schwarz digits

CYBER SECURITY REPORT 2026

EN

PREFACE

SOVEREIGNTY SHIELD – EUROPE'S DIGITAL ABILITY TO ACT UNDER THREAT

In cyberspace, the threat situation is anything but abstract. Every day we bear witness to criminal or state-sponsored cyberattacks. Cyberspace has become a battlefield on which combat is constant, uncontrolled, and uncompromising. In other words, the gloves are off. Aggressors are always one step ahead of those defending. Their goal is to shake the foundations of our economy, and the stability of our political and social order. Ever faster cycles of digital innovation are overwhelming the bureaucratic processes in many companies and organizations around the globe.

This report illustrates that cybercriminals are continuing to increase the intensity and professionalism of their attacks – boosted by artificial intelligence and collaborative business models that are effectively dismantling the technical barriers to launching cyberattacks. The private sector and public authorities, in stark contrast, tend to adopt a reactive stance. With economic damage estimated to have exceeded €202 billion in Germany alone, cybersecurity is no longer just an IT issue but a matter of survival for every CEO and institution. Imagine this damage were physical.

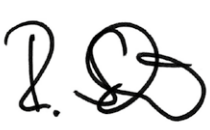
Digital sovereignty is rapidly becoming a strategic imperative. Entering into unilateral dependencies on non-European platforms means sacrificing the ability to act independently. Today, digital sovereignty indicates the ability to exercise self-determination across cyberspace – from business-critical data to AI models.

This report offers far more than an inventory of current risks. It provides:

- A representative Germany-wide survey: A detailed assessment of cybersecurity topics and digital sovereignty.
- Analysis of critical exposures: In-depth insight into the risks posed and potential offered by robotics and the frequently underestimated "digital estate".
- Putting digital sovereignty into operational practice: The first comprehensive application of the EU Cloud Sovereignty Framework in the context of the European software ecosystem, with insights into the assessment and management of software and AI sovereignty.
- Underlying principles for making strategic decisions: Why "exit-by-design" and European infrastructures lay the groundwork for a competitive future.

We invite you to use the following pages as a wake-up call and a roadmap. Our mission is to accomplish digital transformation without compromising on security and sovereignty.

For their valuable input, we would like to thank all the experts who contributed to this visionary report, as well as over 1,000 small and large companies that participated in the survey.



Rolf Schumann
Co-CEO Schwarz Digits

Christian Müller
Co-CEO Schwarz Digits

EXECUTIVE SUMMARY

This report provides a comprehensive analysis of the current cybersecurity situation, examining the structural consolidation of global threats, the growing convergence of physical and digital risks in robotics, and the critical discrepancy between the perceived resilience and operational reality at German companies. Another key area is the first ever application of the EU Cloud Sovereignty Framework to common enterprise software products, which marks a crucial step forward in making digital sovereignty measurable and practicable. The report generally strives to provide decision-makers across all levels of technical expertise with a concise, up-to-date overview of global threats and other less widely discussed topics relevant to cybersecurity and related fields.

Geopolitical risks and the new normal in cyber threats

This comparative analysis draws on global publications on cybersecurity released between summer 2025 and February 2026. The situation in 2025/26 is characterized by the entrenchment of structures and the convergence of existing threats. Cyberattacks are occurring in parallel with geopolitical developments and endangering national stability, global supply chains, and public order. The synergistic activities of state actors, criminals, and ideological groups are leading to an increasing confluence of espionage, sabotage, and exploitation. While hacktivism and critical infrastructure espionage are dominant in Europe, the sabotage of undersea cables and escalation of attacks on Taiwan – amounting to 2.63 million attacks per day – highlight the global dimension. Cloud convergence has heightened the focus on systemic risks. Ransomware, meanwhile, continues to operate as an industrialized, highly damaging and costly ecosystem. In Germany, cyberattacks now cause 70 percent of all economic damage (€202.4 billion). Recovery times of up to 30 days and debilitating psychological pressure on decision-making processes are especially critical as they directly undermine operational capacity.

The real impact of cyber security on the German economy

Our representative survey of 1,001 German companies reveals a deep discrepancy between perceived preparedness and structural resilience. While 65 percent of companies rate their defense readiness favorably, the rate of companies falling victim is in fact 20 percent (large enterprises: 33 percent). Cyber security budgets have increased to 17 percent of the IT budget, yet they remain reactive and largely driven by regulation (NIS 2). Deficiencies in management are reflected in the absence of CISOs (57 percent) and failure to conduct comprehensive risk analyses (40 percent). These shortcomings also extend to AI governance. Despite recognizing the risks posed by AI-based social engineering, only 25 percent of organizations have implemented binding guidelines.

The supply chain remains a critical security risk. Seventy-five percent of the companies surveyed still do not audit their suppliers, even though every second company has already become aware of attacks on suppliers. Finally, a high level of support for offensive countermeasures underscores the desire for the ability to take action in cyber defense. Seventy-nine percent of the respondents are in favor of government hackbacks, with 59 percent even calling for such powers to be extended to private actors. At the same time, there is a striking gap in the implementation of digital sovereignty. Eighty-seven percent of organizations have not invested in reducing their technological dependencies, despite 42 percent expressing a willingness to pay higher prices for sovereign solutions.

Robotics and the convergence of physical and digital security risks

The rapidly advancing integration of humanoid and autonomous systems into industrial manufacturing processes, national security agencies, and military structures marks a point of convergence where the boundary between physical and digital functionality is effectively erased. Modern robotic platforms are highly networked systems that combine mechanical mobility

with sensor-based data processing and artificial intelligence. Consequently, any technical vulnerability can directly lead to kinetic and operational consequences. When such systems are used in environments where security is critical, such as border security or armed conflicts, their reliability is entirely dependent on the integrity of the digital infrastructure. Experience gained from current conflicts, particularly in Ukraine, demonstrates how agile innovation processes, often supported by civil society, can modify robotic systems in a very short time – challenging the established, bureaucratic procurement cycles typical in Western states. This development necessitates a reassessment of the state's ability to take action in cyberspace, as mastery of these technologies is not only a matter of mechanical superiority, but primarily a question of digital sovereignty and the ability to secure complex supply chains for hardware and software.

Digital sovereignty as a strategic priority and operative performance indicator

Due to the changing geopolitical situation, digital sovereignty has evolved from a political goal to a strategic necessity that inextricably links national security, global competition, and organizational resilience. Published in October 2025, the EU's Cloud Sovereignty Framework (CSF) offers a structured approach for use in public tenders. The EU CSF still has some weaknesses and does not cover software or its deployment models in detail. Based on the CSF, a Software Sovereignty Framework (SSF) was developed to assess 27 software products in key enterprise software categories. While open-source solutions offered by European companies dominate the rankings, non-European proprietary platforms consistently receive low scores. Particularly when it comes to artificial intelligence, sovereignty criteria are currently more an aspiration than a reality. These outcomes show that in 2026 digital sovereignty is not achieved by means of a static certificate but rather needs to be managed actively through targeted technical and organizational measures. Sovereign cloud infrastructures also play a crucial role in the provision of sovereign software offerings.

The digital footprint left behind after death poses a systemic risk

One aspect of cybersecurity that is frequently underestimated is the ever-increasing fragmentation of digital identities, which extends far beyond the conscious use of specific services. While people often consider their digital footprint to be limited to a small number of services, the average user actually holds hundreds of digital accounts and leaves thousands of digital traces (e.g., comments on social networks, online and mobile behavior, purchases, location data from apps). Even after a person passes away, their digital legacy lives on as a target for attack. Identity theft and unauthorized access are increasingly achieved through the exploitation of valid user accounts, including those of deceased or inactive users. These legitimate login details naturally do not trigger any typical alert mechanisms. How large platforms go about managing these data sets raises ethical and emotional questions for the bereaved while also posing risks for companies and public authorities. Dealing professionally with one's digital estate and reducing one's digital footprint has thus become just as important as drawing up a will or inheritance contract, creating a living will, or transferring assets.

CONTENTS

CHAPTER 1

STATE OF PLAY
CYBERSECURITY TRENDS 2026

Facts & Figures on impacted countries

(2025, among the top 10 affected nations)

Ransomware victims

Average cost per data breach

State actor activities detected

GER
296
4.03 million US$
74

USA
3,769
10.22 million US$
623

GBR
283
4.14 million US$
144

CAN
387
4.84 million US$
51

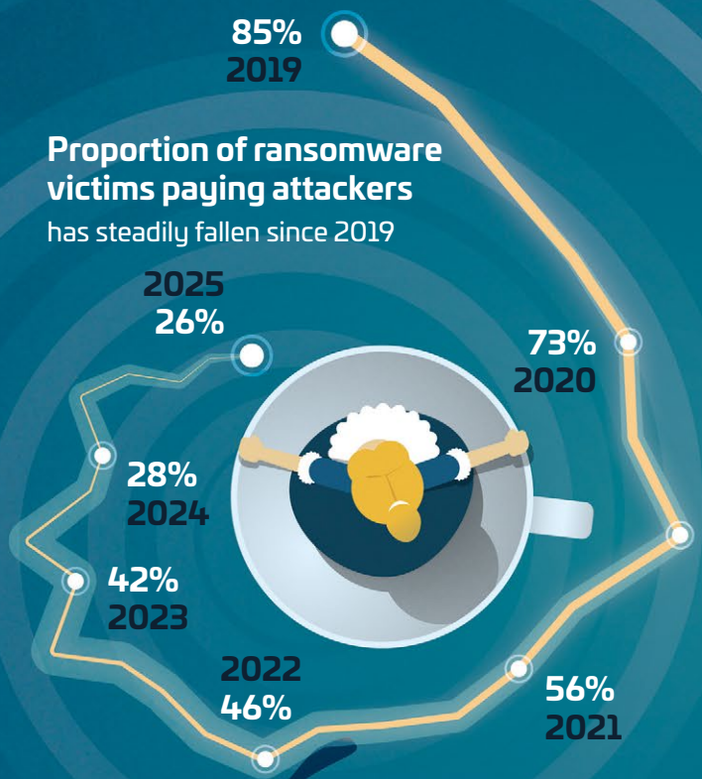
ITA
166
3.44 million US$
51

North Korean IT Operatives

infiltrate companies as remote workers

Proportion of ransomware victims paying attackers

has steadily fallen since 2019



Top 5 fields of investment

(in 20 countries around the globe)

- Technology **70%**
- Planning & preparation **68%**
- Human resources **67%**
- Training & awareness **66%**
- Insurance **65%**

Technical vectors of ransomware attacks

(2023–2025)

Prompt leakage attacks on leading LLM models and service providers

(success rate in %)

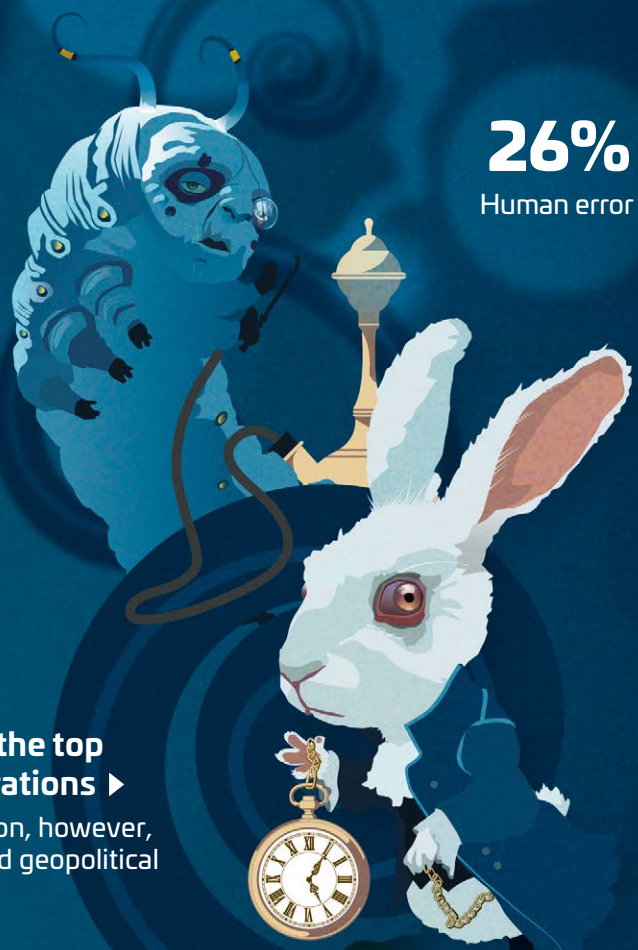
Cause of data breaches

(percentage across all impacted organizations)

51%
Malicious or criminal attack

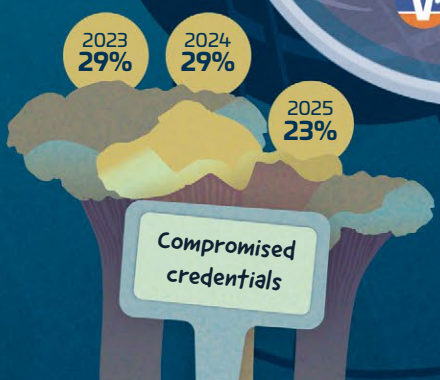
23%
Technical error / vulnerabilities

26%
Human error



Cyberattacks are the top global risk to operations

In strategic prioritization, however, they **rank 5th** – behind geopolitical and social crises



Modern multifactor authentication

reduces the risk of identity theft **by over 99%**

Source: [4], [49], [88], [109], [187], [241], [248], [316], [333], [337], [349], Own diagram

1 STATE OF PLAY – CYBERSECURITY TRENDS 2026

1.1 GLOBAL CYBERSECURITY OVERVIEW

The global cybersecurity situation is inextricably intertwined with geopolitical tensions. It is characterized by the interplay of cybercrime, political conflicts, and technological change in which state actors, cybercriminal networks, and ideologically motivated groups operate concurrently [28], [139], [286]. While they often use identical infrastructure and exploit the same vulnerabilities, these actors are pursuing a variety of different objectives, such as espionage, sabotage, extortion, and fraud [86], [139]. The scope and focus of these activities may also vary depending on the regional, political, and technological context. Consequently, cyberspace plays a dual role as both a field of attack and a driver for the development and positioning of security policy.

In highly digitalized economies, the economic repercussions extend from organizational damage to macroeconomic effects [348]. Cyberattacks increasingly play an integral part in hybrid conflicts [341]. These attacks especially have a negative impact on the stability of the state and public order [62], [73], [111], [132], [139], [140], [183], [347].

1.1.1 Geopolitical tensions and their impacts

Geopolitical tensions are increasingly the driving force behind digital attacks, influencing their intensity, targeting, and conception. States, state-sponsored actors, and ideologically motivated groups are specifically employing cyber operations as means of exerting political influence and deterrence. Their focus is less on causing short-term disruption to systems and more on gaining an intelligence advantage, influencing critical processes, and creating social insecurity [111], [139], [248], [347].

Given the global interconnectedness of communication, cloud, and service infrastructures, such operations are seldom confined within national borders. This means that cyber operations are conducted parallel to diplomatic, economic, and military developments, serving to reinforce existing conflict dynamics [111], [139].

The regional considerations outlined below illustrate how this geopolitically driven threat manifests itself in various regions of the world. The constellation of threat actors, targeted systems, and attack patterns differs depending on regional power relations, economic dependencies, and security policy priorities.

