was identified as an accident which occurred during construction work. On Christmas Day, however, the 650-megawatt Estlink 2 power cable was disrupted. Suspicions were soon confirmed that this may have been another deliberate act of sabotage. Reacting quickly, the Finnish authorities detained the suspected tanker "Eagle S", which is associated with the Russian shadow fleet, and launched an investigation into the incident. These disruptions are not limited to the Baltic Sea. On January 3, 2025, an important data cable belonging to the Trans-Pacific Express cable system, which connects Taiwan with the west coast of the United States, was damaged by the Chinese cargo ship "Shunxing 39". Although it is not easy to prove intent to cause sabotage in such cases, the Swedish Minister for Civil Defense pointed out with regard to the Yi Peng 3 investigation that you should definitely notice if you are dragging your anchor 150 kilometers behind your ship [194].

In addition, power cables are typically buried in the seabed, both to mitigate the risk of such accidents occurring and to comply with environmental regulations. To minimize the potential impact on marine flora and fauna, for example, the temperature increase at a depth of 20 centimeters below the seabed's surface is not allowed to exceed 2° Kelvin in the coastal areas of the North Sea. To achieve this, the cables must be laid at depths of at least 1 to 1.5 meters by means of jetting or ploughing to create trenches [40]. The 2Africa submarine cable is even set to be laid at a depth of up to 3 meters.

However, the dangers do not only come from anchors that are towed accidentally or deliberately. Russia has a range of specialized ships and submarines which have explicitly been designed to carry out reconnaissance and sabotage operations. In recent years, several of these vessels have repeatedly been observed spending hours or even days in the vicinity of wind farms or submarine cables, for instance the "Yantar". Transverse thrusters and special propulsion pods enable the ship to remain stationary above a specific position. It carries various mini-submarines and a range of remotely operated vehicles (ROVs) in its hangars. Among other capabilities, these underwater vehicles are equipped with gripper arms for working on the seabed and can presumably not only cut fiber optic cables but also insert tapping devices for eavesdropping purposes [280].

Moreover, this diving equipment does not need to be deployed from above the waterline. It is far less conspicuous and more difficult to detect if such operations are executed from specialized submarines. In this context, it is worth mentioning the 1910 Kashalot project, in which two submarines were built and put into service in 1986 and 1991 respectively and now form part of the Russian Ministry of Defense's central deep-sea research administration (GUGI). Using special thrusters, Kashalot submarines can hover close to the seabed and achieve exceptionally high maximum dive depths, estimated at 1,000 meters, due to their titanium hulls. By way of comparison, U.S. Navy submarines are presumed to have maximum operating depths of between 240 and 490 meters, depending on the class of vessel.

In total, GUGI operates more than 50 ships and submarines, which can be deployed in reconnaissance and sabotage operations on the ocean floor.

In light of the growing number of incidents in the Baltic Sea region, NATO launched the "Baltic Sentry" operation in January 2025, aiming to deter further operations against critical infrastructure in the Baltic Sea through the deployment of frigates, surveillance aircraft and maritime drones [210]. Additionally, the HEIST (Hybrid space-submarine architecture Ensuring InfoSec of Telecommunications) project was initiated. The project aims to locate damage to submarine cables to within an accuracy of 1 meter in a very short space of time and immediately reroute data traffic in the event of an incident [101].

In future, these dependencies will continue to grow, for instance through projects such as the planned "Greece-Egypt Electrical Interconnection" (GREGY Interconnector), which will have a capacity of 9.5 gigawatts and transport 75 percent of the electricity generated in Egyptian wind farms to Greece and Europe from 2031 [75]. Various other offshore wind farms and links are currently being planned. Consequently, sabotage capacities such as those possessed by the Kashalot boats increase the risk of hybrid activities, which can be disguised as accidents and are often difficult to attribute [39]. Thus far, it has been possible to compensate for the damage through the redundancy of global data connections. The incidents involving power cables also had no major impact due to the comprehensive networking of the European Interconnected System (EV). By way of 39 transmission network operators, the EV supplies electricity to almost 600 million people accustomed to high levels of grid stability.

3.2 MODERN ARTERIES: THE EUROPEAN INTERCONNECTED SYSTEM

The scenario of a wide-ranging power outage lasting several days no longer belongs to the world of fiction. Shorter, smaller-scale power and Internet outages occur

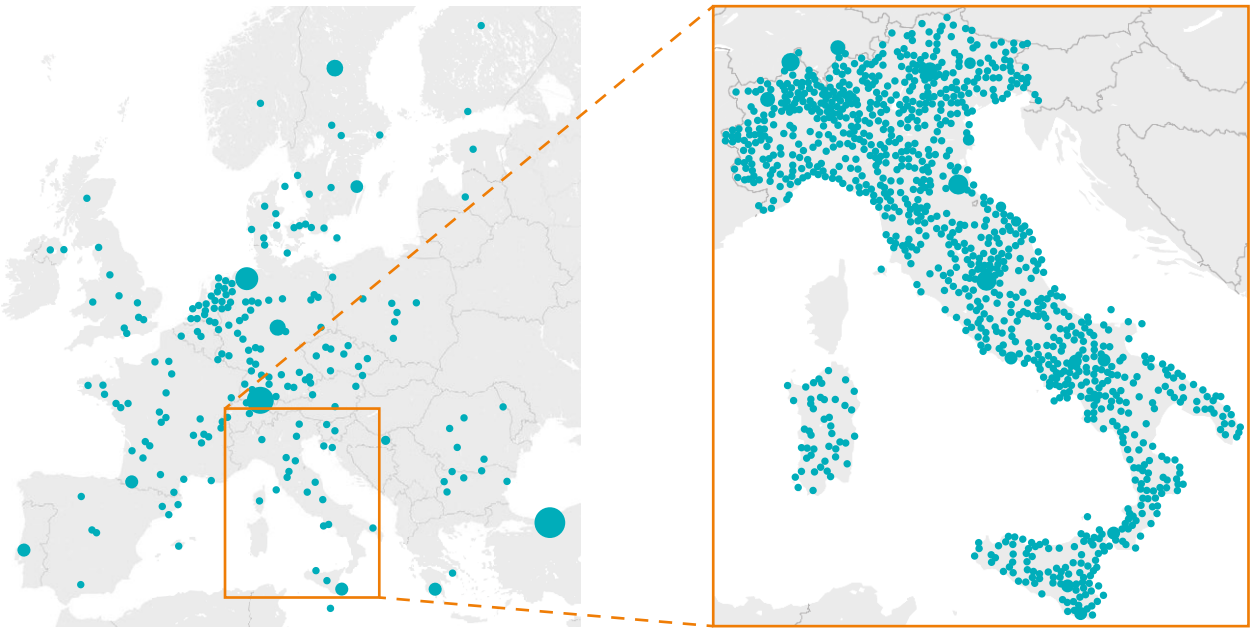
time and again. Most commonly they are caused by environmental influences, cascading effects due to technical faults or human error (see fig. 21). Widespread outages, however, such as the one which resulted in a total blackout in Southeastern Europe on June 21, 2024, impacting Albania, Bosnia and Herzegovina, Montenegro and Croatia, are still the exception.

Repairing damaged submarine cables can take months. The EV operates with N+1 redundancy, which means that even if one of its components fails it remains functional – the same applies to power lines.

However, in the event of lines failing for extended periods of time, the network operators have fewer options for ensuring N+1 redundancy. This could increase the risk that (additional) outages which are deliberately induced locally, may result in wide-ranging effects. So, should the increased frequency of incidents over the past few months be seen as a systematic testing of the impact on and resilience of the respective networks, in addition to the reactions, processes and speed of response of Western nations? In any case, it is crucial to be prepared.

In doing so, it is important to bear in mind that supplying the power which lays the foundations for almost all areas of our modern society relies on an extremely complex system, which constantly needs to be monitored and balanced.

Due to climate change and the new, constantly evolving and adjusting mix of power generation, the interconnected systems are increasingly operating under critical conditions [269]. The infrastructure is not yet sufficiently



Source: [269]

Figure 21: Analysis of blackouts across the whole of Europe and locally in Italy

prepared for the continued transition to renewable power generation in all countries [139]. This gives rise to new cyber risks, which may not immediately be apparent.

To ensure the power supply continues to function in a stable way, the generation and consumption of electricity must constantly remain evenly balanced. One indicator showing whether too much or too little electricity is being generated or consumed, is the grid frequency. The European power grid is based on alternating current (AC) with a network frequency of 50 hertz. When more electricity is consumed than produced, the frequency rises. When too little power is generated, the frequency falls. An excessive deviation in grid frequency may result in damage to generators, so it needs to be adjusted continually.

When the frequency drops, the power utilities first activate reserves to cover the additional demand. If this is not sufficient to cover the shortfall, load shedding takes place – individual districts are disconnected from the power grid in a controlled manner. Should this still prove insufficient, at frequencies of less than 47.5 hertz the power plants are then disconnected from the grid to prevent them from being damaged and a blackout ensues. Conversely, when the frequency rises beyond 50 hertz, electricity production has to be scaled back. However, this cannot be achieved abruptly for large power plants and may take several minutes.

Photovoltaic systems (PV systems) are easier to manage, which is why systems built up to 2012 stop feeding into the grid abruptly from a frequency of 50.2 hertz. As photovoltaics have now been adopted very extensively – a total capacity of 328 gigawatts is expected in Europe by 2025 – the sudden removal or absence of these systems could have resulted in an undersupply and risked causing a blackout. To counteract this risk, newer systems therefore initially throttle the feed and only switch off at 51.5 hertz.

As frequency fluctuations are constantly occurring in the electricity grid, they also have to be balanced out continuously. This can be done, for example, by using the rotational energy provided by the flywheel mass in a power plant generator, which acts as an instantaneous power reserve. As renewable energy sources do not provide this instantaneous reserve, stability increasingly needs to be ensured by way of intelligent systems, power electronics and battery storage. This is a complex system which crucially requires a high level of cybersecurity. However, in contrast to electricity grid and power plant operators, private PV systems are hardly subject to any regulations.

This has a direct impact on cybersecurity. As in many other areas, intensive competition over the years has led to the outsourcing of production facilities and supply chains. For example, Beijing's "Made in China 2025" (MIC2025) initiative, launched in 2015, and huge subsidies worth billions of US dollars have enabled China to build extensive capacities and achieve a dominant position in the PV market. Currently, 85 percent of all PV modules are manufactured in China.

3.3 DEPENDENCIES WITHOUT BORDERS

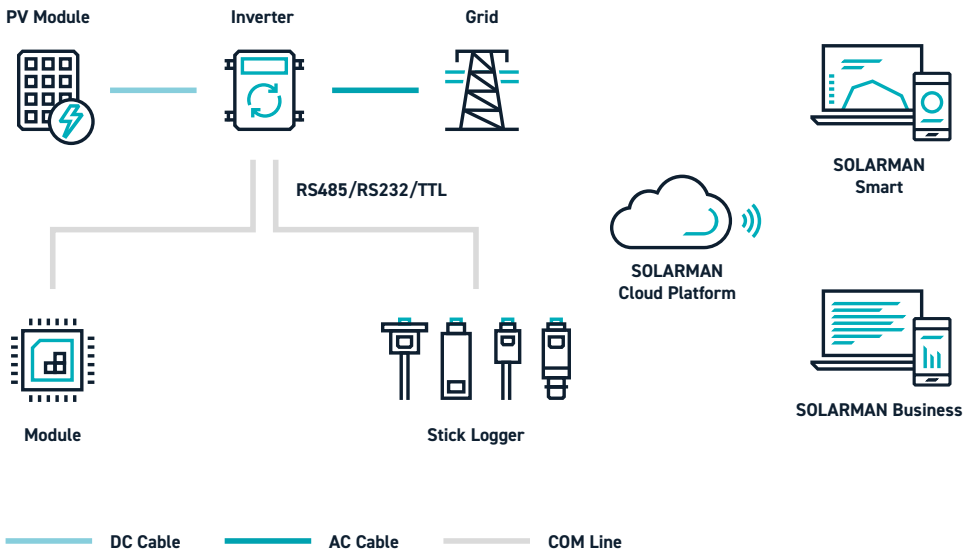
Time to market and price advantage are often the decisive factors on the market. As a result, cybersecurity suffers. This has been identified as a problem when it comes to the inverters which convert the direct current generated by PV modules into the alternating current needed for the local power grids (see fig. 22). For example, significant vulnerabilities were identified in the PV monitoring platforms offered by Solarman and Deye, which an attacker could exploit to manipulate the inverter settings [173]. By way of a calculated, coordinated attack on a large number of affected systems, a blackout could have been triggered.

While in this case the vulnerabilities were reported and patches made available in time to prevent an attack, an incident in Japan saw attackers take over 800 PV systems by exploiting a known vulnerability. These hijacked systems were then used to spread the Mirai botnet. While the intention was not to attack the electricity grid in this case, it could also easily have been the aim [37].

However, the threat does not only emanate from vulnerabilities in the inverters. That is why you cannot simply rest assured if your own PV systems are set up not to be accessible from the Internet due to their configuration or firewalls. A lot of the PV systems installed nowadays are monitored and managed by way of cloud services – many of which are running in Chinese data centers. The total capacity of electricity which is effectively controlled by external means amounts to many gigawatts, far exceeding the emergency capacity of the European Interconnected System. By controlling these cloud services, an attacker would be able to instigate a blackout without requiring any submarines or cable cutters.

This is by no means an isolated scenario. Decades of optimizing costs and efficiency by outsourcing and offshoring production facilities and supply chains have had an impact on all areas of IT. The issue is more than just the levels of security, which are often negligible, or the fact that the clouds are operated from China. Rather, it is the risk that a strategically minded actor may have an opportunity to exert considerable influence over cyberspace by presciently placing persistent backdoors in the systems of future parties to a conflict.

Even though few examples of hardware manipulation have been documented, and all cases have been vehemently denied by all parties involved, the potential harm and danger are undeniable. In the case of the Microsemi ProASIC3 Chips, the discussion regarding whether an undocumented function allowing access to the whole chip is a feature to support debugging or actually a hidden backdoor illustrates the challenges in this area. On the one hand, it is extremely difficult to prove this kind of tampering and, on the other, backdoors which have been skillfully installed can be credibly repudiated. The opportunities presented by complex, dispersed global supply chains have further exacerbated the situation, which became strikingly clear with the explosion of Hezbollah's manipulated pagers and walkie-talkies.



Source: [173]

Figure 22: Photovoltaic systems with vulnerabilities can pose a risk to the stability of power grids

Consequently, it is easy to understand the efforts of many countries to increase their own production capacities, tighten up the security along their supply chains and reduce dependencies. To reverse the trend towards a sharp fall in domestic production capabilities and against this backdrop of a growing impact on security, the White House passed the "Creating Helpful Incentives to Produce Semiconductors for America Act" (CHIPS for America Act) in 2022. The legislative package makes USD 52 billion available as funding for domestic semiconductor production – covering everything from research and development to the security of the associated supply chains. In the meanwhile, the program has led to the investment of nearly USD 400 billion into several dozen companies. Hence, among other outcomes, 73 new semiconductor plants are currently being built or existing ones expanded. In this manner, the US is aiming to increase its share of production back up to 30 percent of global market capacity by 2032, having fallen to below 10 percent at the present time.

Europe is finding it much more difficult to advance its role in semiconductor production. This is not solely due to raising the tens of billions of euros a modern plant costs or finding the skilled labor required to operate it. The challenge lies more in the wider ecosystem, where fewer of the basic preconditions are available than, for example, in the United States. This may be one of the reasons why the EU Chips Act, which at EUR 43 billion at least comes close to the CHIPS for America Act, has not yet succeeded in generating similar momentum. As a result, it remains to be seen whether the EU's target of 20 percent of global market share by 2030 can be achieved.

However, this is not the only area in which Europe needs to catch up. Instead, the greatest damage and most difficult challenges will initially continue to be caused by cybercrime and the rapidly evolving ecosystem of professional attacker groups (advanced persistent threats, APTs).

3.4 GROWING SOPHISTICATION OF ATTACKERS

The growing complexity of today's global IT systems and networks harbors many risks. For example, the threat actor group Salt Typhoon (APT-40), which is associated with the Chinese state, made headlines at the end of 2024 when it succeeded in penetrating deep into the networks of several US telecommunications providers and managed to eavesdrop on conversations held by Donald Trump and other political figures. Contrary to initial assumptions that the attacks targeted systems that had been specially installed by US authorities for eavesdropping purposes (known as "lawful interception") after obtaining the required court orders, the operation was discovered to have been much broader in scope and had been running for many months or even years.

It is particularly worrying that even once the assailants had been detected, it was still not possible to remove them from the networks completely and, even more seriously, the precise status of the ongoing security breaches could not be determined. The incident even resulted in the US authorities, which usually adopt a rather skeptical stance on encryption, issuing recommendations for communications to be secured using end-to-end encryption [81]. In any case, the scale of the exposure appears immense. The stolen metadata could, for instance, help China to identify key figures in politics and industry.

However, even if the recorded conversations and video teleconferences (VTCs) contained no confidential or explosive content, the incident has raised concerns about the creation of deepfakes based on them by generative artificial intelligence (GenAI). Due to the rapid development of this technology, it is increasingly difficult to differentiate between real and fake communication, even with the support of machines and good training data.

Although the incidents reported thus far have "only" affected the United States, the wording of a warning issued by the powerful Five Eyes Alliance (FVEY), which comprises the intelligence services of Australia, Canada, New Zealand, the United Kingdom and the United States, underscores the severity of the incident. Although the

United Kingdom was not party to the joint warning issued by the other four members, the nebulous wording used by Australian intelligence indicates that it was most probably not only systems in the USA that were hit.

This would hardly be surprising, as the number of manufacturers of such equipment is limited. In addition, the globally active telecommunications service providers tend to operate their networks and systems in different countries with very similar structures. If countries one would expect to be in the focus of Chinese intelligence have not actually been impacted by such massive espionage operations, this is more likely due to capacity limitations on the part of the attackers. Given the suitability of AI in such operations, however, and especially China's considerable resources for such activities these days, such considerations are likely to be of secondary importance.

Besides extensive state and state-affiliated actors, there is a thriving industry offering hacking and entire cyber operations as a service. The i-Soon leaks provided important insights in this regard. In early 2024, a comprehensive set of documents originating from the Chinese cybersecurity company was published by an anonymous source. The presentations and lists of bookable cyber operations included in the leak reveal how the company cooperated with Chinese intelligence services and institutions on a commercial level [55].

Considering the wide-ranging activities of cyber groups active on both sides of the Ukraine war, it is highly likely that some states will increasingly resort to leveraging these types of services when carrying out illegal or gray zone operations, as they allow them to deny responsibility or avoid being identified as the source of the attack. The challenges to cyber defense associated with the growing professionalism and privatization of cyber operations can already be illustrated with concrete examples, as taking a closer look at operational relay box (ORB) networks and protection mechanisms such as firewalls shows.

3.5 PLAYING CAT AND MOUSE

The use of ORBs grants attackers significantly more options for covering their tracks. Thus far attackers have especially relied on proxy servers, which only forward data traffic using their own IP address (pseudonymization), and virtual private networks (VPNs). In both cases, an observer does not see the address of the actual originator of a connection, but only that of the intermediary service. However, as all the necessary information is available on the proxy servers or VPN nodes, access to the server in question is all that is needed to identify a user.

True anonymization can be achieved by way of "The Onion Router" (TOR). Using additional, but very easy-to-use software, data traffic can be encrypted in multiple layers and forwarded via several instances. Each node in the connection only knows the previous and next system in the chain. The actual message is analogous to postal ballot documents which have been enclosed within several (encrypted) envelopes. Each node is only able to open one of these envelopes and then forwards the remainder to the next instance. Thus, nobody in the chain apart from the sender has information about both the originator and the end destination of the communication (see fig. 23).

There are, however, safeguards against both pseudonymization and true anonymization of sender addresses. Numerous websites list the proxy servers available worldwide. These are updated almost on a minute-by-minute basis to allow the addresses in question to be blocked.

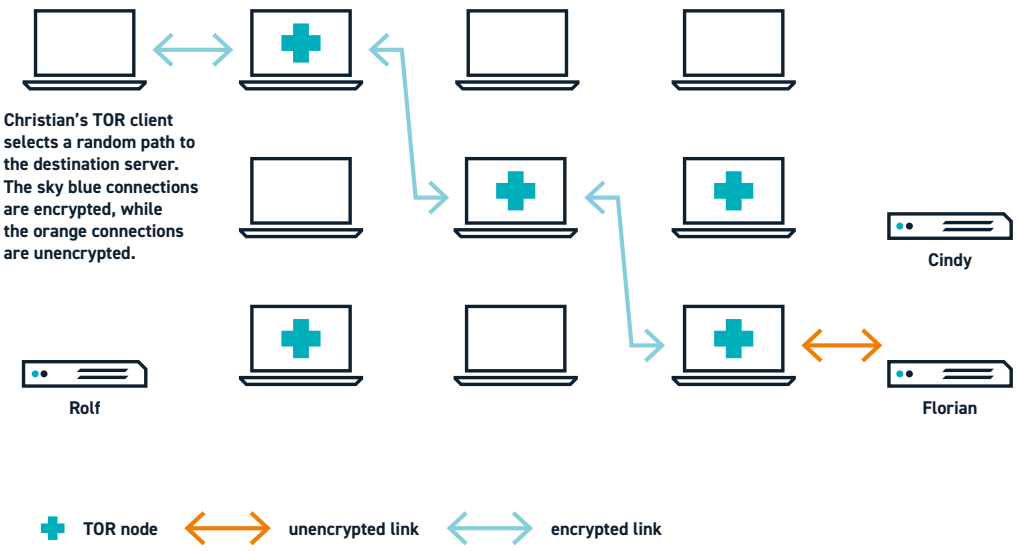
The TOR network can also be repelled effectively. The number of "exit nodes", i.e. computers providing their IP addresses so that data traffic can be forwarded to the Internet in their names, is very limited and has hardly increased over many years. This is hardly surprising in the light of legal considerations and the liability laws in the various countries. After a long time in which there were around 1,000 of these computers, the number has meanwhile levelled off at roughly 2,300 nodes – a short, easily processed list in the digital era. Measured against the 30 billion network devices currently in use, the number of TOR exit nodes is truly negligible.

As the address details of the computers in the TOR network are freely available for functional purposes, an up-to-date list is always available, which makes it easy to block the TOR nodes. When it comes to proxy servers, the possible address ranges are significantly more dynamic, and the array of potential IP addresses is much greater. Nevertheless, creating and maintaining deny lists to block the relevant communication partners is basically not much more complex.

To cover their tracks, professional assailants need inconspicuous IP addresses, which cannot be traced, are not already blocked, and cannot easily be deterred by automated means. This is where ORBs come into play.

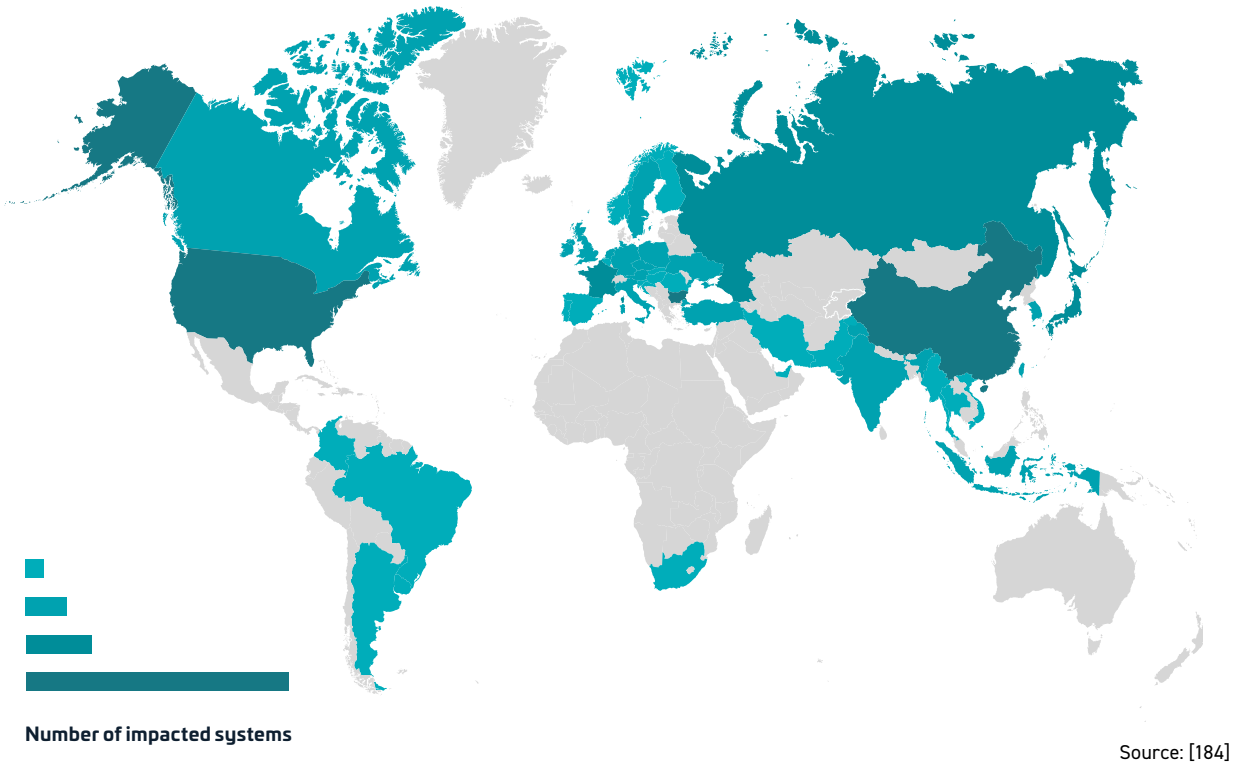
An ORB is part of a network set up to forward data traffic on the Internet. As opposed to proxy servers or participants in TOR networks, in the case of an ORB the data is transferred unknown to the owner of the respective device. To achieve this, attackers gain control over poorly secured IoT systems, home routers and Wi-Fi devices in private households or companies and add them to the ORB networks. Even though the security situation has improved somewhat with regard to home routers and similar systems over the past few years, vulnerabilities and poor patch management are still widespread and pre-installed backdoors have shed a very negative light on some manufacturers. However, once truly professional adversaries have gained access, they do not stop there. If possible, they will close the vulnerability behind them, to shut out other attackers.