Europe

In Europe, the threat situation is characterized by a high proportion of hacktivist activities pursuing symbolic and media-related objectives. Between July 2024 and June 2025, 4,875 security-related incidents were recorded and classified according to whether they were perpetrated by cybercriminals, state actors, or hacktivists [111]. Phishing was the most common attack vector, accounting for 60 percent of all incidents, followed by the exploitation of vulnerabilities (21.3 percent) and botnet activities (9.9 percent) [111]. Around 79 percent of the incidents recorded have been attributed to hacktivist actors. These activities mainly took the form of DDoS attacks (overload attacks on IT services) or digital disruption. While the technical complexity of such attacks is usually low, the political and public impact is high [34], [111], [129]. In the field of telecommunications, DDoS attacks with peak loads of up to ten terabits per second were observed for the first time. Approximately 78 percent of the attack waves lasted less than five minutes [261].

In contrast, state-aligned activities have primarily taken the form of espionage aimed at gathering intelligence. Sectors such as telecommunications, transport, industrial production, and public administration are most affected. In this context, actors with links to Russia, China, and North Korea, among other countries, were named [111], [129], [131].

Regional crises within Europe quickly have international repercussions due to the globally interconnected nature of digital infrastructures. Compared to other regions of the world, Europe is more prone to politically motivated, publicly impactful attacks [111], [332]. Germany and Belgium are especially targeted by state-affiliated

actors, while France, Italy, and Poland experience the highest levels of hacktivist-motivated incidents [111]. This dynamic is exacerbated by Europe's structural dependence on US providers when it comes to cybersecurity technologies and threat analysis, restricting the EU's strategic sovereignty in repelling and combatting critical threats [274].

The Middle East

In the Middle East, the cyber threat situation is closely linked to regional power struggles and hybrid threat scenarios. Cyber operations are primarily instrumentalized for state security and influence strategies. They tend to go hand in hand with political, military, and economic tensions within a region [166], [203], [270].

Governments and state-affiliated actors strategically use digital attacks for the purpose of espionage, influence, and destabilization of state or economic institutions and systems. This weaponization by states is particularly evident in recurring, politically motivated cyber campaigns related to regional rivalries.

Groups closely affiliated with Iran are believed to be responsible for conducting targeted espionage against government agencies and subsequently publishing sensitive data. These cyber operations have an immediate political impact and are used specifically to exert strategic pressure against Israel [166], [270].

Countries such as the United Arab Emirates and Qatar are described as targets of politically motivated cyberattacks on government and infrastructure networks as well as being actively involved in national security operations and acting as regional collaboration hubs [166], [203].

Besides state-backed cyber operations, the region is also affected by cybercriminal activities [166]. In countries such as Egypt, cybersecurity is increasingly seen as a matter of national security and associated with increased statutory measures to safeguard government networks and critical infrastructure [91], [166], [298].

North America

In North America, the cyber threat situation is greatly influenced by the economic and technological significance of the region. Due to their high levels of digital penetration, the dense concentration of data-intensive industries, and the prominent role of global cloud and platform providers, the US and Canada are among the most attractive targets for cyberattacks worldwide [139], [140].

In stark contrast to the more symbolic attack patterns prevalent in Europe, attacks in the US mainly target high-value data sets, intellectual property, and business-critical infrastructures. Accordingly, economically motivated attacks aimed at unauthorized access, identity theft, and the targeted compromise of digital environments tend to predominate. These often result in the large-scale exfiltration of data [140].

Apart from cybercriminal activities, an increased presence of state and state-affiliated actors has also been noted. North America is considered a strategic target for long-term espionage and intelligence gathering. Actors linked to China, Russia, Iran, and North Korea are among the countries mentioned in this respect [248].

Data and knowledge intensive sectors such as finance and insurance, health and social services, and professional services are impacted particularly heavily [139], [140], [187]. From a government perspective, digital infrastructures, data ecosystems, and cloud-based platforms are considered both the foundation of national competitiveness and a core resource to be protected through the national security policy [332].

Asia Pacific

In the Asia-Pacific region, the cyber threat landscape is characterized by tightly interwoven economic interests, technological dependencies, and geopolitical power struggles. Cyber operations serve both to exert state influence and to further economic interests. Targeted, long-term operations tend to predominate [235], [248], [344].

The main focus is on establishing permanent access and means of influence. Attackers exploit known vulnerabilities or misuse existing credentials to gain initial access to IT systems. This access is then used to establish a persistent presence in the system [235], [344].

This focus is most evident in the national security context. In 2025, Chinese threat actors launched an average of 2.63 million cyber intrusion attempts per day against Taiwan's critical infrastructure. This represents an increase of approximately 6 percent over the previous year [256]. Energy, communications, transportation, emergency response, and administrative systems were especially affected. More than half of these attacks

involved the exploitation of vulnerabilities in hardware and software. Notably, there was a more than tenfold increase in attacks on energy infrastructure and a sharp rise in the number of attacks on health and emergency services [256].

Alongside organized cybercrime, state-sponsored actors have emerged as a prominent threat in the region. Groups with ties to China, Russia, Iran, and North Korea are targeting telecommunications networks, research institutions, government institutions and IT-related organizations in an effort to gain long-term access to sensitive information, technological developments, and strategic infrastructure [68], [234], [236], [238], [239], [248].

The threat landscape is further exacerbated by regional tensions and hybrid patterns of conflict. Digital attacks frequently coincide with political, military, or diplomatic developments. In some cases, they are combined with physical, real-world vulnerabilities. Waves of attacks have also been observed between India and Pakistan [87].

1.1.2 Technological developments and global trends

In addition to geopolitical factors, technological and structural developments are further escalating the threat situation. Attacks are marked by increasing scalability, higher speeds, and growing organizational maturity [63], [139], [140], [344]. Technological developments, in particular, have had the effect of amplifying existing threats, changing the way in which attacks are prepared, carried out, and monetized.

Professionalization and division of labor in cybercrime

As professionalization of cyber operations gains pace, the ability to execute attacks quickly, automatically and at scale is becoming increasingly important. A structure in which tasks are divided among different actors paves the way for shorter exploit cycles – the time between the discovery of a security vulnerability and its active exploitation – and the increasing predominance of automated attack chains [139], [140], [344], [347].

What were once isolated, opportunistic attacks are evolving into a labor-divided attack economy in which specialized actors carry out individual phases of the attack chain [139], [140], [344]. Key to this development is the emergence of specialized markets for credentials, malware, and attack resources, which can be utilized to prepare and scale attacks efficiently [139], [140], [197], [235].

The availability of large quantities of compromised identity data serves as a key factor in scaling up these attacks. During the first half of 2025 alone, an estimated 16 billion sets of login credentials were recorded worldwide [145]. Around 1.8 billion of these were used to carry out follow-up attacks [140]. Government intervention and international law enforcement efforts can significantly disrupt criminal infrastructures over the short term. However, the impact on the underlying labor-dividing structures has been limited to date, as criminal platforms and networks are often able to quickly reconstitute themselves [32], [33], [34], [35], [139], [200], [347].

Speed, automation, and exploit cycles

Along with the increased professionalism of these groups, the speed of modern cyberattacks is also accelerating significantly [75], [140], [149]. In 2025, more than 48,000 new vulnerabilities were disclosed worldwide. For a significant proportion of these, functional exploit code was available shortly thereafter, meaning ready-made software tools were soon at hand to exploit these gaps with targeted attacks [140], [260].

Automated scanning, standardized exploit kits, and ready-to-use attack modules enable attackers to identify and exploit vulnerabilities in near real time. The balance of power between attackers and defenders is thus increasingly shifting in favor of those who use quicker automated processes than their opponents.

Security incidents are often the result of a combination of multiple moderate weaknesses and structural deficits. Of particular concern are issues related to patch management, prioritization, and responsiveness [74], [140], [235], [344], which are further exacerbated by reliance on US-centric infrastructures such as the Common Vulnerabilities and Exposures (CVE) system and the National Vulnerability Database (NVD) [274].

Due to the rapid advances in automation, the focus of future attacks is increasingly shifting away from individual technical vulnerabilities towards attempts to exploit systemic attack surfaces. Centralized platforms, cloud services, and authentication infrastructures enabling large-scale automated access are particularly vulnerable [75], [140], [149], [344].

Artificial intelligence in attack and defense

Artificial intelligence (AI) is reshaping the global cybersecurity landscape by significantly accelerating and scaling existing threats. It enhances both efficiency and range, allowing attacks to be prepared more quickly, targeted more precisely and carried out on a larger scale [139], [140], [232], [237], [248], [337], [344].

Adversaries are increasingly leveraging AI to automate each step in existing attack chains and efficiently orchestrate entire campaigns. This notably includes the creation of deceptively authentic content for phishing and fraud campaigns, the selection of suitable target groups, and the tailoring of attacks to react to their victims' responses [67], [139], [140], [337], [338], [344].

Generative models also lower the barriers to entry in terms of language and content. They facilitate the creation of credible communication patterns without in-depth specialist or cultural knowledge, increasing the likelihood that social manipulation will succeed [140], [337]. Given that AI-generated content is virtually indistinguishable from legitimate communication with regard to language and context, purely content-based detection mechanisms are becoming less effective. Increasingly, they need to be supplemented by approaches focusing on identity and behavior [338].

The effects of this can also be observed in the current wave of attacks. AI-supported phishing campaigns, particularly those involving email, continue to increase in volume and improve in linguistic quality. In the second quarter of 2025, over 1.13 million phishing attacks were registered worldwide, with significant growth in business email compromise – a form of fraud involving fake business emails to trigger erroneous payments. A significant proportion of these attacks leveraged AI for adaptation [7], [111], [181], [182], [337], [344]. What's more, AI is now integrated directly into attack tools, enabling malware to dynamically adapt its behavior to bypass filters, for instance, and facilitating the use of deepfakes for CEO and identity fraud [61], [64], [68], [164], [190], [196], [331].

The use of AI-supported approaches is also increasing on the part of defenders, with security solutions relying on machine learning to detect anomalies, prioritize alerts and assist in responding to incidents [187], [330], [344], [347]. Automated analysis and support for decision-making help security teams keep pace with the increasing speed of modern attacks, reduce detection and response times, and partly compensate for personnel bottlenecks [187], [201], [316], [330]. Meanwhile, the actual maturity level remains limited at many organizations. Currently, only 14 percent of the organizations surveyed consider their existing AI-based security measures to be fully effective. This points to shortcomings in integration, governance, and data quality [187], [261], [330]. The result is an imbalance, as attackers can experiment more quickly and freely, while defenders are bound by regulatory, organizational, and operational constraints [139], [337], [344]. Going forward, it is therefore crucial for organizations to be able to embed AI in their existing security processes in a controlled and professional manner if they are to stand up to the automated attack ecosystem [60], [75], [139], [330], [337], [344].

1.1.3 Ransomware: A systemic threat

Initially a standalone attack method, ransomware has evolved into a globally organized ecosystem in its own right and now represents a predominant threat. Ransomware remains one of the most prevalent forms of financially motivated attacks around the globe and is increasingly organized like a structured business workflow. Observed ransomware activity rose by roughly 179 percent internationally during the first half of 2025 and it currently accounts for approximately 44 percent of all security incidents investigated [139], [140], [235], [344]. Technological automation, division of labor approaches, and new monetization strategies have contributed to ransomware campaigns scaling faster, operating more flexibly, and becoming more resilient to law enforcement measures than in previous years [139], [140], [347].

Ransomware-as-a-Service: A highly successful approach

A key factor in the continued proliferation of ransomware is the rise of the ransomware-as-a-service (RaaS) approach. There has been a clear progression from isolated groups of perpetrators to more collaborative, platform-based models, with developers, operators, and those carrying out the attacks each taking on separate roles [139], [140], [193], [235]. RaaS providers supply the encryption software, payment infrastructure, negotiation guidelines, and data leak sites. Groups or individuals known as affiliates then conduct the actual attacks.

Source: [316]

Figure 1: Effect of a ransomware attack on IT and security teams (n=1,700)

The RaaS model lowers barriers to entry, enabling less tech-savvy actors to carry out highly effective extortion campaigns [69], [139], [140]. At the same time, the division of labor also increases scalability. Multiple campaigns can be run in parallel, rapid modifications can be made to target specific regions or industries, and successful techniques can spread throughout the ecosystem within a short time [140], [235], [344]. Business models based on the division of labor are still considered to be largely resilient to government intervention, as success by law enforcement agencies often only has short-term, isolated effects, while the criminal ecosystem is able to keep reconstituting itself over the long term due to its decentralized structure [195].

Shifting targets and breakdown by sector

The distribution of ransomware attacks indicates a shift in target selection. While large companies and critical infrastructures remain the primary focus, attacks on small and medium-sized organizations and sectors with less protection are on the rise [140], [315], [344]. This is mainly facilitated by automation and the large-scale availability of compromised access credentials [139], [140].

Among the sectors most often impacted are manufacturing, technology companies, trade and retail, healthcare, and services [140], [316], [344]. Regionally, many documented ransomware cases are centered on highly digitalized economies, particularly those in North America and Europe. Meanwhile, other regions are often indirectly affected via their supply chains and service providers [111], [140], [344].

Increasingly, identity-based entry points are leveraged. For this reason, ransomware is becoming more closely interlinked with other forms of data theft and espionage [235], [248], [344]. The lines between classic data theft, espionage, and extortion have become blurred. Due to the combination of labor-dividing RaaS models and diversified monetization strategies, attackers are able to flexibly scale campaigns and quickly regroup when faced with government intervention. At the same time, the availability of massive amounts of compromised log-in details is leading to a strategic realignment. Since access is increasingly gained using valid identities, the structural vulnerabilities of organizations are gaining significance compared with their technical security measures. Attackers can aim to infiltrate specific players with high digital interdependency and extensive supply chain interconnections, with the aim of establishing sustained access. This means that ransomware should now be understood less in terms of a one-off extortion attack and increasingly as part of long-term exploitation and coercion strategies within a globalized attack economy [139], [140], [235], [248], [315], [344].

Psychological and political impacts of extortion

In addition to causing financial damage, attacks involving extortion have a profound psychological effect on organizations and their management. The combination of time pressure and uncertainty about the actual extent of the damage, coupled with the threat of further consequences, places a considerable strain on the decision-making process [41], [316]. This psychological dimension is a key component in the effectiveness of extortion, as it deliberately induces stress and impedes

rational decision making (see more details about this and other psychological impacts in Figure 1) [111].

Ransomware not only influences management decisions but also places considerable strain on the employees involved. Following serious incidents, IT and security managers often report experiencing ongoing stress, increased workloads, and exhaustion. These repercussions can impair the response capabilities of organizations over the long term [41], [314].

From an organizational perspective, attacks involving extortion increase uncertainty and insecurity regarding responsibilities, liability issues, and public communication. Anticipation of reputational damage, regulatory consequences, or political attention also affect internal organizational decision-making processes [41], [111].

1.1.4 Economic damage and the cost of cyber attacks

Across organizations, cyberattacks frequently lead to major disruptions to productivity and operational capacity. A large proportion of incidents entail the failure of core IT systems, the interruption of digital business processes, or temporary stoppages in production and services [28], [187]. In addition, cyber incidents not only cause direct costs but also lead to reputational damage, loss of trust, and strategic limitations [28], [187], [316].

Internationally, in the median case, it takes an average of 181 days to detect an incident [187]. Ransomware incidents are discovered more quickly than other types of attacks, with a median detection time of around six days [235].

In the wake of severe security incidents, organizations often experience reduced operational capacity for several days or weeks. Containment takes 64 days on average. Depending on the type of attack and the system architecture, recovery times range from around ten days to upwards of 30 days [158], [187], [316].

The long duration of security incidents means that they tie up considerable amounts of human and technical resources. Operations can be constrained for several months as a result [158].