ORBs are hardly new. As early as 2013, the Snowden documents revealed that the FVEY alliance was identifying vulnerable computers on an annual basis, taking them over and organizing them into a network. What has changed in recent times, however, are the dimensions, speed and barriers to entry. Previously only available to a few powerful intelligence services, the use of ORBs can now be procured for relatively little money in the cyber-



Source: [292]

Figure 23: How TOR works



Source: [184]

Figure 24: Overview of the distribution of IP addresses in an ORB network

crime as a service economy (CaaS). The updating of the members in an ORB network has long since ceased to follow an annual rhythm and is now based on demand. Cyber operations launched from China are increasingly relying on these commercial ORB networks (see fig. 24). Considering that their nodes are sometimes active for less than 31 days, it can be more difficult to defend against attacks conducted via such ORBs, as they may not be found on any lists.

As far as detection is concerned, this means that IP addresses are playing a diminishing role as a means of identifying attackers or the sources of malicious activities, while losing even more value as an indicator of compromise (IOC).

This situation is exacerbated further when ORB operators no longer even have to search for and take control of vulnerable devices but can use services that have already been installed by shady companies. A manufacturer of firmware for smartphones, i.e. programs embedded deep in the system that facilitate communication and control between the operating system and built-in hardware components, was found to have integrated additional, undocumented functionalities. This included a hidden proxy access, which the provider rented out in the form of an opportunity to access the device for 15 minutes. The affected smartphones were then used to forward data traffic for third parties from their own IP addresses without their owners being aware. The motivation of the manufacturer was to bolster the dwindling revenue from the sale of hardware, which had become unprofitable, by creating a new source of income. Even though only a relatively small number of smartphone owners in Asia were affected, the case underscores the risks posed by global IT supply chains.

3.6 EVERYDAY "CYBERWAR"

Even if a device is sourced from a trustworthy manufacturer and the supply chain has been checked and controlled, it is important to remain vigilant. Attackers are especially interested in security components such as firewalls or systems designed to detect intrusion, as gaining control over such systems means they can easily penetrate the networks beyond. In the past few months, this has included attacks on firewalls manufactured by Fortinet, Palo Alto Networks, Zyxel, SonicWall and Cisco.

British cybersecurity experts Sophos recently provided impressive insight into how intensively cyber operations are now being carried out. Over a period of five years, the firewalls provided by the company came under attack from Chinese assailants in Operation Pacific Rim [186]. What began with infiltration and spying on a branch office in India, soon resulted in the mass infection of tens of thousands of firewalls around the globe, which were then made available as components in ORB networks. This was followed by numerous targeted, well concealed attacks on organizations including nuclear energy providers, military facilities, telecommunications providers, intelligence services and the airport in an unspecified capital city.

Source: [288]

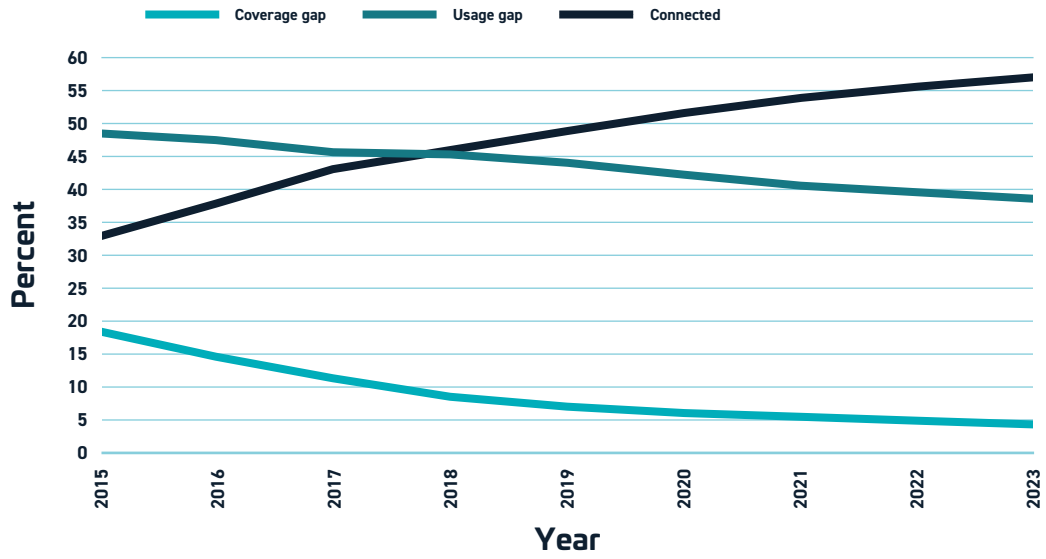
Figure 25: New opportunities offered by 5G in the agriculture sector

The persistence of the attackers prompted Sophos to launch an elaborate operation to track down the firewalls on which the attacks had initially been developed and tested. Sophos then inserted implants into the devices in order to observe the intruders' actions. Finally, Sophos gained access to the malware under development. In this way, the operation which had been running for years could be traced back to a specific network of security researchers in Chengdu, China. The detailed report issued by Sophos warns of cyber actors adopting an increasingly aggressive and creative approach, while also emphasizing that hardware and software manufacturers have a responsibility to be transparent. Many manufacturing companies remain shrouded in silence in the wake of serious security incidents. Especially when it comes to cybersecurity products, this can have drastic consequences for their customers.

Though already substantial, we may well still see a massive increase in the attack surface due to new services and a plethora of other systems, particularly in the area of IoT. The rapid pace of technological development is constantly opening up new opportunities that could fundamentally transform entire aspects of our lives. In many areas, we are far from exhausting the potential for optimization which needs to be achieved in the face of challenges such as climate change and the importance of reducing carbon footprints. In the field of logistics, for instance, significant savings can be achieved by optimizing routes and using predictive maintenance, in which maintenance is not carried out routinely but only when a need is identified. While such approaches are not new, already having been in use since the 1990s, the IoT leverages a multitude of new sensors and AI-supported analysis of the extensive data generated (big data) to facilitate unprecedented accuracy, deep system insights and countless new use cases.

3.7 DEVELOPING THE IT LANDSCAPE

The agriculture sector, in which digitalization offers considerable potential for optimization, represents a good example of these developments (for new opportunities offered by 5G in the agriculture sector see fig. 25). The data obtained through all-encompassing IoT sensor technology can assist in the continuous analysis of soil conditions and weather developments, while also monitoring the health of plants. Based on this, it is possible to ensure the optimal supply of water, fertilizers and pesticides. These, in turn, are only used in the absolutely necessary quantity and with a minimum of human labor, thanks to the precise navigation and controlling of the most appropriate machinery. Agricultural machinery giant John Deere, for example, has introduced a technology called ExactShot, in which a sensor registers exactly when each individual seed is placed in the soil, after which a small amount of fertilizer is sprayed directly onto the seed rather than fertilizing the entire terrain. With wide-ranging deployment, this could save 352 million liters of fertilizer per year in the United States alone [84].



Source: [123]

Figure 26: Development of coverage and usage of cellular networks

Equipped with the necessary sensors and backed up with the required data analysis, in addition to reducing fertilizer and water volumes, harvests can be initiated at the best possible time and plant diseases detected at an early stage. The interplay between the soil sensors, drones and automated machinery, along with their connectivity, plays a fundamental role. The downside of these developments is that manufacturers are constantly trying to secure and expand their market positions, for example by restricting interoperability (known as vendor lock-in) or blocking access to functions and the inner workings of their systems. John Deere, for instance, has come under fire for practices preventing third party workshops from being able to carry out repairs, for instance by using proprietary fault codes and coupling machine parts to the tractor's vehicle identification number (VIN). Having remote access at all times, also allows the manufacturer to take measures such as disabling the system. This is likely to have occurred with the machines stolen by the attackers during the Russian occupation of Melitopol in early 2022 [179]. While this particular example may be seen in a positive light, secure implementation of such functionalities and the ways of accessing them is indeed of critical importance. As far back as 2010, media reports emerged of an incident in which a hacker had managed to disable a fleet of more than 100 vehicles by hacking into a system actually only intended to prevent the use of vehicles in the event of late payment [235]. In this context, it is also worth remembering Volkswagen's data breach in the AWS Cloud, which made it possible to generate precise user profiles including their movement behavior for over 600,000 customers with vehicles [169].

3.8 CONNECTIVITY IS AN ESSENTIAL PREREQUISITE

Bringing these new application fields to life first of all requires dependable, wide-ranging availability of network connections. Especially in rural areas, this can often pose a challenge. According to information provided by the GSM Association [123], 96 percent of the world's population now has access to mobile broadband and 57 percent of the world's population, almost 4.6 billion people, are already using mobile Internet on their own devices (see fig. 26).

This is made possible through a complex infrastructure involving almost 1,400 telecommunications providers transmitting via mobile networks from an estimated 7 million transmission towers using standards ranging from 2G to 5G. While 80 percent of smartphones currently in use already support 4G or 5G, earlier generations enable access for older devices. Often, these are not phone devices in the hands of users, but rather services that are running in the background. For example, some emergency call systems are still based on 2G. As many European countries are pushing ahead with switching off the old network generations, activating the emergency button in the elevator may soon have no effect, unless it is upgraded in time.

While this may sound regrettable, it is in fact long overdue as European countries are lagging well behind. Australia already initiated the discontinuation of its 2G infrastructure in 2016 and had concluded it by 2018. Not

only does this make sense with regard to releasing and reassigning the respective frequencies for newer network generations, but also due to security aspects. The advanced age of the technology is not the only factor (2G was developed back in the 1980s). The security model itself is simply inadequate from a modern perspective. While mobile devices have to identify themselves to the provider in 2G networks, the network – in other words, the local transmission tower – does not have to identify itself to the telephone. As a consequence, it is relatively easy to introduce malicious radio cells in 2G and take over connections.

So, switching off these old, insecure systems is well overdue, as they further increase the attack surface within the infrastructures of the telecommunications providers, in part due to using outdated protocols but also because of the steep difference in security between various network generations – all in all, it is a highly complex system.

Nevertheless, the network is not able to reach every part of the globe. The fact that 96 percent of the world's population is covered is mainly due to the large urban centers in which many people are concentrated. Meanwhile, rural areas still suffer from insufficient coverage. But here, too, a solution is already available, and new technologies could rapidly close the gap.

The 3rd Generation Partnership Project (3GPP), the association of standardization organizations which specified the LTE and 5G technologies, among others, has also laid the foundations for the introduction of "massive IoT", meaning networks with a very high number of devices that typically have simple structures, consume little energy and are relatively inexpensive [123]. The related standards for narrowband IoT (NB-IoT) and LTE-M (long-term evolution machine type communications) are co-existing with today's 5G standard. Not only can they be transmitted from terrestrial, cellular mobile networks (terrestrial network, TN), but also from satellites (non-terrestrial network, NTN).

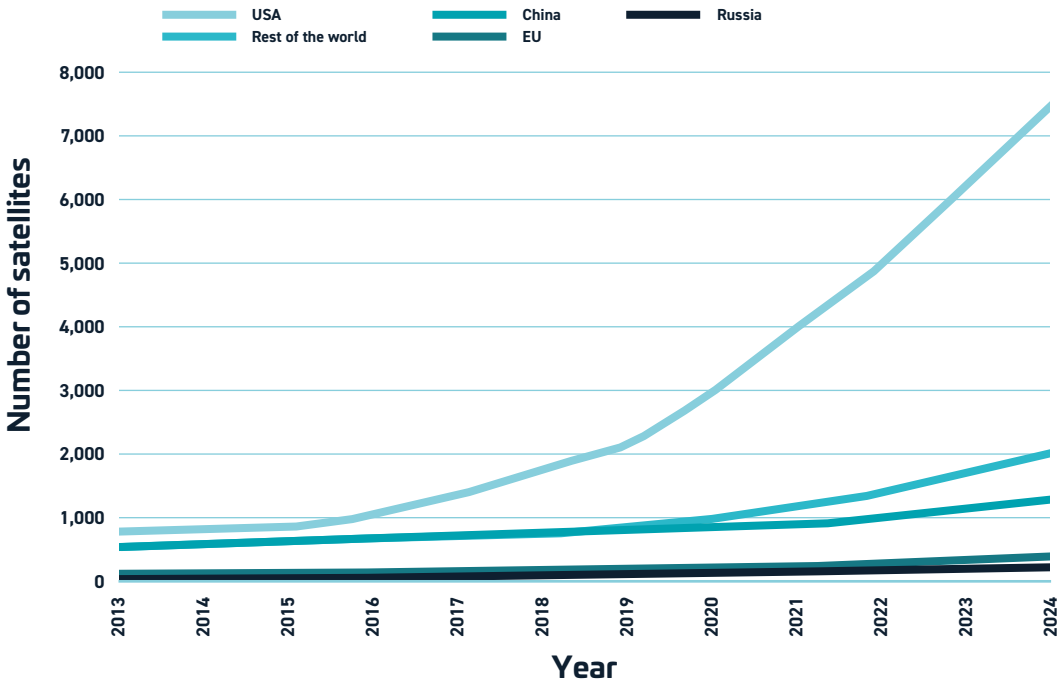
The first satellites specialized for 5G narrowband IoT are already in orbit and will enable global, gapless coverage and connection of IoT devices in the future. In practical terms, this means that an IoT device will communicate via the masts of a mobile phone network if they are in close proximity. Should this not be the case, it can send its data via satellites designed specifically for this purpose, thereby enabling IoT scenarios such as those described above for agriculture anytime and anywhere in the world.

3.9 CYBER IN OUTER SPACE

New technological possibilities have been driving a phenomenal amount of space infrastructure development in recent years, for instance in the realm of high-speed Internet access.

In days gone by, communication satellites were mainly placed in geostationary Earth orbit (GEO) at an altitude of just under 36,000 kilometers above a point on the earth. The advantage of this high altitude is that it allows a greater surface of the earth to be covered by fewer satellites. However, due to the great distance, GEO satellites have long signal propagation times and relatively low data transmission rates owing to the high number of simultaneous connections.

Medium Earth orbit (MEO) primarily contains satellites belonging to navigation systems, such as the Global Positioning System (GPS). The altitude and orbits flown by the satellites allow each point on Earth to be seen by at least four satellites at any given time, which is essential for determining a location precisely. The satellites in orbit closest to Earth, known as low Earth orbit (LEO), fly relatively close to the earth by comparison. For global coverage, a very large number of satellites are required. As a result, this was the area previously reserved for Earth observation and reconnaissance satellites, which need between one and three days to cover the entire surface of the earth, depending on their exact altitude. Due to the high costs, however, the number of systems has remained within limits. Especially when the first satellite-based commercial telecommunications systems were being established in the 1980s and 1990s, sever-



Source: own diagram

Figure 27: Development of the number of satellites by nation

al companies, such as Iridium and Globalstar, had to file for bankruptcy [183], [230]. However, thanks to investors and restructuring, these companies were later able to resume operations.

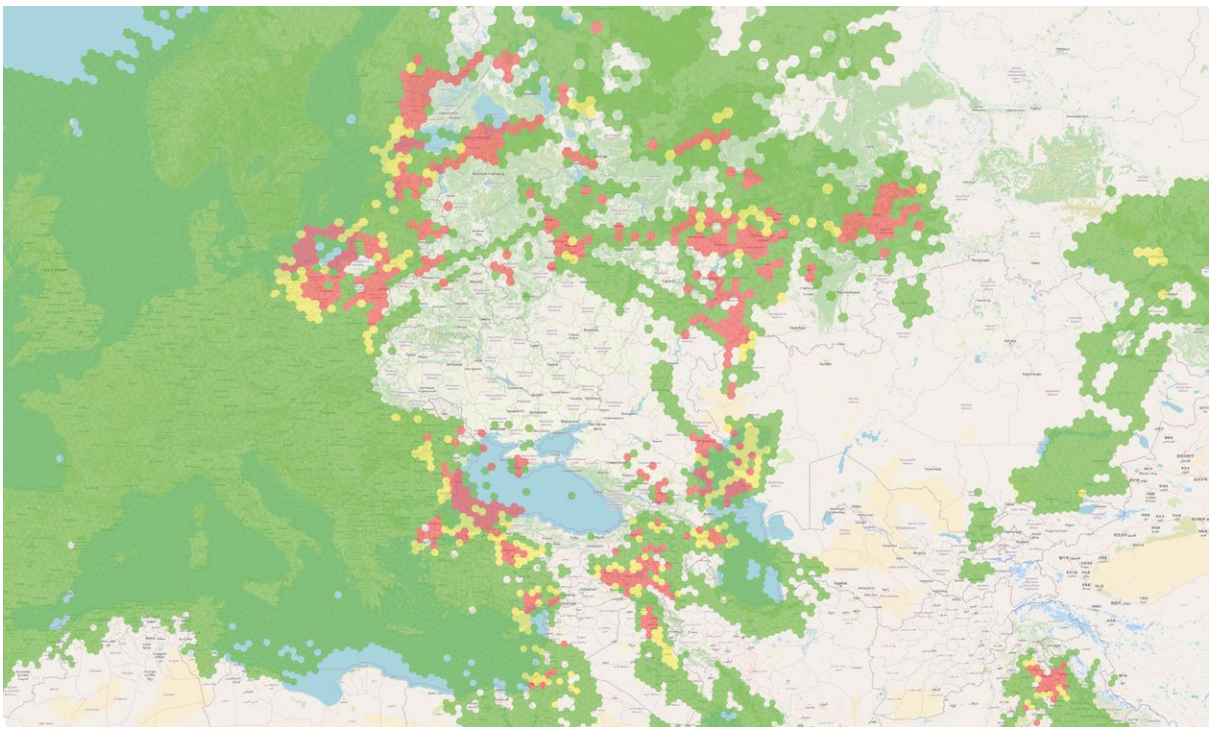
The reuse of rockets and the resulting reduction in transport costs, coupled with lower costs for new satellites, have paved the way for powerful new mega-constellations in LEO. Starlink's satellites, for instance, are orbiting at an altitude of 550 kilometers. The transit time for the signal is only 25 milliseconds at this height, whereas a signal from a geostationary satellite has a lag time of 500-600 milliseconds due to its altitude. For many of today's Internet services, this would no longer be acceptable. The low orbit and relatively small coverage area for each satellite, moreover, enable high data transmission rates. These performance parameters mean that Starlink has not only proven a reliable, fast Internet access point in remote regions, but also offers new possibilities for planes and ships around the world. In addition, it is playing a key role in the Ukraine war.

The potential use cases and economic prospects are driving development in this field forward at a breathtaking pace. A number of other mega-constellations are waiting in the wings. While Starlink currently dominates the orbit by a big margin with over 6,900 satellites [240], OneWeb already has well over 600 satellites in orbit, and projects such as China's Qianfan, which is planning 15,000 satellites, or Amazon's Kuiper project with 3,236 satellites are set to crowd the skies (see fig. 27). The EU has also recently committed 10 billion euros to the "Infrastructure for Resilience, Interconnectivity and Security by Satellite" (IRIS^2) project, which aims to provide Europe with secure, autonomous communication via 290 satellites by 2030 [93].

It would be impossible to achieve 100 percent global network coverage with conventional TN due to the high effort and associated costs involved. With the new satellite systems in LEO, it is now set to become a reality.

While this will unlock many new use cases, as already mentioned in the example of agriculture, new challenges are also sure to arise. After Starlink had developed into a critical system for Ukraine in fighting against the Russian invaders, Moscow announced that it could now be considered a legitimate military target. However, the Kremlin has thus far limited its activities to disruptive measures using jamming tools such as Tobol or Tirada-2, because Russia itself uses Starlink – albeit with illegally obtained terminals. Furthermore, a comprehensive attack on the satellites of an American provider carries considerable potential for escalation.

Attempts to interfere with or jam satellite signals are nothing new and may sometimes come from very unexpected sources. In one case, a truck driver in Newark, USA, used a GPS jammer back in 2013 to interfere with a company system designed to track the routes of vehicles in real time – perhaps in order to take unrecorded breaks. However, his routes also repeatedly led to Newark Liberty International Airport, where air traffic was disrupted by the signal jammer. The cause was discov-



Source: [329]

Figure 28: Interference with GPS signals

ered, and the driver was fined almost USD 32,000 – and dismissed by his company [93].

While such disruptions were once isolated incidents, the volatile geopolitical situation with its multitude of trouble spots and wars has meanwhile resulted in continual, widespread interference. At the very latest, since the war in Ukraine began with the Russian invasion in February 2022, the jamming of signals has become an everyday reality, both in war zones and in other imperiled regions with critical infrastructure.

The attempts to jam signals are intended to confuse drones and guided missiles which depend on satellite navigation in order to divert them away from their actual targets. It is estimated that 75 percent of the drones on both sides of the Ukraine war have been eliminated by way of electronic jamming measures. These activities also impact on other areas, such as civil aviation. Air traffic has already been restricted on several occasions in the Baltic Sea region. Finnair, for instance, had to suspend its flights to Tartu for a month at the beginning of 2024 due to widespread GPS jamming in the Baltic Sea region, presumably originating from Russia [244]. Websites such as GPSJAM provide an overview regarding the current situation, while also providing historical data (see fig. 28), to illustrate the current extent of such activities.

More dangerous than simply jamming signals is tampering with or altering them, also known as spoofing. In such cases, the signal is not simply overlaid by a stronger signal to make it "disappear" or become unusable for a receiver. Instead, a signal which appears to be correct (again stronger than the original signal) is generated so that the receiver only "sees" and processes this signal, which may then reflect an incorrect GPS position. If the offset is only small, this can initially be barely noticeable, for example in narrow shipping lanes, yet can quickly lead to catastrophic consequences. In this context, it is worth considering the repercussions suffered by shipping and the global economy, when the Ever Given container ship blocked the Suez Canal for six days in March 2021. Although the incident was not due to a cyberattack on the ship's positioning or control systems, but rather to strong winds, the opportunities for a malicious actor are self-evident.

Even barring a targeted attack on a specific vehicle, the extensive activities and affected areas now pose a threat to civil aviation. Last year, a 500 percent increase in spoofing was observed. While in the first half of 2024 nearly 300 flights per day were given incorrect position details by their GPS systems, this rose to almost 1,500 per day during the second half of the year. In concrete terms, this results in an incorrect position being displayed in the cockpit, which may not be noticed by the pilots. Displaying incorrect positions can only be prevented if pilots have timely information about GPS disruptions in an area and can activate their processing in the system.

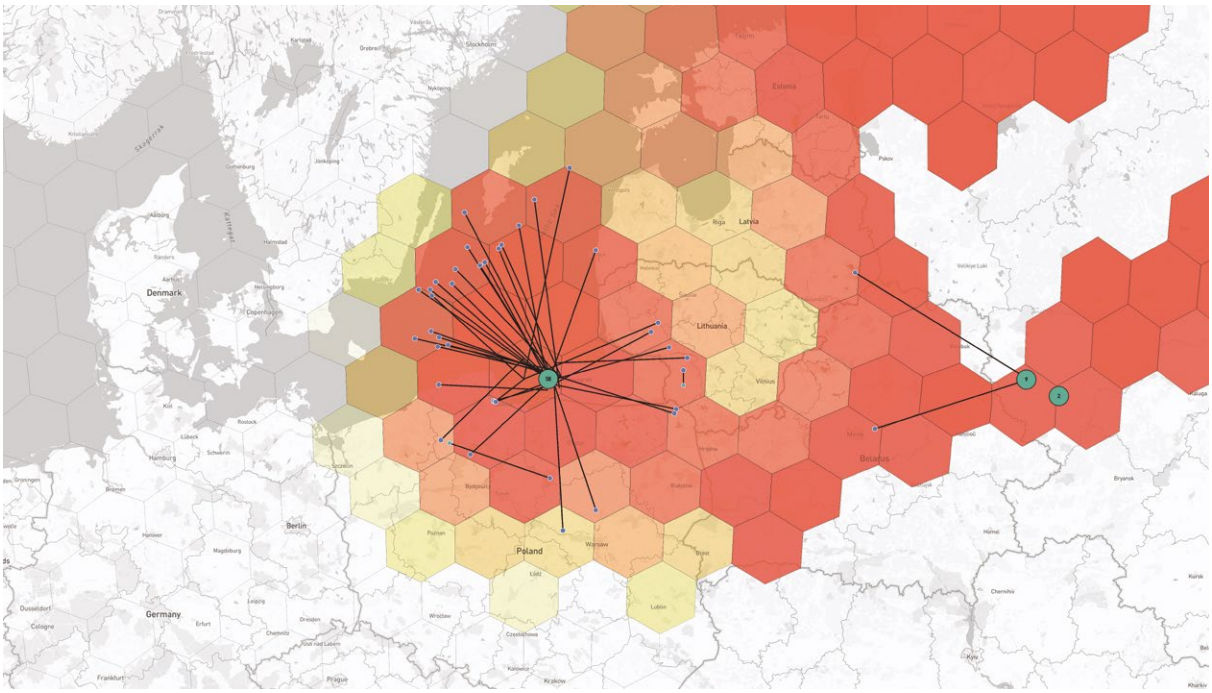
The day-to-day impact and resulting threat to civil aviation becomes clear when taking a closer look at the respective tracking screens. While the blue dots mark the

actual positions of the aircraft, their system positions are faked to show up in the areas marked with green dots – on January 11, 2025, for instance, at least 58 flights around Kaliningrad were displayed in incorrect positions (see fig. 29).

Critically, this also affects highly security-relevant systems such as the Ground Proximity Warning System (GPWS). In at least one aircraft type, moreover, various on-board avionics systems have been identified which failed to return to correct operations following a spoofing attack – even once the malfunction had ceased [220] – including the GPWS.

This can result in the system issuing a considerable number of error messages during the flight, thus leading to the effect known as alert fatigue, in which an overwhelming number of false alerts quickly leads to desensitization. If a genuine alert then shows up among all the false alarms, it will not be given the attention it should, as it will seem to be just another of many false ones. Such a scenario could have fatal consequences. The electronics of many of the 200,000 or so aircraft that fly around the world each day appear to be far from prepared for this. In one case, it was reported that an aircraft had to be taken out of service for several weeks of repairs, after spoofing caused the system time to jump far into the future [199]. Although the pilots were able to bring the aircraft down safely, the systems could only be brought back into working order by reinstalling them later.

Our increasing dependence on the space sector has further exacerbated this situation. Smaller airports, for example, have begun to decommission older instru-



Source: [261]

Figure 29: Example of GPS spoofing in the field of civil aviation in January 2025

ment landing systems (ILS) due to their high operating costs and replace them with localizer performance with vertical guidance (LPV), a GPS-based approach. If the GPS-reliant systems on board the aircraft are disrupted, ILS offers a safe, independent technology for landing safely – even in poor weather conditions and low visibility. If only LPV is available, the crew would have a serious problem in such situations.

The demanding requirements in the aviation sector, due to safety and security concerns, also make it more difficult to close any known vulnerabilities in an aircraft's IT systems in a timely manner. The testing and recertification required can take months or even longer. It is therefore advisable to continue to maintain redundant technologies such as ILS across the board wherever possible. A survey conducted last year revealed that almost 70 percent of air crews consider the impact of GPS spoofing on flight safety to be very high or extreme [220]. Aviation is not the only sector at risk from signal tampering. This became clear, for example, through observations showing falsified positions of ships in the port of Shanghai from 2019.

Against the backdrop of these massive operations against services such as GPS, concerns expressed about Russian activities involving the COSMOS 2553 satellite, which was launched into a very unusual orbit on February 5, 2022, are understandable. This satellite is located within a graveyard orbit, in which satellites usually do not operate due to the high levels of radiation. Usually, these orbits only contain systems which have long been disused or obsolete.

According to Moscow, COSMOS 2553 is tasked with testing new systems under high radiation exposure, whereas NASA has included the system in its archives as a possible radar intelligence satellite. However, Washington has also communicated concerns that the satellite could be used to test technologies for placing a nuclear warhead in orbit [131].

The considerable devastation that a nuclear detonation at such a high altitude would wreak was already investigated by the USA in the Starfish Prime project as far back as 1962. The electromagnetic impulse generated by a hydrogen bomb detonated at an altitude of 400 kilometers above the Pacific Ocean with an explosive force of 1.4 megatons even destroyed infrastructure in Hawaii, while the increased radiation in orbit resulting from the explosion affected numerous satellites and was responsible for failures even months later. The explosion destroyed a third of the (comparatively small number of) active satellites at the time. These effects, much more severe than the scientists had been expecting, ultimately led to the signing of the Outer Space Treaty of 1967, banning the placement of nuclear weapons in space.

Even though such a scenario seems rather unlikely, it cannot be ruled out entirely given today's geopolitical tensions. In many realms, such as the military, intelligence and the economy, the USA and many other nations are far more dependent on satellites than Russia. An attack of this nature would thus have a disproportionately huge impact on Western nations. The non-availability of global navigation satellite systems (GNSS), and above all GPS, would have a massive impact on aviation and shipping, as previously described, but also on land logistics. Likewise, numerous weapons systems, for instance GPS-based precision guided munitions, would only be usable to a limited extent or in some cases not at all. This is one of the reasons for the massive use of interference measures in Ukraine and Russia. Therefore, the calls made by American think tanks for special safeguards against EMP and radiation hazards for satellites in LEO, which are particularly important for the command and control of nuclear capabilities, make a lot of sense [17].

However, the exact position is not the only variable that can be calculated from the signals of the navigation satellites by way of trilateration [127]. Another crucial aspect is time.

Navigation satellites transmit signals including both information about the satellite's position in orbit and a time stamp from the high-precision internal atomic clocks that each satellite contains. If a receiver has several satellites within its field of view, it can use this data to calculate its own position, and also synchronize its own internal, far less accurate clock with the high-precision

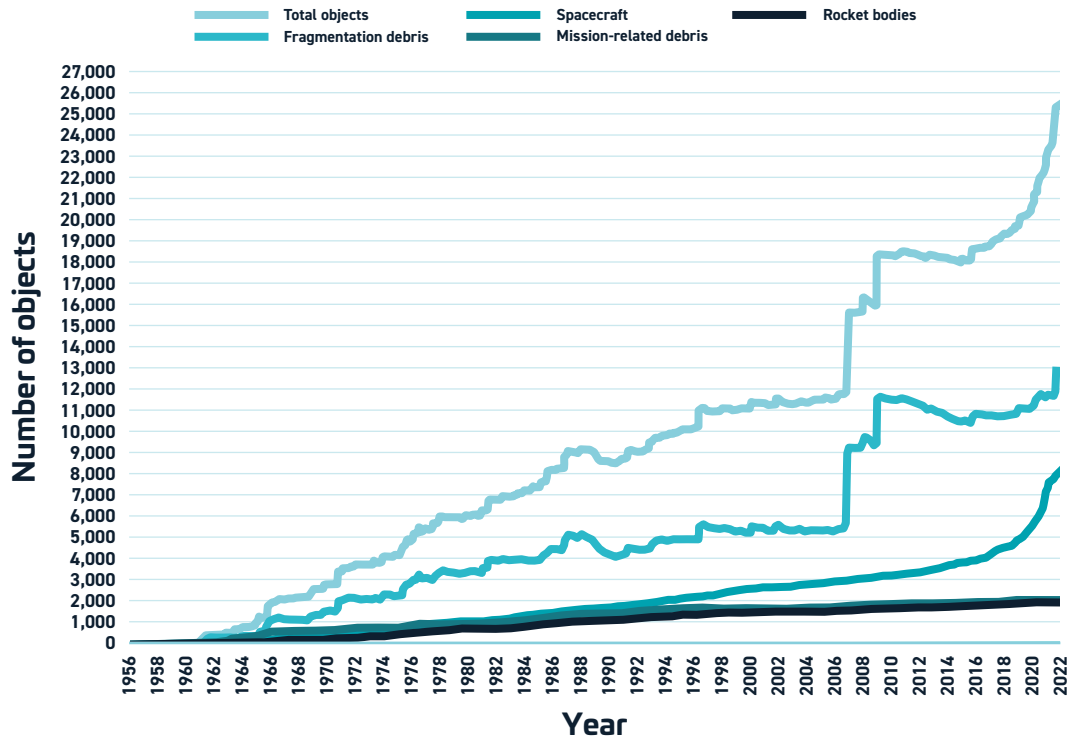
atomic clocks. As this procedure is taking place continuously, precision of up to 100 billionths of a second can be achieved [203] without the receiver needing to have an expensive, high-precision atomic clock. This extreme accuracy has resulted in a widespread dependency in many fields. For example, in financial trading and on stock exchanges, the internal system clocks are synchronized with GPS time in order to create time stamps for transactions. The highly accurate GPS time is also used to synchronize the base stations, i.e. the radio towers, of mobile phone providers. Energy utility companies use it to achieve synchronization in power stations and substations as well as in the rapid detection of faults in the power grid. The clocks in routers, the systems that forward data traffic over the Internet, are also synchronized using satellite time. In addition to such basic examples related to critical infrastructure, GPS time is also used in many other areas, such as the fast and precise pinpointing of seismic activities – the list is almost endless. Exactly how the malfunctioning of the dissemination of highly precise time will impact each of these areas and how quickly a time deviation could affect operational processes depends on the respective application, but in general it is hardly foreseeable. The dependencies are just too complex. It is, nonetheless, clear that the wide-ranging failure of our current satellite systems would have drastic consequences in all areas of life, suggesting that detonating a nuclear bomb in orbit could only be expected as a last resort in an existential war where one party has nothing left to lose.

Even if this disastrous scenario never comes to pass in outer space, one thing is clear – competition for dominance in orbit is steadily growing. From communications satellites to constellations specially developed for massive IoT, early warning systems which can detect rocket launches worldwide with infrared technology or reconnaissance satellites with optical or radar sensors – the variety of satellites and the opportunities they offer are constantly increasing. Military reconnaissance satellites are, of course, nothing new – even if very few details are known about them. However, a tweet from Donald Trump on X provided insight into the high performance of US systems. The post revealed an image which, according to analysts, originates from the USA 224 satellite. Based on the position of the satellite at the moment the image was captured, as well as its quality and detail, experts are assuming a display resolution of 10 centimeters or better. Bearing this in mind, it is hardly surprising that several nations have long been developing systems to prevent such high-precision visibility from above [36].

The testing of anti-satellite weapons (ASAT) began as early as the late 1950s, initially by the USA. In those days, aircraft were required to transport missiles to a high enough position from where they could be launched against satellites. However, modern systems such as the US military's Standard Missile 3 (SM3) can now be deployed against satellites from the ground and at sea. In addition to the United States, China also conducted successful ASAT testing in 2007, India in 2019 and Russia in November 2021 [247]. These tests repeatedly met with intense international criticism, as the destruction of satellites often produces innumerable bits of space debris, which sometimes remain in orbit for years or decades until they finally descend and burn up. The last remaining debris from a Solwind satellite destroyed by the US using ASAT in 1985, for instance, entered the Earth's atmosphere 19 years later. The Chinese ASAT test in which Fengyun-1C was destroyed in 2007 left behind nearly 3,400 larger pieces of debris, many of which are still in orbit.

Due to the high velocities and the resulting energy involved in a collision in orbit, even small particles can cause substantial damage. In the event of a collision, objects larger than 5 millimeters could quickly spell the end of a mission or completely destroy systems, while even objects smaller than 1 millimeter can lead to errors, defects or curtailment of activities.

In the meantime, there are already more than 29,000 objects in orbit with a size exceeding 10 centimeters, in some cases up to several meters. In addition, there are an estimated 670,000 objects with a size of between 1 and 10 centimeters and over 170 million objects between 1 millimeter and 1 centimeter in size. The ASAT tests, in particular, have led to huge surges in the amount of space debris and fragments (see fig. 30).



Source: [73]

Figure 30: Accumulation of debris and the effects of ASAT testing

A sharp increase in the number of rocket launches and new systems has added to Earth orbit becoming increasingly crowded. As the number of objects increases, so does the risk that accidental collisions and the resulting debris will lead to a cascading effect, known as Kessler syndrome, causing more and more functional systems to be damaged or destroyed. This means that in a worst-case scenario almost the entire space infrastructure could fail. To counteract this, there are several programs focused on removing debris from Earth orbits, for instance the Active Debris Removal/In-Orbit Servicing (ADRIOS) project led by the European Space Agency (ESA) [94], [233].

Since debris is not able to discriminate, the ever-increasing number of scrap particles jeopardizes any functional systems regardless of which nations they belong to. The use of kinetic ASAT weapons should thus be increasingly unappealing for most nations. And not only for that reason. The initial ASAT systems were developed when the orbit was relatively empty and there were only a few military high value systems in space, which were usually deployed for decades. Hence, there was a realistic chance that the intelligence capabilities of an adversary could be hampered by destroying a small number of systems.

The commercialization of space travel, along with rapid technological progress and the success of private sector companies, has fundamentally transformed this situation. Even if display resolutions below 10 centimeters in optical reconnaissance are still the reserve of the military, this is actually due more to government regulations than technical capabilities. For instance, the US government prohibits private companies from producing satellite images with resolutions smaller than 25 centimeters and also curbs the use of frequency bands. The fact that these new technologies have fundamentally redrawn the status quo has become clear through services such as Maxar, whose satellite images have also become well known in connection with various analyses of the situation in Ukraine.

The emergence of these new offerings on the market have made it possible to now buy highly detailed images with resolutions of up to 30 centimetres, which are updated up to 15 times a day for important areas of the earth. Not only have these changes taken away the unique position states previously enjoyed, but the new reconnaissance fleets offered by private companies enable much more – monitoring of the earth's surface in near real-time with constantly growing coverage. It is already possible to use the data collected by a high number of relatively simple satellites to commission data services such as AI-based analyses of changes occurring over time or the tracking of objects such as ships. The small number of extremely powerful military satellites, on the other hand, typically have to focus on specific regions and the revisit times may be lower.

Due to the immense possibilities of these new mega-constellations, the United States quickly realized that it would also have to put them to military use in order to maintain its technological lead. Accordingly, it began deploying a new reconnaissance approach known as "pro-

liferated architecture", which comprises a large number of smaller satellites. Although not much is known about it, the systems put in place thus far through the NROL-146, NROL-186, NROL-113, NROL-167 and NROL-126 missions appear to involve Starshield satellites, based on the Starlink Internet satellites but additionally equipped with a reconnaissance component [317].

This is also the reason conventional kinetic ASAT weapons have been losing their value. Dispersing the sensors across a large number of smaller platforms in LEO means that a correspondingly massive deployment of ASAT weapons would be required, increasing the risk of triggering unintentional, indiscriminate cascading and thus also putting the attacker's own systems at risk. At the same time, the new opportunities created by the civil sector are advancing at such a fast pace that this could become a challenge for the military.

One example is the European Space Agency's Copernicus Sentinel-1 mission. The pair of Sentinel-1 satellites were brought into service in 2014 and 2016 respectively. Sentinel-1B failed in December 2021 and will be replaced by Sentinel-1C, which was launched into orbit in December 2024. In the meantime, only Sentinel-1A has been providing data. The Sentinel satellites are equipped with radar systems which generate images of Earth's surface at any time of day or night and in all weather conditions. To achieve this, the satellites continuously transmit microwave pulses with a frequency of 5.4 gigahertz, which are reflected by the surface of the earth (this also explains the name Sentinel-1 C-Synthetic Aperture Radar, Sentinel-1 C-SAR, as the 5.4 gigahertz frequency is located within the C band). Based on changes in the reflected signals, or backscatter, and knowledge about the position and movement of the satellites, a very precise, two-dimensional image can ultimately be generated [95].

It is always possible, however, that a signal experiences interference on its way to Earth or back to the satellite. Especially when systems on the ground are operating at the same frequency, interference (i.e., the unwanted overlapping of signals) can occur, which can show up as errors in the rendering of the image.

If radar systems on the ground are operating in the same frequency range as the Sentinel-1 satellites, significant errors appear in the image. It was possible to identify Patriot systems in Israel on this basis, for example, as well as military exercises by Russian frigates of the Admiral Gorshkov class, whose flagship was only brought into service in 2019.

In light of these initially surprising capabilities of Sentinel-1 C-SAR, one image in which particularly intense interference occurred was of special interest. Due to the especially pronounced interference, various analysts presume that it was the result of a deliberate attempt by Russia to disrupt the satellite's reconnaissance activities. However, as the Russian air surveillance radar 96L6 is deployed in Ukraine and likewise operates in the C band, other interpretations suggest that the interference may have been coincidental.

These developments also underscore the urgent need, from a military perspective, to develop capabilities to counteract enemy reconnaissance. Accordingly, a number of nations are working on systems which can temporarily blind or permanently destroy the sensors of enemy reconnaissance platforms. Some of these have already been brought into operation. One example of this kind of activity is the Korla test site in Xinjiang, China, where in addition to anti-satellite lasers, it is also suspected that tests are being conducted on the resistance of electronic equipment to electromagnetic pulses (EMP), such as those generated by nuclear explosions at high altitudes. Another is the Kalina laser at the Russian Krona space surveillance center.

In addition to kinetic options and lasers, there are also several other approaches involving space-based weapons systems, for example by way of jamming, high-power microwaves, spraying certain chemicals, or causing mechanical impacts after approaching the satellite.

An increasing number of satellites are now equipped with a robotic gripper arm, such as the Chinese satellite Shijian-21, which lifted a disused satellite to a higher graveyard orbit. A maneuver of this kind involving a satellite traveling in orbit at a velocity of over 28,000 km/h

is anything but trivial. While in this case the mission was to clear away space debris, these same capabilities could also be brought to bear against satellites belonging to other nations. In this context, manoeuvres have been detected in which Chinese and Russian satellites were brought into close proximity to other satellites, after which they kept them under surveillance and even shadowed them. In May 2024, for example, Russia positioned COSMOS 2576, a so-called inspection satellite, in the close proximity of a US reconnaissance satellite.

The dual-use problem, referring to the potential for systems to be used both for civilian and military purposes, is inherent here – as is generally the case in the cyber realm – and considering the particular sensitivity of the systems in orbit, can pose a serious threat for many nations. A perfect example of this is the research currently being conducted into a system which enables the rapid removal of debris by way of several space-based lasers.

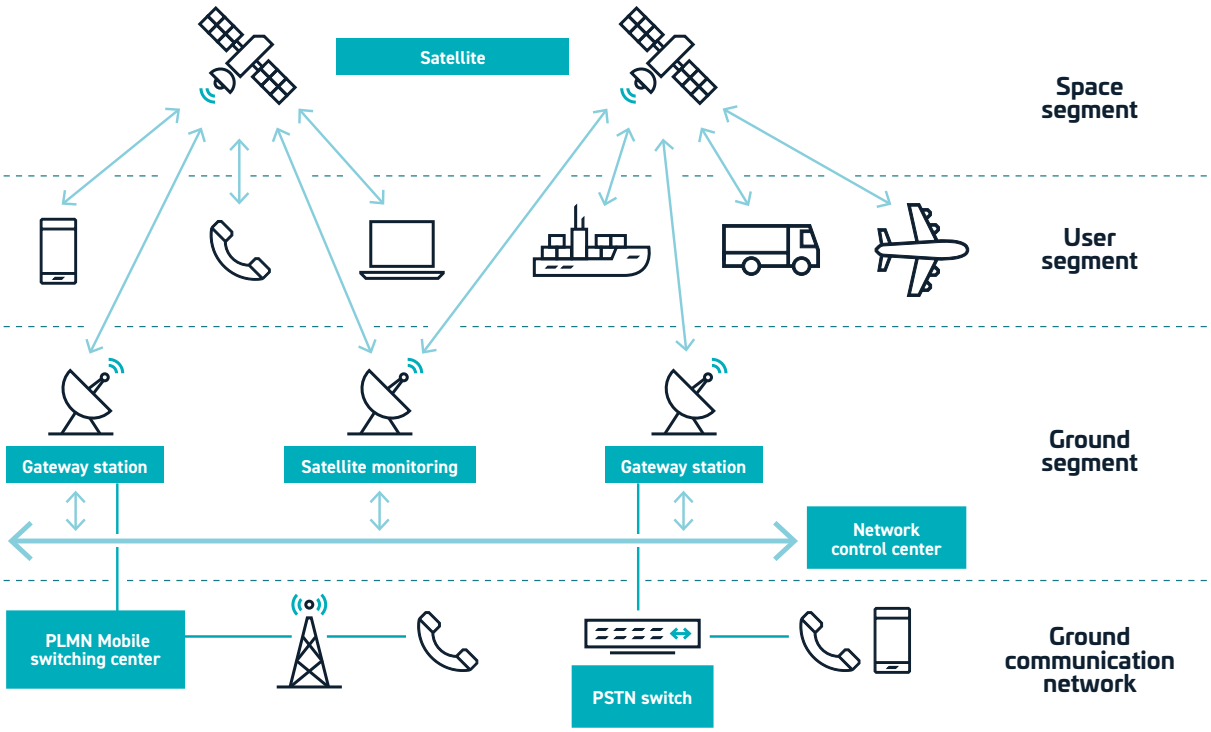
As in many areas relating to space systems, this game is no longer dominated by a just few powerful states. New start-ups, with the potential to impact the future of activities in Earth's orbit, are elbowing their way into the field with innovative ideas and new approaches. The start-up GuardianSat, for instance, has been awarded a grant to research new technologies to protect satellites. The Defense Advanced Research Projects Agency (DARPA), a Pentagon research agency, whose projects have led to successes including the Internet, GPS and Teflon-coated pans, has long recognized the need to involve innovative start-ups as a prerequisite for retaining its position as a technology leader. This is also particularly applicable to the civil space sector [307].

Considering the high number of dependencies and rapidly growing significance of satellites in space, coupled with several nations striving for dominance, the wide range of ambitious activities and schemes, and the new pioneering role played by private companies, one thing becomes clear. The situation is bound to become perilous and difficult to manage, especially in cyberspace.

When considering our artificial celestial bodies, it is particularly important not to forget that they should not be viewed in isolation, but rather as part of a complex, integrated system (see fig. 31). While earlier generations of satellites, for example those used for television transmission, had a very simple design and were actually only relay elements which received, amplified and re-transmitted a signal received from the ground station, more and more functionalities have been devised over the course of time. In addition to highly complex, military reconnaissance satellites, the proliferation of inexpensive, relatively small but highly developed communication satellites, for example in the Starlink network or in the imaging-focused reconnaissance fleets of private companies such as Maxar, BlackSky and Planet, mean that more and more systems can be found in space. With satellite computing, the processing of data directly in orbit to unlock new use cases, this is set to grow even further while the complexity of the systems is sure to increase. As a consequence, the cybersecurity of all the components involved is becoming ever more critical – from IT-laden satellites and the protection of their signals to the ground stations which control them and the elements that connect them to other networks and systems.

While in the past it was the ground-based components that were most at risk of being targeted by attackers, the space sector's rapid development and in particular the insubstantial cybersecurity measures and diminishing technical barriers to entry have combined to make attacking satellites a more interesting prospect. To counteract this development and focus on improving the security of the systems, the US Air Force launched the Hack-a-Sat competition in 2020. Hackers are assigned various tasks, and the outcomes are intended to feed into the development of more secure systems.

The need to bring the security of satellites up to scratch was clearly illustrated when a cyberattack attributed to Russia on ViaSat's KASAT system at the beginning of the Ukraine invasion impacted several thousand customers in Ukraine as well as over 5,800 Enercon wind turbines in Germany. By way of a malicious software update and wiper software, the attackers succeeded in deleting the firmware of the satellite's modem, rendering it unusable. Although this attack may not have been sophisticated, it was certainly effective.



Source: [320]

Figure 31: Architecture of satellite systems. All areas have long been exposed to cyber threats

3.10 THREATS UNLEASHED

This journey from the bottom of the ocean to outer space reveals the complexity of today's rapidly evolving situation and its countless factors and dependencies. Cyber threats are lurking at every turn. From cybercrime right through to state-led cyber operations, the actors are continuously developing and refining their processes to allow them to operate undetected in cyberspace. The sensitive power grids and vulnerable arteries of global communication, themselves dependent on IT, are facing a range of challenges due to rising geopolitical tensions. The growing dependencies and extremely complex global supply chains that have developed over the past decades have made it all too easy for sophisticated actors to cause catastrophic consequences in the real world through actions in cyberspace.

However, the race is not yet lost. A large number of initiatives are tackling fundamental deficiencies, from demands for new IT components and devices to be secure on delivery, without empty or trivial passwords, to grants and subsidies for building up local semiconductor production capacities and the development of a European high-performance processor based on the open RISC-V instruction set architecture. It is vital to increase Europe's sovereignty in all areas, from hardware right through to software. In practice, there has been no shortage of good ideas and suitable programs to date. The problem has rather been the capacity to make use of the available opportunities and implement them resolutely. As long as the selection of products is based on lobbying, a lack of systems expertise and a fear of change rather than security considerations, no headway can be made – and it will only be a matter of time before disaster strikes.