The extent to which operations are affected hinges on the degree of digitization and structural dependence on IT-supported processes. Highly digitalized organizations are especially sensitive, as outages directly impact business-critical core processes. At the same time, less digitalized organizations may also suffer significant declines in productivity due to their reliance on central communication, management, or logistics systems [187], [316].

Accordingly, the average daily cost of outages in highly digitalized environments is 1.5 to 2 times higher [187], [316].

Productivity losses are not only directly due to technical failures. Organizational measures such as emergency shutdowns, restricted access rights, additional coordination and approval processes, or the reassignment of staff are often responsible for prolonging the duration and impact of an incident [28], [187]. A significant proportion of the disruption is attributable to processes related to coordination, decision-making, and resuming operations [316].

Cyberattacks also increasingly have a cascading effect. In roughly 10 to 30 percent of incidents, the failure of individual digital components leads to disruptions affecting external partners, downstream processes, or public services due to the close interconnection of systems and supply chains [111], [344]. Consequently, cyber incidents are rarely confined to individual organizations, but have an impact beyond organizational and system boundaries [28], [111].

Financial losses due to business interruption, recovery, and data protection

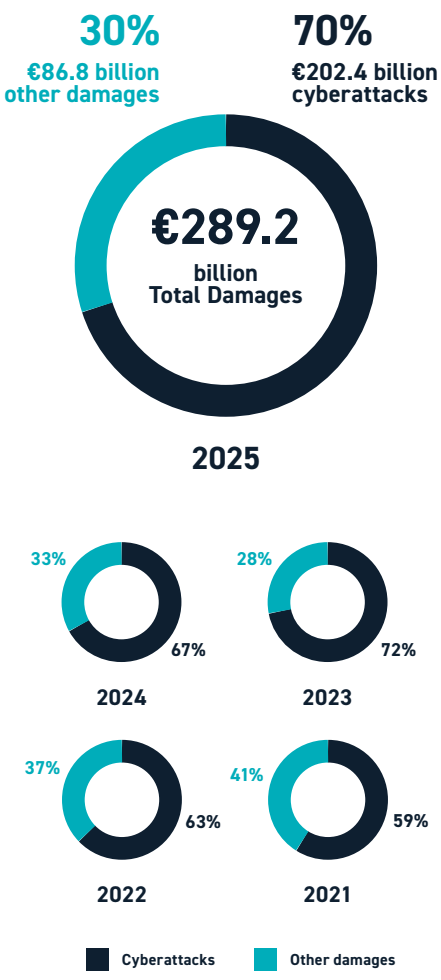
The financial impact of cyberattacks can be quantified both at the macroeconomic level and by examining the costs of individual incidents [28], [49]. The average damage caused by a cyberattack is around US$250,000 (approx. €212,000) per organization. The annual losses to the economy add up to billions of dollars in many industrialized countries [348]. At the global level, the total costs incurred due to cybercrime are predicted to reach around €14.23 trillion by 2029 [158].

A substantial part of the damage caused by cyberattacks in Germany results from business interruptions and consequential costs. Approximately 70 percent of the losses reported by companies due to data theft, industrial espionage, and sabotage are directly attributable to cyberattacks [28]. For 2025, this equates to financial losses of around €202.4 billion (see Figure 2). The biggest factor driving these costs is the failure of key business processes. Temporary or total disruption

of business processes and operations has a direct impact on sales, delivery capabilities, and internal processes. It may also unleash a cascade of repercussions along value and supply chains [28].

Another significant cost factor is recovery following cyber incidents. This includes forensic analysis, system and data recovery, third-party support services, and post-incident security measures. These costs are incurred regardless of whether ransom payments are made [187], [316].

In addition, organizations are faced with consequential costs related to data privacy and compliance. Cyberattacks involving data exfiltration or manipulation generally entail reporting obligations to supervisory authorities, seeking legal advice, conducting internal investigations, and potentially paying fines, especially in regulated industries [28], [111], [187].



Source: [28]

Figure 2: Proportion of cyberattacks as a share of total economic damages in Germany (n=868)

The cost structure varies significantly depending on the type of attack. While business interruption and recovery dominate in ransomware incidents, follow-up costs related to legal, regulatory, and reputational issues are more prominent when it comes to data privacy incidents. This heterogeneity makes generalized calculations difficult and calls for a more nuanced approach to assessing cyber risks [187], [316].

Real impacts on industry: Some examples

Practical experience shows that cyberattacks on German companies often result in prolonged disruptions to key business processes [28], [187]. Processes reliant on IT, such as order acceptance, billing, logistics management, and internal approval procedures are most heavily impacted. Even though physical facilities or services are formally able to continue their operations, financial losses arise due to delayed deliveries, contractual penalties, and a lack of operational control [28].

A recent example from 2025 involved a cyberattack on an external IT service provider for Vodafone. As a result of the incident, the "Vodafone Sales World" central sales platform was down for several days. Partners and employees were unable to access crucial systems and data, which significantly disrupted sales-related business processes [84].

Another incident concerned the dairy company Arla Foods Germany. Compromised IT systems at a production site led to temporary production limitations and delays in supplying products [82].

Adidas also reported an incident in which customer contact details were accessed via a third-party customer service provider. Even though no payment data was leaked, extensive data protection and recovery measures were triggered [324].

In 2025, a cyberattack on car manufacturer Jaguar Land Rover demonstrated just how vulnerable highly interconnected production structures are. Although the attack primarily targeted this one company, economic interdependencies resulted in estimated total damages of £1.9 billion for the British industrial sector. More than 5,000 companies along the supply chain were im-

pacted by weeks of production downtime and massive disruptions. The incident serves as a warning signal for German industry. Due to close international interconnectedness, production stoppages abroad can directly impact local suppliers. Thus, cyber resilience is proving to not only be an operational necessity, but also a vital macroeconomic imperative [85].

Regardless of company size or sector, even technically limited cyberattacks cause significant recovery and consequential costs. These expenses can run to hundreds of thousands within a matter of days. Moreover, they often go hand in hand with long-term effects on reputation and trust [28], [83], [187], [316].

Following cyberattacks, companies report increased difficulty in contract negotiations, more caution on the part of business partners, and rising insurance premiums, particularly in cases where data breaches or prolonged disruption to operations have become public knowledge [28], [41], [187].

1.2 NATIONAL THREAT SITUATION: SPOTLIGHT ON GERMANY

Germany is one of the EU countries most severely impacted by cyberattacks [28], [31], [49], [104], [111], [248]. Roughly 87 percent of companies based in Germany are affected by digital or analog attacks, while 77.5 percent of companies have been victims of at least one successful cyberattack in the past twelve months [158]. These attacks follow recurring patterns which cut across different sectors and company sizes [49], [111], [344]. Organizations with limited resources are especially vulnerable to large-scale attacks [28], [339]. This high level of exposure stems from Germany's economic significance, its strong digital interconnectedness, and the central role German organizations play in European service and supply chains [28], [49], [248].

Ransomware remains one of the most damaging cyber threats in Germany. Attacks often involve the theft of data and cause significant economic losses [28], [187], [235], [316]. The situation is unlikely to ease in the coming years, with forecasts pointing to a further escalation [139], [147], [248], [344], [347].

1.2.1 Attack patterns and targets

The cyberattacks observed in Germany follow clear patterns in terms of points of entry, target groups, and attack objectives. The majority of incidents can be attributed to a few recurring attack vectors which can be exploited regardless of the sector or size of the organization [49], [111], [248], [344]. These include phishing, the misuse of existing log-in credentials, and the malicious use of legitimate services.

Commonly used vectors: Email, legitimate services

Accounting for around 60 percent of attacks, phishing is the predominant entry point in Europe. Germany is one of the countries most severely affected by phishing attacks [111], [248]. Email remains one of the main attack vectors, with analyses of email traffic in German companies revealing that phishing messages systematically target the theft of login details. The messages often imitate well-known brands, such as DHL, or services used for contracts and signatures, such as DocuSign [176], [178].

Deceptively genuine-looking login pages are particularly widespread. They are spread via links or HTML and PDF attachments and targeted at cloud and webmail accounts [65], [176], [344]. This type of attack is growing in importance and increasingly scaled via the misuse of cloud services [59], [177], [182]. Content, sender details and language are varied automatically to avoid detection by filter mechanisms and increase the attack's probability of success [176], [179], [180]. In Germany, phishing often serves as a springboard for account takeovers and subsequent extortion scenarios [176], [248], [344].

In addition to email, other communication channels are gaining in importance. Phishing campaigns are increasingly being launched via messenger services and SMS. In the eyes of the public, these are now perceived as occurring even more frequently than conventional phishing emails [48], [105], [106].

At the same time, legitimate digital services are increasingly being exploited as attack vectors. Cloud applications, file and collaboration services, sharing functions, and user authentication features are now all used to spread malicious content via trusted platforms or to establish unauthorized access [176], [248], [344].

Widespread automation of attacks

The threat situation in Germany is characterized by highly automated attacks specifically targeting chronically exposed, poorly maintained services. Peripheral components, including systems that act as interfaces and connect the internal network directly to the internet, such as VPN access points or firewalls, are particularly vulnerable. As they are visible to the outside world, they often serve as the first point of entry for attackers [139], [140], [315], [344].

A key element, both in Germany and globally, is the reutilization of attack components. Access data, exploits, and malware are made available in collaborative structures and reused across multiple campaigns [139], [140], [344]. This means that known attack patterns remain effective over extended periods of time and can be quickly transferred to new targets [49], [344]. The most frequently exploited infrastructures include outdated web applications, forgotten subdomains, and services that are no longer actively maintained. Despite their limited functional significance, these systems remain persistently exposed. In other words, these attacks are characterized less by new exploits than by structural deficiencies in the lifecycle management and decommissioning of IT services [11], [268].

Automation also accelerates the steps that follow successful first penetration. Lateral movement, data exfiltration or extortion can be prepared or carried out in a partially automated manner. This serves to shorten the time between initial compromise and actual damage [140], [235], [344].

1.2.2 Digital identities and access infrastructures

Digital identities are among the most important gateways for cyberattacks in Germany [111], [139], [140]. Digital identity and access management (IAM) infrastructures have become a critical control layer in many organizations. Nowadays, identity services and single sign-on solutions are used as a means of bundling access to a range of professional applications, cloud services, and administrative functions. Consequently, security incidents occurring at this level do not merely have a localized impact, but often have system-wide repercussions [140], [248], [344].

Attacks increasingly aim to take over these central digital identities, as these grant attackers sustained, inconspicuous access to cloud, on-premises, and hybrid environments [140], [344]. As a consequence, access infrastructures are not only a technical issue, but have also developed into an organizational risk factor, especially in complex IT landscapes where functions and work tasks are shared [248].

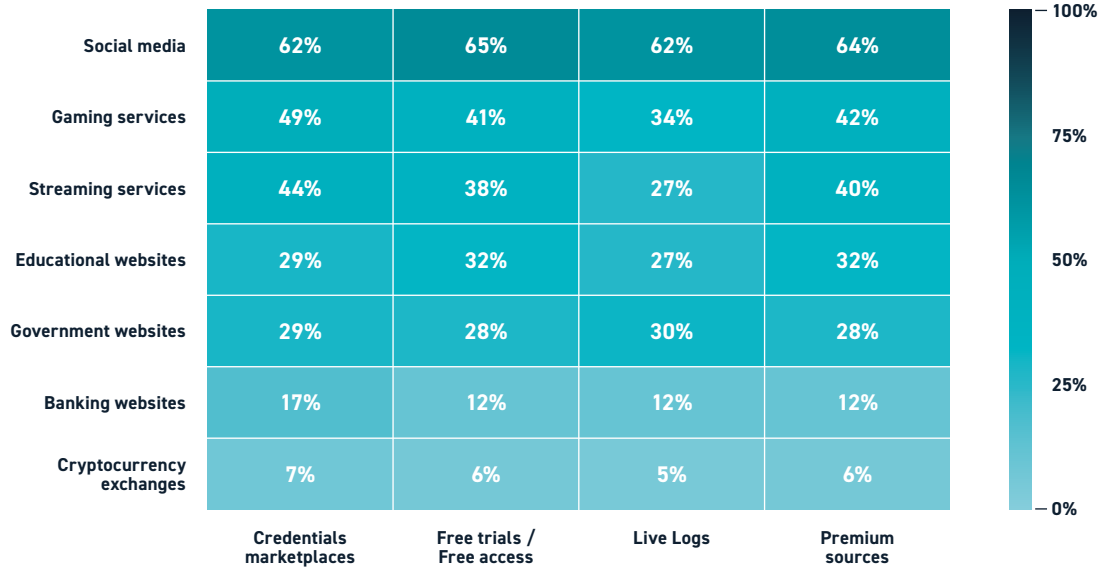
Password spraying, credential stuffing and MFA bypass

Attacks on digital identities often take the form of automated log-in attempts. These approaches are designed for high scalability and low visibility. In particular, password spraying and credential stuffing play a major role [49], [140], [341], [344]. Password spraying involves testing frequently used passwords across many different accounts. Credential stuffing, on the other hand, uses log-in details that have been compromised in past data breaches and may have been employed elsewhere due to the widespread reuse of passwords [140], [344]. There is a clear distinction in preferred approaches for different platform types, with login credentials for social media and gaming services, in particular, being traded extensively via specialized marketplaces and live logs (see Figure 3). Both methods primarily target email accounts, cloud services, and centrally managed applications and can be carried out on a large scale with little effort [49], [111].

In response, many organizations are now turning to multi-factor authentication (MFA). However, attackers are also using methods aimed at bypassing or exploiting MFA. In particular, these include social engineering, session hijacking or technical interception during the login process [140], [344].

One approach seen in the context of cloud-based work platforms is known as an adversary-in-the-middle attack and involves technical interception during the login process. These attacks use deceptively convincing log-in pages to capture not only usernames and passwords, but also session or access tokens, allowing attackers to hijack ongoing log-in activities [176], [233], [344].

Conventional MFA methods are also increasingly circumvented in targeted attacks. The focus of countermeasures is shifting accordingly [214], [248], [344]. Passwordless authentication methods such as passkeys are increasingly gaining traction, particularly for privileged accounts and centralized cloud services, as they can reduce systemic dependencies on human fallibility [139], [248], [344].



Source: [344]

Figure 3: Compromised website credentials around the globe according to various Infostealer sources (n=33,933)

Cloud access and shadow IT pose systemic risks

Cloud-based services are an integral part of key business, communication, and administrative processes. Across the German private sector, 90 percent of companies rely on cloud applications. Approximately 47 percent of IT applications are operated from the cloud, with 62 percent of companies stating that they would no longer be able to operate without cloud solutions [29].

As applications and data have been shifted to the cloud, the number of digital access points and associated identities has also increased significantly [28], [49], [111], [139], [339], [344]. Access to cloud services is closely linked to centralized identity and access infrastructures, extending their reach beyond organizational boundaries [248], [344].

This development adds significantly to the complexity of access control. As companies increasingly open up their IT systems to external partners and service providers, complex access structures are developing. If permissions are not revoked after a project has ended or if a company loses track of these guest accounts, entry points may be left open for attackers to exploit. Deficient management of privileges, outdated or forgotten accounts, and a lack of transparency regarding active cloud logins all frequently contribute to security incidents [49], [344].

The widespread use of shadow IT is another risk factor. Departments often independently resort to using unapproved applications, hardware, or platforms to speed up work processes or meet short-term requirements [28], [49], [339].