CHAPTER 4

REDUCE TO THE MAX
THE CYBERSECURITY SOLUTION DILEMMA

3,500
vendors around the globe, including startups

Up to 6
products per vendor

Up to 336
products in active use at large companies

EUR
5.8 billion
invested in cybersecurity solutions in Germany

Building blocks comprising the cybersecurity landscape and their functions

Minimum	Firewall (FW)	REACTIVE	EXTERIOR	INTERIOR	ZERO TRUST ARCHITECTURE ADVISABLE ACROSS THE BOARD	Secures your systems against external network attacks
	IPS / IDS					Detects and protects your network from predefined attacks
	SIEM					Aggregates security information from various sources for real-time analysis
	VM / EASM / CTEM	PREVENTIVE				Continuous exposure management (XM Cyber)
	Encryption					Required to ensure the necessary protection for stored or transferred data
	Backup					Enables data & systems to be restored, e.g., following a ransomware incident
Advanced	Anti-Virus	REACTIVE				Safeguards user devices against malware
	IAM					Management of users and their rights (e.g., access to systems and data)
	SOAR					Managing security incidents
	OT / IoT Security					Protects production facilities and networked manufacturing equipment
	NDR / EDR / XDR / MDR	PREVENTIVE	EXTERIOR			Advanced, active protection of user devices
	GRC / CCM					Management of risks and compliance requirements
	WAF					The web application firewall (WAF) secures your web applications against attacks
	CTI					Information about threats and threat actors
	Cloud Security					Scans for and reports misconfigurations in cloud instances

64%

of all security teams state that their existing products are not fully interoperable. **This leads to inefficiency and potential security exposures.**

Guidelines for buyers

1. Analyze your problems and requirements

- Understand your own risks, needs and problems
- Create portfolio analyses describing the existing system landscape
- Consider opportunities and constraints

2. Gain an initial overview

- Overview of various product types on the market
- Check compatibility and harmonization with existing solutions
- Question and challenge sales strategies

3. Preselection through screening

- Create a shortlist of viable options
- Principled management of the screening process

4. Test in advance

- Comprehensive, diligent testing of the shortlisted options
- Take certifications and standards into consideration
- Work closely with vendors to evaluate effectiveness
- Speak with reference customers or your own network about their experiences using the cybersecurity solution

5. Final selection

- "Best of breed" approach not only based on technical criteria
- Final selection based on requirements, use case and target group
- Consider usability for the specific target group
- Create a catalogue of requirements for vendors
- Security aspects of the solution included in the contract

Sources: [5], [7], [15], [16], [28], [38], [91], [116], [118], [128], [140], [141], [205], [218], [239], [273], [309], [330], own diagram

4 REDUCE TO THE MAX – THE CYBERSECURITY SOLUTION DILEMMA

4.1 TODAY'S CHALLENGING CYBER-SECURITY PRODUCT LANDSCAPE

In combination with organizational security measures, a wide range of software and hardware solutions make vital contributions to maintaining an organization's cybersecurity. These solutions perform key functions such as preventing and responding to cyberattacks and safeguarding data. Regulatory requirements oblige various industries to implement specific technologies, including attack detection systems, data encryption or vulnerability management, for instance as part of the NIS 2 Implementation and Cybersecurity Strengthening Act (NIS2UmsuCG) [218]. According to the IT security officer at one energy utility, "NIS 2 helps to ensure that even administrators can convince the board of directors of the importance of IT security and obtain the budget required for implementation..." However, the regulation does not seem to have any influence on the solution providers themselves, because "the tools contain whatever the vendors think they need to be able to sell them."

Cybersecurity solutions can provide support, especially where human capabilities reach their limits. They generally perform more efficiently and consistently, and are able to process, automate and analyze much larger volumes of data at speeds unattainable by humans. This allows employees to devote their time to more strategic tasks and boost their productivity. In some cases, these products can also be used in areas beyond cybersecurity (e.g., big data analytics and business intelligence).

Decision-makers are faced with the challenge of identifying the right technologies and combining them to achieve effective protection from cyber threats within the constraints of the available budget. In addition, 80 percent of decision-makers reported making cuts to their cybersecurity spending [141].

Over the past 25 years, the number of cybersecurity vendors has grown dynamically, keeping pace with digital transformation and the resulting expansion of the attack surface. According to recent estimates, there are currently more than 3,500 providers, including start-ups [15], [118]. Many products are highly specialized, standalone solutions, which can also serve as points of entry for attackers (software supply chain) or cause conflicts with other IT systems or IT security solutions [77], [83], [124], [158], [205], [254], [275]. Delta Air Lines, which was impacted by faults in its Falcon sensors in the summer of 2024, held CrowdStrike responsible for losses amounting to USD 500 million [105]. According to a survey, 64 percent of all security teams report that their existing security products do not work well in combination, leading to inefficiencies and potential security vulnerabilities [205].

In some product categories, 200 providers can be identified worldwide. A growing number of vendors are attempting to cover a certain area or even all areas with integrated all-in-one, suite or platform solutions. As of yet, there is no single solution which covers the entire spectrum, despite what some vendors' marketing departments and bundle offers would have you believe. In addition, it is commonplace to publicly announce capabilities or technology partnerships that are then only integrated into products after a long delay. In principle, moreover, all-in-one solutions always harbor the risk of vendor lock-in for their customers [128].

This is why organizations tend to rely on a variety of solutions. Studies reveal a range in which some organizations are using up to 83 products from 29 vendors, while others are using an impressive 336 different products from 57 vendors [16], [118], [141], [309]. Spending on cybersecurity solutions in Germany totaled EUR 5.8 billion in 2024 [28]. The global market for cybersecurity is set to grow to a volume of between USD 247 billion and USD 292 billion by 2029, with annual growth rates of between 8 percent [273] and 17 percent [116], depending on the region in question.

Chapter 1 of this report and the Schwarz Cybersecurity Reports for 2023 and 2024 make it clear that the damage caused by cyberattacks is on the rise around the world. How is this possible when organizations are already investing heavily in cybersecurity solutions in addition to people and processes?

4.2 CYBERSECURITY SOLUTIONS: AN OVERVIEW

Determining which solutions should be chosen to protect an organization depends largely on the size of the organization, the regulatory requirements it has to comply with, its risk profile and the resources available. Any security setup basically needs to provide both preventive and reactive protection for networks, data and terminal devices.

Firewalls are the first line of defense against cyberattacks. They guard against unauthorized access to networks by monitoring and controlling inbound and outbound traffic, and blocking any threats. Previously stand-alone solutions, **intrusion detection and intrusion prevention systems (IDS/IPS)** have become essential components of modern firewalls and provide more comprehensive protection. While conventional firewalls block data packets based on static rules, IDS and IPS enable in-depth examination of the content as well as detection of behavioral patterns and anomalies. IDS monitors networks for suspicious activity, logs it and triggers alerts. IPS, on the other hand, prevents attacks in real time, for instance by blocking suspicious Internet Protocol (IP) addresses which serve as unique identifiers for devices in networks. Modern firewalls are available either as virtual or physical machines. They leverage large threat databases, perform in-depth analyses of data traffic and make use of machine learning.

Supplementing this, **web application firewalls (WAF)** offer targeted protection for organizations whose online services are subject to special security requirements. WAFs monitor HTTP(S) data traffic – i.e. communication between end devices and websites – in order to protect the web applications and application programming interfaces (APIs) which enable communication between different programs and systems from a wide range of attacks.

In industrial plants, the military and intelligence services, unidirectional **data diodes** or bidirectional **security gateways / high assurance guards** are used in addition to firewalls to connect or separate networks of differing criticality or confidentiality levels.

Data loss/leakage prevention (DLP) solutions prevent unauthorized access to and transmission of sensitive data (e.g., via email or file sharing). DLP monitors data at the storage location, in use or during transmission.

Security information and event management (SIEM) systems aggregate and correlate information from various sources such as firewalls, networks, applications (e.g., SAP) or user devices in real time. The aim is to automatically detect complex attacks and generate a holistic overview of the security situation. Alerts, reports and case management support cybersecurity officers in identifying and resolving security incidents. Despite the financial costs and personnel expense involved, SIEM systems can also be valuable for smaller organizations. With more than 85 providers worldwide, there are products suitable for organizations of all sizes.

Nowadays, every PC should have at least one **antivirus program**. Properly administrated **identity & access management (IAM)** regulates the access options and rights for all users, thus safeguarding sensitive information. Just as important are **backup solutions and recovery processes**, that minimize data loss and ensure business continuity. Missing software updates, software vulnerabilities or incorrect configurations allow hackers to be successful in their attacks. Patch management software and vulnerability scanners compare system statuses with known vulnerabilities or available software updates as a preventive measure. **Continuous threat exposure management (CTEM)** platforms extend this approach and combine it with the continuous simulation of attacks on all internal and external systems of an organization, visualization of attack paths or prioritization of measures to harden the system.

Solutions such as **network detection and response (NDR)**, **endpoint detection and response (EDR)**, **extended detection and response (XDR)** and **managed detection and response (MDR)** monitor terminals and servers for threats and automatically implement appropriate countermeasures. They represent the next level of antivirus software. We are seeing increasing convergence with SIEM as ever more data from a variety of sources is integrated and analyzed. In contrast to other detection

systems such as IDS/IPS, they are also designed to recognize more complex attacks, for instance advanced persistent threats (APTs) or zero-day exploits. Even threats posed by perpetrators from within an organization's own ranks can be identified. There are over 110 providers for organizations to choose from.

The full potential of cybersecurity solutions that aggregate data from different sources reveals itself through the use or integration of a **Security orchestration automation and response (SOAR)** platform. This approach automates routine tasks, such as isolating user accounts or blocking passwords in the event of suspicious login attempts, resulting in a faster and more efficient response to security incidents.

GRC (governance, risk management and compliance) and **CCM (continuous controls monitoring)** solutions help organizations manage their policies, processes, risks and regulatory requirements (e.g., PCI DSS, ISO 27001, BSI IT Basic Protection, NIST) and continuously monitor compliance with them. In the past, such solutions required a great deal of manual input and continuous updating to keep them in line with changes in the IT environment and the organization itself. Many of the security requirements for IT systems can now be monitored automatically using appropriate data sources.

In addition, **Cyber Threat Intelligence (CTI)** platforms work to prevent cyber threats by collecting, analyzing and correlating data on cyber threats from various sources. This information is forwarded to specific teams or other security solutions, such as SIEM systems, to facilitate early warnings and more effective defense measures.

4.3 CYBERSECURITY MARKET AND MARKET FAILURES

Some of these cybersecurity products, for example firewalls or antivirus solutions, have been well-established for decades and are constantly being developed further. Others, such as SIEM, SOAR, CTEM or OT security, have only emerged in the last 15 years. In the area of cloud security, certain providers have achieved an annual recurring revenue (ARR) of over EUR 100 million in less than two years.

The growth of the cybersecurity product market reflects the increasing need for companies to respond to the changing digital threat landscape through prevention, detection and response. Every emerging technology, working practice or partnership, as well as every new business model, presents new potential attack vectors for adversaries as well as business opportunities for cybersecurity vendors.

Today, there is no cybersecurity product on the market capable of meeting all customer requirements for automation, pricing, services or integration into the organization's overall solution portfolio [3]. Evaluating cybersecurity products is often a frustrating experience: "It's a maze. If you try to find your way around the cybersecurity market today, you can easily lose your way. It seems like everyone has a solution to a problem that we haven't even identified and assessed yet," says a CISO from the energy sector who was interviewed for this article. What's more, decisions might need to be made under great time pressure – especially following incidents.

The cybersecurity market is characterized by fierce competition in all product categories. Due to the size of the market and the emergence of new threat scenarios, new vendors are continuously entering the market. In 2024, over EUR 14 billion were invested in cybersecurity companies. Developers of cloud security (cloud native application protection – CNAPP) solutions were at the top of the list. Cybersecurity solutions now need to incorporate AI as an integral component in order to become more agile and also signal innovative power [7]. At the same time, leading providers are consolidating, pursuing a platform strategy and expanding their portfolios by acquiring "features". The seamless integration of these new technologies and their teams is another challenge for the major providers [219]. The value of M&A deals exceeded EUR 40 billion in 2024 [239]. Sales cycles vary greatly, depending on the product category and industry concerned. It may take up to three years from initial contact to closing the deal.

A study conducted in 2020 argues that the cybersecurity market is dysfunctional along the lines of Nobel Prize winner George A. Akerlof's "lemons" theory [5], [140]. An IT manager at a German mechanical engineering company interviewed for the article has similar thoughts: "95 percent of the market is just rubbish. One of the biggest challenges for us is to separate the wheat from the chaff."

Within a category, products differ in terms of quality, security architecture, sovereignty or compliance with data protection requirements. They are also competing with solutions from other product categories due to overlapping functions.

Vendors use a wide variety of measures to signal product quality, including:

- marketing
- information markets (e.g., Gartner, IDC)
- reputation (e.g., reference customers, technical expertise of personnel)
- standards and quality seals (e.g., Security Made in Germany, NIST, BSI basic protection), certifications (e.g., CC EAL4+, ISO 27001)
- approvals (e.g., VS-NfD, GEHEIM)
- guarantee statements (e.g., combination of product with cyber insurance)
- free trial periods (e.g., try & buy offers)

It nevertheless takes a great deal of effort, expertise and time for customers to identify differences in quality, benefits or alternatives. Many organizations spend more than necessary on cybersecurity products which they do not use to their full potential [118]. Some features or solutions are often only used minimally or not at all, significantly limiting the effectiveness of the overall cybersecurity [177].

The prices charged for cybersecurity products provide little indication of their benefits and are usually set at the vendors' own discretion. When setting prices, they take into account a variety of factors (price structure within the product category, target customers, target markets) as well as general discounts and margins for the sales channels. Distributors and resellers, such as system integrators or MSSPs, may each receive a discount of up to 40 percent on the list price, depending on whether they are only processing the sale or generating significant new business. Prices vary greatly between solutions. Basic versions of software solutions are often offered either free of charge (freemium approach) or at attractive entry-level prices. However, these often do not cover the customer's actual requirements. After purchasing the solution, add-ons are then required to extend its functionality.

Antivirus or EDR solutions are comparatively affordable at between 1 and 30 euros per device or asset [140], especially for large companies which benefit from volume discounts. Firewalls are also available from as little as 100 euros but could also exceed 1 million euros. SIEM systems are also available in free open-source versions. By contrast, the annual costs for well-established SIEM solutions may set a mid-sized organization back five to six figures per year – including implementation, maintenance and training [38]. Providers of managed cybersecurity services (MSSP) typically charge package or block prices based on the number of systems and bundled services as well as the service level (e.g., 24x7, response times) [289]. These prices are generally expected to be below 10 euros per device.

Even though the market is plagued by information asymmetries, there are no signs of market failure where the risk of consumers choosing a lower quality solution diminishes the supply of higher quality solutions.

4.4 IMPORTANT POINTS TO CONSIDER BEFORE PURCHASING CYBERSECURITY SOLUTIONS

To make an informed purchasing decision, decision-makers need to ask themselves a number of questions:

- What are the risks for your own organization and how should they be prioritized?
- What is the external and internal IT and cybersecurity situation?
- Which solutions are available, and which are actually necessary?
- How can the success of the product be measured?
- How can the internal operation or external control be achieved, and maximum benefit ensured?
- Is it absolutely necessary to operate the solution internally?
- What are the minimum requirements that must be met?
- Are the products scalable? Can they adapt in step with the expansion of an organization?
- What are the price and license model trends on the market for the specific product category?
- Have subsequent costs been taken into account?
- Which operating models are available for the product category in question?
- Is the expertise for evaluating the solution during the procurement process, including proof of concept/value (PoC/PoV), available within the organization or should it be sourced externally?
- What experiences have comparable organizations had with the various providers?
- What requirements do the employee representatives have?
- How can the planned investments be reconciled with the budget?
- Is it more sensible to rely on a single provider or a selection of "best-of-breed" solutions?

Each of these questions raises additional challenges. One of the most significant is how to define appropriate criteria for making a decision. Organizations should avoid opting for any technical solution without a detailed assessment of the risks and security requirements. Another key issue which always needs to be clarified is whether the necessary knowledge, skills and capacities are available for operating and integrating the solution into the existing IT environment and IT security approach. If there are any deficiencies in this regard, there is a significant risk that the organization may be lulled into a false sense of security [160]. There is a reason why they say: "A fool with a tool is just a fool" because the goal is not the product but rather solving the problem and improving cybersecurity.

However, taking this kind of structured approach is all too often spurned in favor of a quick decision.

In some cases, there may be insufficient budget or a lack of commercially available solutions to address and adequately mitigate an organization's specific risks and threats. In such situations, it is critical to pursue alternative approaches to ensure cybersecurity and retain control:

- Combining various established solutions
- Continuously hardening and testing systems for all types of vulnerabilities

4.5 THE VENDOR'S PERSPECTIVE

Apart from the more obvious marketing methods, providers often employ strategies that target psychological mechanisms and emotions:

The FUD strategy (fear, uncertainty, doubt) is one of the oldest and most established approaches in marketing. Decades ago, it already attracted criticism in the IT sector and was partly blamed for the monopoly position attained by some large tech companies [227]. While this method was previously used to stoke distrust of competitors, in today's cybersecurity market it is primarily employed to use fear to emphasize the urgency of buying products. This includes citing statistics on the proliferation of malware, attacks and vulnerabilities or highlighting the financial consequences of cyberattacks. Studies have shown that fear and stress impair the ability to make rational judgment and decisions to the extent that alternatives are often not sufficiently considered [70], [154], [270]. The natural human desire to avoid unpleasant feelings and the threat of loss are deliberately exploited [102]. The approach is increasingly the subject of open and critical discussion among IT security experts.

The FUD strategy relies on creating a sense of urgency, as potential customers tend to make less rational comparisons and faster decisions under time pressure. The stress they feel is often exacerbated by the complex material and an overload of information [229].

In the face of tough competition, vendors do not stop at marketing their own products. They also deliberately fuel doubts about rival products. This approach was used, for example, by Microsoft in its long-standing campaign against Linux to create uncertainty about the quality of other providers [122], [308]. Another widespread method is the use of fake reviews. It is estimated that up to 43 percent of all reviews on major platforms are fake, no matter whether they are positive or negative [330].

Presenting a product as a comprehensive solution (all-in-one) is another common method. This leverages the psychological principle of least effort. In the face of complexity, people tend to favor easy solutions [33].

4.6 THE CHALLENGE POSED BY VENDOR LOCK-IN

Vendor-dependent, customized solutions and proprietary formats may work efficiently within a corporate landscape, but they severely limit flexibility and the capacity for innovation when it comes to selecting other solutions. Changing providers often requires a costly and complex migration of existing systems to the new solutions.

Incompatibilities when implementing other products, as described above, can also hamper the day-to-day work in diversified systems. In practice, organizations are often forced to rely on other products and services from the same provider. This dependency in turn exacerbates operational challenges. It also means that (hefty) price increases on the part of providers are more likely, especially if they can assume that their customers have no real alternatives.

In addition, vendors may not develop their products continuously to enable them to support new technologies and meet rising demands and requirements. Not only might this inhibit a company's potential for innovation, but it can also lead to the emergence of new attack vectors. In such cases, smaller companies in particular may feel they are at the mercy of the big players on the cybersecurity market. An information security officer (ISO) from a municipal energy utility describes this as follows: "The problem is that we can't do much about it. We can point out vulnerabilities, but the providers aren't really interested."

4.7 RECOMMENDATIONS FOR VENDORS

When developing cybersecurity solutions, vendors should take a number of key issues into consideration to improve the quality of their products and increase customer satisfaction.

- Developers should adopt **security-by-design** and **security-by-default** as fundamental principles throughout the development process. These approaches ensure that security mechanisms are taken into account from the outset and activated by default, an approach which is set to become a crucial aspect of quality in the future [7], [91].

- The **shift-left approach to security** should be consistently applied by incorporating security checks and measures as early as possible in the development phase. This requires clear definitions of security requirements, regular training for development teams and additional human resources within teams, for instance specialized software architects or security officers.

- Vendors should have their solutions or organization **certified by independent bodies**, to give their customers and prospects a clear understanding of the true effectiveness of their solutions.

- The usability of the solution should be characterized by a well thought-out **UX/UI-Design**, intuitive user interfaces, and terminology and symbols consistent with the daily work of IT security staff. Close collaboration with customers is crucial, for instance through advisory boards.

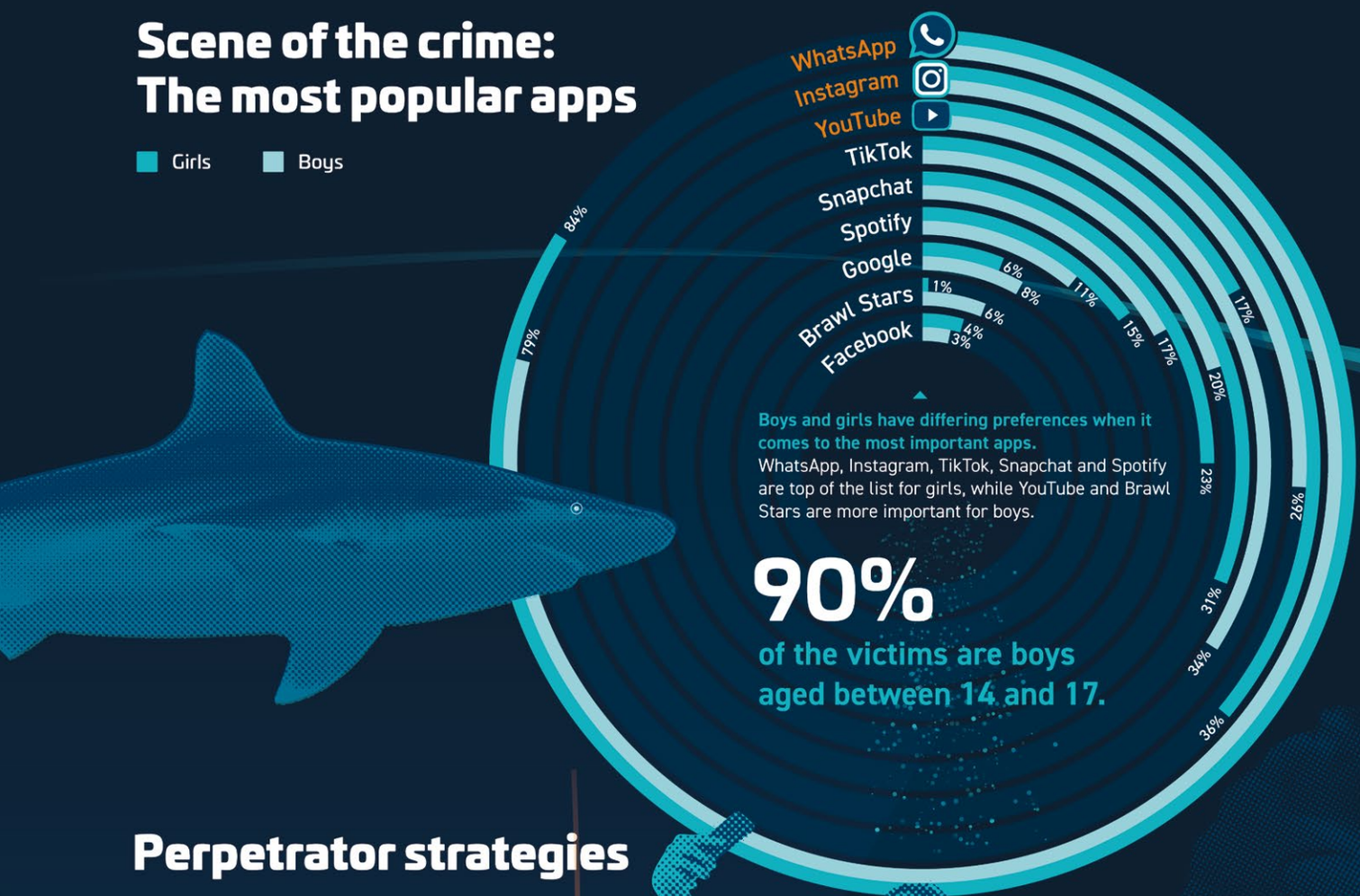
- It must be possible to integrate products seamlessly into existing IT security solution portfolios and they must be highly compatible with other vendors' products. This includes using standardized formats such as the **common event format (CEF)** or the **log event extended format (LEEF)**, which is particularly important in **OT security**.

In conclusion, it is important to note that improving the cybersecurity solution landscape requires close and transparent cooperation among all stakeholders. Only through this collective effort will it be possible to build a more resilient and secure digital future.

CHAPTER 5

TEEN DANGER ZONE
SEXTORTION

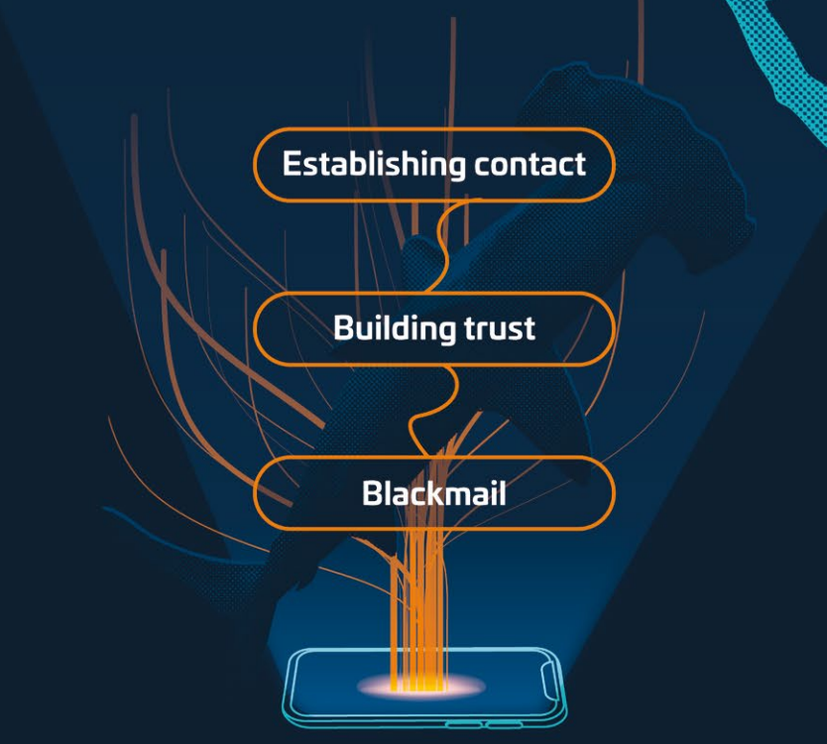
Scene of the crime: The most popular apps



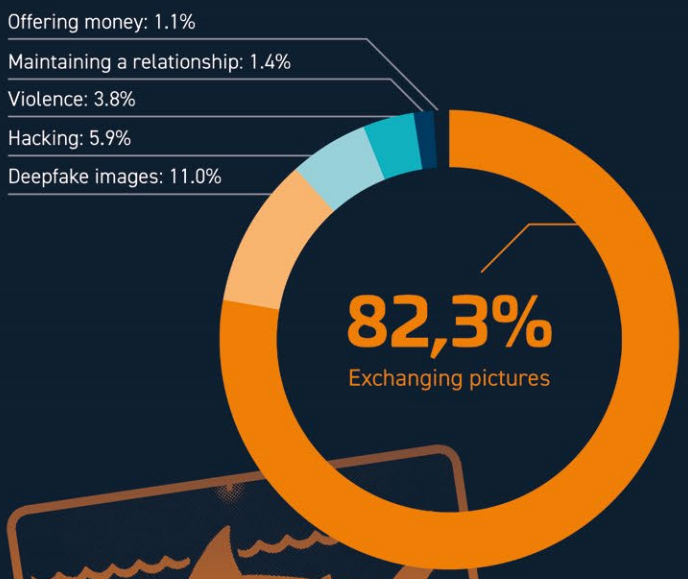
Boys and girls have differing preferences when it comes to the most important apps.
WhatsApp, Instagram, TikTok, Snapchat and Spotify are top of the list for girls, while YouTube and Brawl Stars are more important for boys.

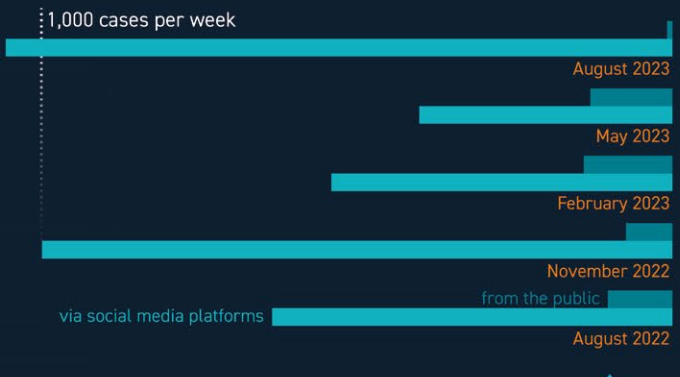
90%
of the victims are boys aged between 14 and 17.

Perpetrator strategies



How perpetrators get hold of intimate contents





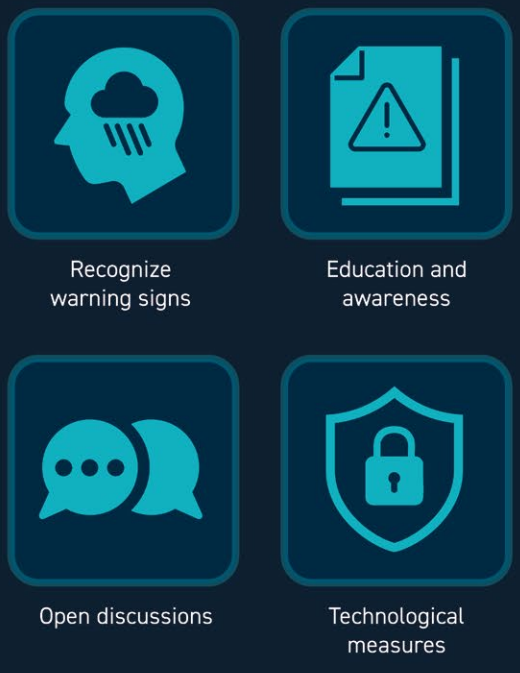
Between 08/2022 and 08/2023, on average 812 sextortion cases a week were reported to the National Center for Missing & Exploited children (NCMEC).

Worldwide, the total number of cases in 2023 was 26,718, more than twice as many as the 10,731 registered the previous year.

27%

of victims who paid the offenders received further demands.

Prevention



Damage limitation

Should one fall victim to sextortion, it is crucial to follow these recommendations ▾

Sources: [23], [43], [59], [78], [68], [130], [176], [190], [295], [231], [243], [294], [295], [296], [306], [318], [324], own diagram

5 TEEN DANGER ZONE – SEXTORTION

There are moments which split your life into before and after – and sometimes they happen so inconspicuously that you only become aware of them once it's already too late.

DAY 1 – THE MESSAGE THAT CHANGED EVERYTHING

It was just a regular Tuesday evening in autumn. It was dark outside, and the rain was drumming against my window. I was sitting at my desk with my textbook open in front of me, staring at the 10th grade math assignment that I should already have long solved. My smartphone vibrated. This was hardly unusual. I was constantly getting messages while I was busy doing other things. But this one was different.

Hi 😊. Is this Max's profile? Haven't we met somewhere?

I gazed at the text. Who on earth could this be? It was one of those messages that immediately arouses your curiosity. One that was hard to ignore.

Yes, it's me. Who are you?

The answer came before I'd had a chance to turn my attention back to my math assignment.

My name is Lena. Sorry if I'm bothering you! I saw your profile picture in a group. You look really nice.

Nice – it was ages since someone had used that word to describe me. Wasn't "nice" another way of saying "boring"? My heart started beating a little faster.

Thanks … erm, in which group was that?

Oh, I can't remember where. Never mind. There seems to be something special about you. 😊

Her profile picture caught my attention. It showed an attractive girl sitting on a park bench, her head tilted to one side and her hair tied back. Her eyes seemed to be looking right at me through the screen. I knew that I should be cautious. But she seemed real enough. Not like those obvious bots and AI generated girls with their bewildering jumble of emojis and absurd propositions that were all over the news.

Oh, okay. Thank you, I guess. 😅

Ha ha, you're really cute when you're nervous.

DAY 2 – THE MESSAGES BECOME ROUTINE

Lena quickly became a fixture of my day. Every free moment I had, I would check my phone – excited to find out whether she had written to me. Our chats became longer, and more personal. She told me that she lived nearby, but had only moved there recently and didn't know anyone yet. She sent me pictures – nothing out of the ordinary, just enough to show me that she was there, and that she was real.

And me? I started to look forward to her messages. It was as if I had found a friend, someone who understood me – someone who was truly interested in me.

It was a strange feeling. Lena texted almost daily. Always friendly, always curious. She asked me about my hobbies, my school and what I liked to do in my spare time. She knew exactly when to sound interested and when to throw in a compliment.

"I bet you're really brilliant at drawing," she wrote one evening, after I had told her that I sometimes drew sketches. Reading something like that made me feel really great – like an affirmation from someone who wanted to understand me.

Lena: **"Would you mind sending me one of your pictures? I bet you're a real little artist!"**

Me: **"Umm, they're not really anything special ..."**

Lena: **"Oh, come on. You can trust me. I'd never show them to anyone else, unless you wanted me to."**

So, I sent her one. A small, insignificant picture I had drawn several months earlier. Lena praised it to the skies, saying how talented I was and how she envied me for my talent. And although I knew it was a bit of an exaggeration, it felt good. Later that evening, while I was writing with her, my mom came into my room.

"Max, have you finished doing your homework?" She stopped in the doorway, her arms crossed. "Almost," I mumbled without looking up from my phone.

"Who are you texting with all the time?" she asked suspiciously. "Just a friend," I lied.

I felt my face getting hot. It was the first time I had concealed Lena's existence, and I didn't understand why.

DAY 4 – TRANSGRESSING THE FIRST BOUNDARY

Our chats quickly became more intimate. Lena was always friendly, but our conversations started to get more personal. Her questions were skillfully worded, and I didn't even realize how much I was revealing about myself. Somehow, she managed to make me feel safe. The shift happened gradually. Perhaps I should have seen it coming. However, when Lena first asked a personal question which felt different, I ignored the feeling in my gut.

One evening, she asked:

Lena: **"Max, I've taken a picture. Would you like to see it? 😉"**

Me: **"Umm, sure!"**

The picture she sent was harmless enough. She was wearing a T-shirt, sitting on her bed with a shy look in her eyes. Yet something about it felt a bit off, like she was waiting expectantly for something.

I felt a tension in the pit of my stomach.

Lena: **"Do you think I'm pretty?"**

Me: **"OMG, totally!"**

Lena: **"Now it's your turn. Show me what you look like right now.😊"**

I hesitated for a moment. "Why not?" I thought to myself. An innocent picture couldn't do any harm. So, I took a selfie and sent it off. Perhaps we would soon meet up in person. Lena answered right away.

Lena: **"Wow, you're so good looking. I really don't think I've ever met anyone like you before."**

I felt myself blush and my heart started beating a little faster. Was this love? Her compliment felt like a warm blanket on a cold day.

DAY 7 – THE FIRST MISTAKE

Lena's messages were like a vortex that pulled me in. Each time, she wanted more – and so did I. And she got it from me. One photo became two, then three. She was always so kind, so admiring, that I didn't notice how deeply involved I had become. Then one night, when I was actually ready for bed, another message arrived.

Lena: **"I've got another photo, but it's a bit more daring. Would you like to see it?"**

Me: **" ... "**

This photo was different than the others. It was a picture that made me feel nervous and aroused me at the same time. Unlike the pictures of models from a marketing campaign for a renowned lingerie brand some friends had recently shown me in the schoolyard. They were sexy but meant nothing to me. Lena did. I could feel my body getting hot and my heart racing.

Lena: **"Now it's your turn. Be brave. You trust me, don't you?"**

I felt a chill run down my spine, a faint whisper telling me that something wasn't quite right. But I ignored it. I didn't want to disappoint her and, somehow, I also wanted more.

DAY 10 – THE THREAT

The message popped up in the afternoon, just as I was making my way home from a normal school day. Lena and I had been writing to each other for more than a week. We were sending each other the most intimate pictures and videos imaginable, and expressing our deepest desires.

Lena: **"I've saved everything, Max. The photos and the videos. If you don't give me 300 euros, I'll share them with everyone. Your friends, your parents, ..."**

I felt nauseous. My heart was pounding and my hands turned to ice. I couldn't find the words. My hands were trembling as I wrote back.

Me: **"Please don't do this. I haven't got the money!"**

Lena: **"Then get it. You've got 24 hours. Otherwise, I'll ruin your life."**

DAY 11 – THE PAYMENT

I couldn't sleep or think straight. Each message I received made my heart pound faster. The threats became more callous, the demands increasingly forceful. Finally, I caved.

I picked up my smartphone and transferred all the money I had via an app – birthday presents, Christmas gifts, newspaper delivery earnings. It was all gone.

Lena: **"Okay, payment received. Good boy!"**

I kept staring at the screen as a feeling of relief washed over me. The nightmare was over!

But the very next day, another message arrived.

Lena: **"I need more. Send me another 500 euros. Then it will be over. I promise."**

I was stunned – overcome by panic. I had no idea how I could ever get out of this.

DAY 12 – THE NERVOUS BREAKDOWN

I sat in my bedroom, my door locked and my phone in my hand. There was no way I could concentrate on my schoolwork. I was suffering from a headache that just wouldn't go away. I had chewed my fingernails down to the skin. It was as if I was observing myself from outside my own body, unable to exert any control over my own life. Every new message was like a punch in the gut. I had nothing left to give. All my money was gone and so, too, was my hope.

My parents noticed that something wasn't right. "Max, what's wrong? You've become so quiet recently," my dad asked at the dinner table. "Nothing," I mumbled, pushing my food around the plate. My mom placed her hand on my arm. "You know that you can speak to us about anything, right?"

My inner voice was like a small child, screaming: "Help me, Mommy and Daddy!" But they couldn't hear me. I was deeply ashamed. Of my stupidity. Of the pictures of my naked body. Of the videos of my body and the desires I had expressed in the chats with Lena.

That night, I sat alone on my bed, staring into the darkness.

Everything was hurtling out of control. My breath came in gasps and I was engulfed by an emptiness inside.

I didn't feel like I wanted to be in this world anymore – or that I could.

There was only one way out of the horror film my life had become.

The next day, I would put an end to it.

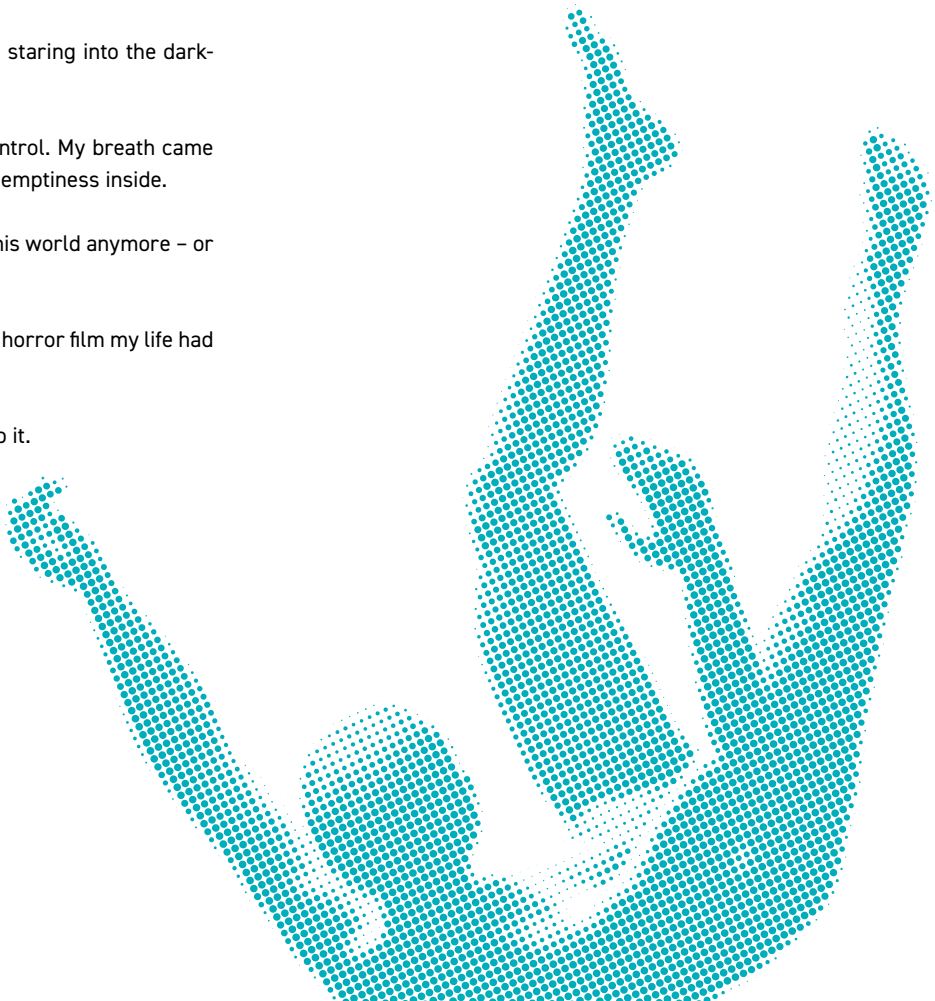
Then I fell asleep – exhausted.

EPILOGUE

Max was one of the lucky ones. Rather than take his own life, he found a way to talk to his parents the following day and his nightmare indeed came to an end. His story is a striking example of how dangerous sextortion can be and just how difficult it is for victims to escape the web the perpetrators have spun around them. Sadly, not all victims can find a way out. Many suffer from long-term psychological and financial harm, often with tragic consequences.

Unfortunately, nobody can help 17-year-old Jordan DeMay from Michigan, in the US. He took his own life in March 2022, fewer than six hours after the perpetrator first contacted him.

Sextortion has long been more than just a few isolated cases. It has become a global phenomenon which is impacting more and more people – especially adolescents. To gain a comprehensive understanding of this threat, it is worth taking a closer look at the mechanisms, repercussions and background of sextortion.



5.1 WHAT IS SEXTORTION?

Sextortion, a portmanteau word made up of "sex" and "extortion", describes a form a digital blackmail, in which psychological manipulation is combined with the targeted use of modern technologies. Perpetrators threaten to publish intimate photos, videos and chats involving the victim in order to coerce them into handing over more intimate content, paying them money or compensating them in some other way [132], [215], [224], [231], [236], [294]. It is especially problematic that both genuine compromising materials and those created by way of deepfake technology can be used to crank up the psychological pressure substantially on victims. These convincing fakes can make threats appear credible and amplify fears of social embarrassment [100]. A typical characteristic of sextortion is the speed with which these crimes can escalate. In some cases, it only takes a few hours from first contact until blackmail is attempted [296], [324].

Digital transformation has fundamentally altered the ways in which people communicate. Social media, messaging services and other digital platforms have become fixtures in our daily lives, along with smartphones. Adolescents use these platforms especially intensively, sharing personal content and maintaining social contacts in the digital realm. Since the COVID-19 pandemic, there has been a growing trend for social interactions to shift to the digital sphere [23]. This change in communication behavior has also created attack surfaces for sextortion, cyberbullying or revenge porn.

Sextortion differs from other forms of online crime due to its explicitly sexual context. While phishing, for instance, aims to obtain access to sensitive data and love scams use emotional manipulation to achieve financial gain, the main focus of sextortion is on using intimate content as leverage for extortion [294]. It is difficult, however, to draw a line between sextortion and cyberbullying, as the mechanisms and repercussions partly overlap. Cyberbullying consists of repeated harassment by way of digital means or channels, often characterized by the anonymity of the attacker and the wide dissemination of explicit images [213], [253]. In contrast, perpetrators of sextortion target the emotional and social vulnerability of their victims with sexualized attacks [133], [224].

The increase in sextortion cases around the globe is alarming. In 2023, more than 26,700 cases were reported – significantly higher than the 10,700 cases in 2022 [130]. Between October 2022 and March 2023, the FBI and Homeland Security registered more than 13,000 reports of financial sexual extortion of minors, with at least 12,600 victims and 20 documented suicides [324], [325]. In addition, the Internet Watch Foundation (IWF) announced that more cases were reported in the first six months of 2023 alone than in the whole of 2022 [151].

A blind spot in crime statistics

Similar to cyberbullying, sextortion has not yet been established as a distinct phenomenon in many statistical surveys around the world. Cyberbullying, for example, was only included in the global surveys conducted by the World Health Organization (WHO) for the first time in 2018. Sextortion is often difficult to delimit in surveys, although data on related offenses, such as receiving or sending images without permission, is already available [106]. The problem is further exacerbated by the high number of unreported offenses.

In Germany, there is still a lack of precise figures, as sextortion is not reported as a separate offense in the police crime statistics (PKS) [59]. In addition, the PKS generally only includes offenses in which the perpetrators are based in Germany. Offenses committed from abroad are usually not taken into account [59]. These gaps in the collection of data make it difficult to gain a clear overview of the actual extent of the offense. Despite the limited data, sextortion is currently considered one of the biggest Internet-based threats [43]. Adjusting the statistics would not be difficult. According to a survey by the Deutsche Presse Agentur (dpa), more than 2,000 such cases were recorded nationwide in 2023. Police investigators are also anticipating a high number of these offenses in 2024, particularly in connection with a rise in crimes committed from abroad [278].

Several federal states in Germany reported contrasting trends in their 2024 statistics. In Hesse, the number of sextortion cases recorded increased from a low three-digit figure in the previous year to a figure in the mid three-digit range by December 2024 [278], [323]. In contrast, the State Criminal Police Office of Baden-Württemberg registered a decline in sextortion in their crime statistics (PKS) – from 308 cases in 2022 to just 102 cases in 2023 [176], [323]. However, this difference is due to an adjustment in the data collection process that distinguishes between domestic and foreign offenses. Hence, the figures do not reflect the actual extent of the phenomenon [59], [176].

In 2024, 7 percent of all victims of online offenses stated that they had been targeted in cyberbullying attacks – a figure which remained constant compared to 2023. When it comes to sextortion, 4 percent of respondents reported falling victim to such incidents, down from 7 percent in 2023. Love scamming showed a similar trend, dropping from 8 percent in 2023 to 6 percent in 2024. Reports of incidents involving deepfake content, moreover, fell from 4 percent to 3 percent over the same period [232]. However, these declines can partly be attributed to the increasing relocation of perpetrator activities abroad, which results in them not being recorded in national statistics.

Many victims do not bring criminal charges, whether out of shame, fear or lack of knowledge about the protection offered by the law [133], [224]. In fact, studies have revealed that many victims fail to tell anyone about their experiences and that not even a fifth of the victims report the offense to the police [259], [318], [333], which impedes both the investigation and the prosecution of offenders.

5.2 OFFENDER STRATEGIES AND APPROACHES

Increasingly, sextortion activities are being carried out by professional, transnational networks which leverage targeted psychological and technological means to manipulate victims. Many of these perpetrators are operating out of countries like Nigeria, the Ivory Coast, India or the Philippines. In some cases, organized crime groups which contact and manipulate victims around the world have been discovered in these countries [100], [326]. In India alone, it is estimated that 500 cases of sextortion are reported daily, but only a fraction of these lead to official charges being brought [334].

These transnational groups use encrypted platforms and increasingly leverage AI-supported technologies such as deepfakes to create deceptively convincing content. In addition, perpetrators also have access to standardized scripts, designed specifically for sextortion attacks, which are circulating in criminal networks. Reports have also shown that victims are often threatened using identical messages, which have been publicly available since 2021 and are still commonly used [241]. To obfuscate their identities and activities, these syndicates also demand payment in cryptocurrencies that are difficult to trace [59], [100], [152], [222], [306], [326], [334]. Besides cryptocurrencies, perpetrators of sextortion are increasingly using alternative payment and commerce platforms such as Etsy, Amazon, PayPal and Selar.co to launder money or conceal their identities. Anonymous online forums and messenger groups also facilitate the exchange of extortion tactics, enabling perpetrators to become more effective and helping them evade prosecution [9].

Extremist online communities, such as the "manosphere" and "incels", specifically disseminate content that aims to legitimize sextortion as a means of exercising power. Perpetrators exchange manipulation and blackmail techniques in related forums as well as on platforms such as Telegram. These communities, which propagate the notion that women are responsible for male suffering, use digital spaces to spout ideology and professionalize perpetrator methods [9]. This shows that digital violence cannot be viewed in isolation, but that perpetrators may form part of a larger ecosystem.

In addition to organized criminal networks, the perpetrators of sextortion also include individuals from the victim's social environment, such as (ex-)partners, friends or family members. They may be driven to commit these offenses by a variety of motives, including emotional triggers such as jealousy, financial interests or the desire for control. Sextortion often occurs in conjunction with violence in intimate relationships – by way of threats, emotional pressure or digital abuse. These cases involve perpetrators using digital platforms to exert power over their victims and underpin their threats [224], [295], [332].

Sextortion follows a clear pattern, which can be sub-divided into several phases:

1. **Making contact:**
   Perpetrators search for potential victims on platforms such as Instagram, Snapchat or TikTok, which are particularly popular with young people for sharing personal content. Using fake profiles or synthetic identities, often containing stolen images or identity details, they pose as peers or individuals with a romantic interest in order to gain the trust of victims [294], [306]. Communication is often quickly shifted to encrypted messaging services or email to avoid being traced or potentially blocked on social media platforms [243], [294], [306], [318].

   The methods typically employed by perpetrators include:

   - Using multiple identities or pretending to be of a different gender in order to create closeness. These additional profiles reinforce the credibility of the perpetrator, for instance, while playing fake roles aims to spark romantic interest or build trust.

   - Accessing publicly available social media profiles with the aim of gathering personal information such as friends lists and preferences.

   - Secretly recording messages or video chats in order to exert pressure at a later stage [306].

2. **Building trust:**
   During the next phase, perpetrators attempt to establish an emotional bond with the victim. They show empathy and appear to be interested in the victim's personal problems and preferences, with the intention of gathering information they can later use as leverage. Young people are particularly susceptible to this type of manipulation, as they often feel flattered by the attention and underestimate the risks [243], [294].

   A frequent strategy is to gain trust via online dating platforms. Many victims judge the trustworthiness of their counterpart based on their communication behavior or profile information. Studies show that these supposed clues can easily be manipulated or falsified, however, making it easier for the perpetrators to deceive potential victims [294].

   This kind of targeted deception uses emotional manipulation and false signals to make it difficult for victims to recognize the perpetrator's true intentions before it is too late, significantly increasing the risk [243], [294].

3. **Blackmail:**
   As soon as intimate content has been shared, the actual blackmail begins. Perpetrators threaten to publish the images or other content if the victim fails to comply with their demands. These typically include sending additional explicit content, financial payments or other compensation [318]. On top of this, perpetrators rely on exerting immense emotional pressure through the use of statements such as "I thought you loved me" to trigger feelings of guilt. The threat of being exposed on social media considerably increases the victims' anxiety. A particularly insidious method sometimes employed by perpetrators is to even threaten self-harm or suicide [306].