Around 12 percent of German companies have reported experiencing problems caused by unregistered IT devices. Meanwhile, approximately 9 percent explicitly consider them a potential gateway for cyberattacks [339]. Shadow IT is often accessed using existing work identities or sensitive organizational data without security configurations, permissions, or logging systems being centrally administered, monitored or reviewed [248], [344].

In this way, shadow IT exacerbates existing risks in identity and access management. Access to the services bypasses formal governance, security policies are circumvented, and compromise remains undetected for longer. At the same time, reliable oversight and rollback processes are lacking in many cases. Only 43 percent of companies regularly scan for unregistered or forgotten devices, while 39 percent have yet to define a process for decommissioning old devices and systems [339].

In combination with centralized identity services, this unsupervised cloud access can significantly expand the attack surface, making it considerably more difficult to trace the source of security incidents [49], [248], [344].

Growing misuse of legitimate admin access

Administrator and privileged access rights, in other words accounts with advanced rights and extended privileges that allow users to make far-reaching changes to configurations and enable access to sensitive data, present a particularly attractive opportunity for attackers in modern IT and cloud environments. These accounts are often compromised indirectly, for instance through targeted social engineering attacks on IT support and help desk structures, the takeover of insufficiently secured administrator accounts, and the escalation of privileges after gaining initial access [140], [344].

Another risk factor arises from the way privileged accounts are used in day-to-day operations. Due to efficiency considerations or a lack of resources, administrator rights are often used more frequently and for longer periods than their intended purpose, for instance for maintenance, support, or emergency access. This increases exposure and the risk of misuse in ways that are not immediately apparent [28], [49], [140], [150], [344].

Looking at the big picture, it becomes apparent that digital identities, cloud access, and privileged accounts are coming together to form a pivotal systemic attack surface. The interplay of automated attacks on login processes, the circumvention of traditional authentication methods, unauthorized use of cloud services, and the misuse of legitimate admin access amplify each other.

As cloud and platform services continue to proliferate, it can be assumed that identity-based attack vectors will continue to be among the most effective entry points in the future. Unless user identities, authorizations, and privileged access are consistently controlled beyond organizational and system boundaries, the risk of organization-wide damage is bound to increase significantly [139], [248], [344].

1.3 STRUCTURED ATTACKERS – THREAT ACTORS, OBJECTIVES, AND METHODS

Cyber threats diverge in terms of the rationale employed by threat actors to plan, coordinate, and strategically deploy them [86], [111], [130], [139]. State actors, organized cybercriminals, hacktivists and hybrid groups are all pursuing different goals within differing timeframes. Nevertheless, they often make use of similar entry points and infrastructures [86], [139], [140], [344].

Only a detailed analysis of the attackers' objectives, methods, and organizational structures can provide a reliable assessment of cyber risks [86], [139], [344]. The following sections distinguish between state actors (advanced persistent threat, APT) and organized cybercrime groups. Hacktivist and hybrid forms are considered cross-sectional phenomena [86], [111], [139], [140], [187], [201], [261], [286].

1.3.1 State actors

State and state-backed actors comprise a key group of threat actors. Unlike attackers who are mainly driven by financial motives, they primarily pursue long-term strategic goals. Cyber operations are utilized as a tool to advance foreign, security, or economic policy. These APTs are characterized by a high degree of operational persistence. They aim to gain sustainable access to information, exert political influence, or prepare strategic options for further actions [86], [111], [130], [261]. Despite having comparable technical bases, APTs differ considerably in terms of their objectives, the sectors affected, and their modes of operation [86], [111], [130], [248]. Three types of objectives can be distinguished in state cyber operations: espionage, sabotage, and exerting influence.

Espionage as the primary goal

Espionage remains the core focus of state cyber activities. Long-term access is established in order to spy on government networks, research institutions, telecommunications providers, and highly technological companies. Conspicuous disruptions are deliberately avoided [139], [235], [248].

APT groups with links to China have repeatedly been accused of systematic economic and technological espionage. Those affected include industrial companies, semiconductor research, telecommunications, and academic institutions [234], [235], [248].

Groups with ties to Russia are pursuing a dual strategy of cyberattacks and disinformation campaigns. These are aimed at deliberately undermining democratic systems, creating political instability, and sustainably eroding public confidence in state institutions and democratic processes [21]. Campaigns against government agencies, diplomatic missions, and security-related infrastructure in Europe and North America have been documented [111], [139], [248].

In Iran, cyber operations are mainly used for regional reconnaissance and spying on government and economic targets. These operations are often carried out in the context of security tensions in the Middle East [166], [270].

North Korean operators have increasingly been using insiders and externally recruited IT specialists who work for foreign companies under false identities. This strategy grants them direct access to sensitive development, cloud and financial systems, allowing them to effectively bypass traditional security mechanisms [139], [140], [248]. Another area of operations is conducting cyberattacks on crypto exchanges (e.g., Bybit 2025) in order to gain access to digital assets [21].

Sabotage remains an effective tool

Sabotage indeed occurs less frequently than other forms of cyber warfare, but it has a high political and symbolic impact. It deliberately aims to cause visible disruption and short-term impacts. Cyber operations are used, for instance, to temporarily disrupt critical processes, expose vulnerabilities, or undermine a state's ability to act [111], [139], [261].

Russian and Iranian actors, in particular, have been linked to attacks on energy, transport, and government infrastructure [111], [261], [270]. Such activities are intended to serve as a deterrent, send a signal, or destabilize an adversary without crossing the threshold to military conflict, but they usually remain within a limited time frame [86], [139].

Hybrid operations are also shifting their focus to strategic digital connections and outsourced IT services. Incidents involving undersea cables – including in the Pacific region near Taiwan – and malicious misuse of IT services have been used as means of gaining covert access to systems and pursuing economic or security policy objectives [139], [140].

Exerting influence and spreading information

Influence cyber operations and information operations refer to cyber activities that deliberately combine technical access with public, political, or social impact. They primarily involve the controlled use of compromised information and leaks or digital disruption operations [111], [130], [133], [139].

Russia-affiliated actors use compromised data and disruptive activities to influence public perception and fuel social tensions [111], [130], [133], [139].

Iranian actors have also engaged in data leaks, threat campaigns, and symbolic attacks in a bid to build political pressure and influence narratives [270].

State actors also indirectly support hacktivist groups or strategically exploit their activities. Their aim is to make it more difficult to identify the state's involvement, but also to increase their impact and reach [111], [129], [130].

In this regard, hacktivist collectives serve to deliberately increase the public visibility of technical cyber operations. Through this combination of technical access, public communication and indirect control, state actors can amplify political effects without revealing their government's involvement [86], [111], [129], [130].

Regional characteristics of state APT actors

From a regional perspective, there are marked differences in the types of targets, modes of action and strategic weighting of state-backed cyber operations. Certain threat actor types engage in cyber operations not only for security policy purposes, but also to further economic and resource-related interests [139], [140], [248].

Western states such as the US are also equipped with sophisticated offensive cyber capabilities, which they combine with information strategy elements in hybrid operations. In the context of events in Venezuela's energy sector that were relevant to US security policy, there was discussion as to whether technical effects were accompanied by prepared narrative infrastructures in order to have an influence on the perception and interpretation of events at an early stage [5].

APTs with ties to Russia are characterized by a high degree of operational flexibility. State agencies, military units and external threat actor structures are closely

interlocked. Separate groups act in a coordinated manner and adapt their activities to geopolitical developments as the situation demands [111], [139], [261]. The boundaries between state operations and external structures are often fluid [86], [111].

Chinese APTs are described as particularly persistent, strategic, and resource intensive. They engage in sustained campaigns and are highly focused on establishing covert, scalable, persistent access capabilities [139], [235], [238], [248]. This strategic focus manifests itself, among other things, in specialized tools such as the BRICKSTORM malware, which enables inconspicuous persistence in critical infrastructures using legitimate admin functions [70]. It is also evident in long-term campaigns such as "Salt Typhoon," which Chinese actors have been conducting since at least 2021 to compromise telecommunications, government and military-related networks worldwide, and use them to achieve strategic prepositioning [206].

Iran-affiliated APTs stand out in international comparison due to their high level of activity, adaptability, and political motivation. Their structures are considered dynamic and strongly influenced by regional conflicts. Government agencies, security forces, and ideologically motivated groups work closely together in this regard [86], [111], [130], [270]. Within the context of the conflict between Israel and Iran, the observed offensive cyber activities carried out by Iranian actors increased by around 700 percent within twelve days. This underscores the high reaction speed and political alignment of these actors [140].

North Korean APTs play a unique role, combining conventional state cyber structures with a consistent focus on financial gain. Today, these operations serve as an important source of state revenue and funding for government programs. What is unprecedented here is the extent to which cyber activities are used to deliberately circumvent international sanctions [21], [139], [140], [248].

With regard to cyber defense, these regional differences make it clear that it is not possible to combat state cyber operations, economically motivated attacks, and hacktivist campaigns with a uniform approach. Different organizational forms, objectives, and mechanisms of action require fitting, differentiated countermeasures [139], [140], [192], [194], [197], [248], [261].

Over the years to come, we can expect to see more interlinking of cyberattacks, data exfiltration, and the publicly impactful use of compromised information by state actors to influence public opinion. This is especially likely to be the case in the run-up to political decisions, elections, or international crises [111], [139], [347].

1.3.2 Organized cybercrime

Organized cybercrime represents a highly dynamic part of the global threat landscape. Unlike state-sponsored APT actors, cybercriminal groups are primarily motivated by economic objectives [139], [140], [344], [347]. Nowadays, their activities are firmly embedded in a shadow economy based on the distribution of tasks to various parties. Leaked or stolen credentials, malware, exploits, infrastructure, and money laundering services are traded on specialized marketplaces and deployed in flexible combinations [139], [140], [194], [197]. This economics-driven approach shapes both the technical infrastructure and attack chains based on the division of labor principle.

Criminal infrastructure

Recent law enforcement campaigns highlight the pivotal role that criminal infrastructures play. In November 2025, bitcoin mixer cryptomixer.io – a service for anonymizing payment flows – was shut down. Since 2016, it had processed more than €1.3 billion in crypto assets from suspected criminal sources. Investigating authorities seized over €25 million in Bitcoin as well as extensive server and log data [128].

At the same time, organized cybercriminal structures are relying on "bulletproof" hosting. These services are designed to be resilient to shutdowns, abuse reports, and law enforcement. Providers either tolerate or actively promote criminal activity, conceal operator identities, and enable the rapid relocation of critical infrastructure when faced with pressure from authorities [71].

Owing to their modular and scalable structures, organized cybercriminal groups can take aim at a wide range of potential targets. Attacks are launched against companies of all sizes, public institutions, and increasingly also against private individuals – provided that the perpetrators can expect to reap financial rewards [140], [315], [344]. Organizations which are heavily dependent on digital technology are particularly attractive targets, as business interruption, data loss, or damage to their reputations are likely to result in immediate financial consequences [28], [316], [344].

Business models of ransomware groups

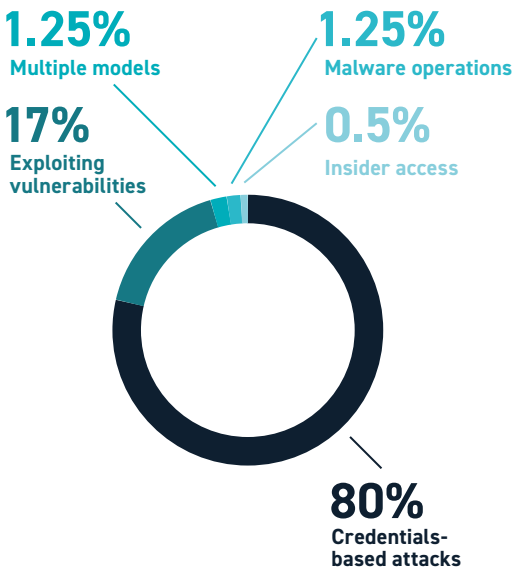
Ransomware is currently the dominant business model within the shadow economy, which is divided into specialized roles [130], [139], [140]. While key players provide malware, infrastructure, and payment processing services, affiliated partners carry out the actual attacks and receive a share of the proceeds [130], [316]. This model lowers the barriers to entry, thus increasing the number of ongoing campaigns. Compromised access credentials, sessions, or remote access are traded on a large scale and exploited in a targeted manner [139], [140], [193], [197].

The targets of ransomware attacks are selected according to strict business principles. RaaS is used wherever business interruption or data losses exert financial pressure [139], [140], [187], [344]. The targets are often in industries with high added value and low tolerance for downtime, including the technology, manufacturing, retail, services, healthcare, and finance sectors.

Extortion methods are also evolving. For several years now, ransomware groups have been taking a combined approach, using data encryption alongside data leaks and threats of publishing stolen data in order to ramp up the pressure on victims during negotiations [235], [316], [344]. The publication of data not only serves to exert pressure on individual victims but also functions as a marketing tool within the underground cybercrime economy. Bringing successful attacks into the public eye increases the credibility of future threats and strengthens the perpetrators' negotiating position [139], [140].

At the same time, attackers have diversified their sources of revenue. In addition to ransom payments, stolen data, for example from cloud, email, and collaboration systems, is increasingly being monetized in other ways [248], [316], [344]. This data is sold on or used as a lever for follow-up extortion attacks [139], [140], [344]. This reduces the dependence of attackers on the willingness of the respective victims to pay ransom. Even organizations that refuse to pay ransom and restore their systems themselves can still suffer significant damage if their data is published or sold. This approach thus limits the effectiveness of established countermeasures.

Ransomware is facilitated by flexible, specialized networks. This development lays the groundwork for further division of roles, such as specialized access sellers, threat and negotiation services, and new attack surfaces in cloud and identity-related environments [130], [139], [140], [316].



Source: [248]

Figure 4: Initial attack vectors employed by access brokers

Despite increased law enforcement efforts, the financial appeal of these attacks remains high, as criminal organizations have managed to quickly rebuild their structures and brands after being taken down by the authorities [139], [140], [195], [347]. With regard to new monetization strategies, leveraging AI serves to accelerate and scale up existing attack and extortion mechanisms. It increases the speed, reach, and reproducibility of existing patterns [139], [248], [338], [344]. With the transition to increasingly agentic systems, capable of orchestrating campaigns, AI is set to bring about even more growth in the attack economy.

Highly specialized: Initial access brokers to extortion campaigns

In the ransomware ecosystem, initial access brokers are specialized actors who sell compromised access to corporate networks and cloud accounts, as well as remote access infrastructures, such as VPNs [139], [193], [197]. Across the globe, 368 active initial access brokers have been observed trafficking access to more than 4,000 compromised organizations. In around 80 percent of these cases, initial access was gained using stolen credentials [248] (see Figure 4). Outsourcing initial access reduces costs and operational risks for ransomware groups while increasing the scalability of attacks [139], [193].

Meanwhile, the subsequent extortion activities are becoming more professional. Ransomware platform operators provide standardized infrastructures for communication, threat campaigns, and monetization. These include leak sites, chronologically phased escalation mechanisms, and well-structured negotiation and payment processes [130], [197], [347].

In more than 50 percent of all documented ransomware cases, the impacted organizations ended up paying less than the original ransom demanded, while only a small number paid the full amount [316].

Digital access, especially related to organization-wide cloud accounts, has a high resale value within the ransomware economy. Trade in these account logins boosts the reach and scalability of collaborative extortion schemes without having to focus on technical details [139], [193], [235], [248], [344].

In the coming years, continued professionalization and standardization of collaborative business models is expected, particularly with regard to ransomware. Rather than being driven by individual groups, these models will be shaped by the variety of available roles, services, and approaches [139], [140], [191], [344], [347].