   The dynamics of such an attack are particularly problematic as they build up a momentum which is difficult to halt. In 27 percent of sextortion cases, the initial extortion is followed by further demands, which forces the victims into a spiral from which they can hardly escape [295]. Even when victims try to break off all communication, the perpetrators often succeed in re-establishing contact – often by way of alternative platforms or other fake identities. This tactic serves to reinforce the feelings of hopelessness and isolation victims experience, bringing them back under the control of the perpetrators [295].

   In many cases, the compromising content merely serves as a means of pressurizing the victims. According to studies, 70 percent of victims who refused to pay the blackmailers report that their images were not published after all [68]. This makes it clear that

the threat is often only aimed at impelling victims to comply with their demands without any actual intention to publish the material.

Perpetrators use a wide range of strategies depending on the target and situation:

- **Social Engineering:**
  Perpetrators use psychological tricks such as social engineering to gain the trust of their victims. This involves behaving empathetically and asking questions designed to promote emotional dependency. Information gathered over a period of weeks or months is later used as a means of exerting pressure [243], [294].

- **Automated attacks:**
  In addition to tailored strategies, perpetrators also rely on automated campaigns. Generic phishing emails are often used in this regard – claiming, for instance, that the victim's webcam has been hacked, and that the perpetrator has obtained pictures or videos of sexual acts. While such threats are often fictitious, they aim to exploit the victim's fears. Payments are usually demanded in cryptocurrencies such as Bitcoin, as they are difficult to track and trace [100], [222].

- **Use of deepfake technology:**
  The availability of deepfake technologies has taken the methods employed by sextortion offenders to a whole new level. Perpetrators generate deceptively real images or videos from their victims' public or shared data which appear to show them in compromising situations. According to recent findings, fakes comprise around 11 percent of extortion materials [295]. In addition, these fakes are also disseminated in extremist online forums in order to isolate victims and put them under further pressure [9]. The content often appears so authentic that it is rarely questioned by those involved. According to Europol, usage of deepfakes is increasing rapidly. These technological advances significantly increase the psychological pressure on victims, as the deception is barely recognizable [46], [100].

- **Other methods:**
  Perpetrators count on deceitful promises, such as modeling contracts, money or online betting vouchers, to lure victims or persuade them to send photos of themselves [306]. The use of chatbots which simulate human communication is also observed to be on the rise [324].

Along with the different phases of an attack and the various strategies perpetrators employ, two main variants of sextortion can be distinguished [174]:

1. **Contact-based sextortion:**
   As described in the majority of cases, perpetrators contact and manipulate their victims directly via social media or messenger services with the goal of obtaining compromising content, which is then used as leverage to make further demands [174].

2. **Data leak based sextortion:**
   However, the danger of criminals gaining access to private information, for instance passwords, through security gaps or data leaks should not be underestimated. Often, perpetrators claim to have compromising content that does not actually exist [162], [174], [222].

5.3 WHO IS IMPACTED? TARGET GROUPS AND RISK FACTORS

Sextortion impacts people of all ages and from all social backgrounds around the world, with certain groups being at particularly high risk [112]. Adolescents comprise one of the most frequently targeted groups [78], [215].

There are clearly discernible differences with regard to gender. Boys and men are more commonly the victims of sex-related blackmail, as perpetrators target the use of compromising content to impose financial or other demands. Girls and women, on the other hand, increasingly fall victim to either sexual harassment or the non-con-

sensual dissemination of explicit images or videos (revenge porn), especially by former partners [78], [215].

Studies reveal that male teenagers between the ages of 14 and 17 fall victim to sextortion above average [68], [78], [215], [231], [295], [306], [326]. Perpetrators specifically aim to exploit the emotional insecurity and often careless use of digital media by adolescents to allow them to build trust and extort intimate content [294].

In cases where the gender is known, 98 percent of the victims are male, of whom 38 percent are under the age of 18 [68]. Perpetrators often manipulate boys by posing as young women and making contact via social networks or online gaming [324], [326]. Boys often feel more confident than girls in their ability to distinguish between real and fake content on the Internet, which actually makes them more susceptible to targeted manipulation [211]. They also tend to use passwords less cautiously, communicate more frequently with strangers online and are more active in communities where abuse such as sextortion is common, for example in online gaming environments or certain social networks [113], [190], [211], [287]. Added to this, a strong need for social recognition, a lack of digital education and the indiscriminate use of social networks also increase susceptibility to sextortion [318], [324].

Teenagers aged between 14 and 18 tend to use social networks and messaging services particularly intensively, putting them at an increased risk of sexting or sharing private content imprudently [190], [318]. Young people spend up to six hours online every day, with platforms such as Instagram, Snapchat, TikTok and Brawl Stars, an online game with a chat feature, being used especially intensively [27], [190]. These platforms offer perpetrators easy access to victims, as teenagers often share personal content without being aware of the risks. Insufficient parental control and a lack of education about digital risks also contribute significantly to adolescents becoming easy victims [98].

However, sextortion offenders also set their sights on adult victims. Men between the ages of 30 and 50 appear to be particularly at risk, as they often have financial resources, a prominent social status and family obligations which make them vulnerable to blackmail [132]. When it comes to adult (male) victims, perpetrators often send out phishing emails in which they claim to have hacked the victim's webcam, or use dating platforms such as Tinder or Bumble to gain trust and obtain intimate content under false pretenses. Women, especially influencers, are also increasingly falling victim to sextortion, often in conjunction with cyberstalking [112].

5.4 PSYCHOLOGICAL AND SOCIAL IMPACT

Sextortion has profound psychological and social repercussions, which are multi-faceted and often go far beyond the acute moment of stress. These effects are particularly serious for adolescents, as individuals in this age group often do not yet have the emotional maturity and resources to cope with such threats. Support from both school and family are of crucial importance, along with political measures to promote digital skills [27].

Research on cyberbullying has shown that the anonymity of the perpetrators amplifies the power imbalance between offender and victim, intensifying feelings of insecurity and helplessness on the part of the victim. This anonymity and lack of clarity about who is behind the threats also play key roles in sextortion and serve to undermine trust in digital spaces [213], [316]. In addition, the potentially wide-ranging reach of digital platforms heightens fears of public humiliation [213].

For the victims, sextortion results in far more than feelings of shame, fear and self-doubt. The so-called "double hit" [327] is particularly distressing for those impacted. In addition to financial losses, the victim often experiences the emotional rupture of a relationship that had been perceived as valuable. Studies reveal that this emotional loss and disappointment often outweigh the financial damage [327]. Many victims blame themselves for their situation, especially if they have voluntarily shared intimate content. In some cases, perpetrators coerce their victims into engaging in unwanted sexual acts, causing particular distress [133], [327]. This shame and self-

recrimination often prevent victims from confiding in others or seeking help. Studies show that many victims withdraw completely from their social environments, leading to additional psychological and social problems in the long term [112], [318]. Many victims also report insomnia, social isolation and paranoia, as they constantly fear the publication of the compromising content. In extreme cases, this stress can lead to suicidal thoughts [112], [207], [214], [224], [318], [332], [333] and in the worst cases to self-harm or suicide [27].

Cyberbullying can have equally devastating consequences for teenagers and children from the age of 10, as it increases the likelihood of suicidal thoughts substantially. Studies have established that 16 percent of young people have had some experience with digital violence [27]. This figure is on the rise, emphasizing the urgent need to implement preventive measures aimed at promoting digital skills and better protecting young people from such threats.

The cases of Jordan DeMay or Amanda Todd[1] show how devastating the consequences of sextortion and cyberbullying can be. The 15-year-old Canadian committed suicide in her parental home on October 10, 2012, after two previous attempts had failed, having been exposed to threats and humiliation on the Internet since 2010. Even changing schools several times could not help. Her tormentor, Aydin Coban from the Netherlands, has been in prison since 2017 for blackmailing other men and women in the USA, Canada and the UK. This example shows how closely sextortion is related to other forms of digital and physical violence, not to mention the grave outcomes such offenses may lead to. The case also illustrates how sextortion can have a lasting impact on the lives of the victims and those in their social environments [112], [318], [333]. The effects are also felt by society as a whole. They manifest themselves in the form of declining attainment of educational qualifications, health problems and an increased need for therapeutic interventions [21], [163].

5.5 LEGAL FRAMEWORKS AND CRIMINAL INVESTIGATION

Sextortion is not clearly defined as a distinct criminal offense under German law. Instead, several sections of the German Criminal Code (StGB) may apply, depending on the context and manner of offense. These range from extortion and sexual coercion to the distribution of child pornographic materials.

- **§ 253 StGB (extortion):** Applicable when perpetrators threaten to reveal or publish intimate content in order to enforce payments or other demands [59], [137].
- **§ 238 StGB (stalking):** This section, which criminalizes stalking, applies in cases where a perpetrator repeatedly threatens or exerts prolonged pressure on a victim [59].
- **§ 184b and § 184c StGB (distribution of child and adolescent pornographic content):** These sections apply if minors are impacted or if intimate images of minors are used as a means of exerting pressure [59], [137], [231].
- **§ 176b StGB (sexual abuse of children):** Intimate recordings and images resulting from sexting can also be punishable in sextortion scenarios, and may be considered child sexual abuse when used as a means of exerting pressure [59], [231].

A global comparative analysis shows that sextortion is not always defined as a separate legal concept in other countries either. In the USA, for instance, sextortion is not listed as a specific criminal offense but is rather covered by existing laws such as extortion or child pornography [333].

The prosecution of sextortion cases poses considerable challenges, as perpetrators use digital technologies to conceal their identities and impede investigation.

Another key challenge is the reluctance of victims to report offenses. Surveys have revealed that less than one fifth of the affected respondents had reported the

1 https://www.amandatoddlegacy.org

offense to the police [259], [318], [333]. In this regard, a fear of not being taken seriously also plays a role. This hesitancy results in a high number of cases going unreported, making it difficult to systematically combat the phenomenon.

Despite all of these challenges, German and international law enforcement agencies are making progress in the fight against sextortion. Innovative approaches and international cooperation play key roles in the success of these investigations:

- **Tracking and tracing cryptocurrencies:** Analyzing flows of money has established itself as a key forensic approach in the fight against cybercrime. Specialized software solutions (e.g., Chainalysis) make it possible to investigate payment flows and trace suspicious transactions in order to identify criminal networks [99], [222].

- **International cooperation:** Working in close cooperation with Europol and Interpol facilitates cross-border investigation and enables the dismantling of global networks. An international police operation, for instance, led to the discovery of a transnational sex trafficking ring which had extorted at least USD 47,000 from victims [152].

- **Raising the awareness of the platform operators:** Social networks and communication services are increasingly being drawn into prevention work. Platform operators such as Instagram and WhatsApp are encouraged to report suspicious activities and develop mechanisms for early detection [241].

This combination of technological, legal and cooperative approaches underlines the complexity of combating sextortion. Nevertheless, effectively tackling the perpetrators and the digital infrastructures they rely on remains a crucial challenge.

5.6 PREVENTION AND INTERVENTION: STRATEGIES AGAINST SEXTORTION

Taking preventive measures is essential in the fight to reduce the number of sextortion cases. Education, technological protective measures and social commitment play key roles in this process. One of the first steps is to recognize warning signs at an early stage.

Warning signs can be detected both in the everyday behavior of those affected as well as in their online actions. Victims often suddenly withdraw from social activities, show fear of notifications or messages, hide their smartphones or computers, or suffer from sleep disorders and loss of appetite. Online, risks often manifest themselves through receiving friend requests from strangers or suddenly being asked intimate or personal questions [306].

Education and activities to raise awareness play essential roles in informing adolescents and adults about the dangers of digital blackmail. Schools should disseminate information on preventive measures, while also promoting the safe use of social networks and secure handling of personal data. Parents should have regular conversations with their children to make them aware of potential threats and let them know that they can always find support if they get into a difficult situation. It is essential that these conversations be non-accusatory and focus on the fact that anyone could fall victim to sextortion – regardless of their age, gender or behavior [58], [103], [231], [306].

In addition, technological safeguards help to prevent sextortion. Platforms such as Instagram and WhatsApp have introduced security mechanisms such as two-factor authentication and automatic detection of suspicious activity. Using secure, hard-to-guess passwords and being wary of suspicious links in emails are also important measures. Regularly checking and fine-tuning their privacy settings on social media platforms also provides users with added protection. Beyond this, regularly updating operating systems and antivirus programs minimizes the risk posed by malware such as infostealers. Continuous protection of one's digital identity by using

monitoring services which check for data leaks in the deep, dark and surface webs also supports prevention. Covering webcams when they are not in use additionally reduces the risk of unauthorized recordings [231], [306].

Safety-conscious behavior in the digital space is a key aspect of prevention. Users should be careful not to accept friend requests from strangers and carefully consider what they choose to share with the world.

Should one fall victim to sextortion nonetheless, it is imperative to follow these recommendations:

- **Do not comply with any demands:** It is important not to make monetary payments or fulfill other demands such as sending (more) pictures or videos [231], [306].
- **Keep calm and seek support:** A non-judgmental attitude from allies such as parents, friends or counseling centers is crucial. Counseling services such as "Weisser Ring", which provides support to victims of crime in Germany, offer quick and professional assistance.
- **Secure the evidence:** All relevant content such as chat histories or messages should be recorded and saved, for example by way of screenshots [306].
- **Break off all contact:** Offenders should be blocked and further messages ignored [231].
- **Take legal action:** Reporting the offense to the central point of contact for cybercrime (ZAC) and informing the platform operators are essential steps in getting any content removed that has already been published.

However, long-term prevention also requires social commitment at all levels. It is essential to break down taboos surrounding sexual content, so that victims can seek help at an early stage without fear of being judged. At the same time, it is crucial that psychological and legal support is easily accessible.

Close cooperation between policymakers, educational institutions and tech companies is indispensable in order to protect victims and take action against this type of crime.

Sextortion represents a serious threat, which can be combated through a combination of preventive measures, technological innovation and social action. Only through a joint effort involving educational institutions, law enforcement agencies and society as a whole can we prevent these attacks – which target the most vulnerable members of our society – and avert harm over the long term.

APPENDIX

ABOUT SCHWARZ GROUP AND SCHWARZ DIGITS

Schwarz Group is an international leader in the retail industry with about 13,900 stores and 575,000 employees in 32 countries. In the 2023 fiscal year, the companies of Schwarz Group generated a total sales volume of 167.2 billion euros. Their unique ecosystem lets them cover the full value cycle: from production and retail to recycling and digitalization. They create solutions to make the lives of billions of people safer, healthier and more sustainable, both right now and in the future – they act ahead. Lidl and Kaufland form the pillars of the food retail market and are an integral part of their 7.2 billion customers' daily lives. Many of the own-brand products and much of the sustainable packaging on their shelves come directly from Schwarz Produktion. Through its recycling management solutions, the environmental service provider PreZero promotes a functional circular economy and is investing in a clean future. The IT and digital division, Schwarz Digits, provides compelling digital products and services that meet the high German data protection standards, thus ensuring the maximum degree of digital sovereignty. As a partner service provider, Schwarz Corporate Solutions assists the companies of Schwarz Group with all matters related to administration, HR, operational activities and everything in between.

Schwarz Digits is the IT and digital division of Schwarz Group and offers impressive digital products and services that meet the high German data protection standards. With the aim of achieving the greatest possible digital sovereignty, Schwarz Digits provides the IT infrastructure and solutions for the extensive ecosystem of Schwarz Group's companies and develops it for the future. In addition, Schwarz Digits creates optimal conditions for the development of trend-setting innovations for end customers, companies and public sector organizations. Schwarz Digits includes 7,500 employees of the brands Schwarz IT, Schwarz Digital, STACKIT, XM Cyber, Lidl e-commerce, Kaufland e-commerce, Schwarz Media and mmmake.

DEFINITIONS & ABBREVIATIONS

GLOSSARY OF DEFINITIONS

Advanced Persistent Threat (APT)	An Advanced Persistent Threat is a sophisticated, long-lasting threat from highly skilled cybercriminals.
Backdoor	A backdoor provides secret, unauthorized access to a target environment or system.
Bot/Botnet	A bot is a remotely controllable malware installation on a host system. The term "botnet" refers to a network of bots that can be controlled remotely via C2 channels. The compromised systems can be instructed to download additional malicious payloads or send stolen data back to the attacker.
Command and control (C2)	Command and control (C2) describes a client/server infrastructure or any number of techniques an attacker can employ to communicate with and control compromised computer systems which have been integrated into a botnet, for example. C2 generally consists of surreptitious communication channels between target systems and platforms controlled by attackers.
Common Vulnerabilities and Exposure (CVE)	Common Vulnerabilities and Exposure is a system run by an independent organization, which assigns a unique identifier to known security vulnerabilities in software and catalogs them.
Cybercrime-as-a-Service (Caas)	Cybercrime-as-a-Service (CaaS) is a construct in which criminals commit crimes on a contract basis, usually in return for financial compensation, and are provided with the tools to carry out these offences.
DevOps	DevOps (a portmanteau word made up of development and operations) is an approach which improves collaboration between software development and IT operations to deliver software faster, more reliably and with higher quality.
DevSecOps	DevSecOps (a portmanteau word made up of development, security and operations) is an approach that already takes application security into account early on in the development process by integrating security measures into the working processes of developers and IT operations teams.
(Distributed) Denial-of-Service	A Denial-of-Service (DoS) attack aims to disrupt or sabotage the availability of services, systems or networks. If such an attack is carried out by several systems in parallel, it is referred to as Distributed DoS (DDoS).
Malware / Malicious Code	Malware or malicious code is software, or a snippet of it, which has specifically been developed to execute undesired, harmful functions on a system.
Malware-as-a-Service	Malware-as-a-Service is a business model in which cybercriminals rent or sell malware to other criminals for a fee.
Managed Security Service Provider	A Managed Security Service Provider is a company to which cybersecurity and IT security is outsourced.
Man-in-the-Middle	Man-in-the-middle (MitM) is a technique in which attackers manage to position themselves between a victim and a legitimate service. This mechanism can also be used to overcome authentication measures such as MFA.
Multi-factor Authentication (MFA)	In multi-factor authentication (MFA), the identity of a user accessing a system is confirmed by way of multiple authentication factors from a variety of categories (verification of biometric features, knowledge query or proof of ownership).
One-Time Password (OTP)	A one-time password is a single-use password which increases the security of online transactions or access to sensitive data.

Phishing	Phishing is derived from “password fishing”. Using fake websites, emails or other messages, cybercriminals carry out phishing campaigns as a way of obtaining the personal data of their potential victims or to trick them into performing harmful actions.
Ransomware	Ransomware is a type of malware which encrypts files on systems. Attackers use it to extort ransom money. In return, they promise to hand over the decryption key.
Ransomware-as-a-Service (Raas)	Ransomware-as-a-Service (RaaS) involves making ransomware or other offers relating to ransomware attacks available as a service. RaaS is a sub-category of CaaS.
Session Hijacking	Session Hijacking is a method in which cybercriminals take over the active session of another user and gain unauthorized access to their accounts or data.
Security Information and Event Management	Security Information and Event Management is a system for collecting, analysing and monitoring security events in an IT environment to detect and ward off threats.
Security Operations Center	A Security Operations Center is a central unit within an organization which monitors the IT security and responds to security incidents.
Social Engineering	Social engineering is an approach used by cybercriminals to exploit perceived human weaknesses such as fear, curiosity or blind obedience to deceive their victims into disclosing sensitive information, bypassing protective measures or installing malware.
Spear Phishing	Spear Phishing is a targeted form of phishing, in which attackers gather specific information about their victims in order to send them personalized, deceptively convincing emails containing malware or links to fake websites.
Threat Intelligence	Threat Intelligence is the collection, analysis and interpretation of information about potential threats a company or organization may be exposed to, e.g., cyberattacks, espionage or sabotage.
The Onion Router (TOR)	The Onion Router is a network that facilitates the anonymous, encrypted exchange of data over the internet by routing the data traffic through multiple connected computers.
Vishing	Vishing is a form of phishing where the attacker tries to trick their victim into revealing confidential information by way of fraudulent phone calls.
Whaling	Whaling is a form of spear phishing which sets its sights on high-ranking leaders and managers.
Zero-day Exploit / Zero-day Vulnerability	Vulnerabilities in a system or software can be exploited by attackers. An exploit is the lever – for instance, a code fragment which enables adversaries to technically exploit the vulnerability. Zero-day exploits are a special class of vulnerability, because neither the manufacturer nor the operator of the system or software is aware of their existence.

LIST OF ABBREVIATIONS

ADRIOS	Active Debris Removal In-Orbit Servicing
AI	Artificial Intelligence
AitM	Adversary-in-the-Middle
API	Application Programming Interface
APT	Advanced Persistent Threat
ARR	Annual Recurring Revenue
ASAT	Anti-satellite weapons
ASIC	Application-Specific Integrated Circuit
b	billion
BKA	German Federal Criminal Police Office
BSI	German Federal Office for Information Security
BYOD	Bring Your Own Device
CaaS	Cybercrime-as-a-Service
CATI	Computer Assisted Telephone Interview
CCM	Continuous Controls Monitoring
CEO	Chief Executive Officer
ChatGPT	Chat Generative Pre-Trained Transformer
CISA	Cybersecurity and Infrastructure Security Agency
CI/CD	Continuous Integration / Continuous Delivery
CNAPP	Cloud Native Application Protection
COVID	Coronavirus Disease
CRA	Cyber Resilience Act
CSA	Cloud Services Appliance
CTEM	Continuous Threat Exposure Management
CTI	Cyber Threat Intelligence
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DARPA	Defense Advanced Research Projects Agency
(D)DoS	(Distributed) Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Leakage Prevention
DoD	U.S. Department of Defense
EDR	Endpoint Detection and Response
EMP	Electromagnetic Pulse
ENISA	European Network and Information Security Agency
ESA	European Space Agency
EU	European Union
EUIBA	European Union Institutions, Bodies and Agencies
EV	European Interconnected System
FBI	Federal Bureau of Investigation
FIDO	Fast Identity Online
FLOP	False Load Output Prediction
FUD	Fear, Uncertainty, Doubt
FVEY	Five Eyes
GB	Gigabyte
GBP	British Pound Sterling
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
G(en)AI	Generative AI
GEO	Geostationary Earth Orbit
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GPWS	Ground Proximity Warning System
GRC	Governance, Risk Management and Compliance
GRU	Russian Military Intelligence Organization
GSM(A)	Global System for Mobile Communications (Association)
GUGI	Russian Main Directorate of Deep-Sea Research
IAM	Identity and Access Management
IBM	International Business Machines Corporation
ICT	Information and communications technology
IDS	Intrusion Detection Systems

IHK	German Chamber of Commerce and Industry
ILS	Instrument Landing System
IO	Information Operations
IOC	Indicator of Compromise
IOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Internet Protocol
IR	Incident Response
IRIS²	Infrastructure for Resilience, Interconnectivity and Security by Satellite
ISO	International Standards Organization
IT	Information Technology
IT-SiG	German IT Security Act
IWF	Internet Watch Foundation
JIT	Just in Time
KRITIS	Critical Infrastructures
LEEF	Log Event Extended Format
LEO	Low Earth Orbit
LKA	State Criminal Police Office
LLM	Large Language Model
LPV	Localizer Performance with Vertical Guidance
LTE(-M)	Long Term Evolution (for Machines)
m	Million
MDR	Managed Detection and Response
MEO	Medium Earth Orbit
MFA	Multi-factor Authentication
MitM	Man-in-the-Middle
ML	Machine Learning
MSSP	Managed Security Service Provider
MTTD	Mean Time to Detect
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NDR	Network Detection and Response
NHS	National Health Services
NIS	Network and Information Security Directive
NIS2UmsuCG	NIS 2 Implementation and Cyber Security Strengthening Act
NTN	Non-Terrestrial Networks
OMB	U.S. Office of Management and Budget
ORB	Operational Relay Box
OSS	Open-Source Software
OT	Operational Technology
OTP	One-Time Password
PAN	Palo Alto Networks
PKS	Police Crime Statistics
PoC	Proof of Concept
PoV	Proof of Value
PSIRT	Product Security Incident Response Team
PV	Photovoltaics
RaaS	Ransomware-as-a-Service
ROV	Remotely Operated Vehicle
SCA	Source Code Analysis
SCSR24	Schwarz Cybersecurity Report 2024
SDLC	Software Development Lifecycle
SIEM	Security Information and Event Management
SLAP	Speculative Load Address Prediction
SME	Small and Medium-sized Enterprises
SOAR	Security Orchestration Automation and Responses
SOC	Security Operations Centre
SQL	Structured Query Language
SSCS	Software Supply Chain Security
SSH(D)	Secure Shell (Daemon)
SSRF	Server Side Request Forgery
StGB	German Criminal Code
TLPT	Threat-Led Penetration Testing
TN	Terrestrial Network
TOR	The Onion Router
UI	User Interface
USD	US Dollars

UX	User Experience
VIN	Vehicle Identification Number
VPN	Virtual Private Network
VTC	Video Teleconference
WAF	Web Application Firewall
WHO	World Health Organisation
XDR	Extended Detection and Response
XML	Extensible Markup Language
ZAC	Central Points of Contact for Cybercrime of the Federal and State Police
ZDE	Zero-Day Exploit
ZIT	Central Office for Combating Internet and Cyber Crime

REFERENCES

[1] Aggarwal, R. (2025). "Who was DeepSeek?", January.

[2] Agora Strategy (n.d.). "How Geopolitics Changes the Global Cyber Threat Landscape".

[3] Aiyer, B., Caso, J., Russel, P. & Sorel, M. (2022). "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers", McKinsey & Company.

[4] Akamai (2024). "Alles, was Sie über die XZ Utils Backdoor wissen müssen", April 1.

[5] Akerlof, G. A. (1970). "The Market for Lemons: Quality and the Market Mechanism", The Quarterly Journal of Economics, 84(3), pp. 488-500

[6] Akshay, J., Moschetta, G., Winslow, E. (2025). "Global Cybersecurity Outlook 2025", World Economic Forum.

[7] Ali, R. (2021). "Looking to the future of the cyber security landscape", Network Security 3, 8-10.

[8] Alspach, K. (2024). "CISA Breached Via Ivanti VPN Vulnerabilities: Report', CRN, March 8.

[9] Alto Intelligence (2024). "Blame the Women. Incels, loneliness and new security threats emerging from the digital sphere".

[10] America's Cyber Defense Agency (2024). "Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways", CISA, February 29.

[11] Andrea, D. M. (2024). "Cybersecurity Outlook for 2025: The Shifting Threat Landscape", KLR, November 21.

[12] Anti-Phishing Working Group (APWG) (2024). "Phishing Activity Trends Report 3rd Quarter 2024", October 14.

[13] Antoniuk, D. (2025). "Slovakia registry cyberattack disrupts land, agriculture services", The Record, January 10.

[14] Apostle, J., Harrison, A., Kawkabani, R., Hewitt, H. & Hardan, O. (2024). "NIS2: Where do European Countries Stand on Implementing Cybersecurity Strategies?", Orrick.

[15] Apple, C. (2024). "ACT closes its first year with 3,500+ cybersecurity tools and several new high-risk communities", Global Cyber Alliance, December 17.

[16] Ariganello, J. (2022). "More is Less: The Challenge of Utilizing Multiple Security Tools", Anomali, April 13.

[17] Atlantic Council (2025). "Scowcroft Center for Strategy and Security".

[18] AWS (2024). "Was ist SDLC (Software Development Lifecycle)?".

[19] Axon, L., Bouckaert, J., Creese, S., Akshay, J. & Saunders, J. (2025). "Artificial Intelligence and Cybersecurity: Balancing Risks and Rewards", World Economic Forum.

[20] Ayenson, M., Forte, E., Mager, M., Bousseaden, S., Groenewoud, R., Nakajima, A., DeJesus, T., Ibarra, J., Pease, A., Donaher, C., Kerr, D., Uhlmann, J., Erkailo, T., King, J., VanNice, A., Faouzi, A, Suryanarayana, S. & Wilhoit, C. (2024). "Elastic Security Labs Global Threat Report 2024", Elastic Security Labs.

[21] Baams, L., Talmage, C. A. & Russell, S. T. (2017). "Economic costs of bias-based bullying" School psychology quarterly, in: APA PsycNet, 32(3), p. 422.

[22] Banco Santander, S. A. (2024). "Statement", May 14.

[23] Barlett, C. P., Simmers, M. M., Roth, B. et al. (2021). "Comparing cyberbullying prevalence and process before and during the COVID-19 pandemic", in: J Soc Psychol, June 15, 161(4): pp. 408-418.

[24] Beiersmann, S. (2024). "Tunnelvision: Exploit umgeht VPN-Verschlüsselung", ZDnet, May 8.

[25] Beuth, P. (2024). "Nicht nur die CDU wurde über Check-Point-Schwachstelle gehackt", Spiegel Netzwelt, June 13.

[26] Beuth, P., Flüpke, Hoppenstedt, M., Kreil, M., Rosenbach, M. & Wilkin, R. (2024). "Wir wissen, wo dein Auto steht", Der Spiegel, December 27.

[27] Bhatnagar, B. & Hancock, J. (2024). "One in six school-aged children experiences cyberbullying, finds new WHO/ Europe study", WHO, March 27.

[28] Bitkom (2024). "Erstmals mehr als 10 Milliarden Euro für Deutschlands Cybersicherheit", October 23.

[29] Bitkom (2024). “Social Engineering: Wenn der Hacker sich als Kollege ausgibt”, October 11.

[30] Bitkom (2024). “Wirtschaftsschutz 2024”, August 28.

[31] Böhm, M. (2023). “FBI erzielt Erfolge gegen berüchtigte Hackergruppe”, Spiegel Netzwelt, December 20.

[32] Born, G. (2024). “Neue Warnung vor Schwachstelle CVE-2024-3400 in Palo Alto Networks Firewalls”, Born City, April 27.

[33] Bracha, H. S. (2014). “Freeze, flight, fight, fright, faint: Adaptationist perspectives on the acute stress response spectrum”, CNS Spectrums 9(9), 679-685.

[34] Bradley, T. (2024). “Illuminating The Dark Corners Of Cyber Defense With Identity”, Forbes, September 17.

[35] British Library (2023). “Cyber Incident Update: Information & FAQ's”.

[36] Brumfiel, G. (2019). “Trump Tweets Sensitive Surveillance Image Of Iran”, NPR.

[37] Brumfield, C. (2024). “Hijack of monitoring devices highlights cyber threat to solar power infrastructure”, CSO Online.

[38] Buchanan Technologies (2024). “Manged SIEM Pricing & Costs”.

[39] Bueger, C. & Liebetrau, T. (2023). “Critical maritime infrastructure protection: What's the trouble? Marine Policy,”, 155, p. 105772.

[40] Bundesamt für Naturschutz (2021). “Seekabel”.

[41] BSI (n.d.). “Die Kryptografie hinter Passkey”.

[42] BSI. (n.d.). “Social Engineering – der Mensch als Schwachstelle”.

[43] BSI (2023). “Die Lage der IT-Sicherheit in Deutschland 2023”, November 2.

[44] BSI (2024). “Aktive Crime-Gruppen in Deutschland”, November 22.

[45] BSI (2024). “CyMon – der Cybersicherheitsmonitor”.

[46] BSI (2024). “Die Lage der IT-Sicherheit in Deutschland 2024”, November 12.

[47] BSI (2024). “Einfluss von KI auf die Cyberbedrohungslandschaft”, April 30, pp. 4, 10.

[48] BSI (2024). “Fehlerhaftes Update von Crowdstrike Falcon”, July 19.

[49] BSI (2024). “Ivanti Cloud Services Appliance Schwachstellen werden aktiv ausgenutzt”, September 20.

[50] BSI (2024). “Kritische Backdoor in XZ für Linux”, April 3. CSW-Nr. 2024-223608-1132, Version 1.1.1.

[51] BSI (2024). “Umsetzung der NIS-2-Richtlinie für die regulierte Wirtschaft”, July 24.

[52] BSI (2024). “Zero-Day Schwachstellen bei CyberAngriffen auf verschiedene Ivanti-Produkte genutzt”, March 1.

[53] BSI (2024). “Version 1.4: Zero-Day Schwachstellen bei Cyber-Angriffen auf verschiedene Ivanti-Produkte genutzt”, March 1.

[54] BSI (2025). “Wahlen in Deutschland 2025”.

[55] Bundesamt für Verfassungsschutz (BfV) (2024). “BfV Cyber Insight – The i-Soon-Leaks: Industrialization of Cyber Espionage”, Bundesamt für Verfassungsschutz – Counter Intelligence.

[56] Bundesamt für Verfassungsschutz (BfV) (2024). “Gefährdung der Bundestagswahl durch unzulässige ausländische Einflussnahme”.

[57] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) (2024). “Cyberversicherungen: hohe Nachfrage – und hohe Risiken?”, February 7.

[58] BKA (2022). “Sextortion: Das Bundeskriminalamt warnt vor sexueller Erpressung im Internet“, October 21.

[59] BKA (2023). “Polizeiliche Kriminalstatistik Bundesrepublik Deutschland. Straftatenkatalog 2023. V 1.0”.

[60] BKA (2024). “Bundeslagebild Cybercrime 2023”, May 13, pp. 17, 24.

[61] BKA (2024). “Cybercrime: Festnahmen in Hessen und Rheinland-Pfalz – Erneuter Schlag gegen Underground Economy im Internet”, November 1.

[62] BKA (2024). “Durchsuchungen bei mutmaßlichen Anführern der Online-Gruppierung ‚New World Order‘”, September 3.

[63] BKA (2024). “Erfolgreicher Schlag gegen die Infrastruktur von digitalen Geldwäschern der Underground Economy”, September 19.

[64] BKA (2024). “Operation ‚Endgame‘: Bundeskriminalamt und internationalen Partnern gelingt bisher größter Schlag gegen weltweite Cybercrime”, May 30.

[65] BKA (2024). "Operation ‚Power OFF': weltweiter Schlag gegen Cybercrime-Infrastruktur", December 11.

[66] BKA (2025). "Internationale Operation Talent: Abschaltung von nulled.to und cracked.io".

[67] Business Wire (2024). "Message from the International Cable Protection Committee: Recent Events Involving Submarine Cables in the Red Sea".

[68] Canadian Centre for Child Protection (C3P) (2022). "An Analysis of Financial Sextortion Victim Posts".

[69] CASIO Computer Co., Ltd. (2024). "Casio issues apology and notice concerning personal information leak due to unauthorized access to server", October 18.

[70] Chanel, O. & Chichilnisky, G. (2009). "The influence of fear in decisions: Experimental evidence". Journal of Risk and Uncertainty 39, 271-298.

[71] Check Point Team (2024). "2025 Cyber Security Predictions – The Rise of AI-Driven Attacks, Quantum Threats, and Social Media Exploitation", October 28.

[72] Clark, H. (2024). "What is the Software Development Life Cycle (SDLC)?", The Product Manager, October 29.

[73] Colvin, T., Karcz, J. & Wusk, G. (2023). "Office of Technology, Policy, and Strategy Cost and Benefit Analysis of Orbital Debris Remediation", NASA Office of Technology, Policy, and Strategy.

[74] Constantin, L. (2024) "Top 7 zero-day exploitation trends of 2024", CSO Online, December 23.

[75] Copelouzos Group (2024). "'GREGY' Interconnector – Copelouzos Group".

[76] Coveware (2024). "Quarterly Report".

[77] Creaplus (2023). "Too many solutions can make your organization less secure".

[78] Cross, C., Holt, K. & Holt, T. J. (2023). "To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud", in: Criminology & Criminal Justice, February 11, 0(0).

[79] CrowdStrike (2024). "Technical Details: Falcon Content Update for Windows Hosts", CrowdStrike Executive Viewpoint, July 20.

[80] Cybersecurity and Infrastructure Security Agency (CISA) (2023). "Zero Trust Maturity Model – Version 2.0", Cybersecurity Division.

[81] Cybersecurity and Infrastructure Security Agency (CISA) (2024). "Mobile Communications Best Practice Guidance | CISA".

[82] Cybersecurity and Infrastructure Security Agency (CISA) (2024). "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure", February 7.

[83] Datensicherheit.de (2020). "Software: 76% der Anwendungen mit mindestens einer Sicherheitslücke".

[84] Deere & Company (2023). "Deere Debuts New Planting Technology & Electric Excavator During CES 2023".

[85] Deloitte (2024). "Global Future of Cyber Survey 2024", October 22.

[86] Deutschlandfunk (2025). "Sabotage in der Ostsee. Was steckt hinter der Zerstörung der Unterseekabel?", January 20.

[87] Di Battista, A., Grayling S., Játiva, X., Leopold, T., Li, R., Sharma, S. & Zahidi, S. (2025). "World Economic Forum Future of Jobs Report 2025", World Economic Forum.

[88] Dr. Datenschutz (2024). "Kritische Linux XZ-Backdoor bedroht digitale Infrastruktur", April 19.

[89] Drive Lock (2024). "Cyberangriffe auf OT: Warum Unternehmen dringend in OT-Sicherheit investieren müssen", April 24.

[90] Epp, S. (2024). "KI-Angriffe mit KI-Abwehr schlagen", Security Insider, September 19.

[91] Eschlberger, S., Vereno, D., Polanec, K. & Neureiter, C. (2024). "Introducing Cybersecurity Toolbox: A modelling framework for smart grid security".

[92] Europäische Union (2022). "Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive)".

[93] European Commission (2024). "IRIS2 | Secure Connectivity – European Commission", defence-industry-space.ec.europa.eu.

[94] European Space Agency (2024). "Active Debris Removal".

[95] European Space Agency (2024). "Sentinel-1B Successfully Passivated – Sentinel Online", Sentinel Online.

[96] European Union Agency for Cybersecurity (ENISA) (2024). "ENISA Threat Landscape 2024", September 19, pp. 7-8, 13-14, 26, 28, 46, 50-51, 53, 78-80, 83.

[97] European Union Agency for Cybersecurity (ENISA) (2024). "Foresight Cybersecurity Threats for 2030 – Update".

[98] European Union Agency for Law Enforcement Cooperation (Europol) (2017). "Online sexual coercion and extortion as a form of crime affecting children Law enforcement perspective", June 19.

[99] European Union Agency for Law Enforcement Cooperation (Europol) (2022). "Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab", April 28.

[100] European Union Agency for Law Enforcement Cooperation (Europol) (2024). "Internet Organised Crime Threat Assessment 2024", July 22, p. 10, 12, 24.

[101] Falco, G. (2024). "Hybrid Space-Submarine Architecture Ensuring Infosec of Telecommunications (HEIST)".

[102] FasterCapital (n.d.). "Angstmarketing Die Psychologie der Angst Ihre Auswirkungen auf Geschaeft und Marketing verstehen".

[103] Federal Bureau of Investigation (FBI) (n.d.). "Sextortion".

[104] Federal Communications Commission (2016). "STATEMENT OF COMMISSIONER JESSICA ROSENWORCEL".

[105] Financial Times (2024). "Delta Airlines sues CrowdStrike over $500mn losses from flight cancellations", January 17.

[106] Fischer, S. M. & Bilz, L. (2024). "Mobbing und Cybermobbing an Schulen in Deutschland: Ergebnisse der HBSC-Studie 2022 und Trends von 2009/10 bis 2022", in: Journal of Health Monitoring, pp. 46-67.

[107] Flügge, A. (n.d.). "Die Komplexität von Softwaresystemen", Object Systems.

[108] Frankfurter Allgemeine Zeitung (2024). "40 Jahre Haft wegen Verrat von CIA-Hackerprogrammen", February 2.

[109] Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM (2024). "Cyber Resilience Act: Drei Sofortmaßnahmen für Unternehmen", October 11.

[110] Fraunhofer-Institut für System- und Innovationsforschung ISI, im Auftrag von TA-SWISS Stiftung für Technologiefolgen-Abschätzung (2024). "Deepfakes und manipulierte Realitäten", June 18.

[111] Fuest, B. (2024). "Und dann fällt dem Microsoft-Mitarbeiter eine halbe Sekunde Verzögerung auf", Welt, April 12.

[112] Gámez-Guadix, M., Mateos-Pérez, E., Wachs, S., Wright, M., Martínez, J. & Íncera, D. (2022). "Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting ('revenge porn') among adolescents", in: Journal of Adolescence, 94(5), pp. 789-799.

[113] Gámez-Guadix, M., Sorrel, M. A. & Martínez-Bacaicoa, J. (2023). "Technology-facilitated sexual violence perpetration and victimization among adolescents: A network analysis", in: Sexuality research and social policy, 20(3), pp. 1000-1012.

[114] Gartner (2022). "Gartner Identifies Top Security and Risk Management Trends for 2022", March 7.

[115] Gartner (2024). "Gartner Forecasts Global Information Security Spending to Grow 15% in 2025", Gartner, August 28.

[116] Gartner (2024). "Information Security Spending: What does the future hold?", November 27.

[117] Generalstaatsanwaltschaft Karlsruhe (2025). "Anklage gegen mutmaßlichen Cybererpresser der Württembergischen Staatstheater Stuttgart".

[118] Gillin, P. (2024). "Cybersecurity tool sprawl is out of control – and it's only going to get worse", SiliconeANGLE, August 5.

[119] Govan, C. (2023). "Unlocking Satellite Connectivity: IoT's Reign of Coverage", floLIVE.

[120] Grealy, A. (2024). "KI-gestützte Cybersicherheit: Prognosen für das Jahr 2025", Armis, December 16.

[121] Greenberg, A. (2024). "Emerging Threats: Cybersecurity Forecast 2025", Google Cloud, November 13.

[122] Greene, T.C. (2002). "MS Struggles to discredit Linux", The Register, January 2.

[123] GSM Association (2024). "Massive IoT | Internet of Things | GSMA", Massive IoT.

[124] Hansen, S. (2023). "Cybersecurity Paradox: How too many solutions makes you less secure", Cryptomathic, June 2.

[125] Haufe (2024). "Cyber Resilience in Deutschland: Ein alarmierender Bericht", November 14.

[126] Hays (2024). "Global Cyber Security Report 2024 – Beyond Traditional Cyber Talent".

[127] Hayward, L. (2023). "Global Navigation Satellite System (GNSS) and Satellite Navigation Explained", Advanced Navigation.

[128] Hase, M. (2019). "Definition. Was ist Vendor Lock-in?", September 20.

[129] Heise online (2024). "CDU-Angriff: Lücke in Check Point Gateway soll Einfallstor gewesen sein", June 3.

[130] Henderson Vaughan, E. (2024). "NCMEC Releases New Sextortion Data", in: NCMEC, April 15.

[131] Hennigan, W.J. (2024). "What One Russian Satellite Tells Us About the Future of Nuclear Warfare. The New York Times", December 5.

[132] Henry, N. & Umbach, R. (2024). "Sextortion: Prevalence and correlates in 10 countries", in: Computers in Human Behavior, Volume: 158.

[133] Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A. & Scott, A. J. (2020). "Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery", in: Routledge, June 11.

[134] Herder, C. (2024). "CISA Takedown of Ivanti Systems Is a Wake-up Call", Dark Reading, July 9.

[135] Hiscox (2024). "Hiscoy Cyber Readiness Report 2024".

[136] Holtermann, F. (2025). "DeepSeek könnte heimlich OpenAI-Daten abgeschöpft haben", Handelsblatt, January 29.

[137] Horten, B., Steffan, C., Weinand, M. & Brettel, H. (2024). "Kriminologischer Beitrag: Sextortion – Intime Aufnahmen als Druckmittel.", in: Journal Club, June 21.

[138] Hotarek, F. (2023). "Die Identitätssicherheit als Basis von Zero Trust", it-daily.net, August 13.

[139] Hradický, J. M., Strauszová, K. & Strapeková, O. (2024). "GLOBSEC Grid Transition Index 2024", GLOBSEC Grid Transition Index 2024.

[140] Hubback, J. (2020). "Research Report: Cybersecurity Technology Efficacy. Is cybersecurity the new 'market for lemons'?".

[141] Hughes, M. & Temsamami, K. (2025). "Capturing the cybersecurity dividend" IBM Institute for Business Value.

[142] IBM Corporation (n.d.). "Was ist Cyber-Resilienz?".

[143] IBM Corporation (2024). "IBM Security X-Force Threat Intelligence Index 2024".

[144] IBM Corporation (2024). "Cost of a Data Breach Report 2024".

[145] Information Systems Audit and Control Association (ISACA) (2024). "State of Cybersecurity 2024", October 1, pp. 31-32.

[146] Insikt Group (2024). "H1 2024: Malware and Vulnerability Trends Report", Recorded Future, September 10.

[147] Intel 471 (2024). "The 471 Cyber Threat Report 2024", May 6.

[148] International Committee of the Red Cross (n.d.). "Cyber and information operations".

[149] International Monetary Fund (IMF) (2025). "GDP, current prices in billions of US dollars".

[150] International Telecommunication Union Development Sector (2024). "Measuring digital development – Facts and Figures 2024", ITU Publications.

[151] Internet Watch Foundation (IWF) (2023). "Hotline reports 'shocking' rise in the sextortion of boys", September 18.

[152] INTERPOL (2022). "Asia: Sextortion ring dismantled by Police", September 5.

[153] IT-Sicherheit (2024). "Mehr Widerstandsfähigkeit für OT-Systeme", July 3.

[154] Janis, I.L. (1982). "Decisionmaking under stress", In Goldberger, L., Breznitz, S. (eds.) Handbook of stress. New York: Free Press, pp. 69-87.

[155] Jaschinsky, M. (2025). "Aktuelle Netzfrequenz (47,5-52,5Hz) – Netzfrequenz.info", NETZFREQUENZ.

[156] Jaye Tillson, J. (2024). "The Crumbling Castle", Cyber Defense Magazine, February 2.

[157] Joos, T. (2024). "Die Gefahren von Schatten-IT", IP Insider, May 8.

[158] Kern, M., Landauer, M., Skopik, F. & Weippl, E. (2024). "A logging maturity and decision model for the selection of intrusion detection cyber security solutions". Computers & Security 141, 103844.

[159] Kim, J., van Schaik, S., Genkin, D. & Yarom, Y. (2023). "iLeakage: Browser-based Timerless Speculative Execution Attacks on Apple Devices".

[160] Klein, D. (2021). "Relying on firewalls? Here`s why you'll be hacked", Network Security 1, 9-12.

[161] Knop, D. (2024). "Kritische Fortinet-Sicherheitslücke wird angegriffen", Heise Online, October 10.

[162] Koch, M.-C. (2024). "Sextortion-Fälle in den USA: Kriminelle schicken Bilder von der Umgebung mit", in heise, September 5.

[163] Kochenderfer-Ladd, B., Ladd, G. W. & Thibault, S. A. (2021). "School bullying and peer victimization: Its role in students' academic achievement" in: P. K. Smith & J. O. Norman (Eds.), The Wiley Blackwell handbook of bullying: A comprehensive and international review of research and intervention (pp. 619-638), March 15.

[164] Koopman, E. (2024). "Remote Code Execution on Ivanti Products Found in the Wild", CliftonLarsonAllen, February 19.

[165] Kovacs, E. (2024). "Casio Confirms Data Breach as Ransomware Group Leaks Files", Security Week, October 14.

[166] KPMG (2024). “Control System Cybersecurity Annual Report 2024”.

[167] KPMG (2024). “KPMG Cybersecurity Survey 2024”, May 13.

[168] Krämer, M.J. (2024). “XZ Utils-Vorfall: Open Source als Software Supply Chain-Falle”, ZDNet, April 9.

[169] Kreil, M. & Flüpke (2024). “Wir wissen wo dein Auto steht”, Media.ccc.de.

[170] Kuhlenkamp, F. (2024). “Angriffe auf die deutsche Wirtschaft nehmen zu”, Bitkom, August 28.

[171] Kuhlenkamp, F. (2024). “Erstmals mehr als 10 Milliarden Euro für Deutschlands Cybersicherheit ”, Bitkom, October 23.

[172] Labašová, D., Dančo, M. (2025). “Ransomware attack on Slovakia’s real estate register causes nationwide outage of all services and databases containing information on immovable property rights”, Kinstellar.

[173] Lakshmanan, R. (2024). “Researchers Uncover Vulnerabilities in Solarman and Deye Solar Systems”, The Hacker News.

[174] Landeskriminalamt Nordrhein-Westphalen (LKA NRW) (2020). “Erpressungsversuche via E-Mail. Präventionshinweise für Betroffene”.

[175] Landtag von Baden-Württemberg (2024). “Schlag gegen mutmaßliche Cybererpresser – hoher Schaden”, October 10.

[176] Landtag von Baden-Württemberg (2024). “Sextortion: Erpressungen mit Nacktaufnahmen nehmen zu”, May 27.

[177] Ledesma, J. (2023). “Why Aren’t Cybersecurity Tools Living up to the Hype?”, Bitdefender.

[178] Lenaerts-Bergmans, B. (2023). “Angriffsvektoren: Was sie sind und wie sie ausgenutzt werden”, CrowdStrike, December 7.

[179] Lister, T. & Fylyppov, O. (2022). “Russians plunder $5M farm vehicles from Ukraine - to find they’ve been remotely disabled”, CNN.

[180] Luber, S. & Schmitz, P. (2021). “Was ist Endpoint Detection and Response (EDR)?”, Security Insider, May 5.

[181] Lyngaas, S. (2024). “Cyberattack forces major US health care network to divert ambulances from hospitals”, CNN, May 10.

[182] Maloney, D. (2023). “Under The Sea: Optical Repeaters For Submarine Cables”, Hackaday.

[183] manager magazin (2002). “Globalstar: Jäher Absturz”.

[184] Mandiant (2024). “IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders”, Google Cloud Blog.

[185] McAfee, LLC (2024). “RockYou2024: das größte Kennwort-Datenleck in der Geschichte”, July 12.

[186] McKerchar, R. (2024). “Pacific Rim: Inside the Counter-Offensive — The TTPs Used to Neutralize China-Based Threats”, Sophos News.

[187] Mäurer, D.K. (2024). “Bedeutender Schlag gegen die Cybercrime-Szene”, Tagesschau, May 30.

[188] Malwarebytes Inc. (2024). “ThreatDown 2024 State of Ransomware”, August 20.

[189] Manuel, R. (2024). “Pro-Russia Hackers Attack Japanese Liberal Democratic Party Website”, The Defence Post, October 18.

[190] Medienpädagogischer Forschungsverband Südwest (2024): “JIM-Studie 2024 – Jugend, Information, Medien”.

[191] Metz, C. (2024). “OpenAI’s internal AI details stolen in 2023 breach, NYT reports”, Reuters, July 5.

[192] Microsoft Corporation (2024). “Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard”, January 19.

[193] Microsoft Corporation (2024). “Microsoft Digital Defense Report 2024”.

[194] Minchin, J. (2025). “Eagle S could have cut more cables, says Finnish police”, Lloyd’s List.