1.4. SECTORS AND STRUCTURES AT PARTICULAR RISK

The incidence of cyberattacks is not evenly distributed across all sectors of society and the economy but rather tends to be concentrated on structures with a high degree of digital dependency and low tolerance for disruptions [111], [139], [187], [248], [261], [344]. Organizations where business-critical processes, sensitive data, and privileged access are all bundled together within networked IT, cloud, and platform environments are most at risk. These structures are typically supplemented by third-party service providers and supply chains, creating additional dependencies [187], [330], [344]. Critical infrastructures (CI – for more details, see "NIS 2 – State of play" in the appendix), government agencies, medium-sized companies and digital service providers with high system and ecosystem relevance are considered to be particularly exposed[139], [140], [187], [248], [261], [330], [341], [344].

1.4.1 Critical infrastructures

Critical infrastructures (CI) have become focal points for cyberattacks around the globe because due to their systemic functions, disruptions to CI organizations have a direct impact on ensuring the provision of basic goods and services, securing public order, and maintaining public trust [49], [52], [111], [261]. Figure 5 provides a general overview of the average cost of a data breach by sector.

Structural causes of the increased risk to critical infrastructures

The particularly high vulnerability of critical infrastructure (CI) stems from the close coupling of IT and OT (operational technology) systems, infrastructures that have developed over time, and complex operator and supplier structures [48], [110], [146], [259]. One key risk factor is the need for sustained external access to systems, particularly in the context of remote maintenance and service provider models. As a result, privileged access and shared operating models become prime attack vectors [246], [259], [342].

Every second CI operator with OT infrastructure reports at least one security-related incident per year. In around 60 percent of these cases, IT and OT systems are impacted simultaneously [111], [146], [187], [261].

Healthcare sector

The healthcare sector is one of the most severely affected CI sectors globally, with cyber incidents frequently having significant economic and social impact [49], [187], [316], [344]. In 2025, healthcare data breaches caused an average of $7.42 million in damage per incident, significantly higher than the sector average of $4.44 million [187]. Healthcare is regularly listed among the sectors most frequently affected by ransomware and serious security incidents [316], [344]. Approximately 44 percent of all incidents recorded worldwide are related to ransomware. Compromised accounts and privileged access frequently serve as entry points [316], [344]. Successful attacks often result in the failure of clinical systems, the postponement of appointments, and disruption of patient care [49], [187].

Structural factors further amplify this vulnerability. Deficiencies in segmentation, access control, and the securing of external maintenance access significantly impede detection and recovery [146], [344], [187].

In approximately 30 percent of the investigated incidents, external service providers or outsourced IT services were involved. In the healthcare sector, this triggers particularly severe operational repercussions [344], [187], [339], [330].

Energy sector

While cyberattacks in the energy sector may be limited in number, they have a particularly high potential to cause damage in terms of energy security and public order [49], [52], [111], [261]. The average cost per security incident in this sector is around $4.16 to $4.89 million, which is higher than the global average [158], [187].

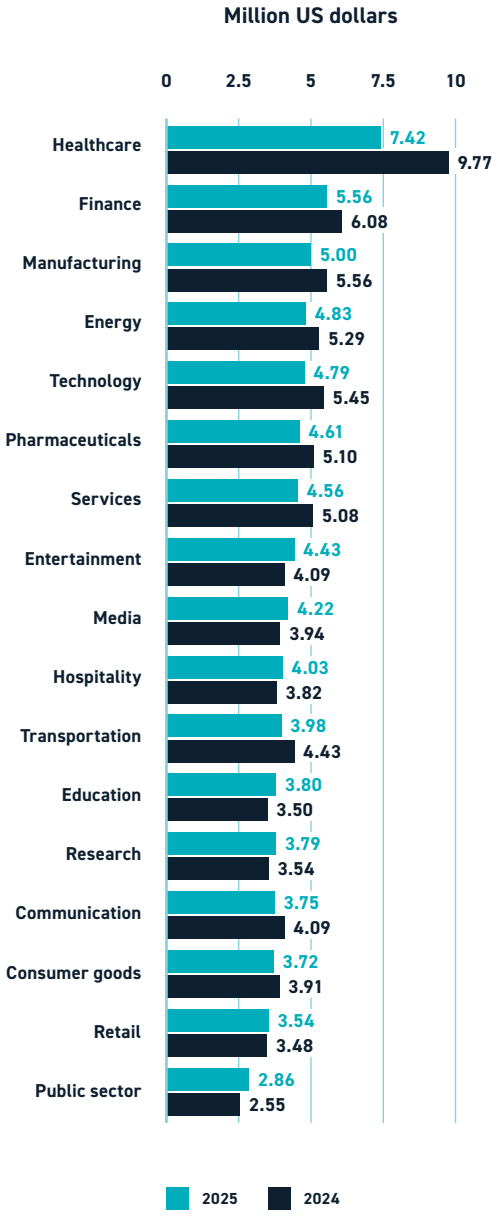
Almost half the energy sector organizations in Germany and the EU have reported operational disruptions or reduced energy provision [111], [146]. Legacy OT components, limited update capabilities, and perpetually active remote access points exacerbate existing vulnerabilities [146], [261]. The access points most frequently exploited are maintenance interfaces and insufficiently segmented networks [111], [146], [261].

In addition, the access points needed to enable service providers and supply chains act as amplifiers. Third parties featured in around 30 percent of the incidents investigated [261], [344].

By 2030, the risk of incidents is expected to rise through digital network management, decentralized energy production and the increasing automation of attacks on network-related components [111], [139], [146], [261].

Public administration

Government agencies and authorities occupy a special position within critical digital structures, as they form the digital basis for the state's ability to function properly. Among the impacted organizations, European administrative institutions and agencies account for the largest share of documented IT and OT-related incidents – around 38 percent [111]. Attacks on the public sector



Source: [187]

Figure 5: Average cost of a data breach by sector (worldwide)

are primarily aimed at disrupting digital processes and leaking sensitive data. From an attacker's point of view, public sector organizations are particularly attractive because successful intrusions immediately have a visible public impact [49], [111].

OT-related incidents mostly affect control systems for buildings and facilities, transportation, and local governments. The frequency of attacks on local authorities and municipalities is above average. Ransomware incidents regularly lead to the disruption of public services and internal administrative processes for weeks or months, directly undermining confidence in the government's ability to act [28], [49], [111], [187].

One critical structural risk factor is the combination of a high degree of digitalization with limited human and financial resources. IT infrastructures in local government have often evolved over long periods of time, tend to be heterogeneous, and suffer from deficiencies in standardization, patch management, centralized security management, and skilled personnel [49], [339].

Similar patterns can be seen in other public institutions with decentralized IT oversight, such as public universities. At these institutions, insufficiently consolidated system landscapes result in a sustained expansion of the attack surface. Around 75 percent of publicly accessible vulnerabilities at both universities and the IT landscapes of the federal states in Germany are more than a year old, indicating structural shortcomings in their patch and vulnerability management [10], [11].

Transportation and logistics

In the transportation and logistics sector, cyberattacks frequently have an impact across sectors and contribute to cascading business disruptions [111], [187], [261], [344]. In Europe, depending on the survey, between three and eight percent of IT and OT-related incidents occur in this sector [111]. The effects often extend beyond the organizations directly impacted and play out downstream along the value chain [28], [187], [344].

Digitalized management and coordination systems are prime targets for attack. Fleet, warehousing, and route management platforms are often interconnected via cloud services, external interfaces, and partner access points [86], [261], [344]. Inadequately secured remote access, compromised accounts, and misuse of maintenance tools are among the most common attack vectors [146], [261], [344].

As operational technology becomes increasingly integrated, the sector's OT exposure is likewise growing, particularly in controlling, interchange, and infrastructure systems involving multiple modes of transportation [111], [146]. Nearly half of organizations with OT components reported security-related incidents last year [146].

Looking ahead to the upcoming years, the level of risk is expected to increase further due to growing digitalization, the rise of platforms, and international dependencies [187], [261], [344].

1.4.2 Mid-sized companies and the pressure of digital transformation

While cyberattacks pose a financial risk to companies of all sizes, their impact and the targeted organization's ability to cope with them vary significantly depending on size. Mid-sized enterprises are particularly vulnerable. Their participation in digital supply and service chains, coupled with limited human and financial resources, significantly increases their exposure [28], [339]. At the same time, small and medium-sized businesses face systematic pressure to transform. Digitalization and platform dependency are steadily increasing, while the intensity of threats and regulatory requirements are growing faster than the available security capacities.

Cloud usage and lack of security policy

As central business processes are shifted to cloud and Software-as-a-Service (SaaS) environments, the risk profile of many companies is evolving. Damage is often caused by a lack of governance. Unclear, distributed responsibilities, and inadequate control of identities, permissions, and third-party access have become critical risk factors [187], [248], [339], [344].

Circumvention of MFA is a growing problem. This is particularly critical for SMEs, as centralized cloud accounts are used across the entire organization. A compromised admin or service account can consequently expose large parts of the IT and data environment [140], [176], [248], [344].

Beyond identity and access risks, there are also shortcomings related to the operational management of cloud usage. SaaS services are often introduced outside of formal IT processes and linked to existing identities. As a result, consistent security configurations and centralized logging are often lacking [28], [49], [248], [344]. This is compounded by a heavy reliance on ex-

ternal service providers. In around 30 percent of the security incidents investigated, the breach occurred via third parties or the supply chain, for instance through compromised service providers or software partners [344]. Particularly in medium-sized businesses, external access is growing faster than the maturity levels of their access separation, MFA enforcement, and monitoring efforts [248], [339], [344].

These shortcomings have a significant economic impact. Internationally, the average cost per security incident is US$4.44 million (according to figures from 2025) [187], [316]. Highly digitalized organizations are especially exposed to business interruptions and time-consuming, costly recovery measures. In German organizations, a lack of cloud governance and poor identity management contribute directly to increased business and supply chain risks. Such structural deficiencies have a particularly pronounced impact in situations where organizational measures to compensate for these shortcomings are limited or lacking [28], [187].

Investment and implementation pressure building at SMEs

At SMEs, security standards are often only partly implemented, while structured risk and emergency processes are frequently lacking [28], [148], [339]. This structural disadvantage is also reflected in available figures. Only 16 percent of small businesses are fully compliant with applicable cybersecurity standards, while around a quarter do not use any such standards at all [339].

The pressure to invest in appropriate solutions continues to build as modern attacks gain in scale and degree of automation. Particularly for organizations with limited resources, the need to adopt new countermeasures to respond to automated attacks is intensifying [49], [111], [248], [344]. At the same time, SMEs have to make ongoing investments in basic measures due to ever-shorter exploit cycles, even though their budgets and human resources are often planned on a project basis rather than for continuous operations [28], [339].

1.4.3 Supply chains and IT service providers under fire

Digital supply chains are a major target. Upstream service providers, software vendors, and technical dependencies make it possible for attackers to access multiple organizations at once with relatively little effort [139], [248], [261], [344].

This vulnerability is reflected in perceptions and organizational measures at SMEs. Around 66 percent of these organizations assess the security maturity of their suppliers, and 65 percent integrate security levels into procurement processes [348].

However, only 27 percent of SMEs simulate cyber incidents in collaboration with partners. Moreover, only 33 percent enjoy complete transparency regarding their supply chain dependencies and coordinate their security strategies with partners in the ecosystem [348]. These self-assessments by SMEs are consistent with empirical findings. Third parties or supply chains played a role in around 30 percent of the security incidents investigated – a rising trend [344].

This exposure stems less from individual technical vulnerabilities than structural dependencies. These include shared identity and access models, standardized platforms, permanently installed remote access, and unclear responsibilities with regard to security management [248], [339], [344].

Business compromise via managed service providers

Managed service providers (MSPs) are considered a particularly effective attack multiplier. They bundle IT operations, remote maintenance, and security functions for multiple customers and require privileged, organization-wide access rights [139], [248], [344]. By targeting MSPs, attackers aim to compromise a large number of customer systems through a single entry point and thus benefit from economies of scale [139], [261]. Technically, this is often achieved by misusing legitimate MSP access, especially by way of centralized remote maintenance and management platforms. Permanently active administration accounts and central management tools are often identified as the initial points of entry, especially in the context of ransomware and data theft campaigns [139], [316], [344]. Incidents involving MSPs lead to longer than average business interruptions and extended recovery times. This is because coordination, forensics, and recovery must be carried out across numerous impacted organizations in parallel [187], [261], [316].

Attacks exploiting update mechanisms and remote access

To target established trust and maintenance chains in modern IT and platform environments, attackers often exploit update mechanisms and remote access. Worldwide, attacks on supply chains and update mechanisms only make up a small fraction of all incidents. However, they rank among the most damaging types of attacks and the incidents requiring the longest recovery times [187], [261], [316]. In 2025, incidents in which compromised update processes or central management systems played a role exceeded the sector's average damage of $4.44 million per incident. They often led to recovery phases lasting several weeks [187], [316].

The reason is that after such attacks, it is not just individual systems that need to be cleaned up. All software versions, update pipelines, and trust chains need to be reassessed [187], [261]. Remote access compounds these risks, especially when it comes to centrally managed updates and management infrastructures. In Europe, depending on the industry in question, 20 to 40 percent of initial access by unauthorized parties is attributed to misuse of remote access, VPN accounts, or external maintenance interfaces [49], [111], [344]. Environments with permanently active maintenance accounts which lack MFA have particularly high exposure.

Abuse of trust exploiting integration partners

Integration partners such as IT system houses, software integrators, or providers of specialized applications have typically established permanent interfaces, service accounts, and API access with direct connections to productive systems in many organizations. Adversaries exploit this implicit trust in a systematic manner to penetrate target environments via existing integrations without having to overcome traditional perimeter or access controls [139], [248], [261], [344].

One documented example is a state-run APT campaign spanning several years, in which an external marketing and communications service provider was repeatedly compromised to gain indirect access to associated target organizations [163]. By leveraging the existing third-party relationship, the adversaries combined personalized phishing campaigns, prepared web content, and the misuse of legitimate integration paths. This enabled them to establish persistent access, keep multiple attack channels open in parallel, and adapt their activities in response to defensive measures [163].

One of the main risks stems from the technical design of such integrations. Service accounts and API tokens are often granted extensive permissions, remain active indefinitely, and are only subject to limited monitoring [248], [344]. In cloud environments, a significant proportion of successful attacks can be attributed to compromised machine identities, which bypass regular user controls and are virtually indistinguishable from legitimate access [140], [248], [344].

Consequently, the impact resulting from such incidents is particularly severe. Attacks involving integration or API access lead to longer detection and recovery times on average. Furthermore, the likelihood of follow-up attacks is increased, as technical dependencies, permissions, and data flows must be analyzed and cleaned up thoroughly across organizations [187], [261], [316].

As platform ecosystems and API-based integration continue to proliferate and expand, this risk is forecast to become even more acute by 2030 [139], [261], [330], [344].

1.5. SECURITY CHALLENGES AND STRUCTURAL GAPS

Despite increasing investment and growing awareness, the defensive capabilities of many organizations are lagging behind the ever-changing threat landscape. The reasons for this are rooted in systemic deficiencies in implementation, integration, and management. In many organizations, defense mechanisms are still heavily focused on isolated vulnerabilities. Meanwhile, attacks are increasingly targeting well-established, long-lasting attack surfaces [140], [248], [344].

Successful attacks prove particularly impactful in areas where control, prioritization, and transparency mechanisms are unable to keep pace with the dynamics of modern attacks [140], [187], [235].