[195] Moody, R. (2025). “Ransomware roundup: 2024 end-of-year report”, Comparitech Ltd., January 9.

[196] Moreno. E (2024). “Ist Ihr Unternehmen wirklich gegen Cyberangriffe versichert?”, Chemie Technik, March 18.

[197] Morgan, E. (2024). “Eroding Global Stability: The Cybersecurity Strategies Of China, Russia, North Korea, And Iran”, Irregular Warfare, August 1.

[198] Müller, Dr. D. (2024). “KI befeuert Cyber-Angriffstechniken”, IT-Business, February 16.

[199] Munro, K. (2024). “GPS Spoofing: It’s About Time, Not Just Position”, PenTestPartners.

[200] Mutzbauer, J. (2024). “Phishing-Attacke: Deutschlandweiter Hackerangriff auf IHK-Unternehmen”, CSO online, March 18.

[201] Naraine, R. (2024). “Ivanti CEO Vows Cybersecurity Makeover After Zero-Day Blitz”, Security Week, April 4.

[202] National Audit Office (2025). “Cyber threat to UK government is severe and advancing quickly, spending watchdog finds”.

[203] National Coordination Office for Space-Based Positioning, Navigation, and Timing (2023). "GPS.gov: Timing Applications", Gps.gov.

[204] Nawrocki, M. (2024). "DDoS Attacks Against Japan", NetScout, October 17.

[205] Netgate (2024). "The Top Cybersecurity Statistics for 2024".

[206] NHS England London (2024). "Update on cyber incident: clinical impact in South East London – Friday 14 June 2024".

[207] Nilsson M. G., Tzani-Pepelasis C., Ioannou M. & Lester D. (2019). "Understanding the link between Sextortion and suicide", in: International Journal of Cyber Criminol 13(1):55–69.

[208] Norddeutscher Rundfunk (NDR) (2024). "Cyberangriff auf Landesbehörden in MV: Internetseiten lahmgelegt", May 24.

[209] North Atlantic Treaty Organization (NATO) (2024). "Cyber defence", July 30.

[210] North Atlantic Treaty Organization (NATO) (2025). "NATO launches 'Baltic Sentry' to increase critical infrastructure security".

[211] Office of Communications (Ofcom) (2024). "Children and Parents. Media Use and Attitudes Report", April 19.

[212] O'Flaherty, K. (2024). "CrowdStrike Reveals What Happened, Why—And What's Changed", Forbes, August 7.

[213] O'Higgins Norman, J. (2020). "Tackling bullying from the inside out: Shifting paradigms in bullying research and interventions", in: Internation Journal of Bullying Preventition 2(3):161–169.

[214] O'Malley, R. L. (2023). "Short-term and long-term impacts of financial Sextortion on victim's mental well-being", in: Journal of Interpers Violence 38(13–14):8563–8592.

[215] O'Malley, R. L. & Holt, K. M. (2022). "Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime", in: Journal of interpersonal violence, 37(1-2), 258-283.

[216] Österreichische Rundfunk (ORF) (2024). "Cyberangriffe auf ÖVP und SPÖ", September 23.

[217] Ohm, M., Plate, H. Sykosch, A. & Meier, M. (2020). "Backstabber's Knife Collection: A Review of Open Source Software Supply Chain Attacks".

[218] OpenKRITIS (2024). "NIS2-Umsetzungsgesetz: Neuerungen für die Cybersicherheit in Deutschland".

[219] OpenVPN (2023). "Navigating Cybersecurity: Choosing Between All-In-One Platforms and Point Solutions".

[220] OPSGROUP Team (2024). "GPS Spoofing: Final Report of the GPS Spoofing WorkGroup", GPS Spoofing: Final Report.

[221] OPSWAT (2024). "Was ist OT Security?", July 2.

[222] Paquet-Clouston, M., Romiti, M., Haslhofer, B. & Charvat, T. (2019). "Spams meet cryptocurrencies: Sextortion in the bitcoin ecosystem", in: ACM Digital Library, pp. 76-88.

[223] Parasoft (2023). "Aufbau von Resilienz in der Softwareentwicklung: Zurück zu den Grundlagen", December 18.

[224] Patchin, J. W. & Hinduja, S. (2020). "Sextortion among adolescents: 'Results from a national survey of U.S. youth.'", in: Sexual Abuse: A Journal of Research and Treatment, 32(1), 30–54.

[225] Patnaik, A. (2024). "Rising Tide of Software Supply Chain Attacks: An Urgent Problem", DarkReading, September 12.

[226] Petrosyan, A. (2024). "Estimated cost of cybercrime worldwide 2018-2029", Statista, July 30 (Data for 2025).

[227] Pfaffenberger, B. (2000). "The rhetoric of dread: Fear, uncertainty, and doubt (FUD) in information technology marketing". Knowledge, Technology & Policy 13, 78-92.

[228] Pfliegl, K. (2024). "CrowdStrike: Das waren die Folgen für deutsche Unternehmen", Digital Business, September 20.

[229] Phillips-Wren, G. & Adya. M. (2020). "Decision making under stress: the role of information overload, time pressure, complexity, and uncertainty", Journal of Decision Systems 29, 213-225.

[230] Pluta, W. (2008). "Iridium-Insolvenzverfahren beendet", Golem.de.

[231] Polizeiliche Kriminalprävention (n.d.). "Sextortion. Vom harmlosen Flirt zur organisierten Erpressung".

[232] Polizeiliche Kriminalprävention der Länder (ProPK) & Bundesamt für Sicherheit in der Informationstechnik (BSI) (2024). "Cybersicherheitsmonitor 2024: Kurzbericht zur Befragung zur Cybersicherheit".

[233] Portuguese Space Agency (2020). "ADRIOS (Active Debris Removal/ In-Orbit Servicing)", Portugal Space Agency.

[234] Poudel, S. S. (2024). "XZ Utils Backdoor: Sicherheitslücke in der Software-Supply-Chain", It-Sicherheit, April 17.

[235] Poulsen, K. (2010). "Hacker Disables More Than 100 Cars Remotely", Wired.

[236] Powell, A. & Henry, N. (2019). "Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults", in: Journal of Interpersonal Violence, Volume: 34(17), pp. 3637-3665.

[237] PricewaterhouseCoopers GmbH (PwC) (2024). "Cybersecurity + geopolitical conflict: What boards and CEOs should know and act upon", January 15.

[238] PricewaterhouseCoopers GmbH (PwC) (2024). "Digital Trust Insights 2025".

[239] Privette, M. (2025). "The State of the Cybersecurity Market in 2024".

[240] Pultarova, T. & Howell, E. (2025). "Starlink: SpaceX's satellite internet project", Space.com.

[241] Raffile, P., Goldenberg, A., McCann, C. & Finkelstein, J. (2024). "A digital pandemic: uncovering the role of 'yahoo boys' in the surge of social media-enabled financial sextortion targeting minors", in: NCRI, January 30.

[242] Rathert, T. (2024). "State of Ransomware 2024: 500 Prozent höhere Lösegeldzahlungen", connect, 6 May.

[243] Ray, A. & Henry, N. (2025). "Sextortion: A Scoping Review. Trauma, Violence, & Abuse", in: Sage Journmals Volume: 26(1), 138-155.

[244] Reuters Staff (2024). "Finnair pauses some Estonia flights due to GPS interference. Reuters", April 29.

[245] Ribeiro, A. (2024). "Growing convergence of geopolitics and cyber warfare continue to threaten OT and ICS environments in 2024", February 18.

[246] Rojoef, M. (2024). "Pro-Russia Hackers Attack Japanese Liberal Democratic Party Website", The Defense Post, October 18.

[247] Roman, N. (2024). "Global Status Of Anti-Satellite (ASAT) Weaponry And Testing | ACE", The Alliance for Citizen Engagement.

[248] Rundfunk Berlin-Brandenburg (RBB) (2024). "AfD Brandenburg meldet Hackerangriff auf Internetseite", August 29.

[249] Rupp, C. (2024). "Navigating the EU Cybersecurity Policy Ecosystem", interface, June 27.

[250] Scarfone, K. (2024). "Die größten OT-Bedrohungen und Security-Herausforderungen", Computer Weekly, August 30.

[251] Schirrmacher, D. (2024). "Nach mehreren IT-Security-Vorfällen: Ivanti gelobt in offenem Brief Besserung", Heise Online, April 8.

[252] Schubert, F. (2024). "Sicherheitslücken in Ivanti Connect Secure VPN", Leipziger Zeitung, December 2.

[253] Schultze-Krumbholz, A., Höher, J., Fiebig, J. et al. (2014). "Wie definieren Jugendliche in Deutschland Cybermobbing? Eine Fokusgruppenstudie unter Jugendlichen einer deutschen Großstadt", in: Praxis der Kinderpsychologie und Kinderpsychiatrie, 63 (2014) 5, pp. 361-378.

[254] Schwartz, K.D. (2024). "Can you have too many security tools?", CIO, August 29.

[255] Schwarz Digits (2024). "Eine quantitative Befragung der Unternehmen in Deutschland zum Thema Cybersecurity".

[256] Seaton, W. & Pandit, K. (2024). "New VPN Risk Report: 56% of Enterprises Attacked via VPN Vulnerabilities", Zscaler, May 7.

[257] Security Insider (2024). "Internationale Ermittler zerschlagen ‚schädlichste Hackergruppe der Welt'", Security Insider, February 21.

[258] Singh, N. (2024). "Palo Alto Networks Surveys the State of OT Security", Palo Alto, March 20.

[259] SINUS (2023). "Ergebnisse einer Repräsentativ-Umfrage unter Jugendlichen 2023/2023".

[260] Skadden (2024). "Navigating the New Cybersecurity Landscape: Key Implications of the EU's NIS 2 Directive", October 11.

[261] SkAI Data Services and Zurich University of Applied Sciences – Centre for Aviation (2024). "Live GPS Spoofing and Jamming Tracker".

[262] Snider, S. (2024). "Snowflake Denies Responsibility for Ticketmaster, Santander Breaches", Information Week, June 3.

[263] Sokolov, D. (2024). "Zerodays bei Ivanti aktiv genutzt: Connect Secure und Policy Secure sinds nicht", Heise Online, January 10.

[264] Sonatype (2024). "10th Annual State of the Software Supply Chain".

[265] Sophos Ltd. (2024). "Sophos 2024 Threat Report: Cybercrime on Main Street", March.

[266] Spanien aktuell (2025). "Rekordsumme: Ransomware-Opfer zahlen 2024 fast 460 Millionen US-Dollar", January 1.

[267] Splunk (2024). "State of Security: The Race to Harness AI".

[268] Stadt Aschaffenburg (2024). "Hackerangriff: Rathaus am Montag wieder geöffnet", November 15.

[269] Stankovski, A., Gjorgiev, B., Locher, L. & Sansavini, G. (2023). "Power Blackouts in Europe: Analyses, Key insights, and Recommendations from Empirical Evidence", Joule, 7(11), pp. 2468-2484.

[270] Starcke, K. & Brand, M. (2012). "Decision making under stress: A selective review. Neuroscience & Biobehavioral Reviews", 36(4), 1228-1248.

[271] Stary, V. (2024). "Kaspersky stellt Cybersecurity-Trends für 2025 vor", Netzwoche, November 19.

[272] Statista (2022). "Estimated costs of cybercrime globally 2016-2027".

[273] Statista (2024). "Cybersecurity – Worldwide".

[274] Statista (2024). "Estimated cost of cybercrime worldwide 2018-2029".

[275] Statista (2024). "Number of common IT security vulnerabilities and exposures (CVEs) worldwide from 2009 to 2024 YTD".

[276] Stöckel, M. (2025). "Datenleck bei KI-Startup: Chatverläufe von DeepSeek frei zugänglich im Netz", Golem.de, January 30.

[277] Subbotin, A. (2024). "CrowdStrike-Ausfall: Globaler IT-Stillstand und Workaround", Byte Snipers, July 19.

[278] Süddeutsche Zeitung (2024). "Sextortion: Vom Flirt zur Erpressung", October 29.

[279] Sutton, H.I. (n.d.). "H I Sutton – Covert Shores".

[280] Sutton, H.I. (2020). "How Russian Spy Submarines Can Interfere With Undersea Internet Cables", Forbes, August 19.

[281] Tagat, A., Phokeer, A. & Kreitem, H. (2024). "Net Loss: an Econometric Method to Measure the Impact of Internet Shutdowns", ACM Journal on Computing and Sustainable Societies, 2(2).

[282] Tagesschau (2024). "Die schleichende Gefahr vor der Europawahl", May 31.

[283] Tagesschau (2024). "Konzerktkarten-Verkäufer Ticketmaster – 560 Millionen Kunden von Hackerangriff betroffen", June 1.

[284] Tagesschau (2024). "Schwerer Cyberangriff auf die CDU", June 1.

[285] Tagesschau (2024). "Verfassungsschutz warnt vor Beeinflussung der Wahl", November 29.

[286] Tagesschau (2025). "Schweden geht nicht mehr von Sabotage aus", February 3.

[287] Tak, S. & Catsambis, S. (2023). "Video games for boys and chatting for girls?: Gender, screen time activities and academic achievement in high school", in: ifip Educ Inf Technol 28, 15415–15443.

[288] Tang, Y., Dananjayan, S., Hou, C., Guo, Q., Luo, S. & He, Y. (2021). "A Survey on the 5G Network and Its Impact on agriculture: Challenges and Opportunities", Computers and Electronics in Agriculture, 180, p. 105895.

[289] Taylor, R. (2024). "Managed IT Services Pricing: What to expect in 2024", Cybercommand, July 26.

[290] TeleGeography (2019). "Submarine Cable Map".

[291] TeleGeography (2022). "Submarine Cable FAQs".

[292] The Tor Project, Inc (2019). "Tor Project: Overview".

[293] The White House (2021). "Executive Order on Improving the Nation's Cybersecurity", The White House, Briefing Room, May 12.

[294] Thiel, C. (2020). "Liebesschwindel im Cyberspace", in: Rüdiger B (Hrsg) Cyberkriminologie. Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden, pp. 241–267, April 1.

[295] Thorn & National Center for Missing and Exploited Children (NCMEC) (2024). "Trends in Financial Sextortion: An investigation of sextortion reports in NCMEC CyberTipline data", June 24.

[296] Tidy, J. (2024). "Dead in 6 hours. How Nigerian sextortion scammers targeted my son", in: BBC, June 9.

[297] Tokmetzis, D. (2024). "Almost 200 Russian Ships Suspected of Spying in the North Sea", Follow the Money – Platform for Investigative Journalism.

[298] Toulas, B. (2024). "Cisco warns of large-scale brute-force attacks against VPN services", Bleeping Computer, April 16.

[299] Toulas, B. (2025). "New Apple CPU side-channel attacks steal data from browsers", BleepingComputer, January 28.

[300] Trevino, A. (2024). "Acht häufige Angriffsvektoren, die Unternehmen kennen müssen", Keeper Security, April 4.

[301] Trio Team (2024). "Die Bedeutung der XZ-Backdoor-Bedrohung verstehen: Ein verdeckter Einbruch in Open-Source-Software", October 20.

[302] TÜV NORD GROUP #explore (2020). "Tiefseekabel als Datenautobahn".

[303] TÜV Rheinland (2024). "Supply-Chain-Attacken".

[304] United Nations (2024). "United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes".

[305] United States Air Force Public Affairs (2018). "First GPS III Satellite Successfully Launched".

[306] United States Immigration and Customs Enforcement (ICE) (2024). "Sextortion".

[307] U.S. General Services Administration (2025). "SAM.gov", Sam.gov.

[308] Vaughan-Nichols, S. J. (2020). "How Microsoft went from Linux is a cancer to Microsoft Loves Linux", InsiderPro (archiviert), October 11.

[309] Vellante, D. & Bradley, E. (2024). "Breaking Analysis: Security budgets are growing but so is vendor sprawl", theCUBEResearch, April 27.

[310] Verbraucherzentrale (2024). "Umfrage: Account gehackt – das erwarten Betroffene von den Unternehmen", November 13.

[311] Verizon, (2024). "Data Breach Investigations Report 2024", July 11.

[312] Vicens, A.J. (2024). "Low-level cybercriminals are pouncing on CrowdStrike-connected outage", Cyberscoop, July 23.

[313] Vicens, A.J. (2024). "US adds 9th telcom to list of companies hacked by Chinese-backed Salt Typhoon cyberespionage", Reuters, December 27.

[314] Volpenhein, S. (2024). "Ascension was hacked after worker mistakenly downloaded malicious file Unclear how many patients' data exposed", Milwaukee Journal Sentinel, June 13.

[315] V. Samson, F. (2024). "Nach XZ-Backdoor: Open-Source-Software als Risiko oder strategischer Vorteil?", Heise Online, April 20.

[316] Waasdorp, T. E. & Bradshaw, C. P. (2015). "The overlap between cyberbullying and traditional bullying", in: Journal of adolescent health, 56(5), 483-488.

[317] Wall, M. (2024). "SpaceX launches 6th batch of next-gen US spy satellites from California (video)", Space.com.

[318] Walsh, W. A. & Tener, D. (2022). "If you don't send me five other pictures I am going to post the photo online: A qualitative analysis of experiences of survivors of sextortion", in: Journal of child sexual abuse, 31(4), 447-465.

[319] Walther, E. (2024). "Die Geopolitik hat Einzug in unsere Netze gehalten: Einblicke in den Cyber Underground", Handelsblatt Live, July 26.

[320] Wang, Q., Li, W., Yu, Z., Imran, M., Ansari, S., Sambo, Y., Wu, L., Li, Q. & Zhu, T. (2023). "An Overview of Emergency Communication Networks", Remote Sensing, 15(6), pp. 1595-1595.

[321] Weishaupt, J. (2019). "Competing in Space: Space-Based Weapons", October 31, Defense Visual Information Distribution Service.

[322] Weissmann, P. (2024). "NIS2 Umsetzungsgesetz", OpenKritis.

[323] Welter, I. (2024). "Der Kampf gegen Erpressung mit Nacktbildern", in: zdfheute, August 17.

[324] WeProtect Global Alliance (2024a). "A web of deceit. Financial sexual extortion of children and young people. Briefing Paper".

[325] WeProtect Global Alliance (2024b). "Tackling the rising incidence of financial sexual extortion, Takeaways from a cross-sector innovation forum", in: PA-consulting.

[326] Whitehurst, L. (2022). "FBI: Steep climb in teens targeted by online 'sextortion'", in: AP News, December 19.

[327] Whitty, M. T. & Buchanan, T. (2016). "The online dating romance scam: The psychological impact on victims-both financial and non-financial", in: Criminology & Criminal Justice, 16(2), 176–194.

[328] WirtschaftsWoche (2024). "CrowdStrike-Panne legte 8,5 Millionen Windows-Geräte lahm", July 21.

[329] Wiseman, J. (2022). "GPSJam GPS/GNSS Interference Map", gpsjam.org.

[330] Wisernotify (2025). "15 Fake Review Statistics You Can't Ignore (2025)".

[331] Wittenberg, K. (2024). "Sicherheitsexperten schlagen Alarm: Globale Welle von Hackerangriffen auf VPN-Dienste", Chip, April 19.

[332] Wolak, J. & Finkelhor, D. (2016). "Sextortion: Keys findings from an online survey of 1631 victims", in: Crime Against Children Research Center & Thorn.

[333] Wolak, J., Finkelhor, D., Walsh, W. & Treitman, L. (2018). "Sextortion of minors: Characteristics and dynamics", in: Journal of Adolescent Health, 62(1), 72–79.

[334] Yadav, Y. (2022). “India becoming sextortion capital of the world?”, in: The Times of India, March 9.

[335] ZDF heute (2024). “Bitkom: Mehr Cyberangriffe aus dem Ausland”, May 13.

[336] ZDF heute (2024). “Wahlbeeinflussung in Rumänien: Experte: Demokratien vor Desinformation schützen”, December 7.

[337] Zeit online (2024). “Cyberangriff auf überregionalen Krankenhausbetreiber”, October 14.

CYBER THREATS TIMELINE

2010 2013

- State-sponsored hacker group
- Criminal hacker group
- Hacktivists
- Global damage caused by cyberattacks (estimated) [1]

The cases presented here are only a selection and by no means complete.

Former NSA employee Edward Snowden leaks documents to journalists. They exposed the global surveillance programs run by the secret services of the USA and UK, leading to a public debate about the limits of state surveillance.

Edward Snowden leaks

Yahoo! data theft

Stuxnet worm

FIN7

DOUBLE DRAGON

LAZARUS GROUP SINCE 2009

Target data theft

COZY BEAR SINCE 2008

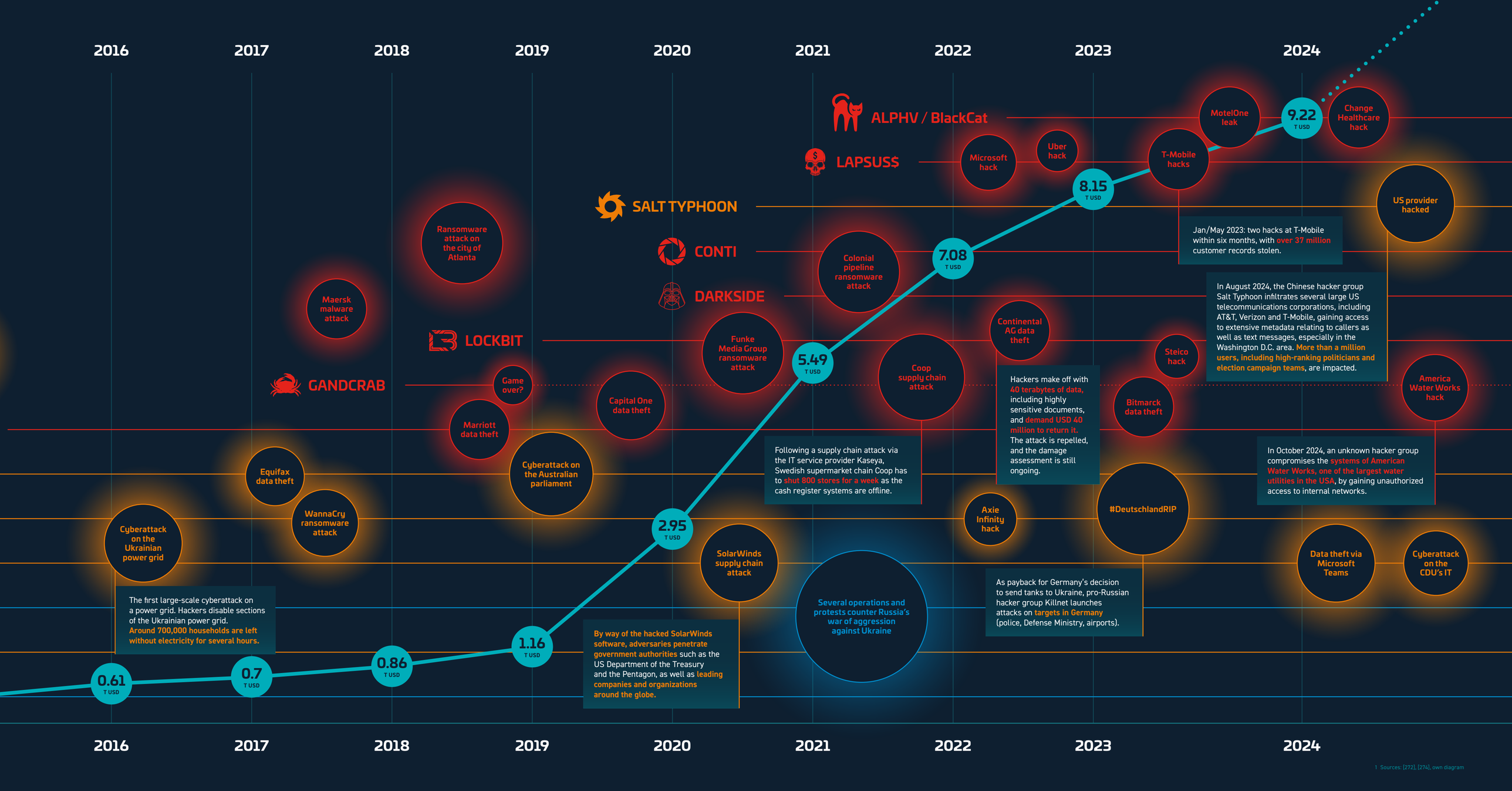
ANONYMOUS SINCE 2003

Operation Payback

EQUATION GROUP SINCE 2001

CULT OF THE DEAD COW SINCE 1984

2010 2013



1 Sources: [272], [274], own diagram

IMPRINT

PUBLISHER

Schwarz Digits KG
Stiftsbergstr. 1
74172 Neckarsulm
Germany

Registered Office: Neckarsulm
Local District Court: Stuttgart HRA 737212
Sales tax identification number: DE335467503

Email: info@schwarz-digits.de
Website: www.schwarz-digits.de

Scientific Director: Dr. Alexander Schellong

Authors: Dr. Henrike Helmer, PD Dr. Robert Koch,
Dr. Patricia Köpfer, Dr. Alexander Schellong, Tolga Yilmaz

Design: André Renvert, Lukas Breitkreutz (infotectures)

Schwarz Digits KG is represented by Ny-Stiftung, with its registered office in Dresden, Landesdirektion Sachsen, AZ 20-2245/589, which in turn is jointly represented by two board members with joint power of representation, including Mr. Christian Müller and Mr. Rolf Schumann.