These structural deficiencies affect just about every sector. Companies, public administrations, and operators of critical infrastructure consistently report shortcomings in governance, insufficiently secured identities, a shortage of skilled workers, as well as a growing discrepancy between technical complexity and organizational maturity [28], [49], [248], [339].

This imbalance is expected to become even more pronounced in coming years. Attacks are happening faster, involve more automation and increasingly focus on

Source: [202]

Figure 6: Main reasons for skills shortages in cybersecurity teams

platforms and identity, leaving the targeted organizations little time to implement defensive adjustments [139], [261], [344], [347].

1.5.1 Technical attack surfaces and vulnerabilities

At the technical level, the shortcomings become particularly evident in the handling of vulnerabilities, misconfigurations, and lacking transparency in complex IT and cloud environments [140], [235], [248], [344]. These issues are exacerbated in the context of AI-driven software development. A significant proportion of AI-generated code contains security vulnerabilities that can be multiplied through replication and automation [338].

At the same time, 60 to 80 percent of successful attacks exploit vulnerabilities or misconfigurations that are already known and for which countermeasures are already available [49], [140], [344]. This suggests that the main bottlenecks are related to prioritization and timely implementation under real operating conditions [74], [140], [187].

Vulnerability management and prioritization gaps

In practice, vulnerability management often fails due to limited capacity for remediation. Organizations are simply unable to close a significant proportion of vulnerabilities classified as critical within the recommended time frame [140], [344]. The problem, however, is not one of detection but of implementation [140], [187]. It often takes several weeks to fix critical vulnerabilities on business-critical systems, and patch cycles of more than 30 days are no exception to the rule [112].

The majority of organizations consider a reduction in cybersecurity personnel to be a factor that increases the likelihood of successful attacks. This assessment coincides with staff shortages, with 33 percent of organizations having insufficient budgets to adequately staff their cybersecurity teams [202]. Of these, 29 percent report not being able to afford qualified specialists (see Figure 6 for these and other reasons for skills shortages in cybersecurity teams).

At the same time, 36 percent of organizations report budgetary cuts in their cybersecurity departments, while 24 percent have reduced their numbers of cybersecurity staff [202]. These structural deficiencies and resource constraints are particularly acute in cloud and third-party environments, where responsibilities are fragmented and patch cycles are interdependent [248], [344]. Against this backdrop, vulnerability management is evolving from an operational task to a coordination and management issue, which requires clear rules governing responsibilities, dependencies, and escalation mechanisms.

In addition to this, prioritization suffers from systematic misjudgments in the weighting of attack points. Vulnerabilities are often assessed according to formal severity levels, while real exposure and actual exploitability

are not sufficiently taken into account [140], [235], [344]. Since attacks empirically concentrate on only a small portion of the vulnerabilities that can actually be exploited, a lack of risk-based prioritization increases the effectiveness of automated attacks [140], [187].

Misconfigurations and default access details

Misconfigurations are a frequently underestimated risk factor in their own right. Insecure default settings, accounts with excessive privileges, or incorrectly configured cloud and network risks are contributing factors in 20 to 30 percent of documented security incidents [140], [248], [344]. Unlike typical software vulnerabilities, these risks primarily arise from operational decisions, suboptimal implementation of standards, and inconsistent configuration changes [339], [344].

Access and identity configurations are particularly important in this regard. A significant proportion of cloud incidents can be traced back to overprivileged accounts, publicly accessible admin interfaces, or inadequately secured API and data storage resources [140], [248], [344]. In these cases, misconfigurations extend the reach and amplify the impact of compromised access, thus aggravating identity-based attacks. Default access details and weak authentication practices remain a factor in 20 to 32 percent of successful initial intrusion, particularly in network, administration and OT environments [49], [111], [344]. Incidents involving misconfiguration lead to longer detection times and higher recovery costs on average than attacks via clearly identifiable software vulnerabilities [187], [316].

Visibility and transparency deficiencies

Insufficient visibility exacerbates the risks arising from vulnerabilities and misconfigurations, as it hinders prioritization and prolongs response times [187], [344]. Internationally, 25 to 40 percent of organizations are unable to gain a complete overview of their productive IT assets, cloud resources, or externally accessible services [28], [248], [339]. As a result, they often lack robust, risk-based management of their technical security measures.

A lack of transparency is particularly pronounced in cloud and platform environments with dynamic and short-lived resources. Their status changes faster than existing tracking, monitoring, and controlling mechanisms are able to keep up with [248], [344].

1.5.2 Digital identities – an underestimated risk

Digital identities have become one of the most important and yet most difficult-to-control exposures in modern IT landscapes [139], [344], [347]. In many organizations, they constitute the primary control and access layer. However, mechanisms ensuring protection, control, and emergency response have not been developed to the same extent [66], [140], [344]. Risks related to digital identities are difficult to isolate because they simultaneously involve organizational, technical, and external dependencies.

Of all the security incidents investigated, 40 to 60 percent are wholly or partly attributable to the misuse of valid credentials [140], [248], [344].

Cloud-based services, federated authentication models, and third-party service providers are compounding this trend. As digital identities are increasingly valid across multiple systems and organizations, a single compromise can have far-reaching consequences [248], [344].

Identity theft: Access for every stage of an attack

Digital identities are gradually supplementing and supplanting traditional exploits as the main means of attack. Not only are they used to gain initial access but also employed across multiple stages of an attack. Compromised identities are used for lateral movement, escalation of privileges, and persistence in more than half of ransomware and data theft incidents [235], [316], [344].

Multiple use of identities increases the efficiency and reach of attacks. Incidents involving digital identities are typically associated with longer dwell times and higher recovery costs than attacks based on technical exploits [187], [316]. In highly cloud- and platform-centric environments, digital identities increasingly serve as a common thread running through the entire attack chain [139], [248], [344], [347].

Reliance on few login services

The increasing concentration of authentication activities on a small number of predominant login services poses a growing systemic risk. Countless organizations manage their business-critical processes – from communication to collaboration and administration – via a handful of centralized identity platforms [140], [248], [344].

The compromise of individual identity services or privileged roles thus has a wide-ranging impact throughout the organization and across services [248], [344].

Accordingly, incidents in highly centralized identity environments result in higher median recovery costs and longer business interruptions [187], [316]. Global admin roles, service accounts, and insufficiently controlled third-party access are especially at risk [248], [339], [344]. Furthermore, the number of destructive campaigns, in which productive workloads and data sets are deliberately deleted or tampered with, is reported to have increased by up to 87 percent [248].

Platform consolidation, single sign-on, and federated identity models reinforce this dependency. Without implementing additional security measures for privileged access, a clear separation concept, and contingency plans, the reliance on a small number of login services remains a key risk factor in modern IT landscapes [139], [261], [344], [347].

1.5.3 AI accelerates structural imbalances

Overall, AI does not appear to give one side a clear advantage, but rather to amplify existing structural imbalances [139], [248], [344]. While 94 percent of organizations view AI as one of the main forces shaping the cybersecurity landscape, 77 percent of them are already using AI to support security functions. Despite this, only 40 percent regularly screen AI tools before deploying them, while 29 percent do not perform any security checks at all [348].

Opportunities and risks posed by open models

Open AI models are particularly relevant in this context, as they are flexible, adaptable, and can be used without dependence on proprietary platform providers. Their use unlocks opportunities for faster innovation, greater transparency, and technological sovereignty – also when it comes to security [139], [261], [344], [347]. At the same time, however, open models make powerful AI more accessible to attackers, because they can be modified and misused in the absence of any centralized usage controls [139], [140], [337]. Additional risks arise due to inadequately secured AI infrastructures. Even self-operated models, vector databases, and inference services represent new attack surfaces, for instance by way of public APIs, corrupted training data, or model updates which have not been adequately checked or tested [261], [337].

In this way, open models reinforce the ambivalence of AI in the security context. While they boost independence and innovation, they also ramp up the requirements for governance, operational security, and access control [139], [261], [344], [347]. The use of AI amplifies any existing structural weaknesses in control, responsibility, and prioritization. It acts as an accelerator of risks, especially where governance structures, responsibilities, and decision-making processes have not kept pace with the reach of modern IT, cloud, and platform architectures [139], [261], [344], [347]. As a result, the core issue is shifting from the effectiveness of individual technical measures to considerations regarding the organizational and regulatory embedding of cybersecurity.

1.6 GOVERNANCE, REGULATION, AND MANAGEMENT RESPONSIBILITY

The systemic shortcomings described above clearly demonstrate that cybersecurity is increasingly determined by issues of governance, assignment of responsibility, and the ability to make decisions. The success of many cyberattacks is not due to technological failings, but rather the result of unclear responsibilities, fragmented governance, and a lack of strategic involvement at management level [72], [76], [139], [187], [261], [332], [344].

Cybersecurity as a management and control task

Organizations that have clearly defined governance structures and unambiguous management responsibilities are significantly more resilient to cyber incidents than organizations where cybersecurity is considered primarily an operational or technical issue [187], [261], [339]. Incidents can be contained more quickly in organizations where senior management demonstrates visible support. Moreover, organizations with established compliance and governance programs are significantly less likely to experience serious data breaches (78% to 21%) [330]. Deficiencies are particularly evident at organizations where cyber risks are not systematically integrated into risk management, business strategy, and formal decision-making processes. This lack of integration limits prioritization, control over investments, and responsiveness [28], [339], [344]. A lack of commitment from senior management is thus identified as a risk factor [201].

Even though cybersecurity is recognized as a relevant risk, clearly defined decision-making, escalation, and reporting lines are lacking. This gives rise to reactive investments, inconsistent implementation, and insufficient assessment of effectiveness [28], [187], [339]. Organizations that regularly report on cyber risks at the board or senior management level, on the other hand, have shorter response times and suffer less consequential damage [187], [261], [316].

Liability and decisions

Executive boards, management teams, and government agency heads are increasingly held accountable for security failings, for example in the context of supervisory proceedings, liability cases, or political reviews [28], [286], [339].

However, management decisions are often made under conditions where clarity is lacking due to limited transparency regarding attack surfaces, dependencies, and the effectiveness of security measures [248], [339], [344]. Governance structures are increasingly important in this context, as they are designed to facilitate decision-making even in situations where information is incomplete [187], [261].

No guarantee: Regulation ensures minimum security standards

Recent years have seen a significant hardening of cybersecurity regulations. National and European frameworks are increasingly mandating minimum requirements for risk management, reporting obligations, and protective measures [49], [111], [124], [286].

While it is true that highly regulated organizations are more likely to implement formal security processes, successful attacks also occur in these sectors – for instance, at critical infrastructure (CI) operators, in public administration, or in the financial sector [49], [111], [187].

One common reason for this is that regulatory requirements are formally met but not translated into operational measures [261], [339]. For example, regarding the implementation of NIS 2 requirements (see addendum for more details), organizational and resource-related factors are cited more frequently than technical aspects [112]. Regulation also continues to lag behind the development of threats in a structural sense. While attacks are increasingly targeting identities, platforms, and supply chains, many requirements are still based on the conventional defense of system and perimeter boundaries [139], [261], [344].

While regulation thus represents a necessary basis, it is not sufficient on its own to ensure effective cybersecurity management [261], [344], [347].

Organizational maturity, resources, and implementation reality

A key governance problem lies in the discrepancy between requirements and implementation capability [28], [286], [339]. Ninety-five percent of organizations state that they are currently unable to meet at least one relevant skill requirement. Fifty-nine percent have critical or significant skill gaps. AI skills (41 percent), cloud security skills (36 percent), risk assessment (29 percent), application security (28 percent), and GRC skills (27 percent) are particularly affected [202].

Security maturity depends less on the number of tools used than the clarity of processes, responsibilities, and prioritization mechanisms [187], [261]. Organizations with greater maturity have defined acceptable levels of risk, conduct regular reviews, and have well-established decision-making processes to follow in the event of a crisis [187], [316]. By contrast, a lack of governance often leads to reactive behavior, delays in communication, and the inefficient use of resources [28], [339].

From compliance to resilience

Over the coming years, we are likely to see a continued shift away from formal compliance and towards operational resilience. Cybersecurity is increasingly recognized to be an ongoing endeavor that requires continuous refinement, practice, and strategic leadership [139], [261], [344], [347].

To be successful, organizations will have to embrace cybersecurity as an integral part of their business and management activities, comparable with financial, human resources, or production risks [28], [187], [261].

Addressing the cybersecurity situation successfully hinges on the ability of organizations and decision-makers to take responsibility, set priorities transparently, and classify cybersecurity risks as an ongoing management issue [139], [187], [261], [344], [347].

Cybersecurity cannot be treated as a secondary technical task. On the contrary, it is a core management issue. Its effectiveness is measured in terms of resilience, ability to make decisions, and organizational maturity.

1.7 OUTLOOK 2026-2035

In the coming years, security architecture will be shaped by the convergence of systemic risks posed by artificial intelligence, the threat of decryption by quantum computing, and an increasingly vulnerable physical infrastructure. While climate change poses a threat to the hardware infrastructure, the emergence of autonomous systems and digital central bank currencies is resulting in the objectives of attacks shifting from pure data espionage to kinetic violence and state destabilization [330], [349].

AI as a global risk

By 2035, the "adverse outcomes of AI technologies" will rank among the top global risks, with systemic damage extending far beyond simple fraud [349]. Both adversaries and defenders will use AI on an ever-larger scale. Autonomous AI agents will carry out increasingly complex, multi-stage attacks with minimal human oversight [338]. These agents will be capable of making decisions, analyzing data, and adapting attack vectors in real time [338]. In addition, deepfakes and social engineering will become even more convincing and difficult to detect [147]. The use of AI-powered tools and "vibe coding" will continue to accelerate software development but also result in insecure code that creates new vulnerabilities [338].

While cyber espionage and digital warfare are set to remain permanent fixtures at the top of risk rankings, climate change increasingly acts as a risk multiplier. Extreme weather threatens physical IT infrastructure (data centers, submarine cables) and complicates efforts to secure it [349].

Encryption under threat (Q-Day)

Quantum Day (Q-Day) marks the point in time (estimated sometime between 2030 and 2035) when quantum computers will have the capacity to break today's standard encryption methods [330]. Since these techniques form the bedrock on which internet security is built, governments are calling for a switch to post-quantum cryptography by 2035 at the latest. For critical systems, the deadline is set at 2030 [248]. Another urgent, concerning issue is the "harvest now, decrypt later" strategy. Attackers are already stealing encrypted data today with the intention of decrypting it later. This means that quantum security is already crucial today for data which needs to remain secret over the long term [248], [330], [341].

Technological transformation expanding the attack surface

Technological transformation will give rise to new critical areas of risk by 2030 which have hardly been in focus to date. One area concerns the vulnerability of physical infrastructure and its interface with robotics. Cyberattacks on satellite infrastructure or undersea cables – a topic already explored in depth in Schwarz Digits Cyber Security Report 2025 – remain a major threat to the global economy [349].

In combination with the infiltration of autonomous, humanoid systems, such attacks could cause direct material damage or physical violence in the future. Given that such systems operate in milliseconds, they mark a transition from digital espionage to kinetic threat scenarios and modern warfare (see Chapter 3 of this Cyber Security Report) [349].

At the same time, new systemic risks are emerging in the financial sector. The introduction of digital central bank currencies is creating highly complex architectures that present new targets of attack capable of destabilizing entire economies [349].

These qualitatively new dangers are compounded by explosive quantitative growth in the IT landscape. The German federal states exemplify this trend, with the number of IT services expected to quadruple to 400,000 by 2035. Outdated systems and a "patch backlog" also pose significant risks. With the threat of critical vulnerabilities increasing tenfold, automated defense systems will become indispensable for ensuring the state's ability to act in such highly dynamic environments [10].

CHAPTER 2

GERMAN BUSINESS SURVEY
CYBERSECURITY AND DIGITAL SOVEREIGNTY

Share of overall IT budget devoted to IT security

2024
8%

2025
17%

High levels of acceptance for active security countermeasures

79%

of the companies surveyed were in favor of state orchestrated “hackbacks” against foreign attackers

Insufficient risk prevention

Only
36%
of the companies surveyed carry out penetration testing

42%
willing to pay more for digital sovereignty

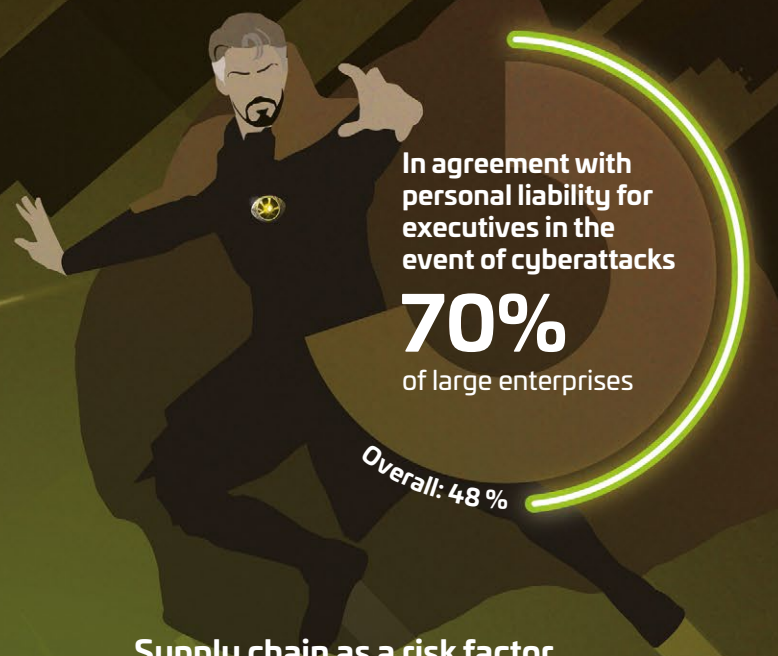
Only every 8th company
has concrete plans to invest in reducing dependencies (13%)

Has the company implemented binding guidelines for the use of GenAI applications?

at 73% of large enterprises

at 26% of all companies

Source: Own survey



In agreement with personal liability for executives in the event of cyberattacks

70%

of large enterprises

Overall: 48 %

CISO position established?

NO

57%

Yes, only 43%

Supply chain as a risk factor

51%

of companies reported cyberattacks at their suppliers

75%

of companies nevertheless forego auditing suppliers

67%

of repondents find state support inadequate to protect them from cyberattacks

Do European Data Spaces boost digital sovereignty in the EU?

YES: **50%**

59%

agreement in the financial sector

European Financial Data Space

68%

agreement in the healthcare sector

European Health Data Space

Well positioned to combat cyber threats?

15%
Federal government

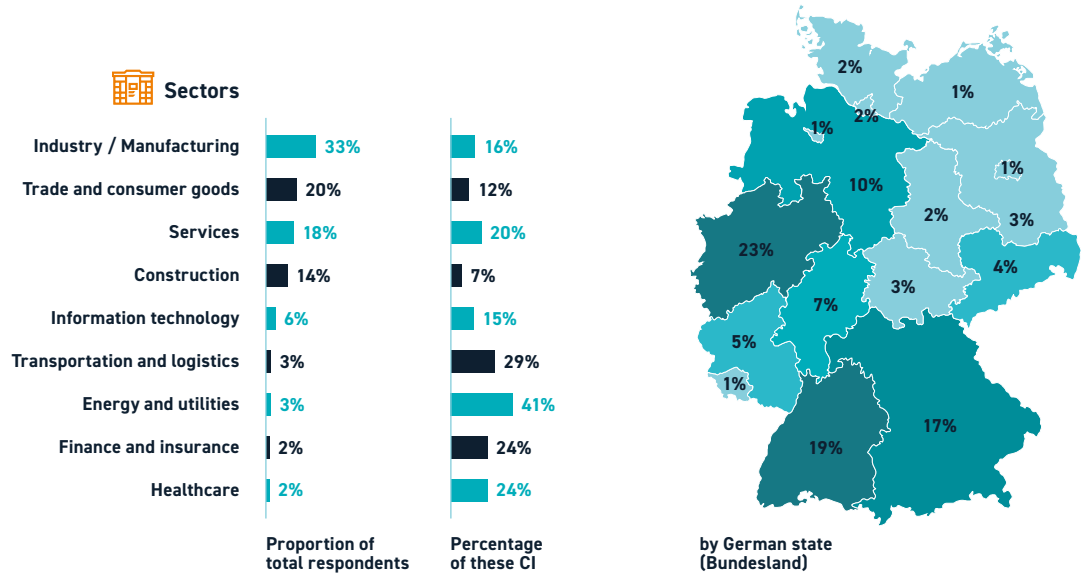
12% States (Bundesländer)

7%
Local / municipal administration

2 GERMAN BUSINESS SURVEY – CYBERSECURITY AND DIGITAL SOVEREIGNTY

German businesses are operating in an environment characterized by dynamic threats and mounting regulatory pressure. At the same time, there is a growing need for digital sovereignty to sustainably reduce technological dependencies in global supply chains and build up digital resilience.

In this climate, cybersecurity is no longer just an operational IT task, but a key strategic challenge that has a decisive impact on the ability of German companies to achieve long-term commercial success.



Any discrepancy in aggregate values is due to the rounding of numbers.
This applies to all figures in the text and illustrations in this chapter.

Source: Own survey

Figure 7: Overview of the survey sample by sector, federal state, company size, and internationality (in %)

	(C)ISO		
	Total	Yes	No
N	1001	466	535
Very good level of preparedness	17%	22%[1]	14%
Good level of preparedness	48%	51%	46%
Average level of preparedness	28%	22%	31%[1]
Insufficient level of preparedness	4%	3%	6%[1]
No response	3%	2%	4%

1 The results are statistically significant at a level of α = 0.01

Source: Own survey

Table 1: Correlation between having a (C)ISO and self-assessment of preparedness to deal with threats

2.1 STUDY DESIGN

This study is based on a representative survey among small and medium-sized businesses (SMB) as well as enterprises on cybersecurity and digital sovereignty in Germany, which was conducted in the fourth quarter of 2025.

The survey covers strategic, organizational, and operational aspects of cybersecurity. This study builds on the previous survey conducted in the fourth quarter of 2024 [302] to generate longitudinal and trend data.

The data was collected using computer-assisted telephone interviews (CATI) with 1,001 companies in Germany. The survey targeted experts in IT roles who have insight into their organizations' security structures. Thanks to representative weighting, the sample provides a reliable picture of the German corporate landscape (see Figure 7).

2.2 PERCEPTION OF THREATS

How companies perceive cyber threats and their own vulnerability has a significant impact on how they organize and prioritize cybersecurity strategies. Assessments regarding their own preparedness, extent of the damage, and new technological risks provide insight into how seriously cybersecurity is taken as a business risk, as well as where there may be discrepancies between self-perception and reality.

Large enterprises feel better prepared to deal with cyber threats

The majority of companies surveyed in Germany rate their cybersecurity preparedness as good to very good. Overall, 65 percent of respondents say they are (very) well prepared. This assessment is stable over time, with 66 percent stating they were well prepared in 2024 [302].

The picture is consistent across all company sizes, but differs in the degree of confidence.

Large enterprises rate their level of preparedness as very good significantly more often than SMBs. While 28 percent of large enterprises consider themselves very well prepared, only 16 percent of small companies and 18 percent of medium-sized companies do so.

Moreover, companies with a dedicated (Chief) Information Security Officer ((C)ISO) role are significantly more likely to rate themselves as very well prepared than those without one (see Table 1).

Compared to other German studies [339], in which 91 percent of companies rate themselves as well protected, results in this survey are more modest. At the same time, a contrast remains between perceived preparedness and the growing number of cyberattacks.

In terms of internal threats, such as data exfiltration due to carelessness or insiders, 56 percent of companies rate their cybersecurity as at least good, with large enterprises particularly likely to rate their resilience as very good (26 percent). This is in line with global studies, according to which 77 percent of all organizations have recorded at least one data protection-related incident caused by insiders within the last 18 months [148].

Twenty percent of companies have already fallen victim to a cyberattack

Few companies report having experienced attacks themselves. Overall, 20 percent have already suffered a cyberattack. Large enterprises are affected significantly more often, with 33 percent reporting at least one attack. A study on data theft [135] in 2025 showed similar results, with 33 percent of responding companies impacted. However, since two-thirds of respondents in the study had annual revenues of more than €25 million, no conclusions can be drawn regarding SMBs.

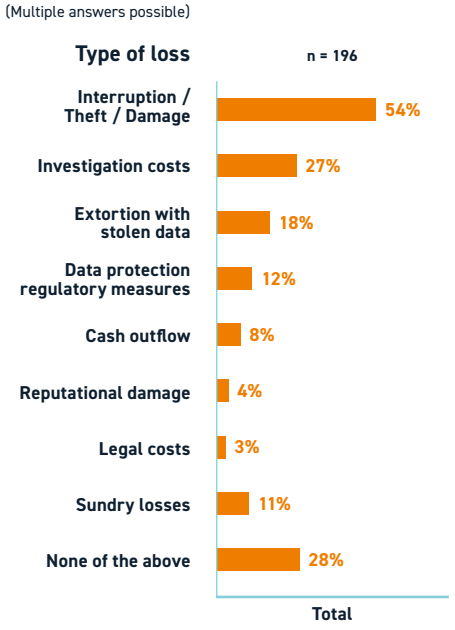
When classifying cyberattacks in terms of when they occurred, significant differences emerge depending on company size. Large companies report more recent incidents considerably more often, with 41 percent stating that they were victims of a cyberattack in 2023 or 2024. Small and medium-sized companies, on the other hand, report attacks which took place in the more distant past significantly more often, with the majority citing incidents in 2022 or earlier (65 percent in each case). Only 20 percent of respondents reported having fallen victim in 2025.

Outages, theft, and reputational harm are the most common types of damage

The consequences of cyberattacks manifest themselves in various forms of loss (see Figure 8). Outages, theft, and reputational damage are the most frequently cited. In addition, 27 percent of the impacted companies report incurring costs associated with investigating the incident. These are significantly more common in companies without a (C)ISO. In addition, large enterprises suffer harm to their image much more frequently (21 percent). There are also differences between industries. In the finance and insurance sectors, as well as in healthcare, extortion involving stolen data is reported much more frequently than in other sectors.

Overall damage of €202 billion from cyberattacks seems realistic for three-quarters of companies

Against this backdrop, companies were asked how realistic they consider the estimated damage from cyberattacks to the German economy of €202 billion, as reported in Bitkom's frequently cited study [28]. Three-quarters of respondents consider this figure to be realistic. While 76 percent agree with this estimate, 11 percent consider it unrealistic. SMBs are significantly more likely to respond that they are unable or unwilling to give an assessment. Large companies are significantly more likely to consider the amount of damage to be realistic (86 percent). Among companies that consider the Bitkom study's figure unrealistic, the prevailing opinion is that the actual damage has been underestimated.



Source: Own survey

Figure 8: Losses resulting from cyberattacks

AI is only partially on the risk radar despite new attack vectors

In addition to conventional attack scenarios, the use of artificial intelligence (AI) is increasingly a focus of risk perception. Nevertheless, more than half of companies rate the cybersecurity risk posed by the use of AI as non-existent or negligible (54 percent). A closer look shows figures of 55 percent for small companies and 32 percent for large companies. Indeed, medium-sized and large companies are significantly more likely to rate the risk as very high (see Figure 9).

Companies cite shadow AI and uncontrolled data leakage by employees (38 percent) as the major new attack vectors associated with the use of AI and large language models (LLM). They see further risks in the AI-supported refinement of social media attacks (24 percent) and in attacks on AI systems and their results, for example through prompt injection (11 percent). Critical infrastructure (CI) companies are significantly more likely (48 percent) to point out the potential dangers of shadow AI and uncontrolled data leakage than other companies. In the finance and insurance industry, on the other hand, the risk posed by social engineering is highlighted significantly more often than in other sectors.

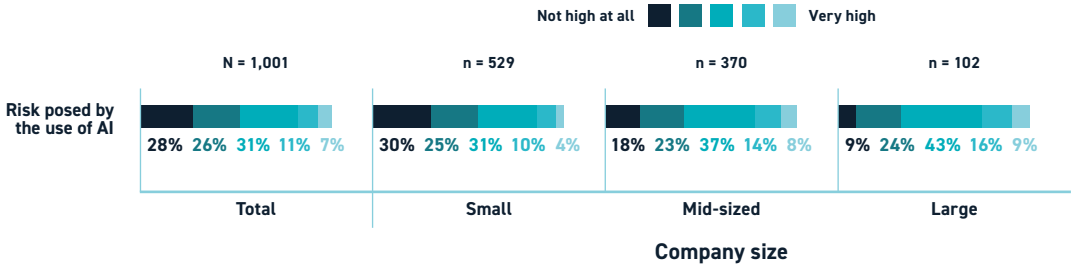
2.3 IT SECURITY BUDGETS

As company size increases, both their overall IT budgets and the proportion allocated to IT security rise. At the same time, the majority of the companies surveyed operate with comparatively limited IT budgets. Overall, 70 percent have an annual IT budget of less than €100,000. Among medium-sized companies, the proportion is still around 50 percent, but the picture changes significantly among large companies, where 27 percent say they have an IT budget of at least €1 million. CI companies also stand out in this respect, with around 60 percent of them having an IT budget exceeding €100,000.

IT security budget as share of total IT budget rises sharply from 2024 to 2025

The share of the IT budget devoted to IT security averages 17 percent and varies depending on company size. While small companies also spend around 17 percent on average, the proportion rises to 22 percent for large companies. Over time, there has been a significant shift in this regard. While the overall IT budget has increased, the proportion of funds earmarked for IT security has more than doubled from 8 percent in 2024.

This places the reported proportion at a similar level to the Bitkom study [28], which reveals an average IT security share of 18 percent for companies with annual revenues of at least one million euros. Given the broader range of companies covered by this survey, the result appears consistent.



Source: Own survey

Figure 9: Perceived risk of using AI increases in correlation with company size

A look at the total cybersecurity budgets reported in the current survey, excluding personnel costs but including tech expenditure and external service providers, highlights the disparity between companies of different sizes. Overall, 85 percent of companies have an annual cybersecurity budget of less than €100,000. Among large enterprises, this proportion is significantly lower, at 41 percent.

A comparison with international data from the EU cybersecurity agency, European Network and Information Security Agency (ENISA), puts these results into context. In their EU-wide survey, covering all 27 member states and all NIS 2 sectors, the median IT budget allocated to cybersecurity is around nine percent of the total IT budget. The average investment per organization is around 1.5 million euros [112].

Cybersecurity budgets are on the rise

Over the past twelve months, 36 percent of the companies surveyed increased their cybersecurity budgets. Among large companies this trend is particularly pronounced, with more than half of them (53 percent) reporting higher budgets. In contrast, the budgets of small companies mostly remained unchanged, with 65 percent making no budgetary adjustments.

In a comparable global survey, around 50 percent of companies reported having increased their cybersecurity budgets, while a third said their budgets had remained unchanged. At the same time, this trend appears to be slowing down, as budget increases were cited at a higher rate in the years prior to 2025. Correspondingly, the proportion of unchanged or reduced budgets has increased, which indicates a more restrained approach to cybersecurity budget planning at present [36]. This picture is consistent with data for Europe published by ENISA, which indicates that investment for the current year has remained level with the previous year [112].

A key factor driving budget increases is the response to the heightened threat situation, with a rise in phishing attacks and incidents in the company's immediate business environment, such as hacks suffered by partner companies or industry peers, acting as catalysts. In sectors such as manufacturing and heavy industry, cybersecurity is becoming a strategic priority due to the NIS 2 Directive. In the healthcare and energy sectors, however, the focus is primarily on the personal liability of management and the prevention of potentially life-threatening system failures due to ransomware. In retail, on the other hand, media awareness, protecting company reputation, and involuntary cost increases for software licenses often push up spending, along with the necessary modernization cycles and cyber insurance requirements.

These spending requirements are countered by targeted budget reductions, which respondents often attribute to the elimination of one-time costs following the completion of projects or efficiency gains through cloud migrations. Nevertheless, critical cost-cutting measures are also driven by general economic pressure, staff reductions, or a dangerous underestimation of the actual risk.

The findings are consistent with a broader European trend. Across Europe, 70 percent of companies state that regulatory compliance requirements such as NIS 2, the Digital Operational Resilience Act (DORA), or the Cyber Resilience Act (CRA) were the primary reason for their investment in cybersecurity [112]. This makes it clear that the regulatory framework will serve as the primary driving force behind the financial prioritization of security measures in 2026.

2.4 IT STAFFING: ORGANIZATIONAL STRUCTURE AND COMPLIANCE ROLES

The personnel structure for IT security and compliance plays a decisive role in determining whether cyber resilience is understood merely as a regulatory obligation or as a living strategy within an organization. The present data reveals a clear discrepancy between the stable staffing of legally prescribed data protection roles and the inconsistent establishment of dedicated security officer positions, such as a CISO.

Corporate IT jobs are increasing, yet IT security positions remain sporadic

Nearly 69 percent of companies report having a maximum of ten IT positions, while an additional 15 percent report having up to 25 employees working in IT. Only in large corporations does a significantly different structure emerge, with 20 percent of these companies reporting more than 100 IT positions. The difference is particularly striking in CI companies, which are significantly more likely to have larger IT departments. Around 32 percent of CI companies employ 26 or more IT staff, compared to 14 percent of non-CI companies.

In a year-on-year comparison, the total number of IT workers per company has increased. While in 2024, 91 percent of companies still reported a maximum of ten IT positions, this proportion has now decreased. Conversely, the proportion of companies with more than ten IT employees has grown [302].

Staffing levels are significantly lower when it comes to IT security. Nearly all companies (94 percent) have a maximum of ten jobs that deal exclusively or mainly with IT security. This picture has remained consistent over time. In 2024, 97 percent of companies reported having a maximum of ten such positions [302].

On average, a third of data protection officers (DPOs) are company employees, with this figure rising for the IT, finance, and insurance sectors

A more nuanced picture emerges when it comes to the form compliance roles take, particularly with regard to data protection. The vast majority of companies, 91 percent, have a designated data protection officer. External appointments predominate, accounting for 58 percent, while around one-third (33 percent) employ a DPO internally. Only nine percent of companies report currently having no one filling this role.

This structure is largely shaped by the legal requirements set out in the Federal Data Protection Act. According to Section 38 (1) clause 1, organizations are required to appoint a data protection officer if at least 20 people are regularly involved in the automated processing of personal data. While large enterprises are slightly more likely to appoint internally employed data protection officers (DPOs) and only seldom forgo this role entirely, small and medium-sized businesses predominantly resort to external solutions. However, there are clear sector-specific trends. In the financial and insurance sectors, as well as in information technology, data protection officers are more often appointed as company employees. In the industrial/manufacturing, retail and consumer goods sectors, on the other hand, external models clearly dominate.

A (C)ISO role has not been established in 57 percent of companies

This is in stark contrast to the (C)ISO role, which is much less common. Overall, 19 percent of companies have an internally employed (C)ISO and 24 percent have an external (C)ISO, while 57 percent have no (C)ISO position. There are significant differences depending on company size. While around 60 percent of small companies do not have a (C)ISO, this figure drops to just under 49 percent for medium-sized companies and 34 percent for large enterprises. Accordingly, the proportion of internal (C)ISOs increases significantly in large enterprises. Internationally active companies are also significantly more likely to have a (C)ISO than organizations only operating domestically.

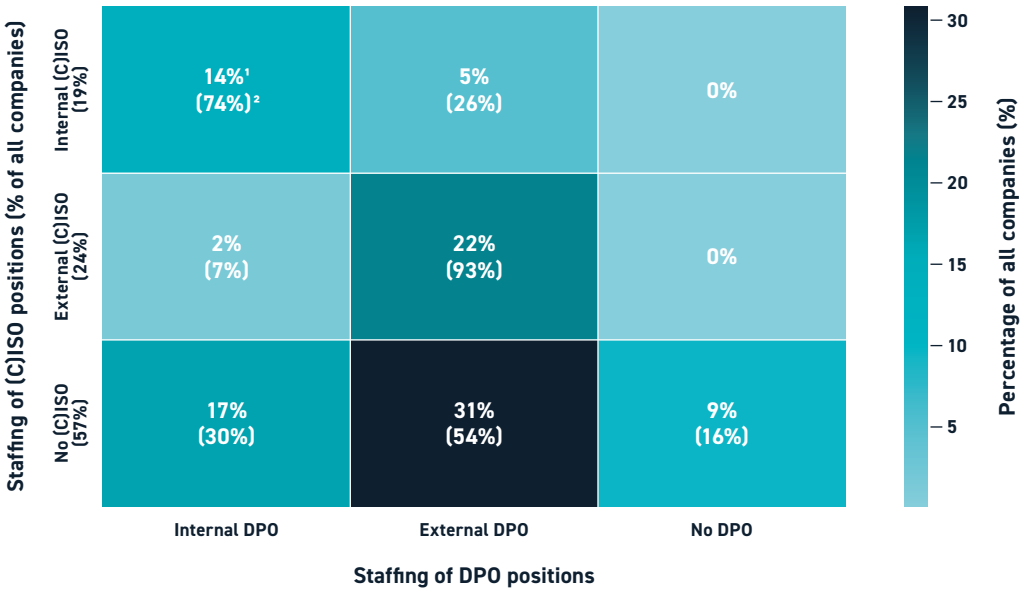
Internal staffing of (C)ISO and DPO positions correlate, internal DPOs decline

Analysis of security staffing structures at the companies surveyed reveals them to be largely shaped by compliance-driven organizational principles. While the majority of companies have data protection officers, the (C)ISO role remains unfilled significantly more often. This suggests that data protection is primarily understood as a legally mandated function, the filling of which directly results from regulatory requirements. In contrast, responsibility for information security is less often established as an independent strategic role.

The choice of staffing strategy follows recognizable patterns. Companies with an internal (C)ISO also have an internal DPO in around 74 percent of cases. Conversely, in companies with an external DPO, there is no (C)ISO in over 70 percent of cases, which is also the most common combination. Another significant finding is that companies with an existing (C)ISO (internal or external) are significantly more likely (65 percent) to appoint an external DPO than companies without a (C)ISO (54 percent). If there is no DPO at all, there is almost always no (C)ISO either (see Figure 10). Against this backdrop, it is striking that the presence of internally employed DPOs is in decline. While 38 percent of companies still had an internally employed DPO in 2024 [302], this proportion is now significantly lower.

Sixty percent consider a gross annual salary of less than €100,000 appropriate for CISOs

An assessment of the market value of the CISO role highlights profound systemic differences in the perception of information security. Around 60 percent of the companies surveyed consider an annual gross salary of less than €100,000 to be commensurate, while 15 percent consider remuneration in the range of €100,000 to €150,000 to be appropriate. This assessment is significantly below the market values observed in Germany, which show median remuneration of around €198,000 across all experience levels (see Figure 11).



1 The first number represents the proportion of all participating companies (the sum of all fields = 100%).
2 The percentage shown in brackets indicates the proportion within the respective (C)ISO group (corresponds to the values in the text).

Source: Own survey

Figure 10: Staffing strategies for (C)ISO and DPO positions

Considering this discrepancy, it becomes clear that finding qualified experts is proving to be an impossible task for many companies. International comparisons further exacerbate this discrepancy. In the US, for example, the median salary for CISOs ranges between $385,000 [296] and $392,000 [186]. Meanwhile, European studies reveal significant difficulties in filling cybersecurity positions. Around three-quarters of organizations report having difficulty filling open positions [112].

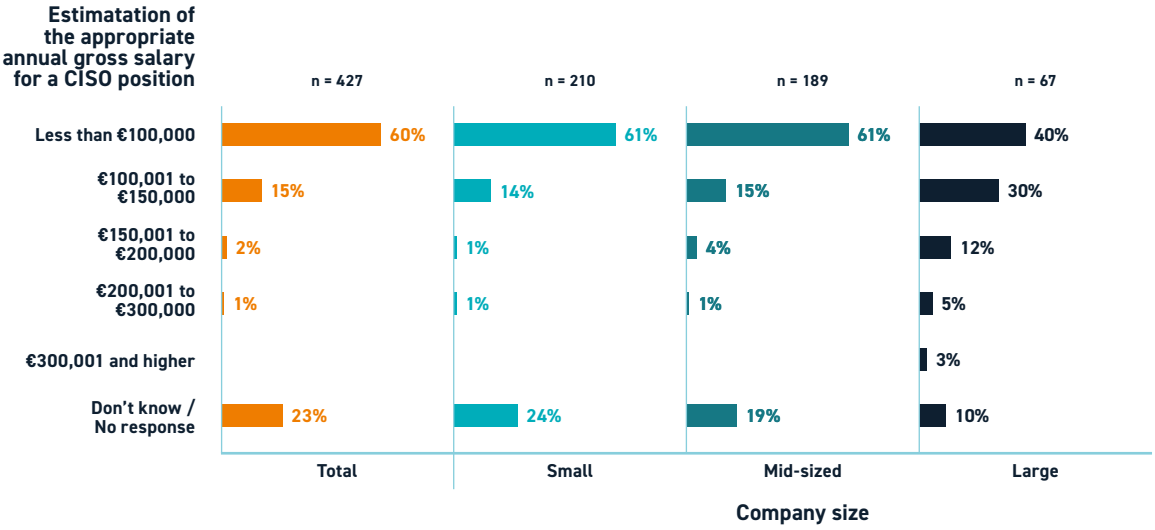
2.5 RISK MANAGEMENT AND PREVENTION

Security operations to safeguard IT infrastructure at German companies paints an ambivalent picture, ranging from sophisticated monitoring to significant gaps in preventive risk analysis.

Risk analyses and penetration tests are still uncharted territory for many companies

One of the key components, the comprehensive analysis of risks and exposures, remains far from being implemented across the board. On average, 40 percent of companies indicate that they have never conducted such an analysis, with this gap particularly pronounced among small businesses (43 percent). While medium-sized companies and large enterprises have often conducted such analyses relatively recently, smaller players tend to have less depth of planning in this regard. While 40 percent of medium-sized businesses and 46 percent of large enterprises are planning an analysis for 2026, 67 percent of small enterprises have not yet made any plans for such measures.

A similar situation prevails with penetration tests, which are only carried out by 36 percent of all companies. While medium-sized companies and large enterprises use these tests much more frequently and on a more regular basis, 61 percent of small companies forgo them entirely (compared with 56 percent on average). Where pen tests are carried out, 40 percent do so once a year, while 27 percent perform them on an ad hoc basis as considered necessary. Compared to the previous year, there has been a slight shift here. While in 2024, 62 percent of respondents said they did not carry out pen tests [302], the proportion of those who carried out tests on an ad hoc basis rose from 15 percent in 2024 to 27 percent in 2025. Currently, 58 percent of the companies that conduct pen tests state that they completed their last test in the survey year 2025.



Source: Own survey

Figure 11: Estimating the appropriate annual gross salary for a CISO position

Sixty-nine percent of companies rely on external service providers for system monitoring

Despite shortcomings when it comes to risk analysis, more than two-thirds of companies based in Germany (69 percent) rely on third-party service providers for system monitoring, including security operations centers (SOCs) or managed security services (MSS). The information technology sector is an exception to this trend, with 55 percent of IT companies choosing not to use external monitoring and instead managing these tasks in-house significantly more often.

To combat internal IT threats, German companies primarily rely on monitoring access rights (76 percent) and awareness training (70 percent). At large and medium-sized companies, training courses are the top priority, with adoption rates of up to 95 percent. Regular audits (42 percent) and employee screening (2 percent) follow with a significant gap, the latter having decreased compared to 2024 levels (51 percent) [302]. These measures are supplemented by firewalls, backups, and two-factor authentication, as well as reactive SOC structures.

There is a clear divergence in governance approaches when it comes to generative AI, depending on company size. While 72 percent of large enterprises already have high levels of rules and regulations in place, only 19 percent of small companies currently have corresponding guidelines (and 26 percent of all companies surveyed). There is also a lack of governance in the area of critical infrastructure. To date, only 60 percent of these companies have implemented binding guidelines for the use of generative AI applications.

2.6 SUPPLY CHAIN RISK

Securing the supply chain presents German companies with considerable challenges, particularly with regard to their dependence on external partners and global service providers.

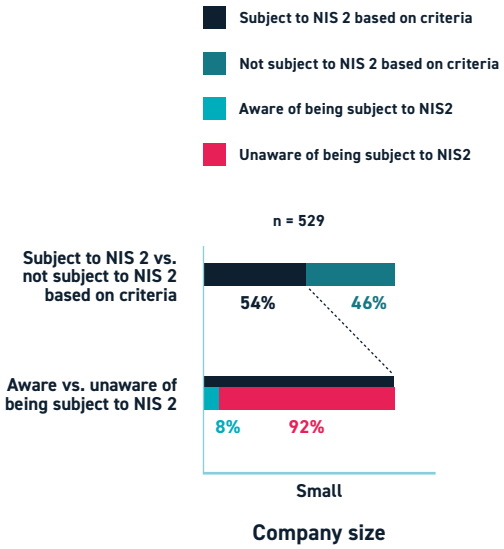
More than two-thirds of companies do not regularly assess suppliers' cybersecurity

While 51 percent of companies already report that one or more of their suppliers has fallen victim to a cyberattack, the rate is significantly higher among large enterprises at 65 percent. Despite these incidents, proactive checks for security vulnerabilities among partners are rarely carried out. Around 66 percent of respondents do not conduct any checks whatsoever. Only large enterprises show more active supervision, with 27 percent of them identifying one to four security vulnerabilities among their suppliers over the past year. The range of responses to incidents at suppliers varies widely, from immediately blocking communication and cutting all ties to cooperative problem-solving and activation of internal emergency protocols. In addition, technical security measures are implemented to safeguard the company's own systems, and awareness training is provided for its own employees. Nonetheless, 75 percent of companies do not conduct regular audits or assessments to evaluate the cybersecurity of their suppliers. Larger companies are more likely to carry out such checks, in most cases annually or more frequently (19 percent). These supplier audit processes are primarily found in the CI sector, where 51 percent of companies carry out audits, mostly annually or more frequently (24 percent).

Supply chain disruption, including from the US, considered a potential risk with limited alternatives available

Regarding the risk for supply chain disruptions of critical digital services from the US, a wide range of assessments were expressed. Across all companies, 27 percent rate the risk as low, 30 percent as medium, and 20 percent as high. However, large enterprises take a much more critical view, with 39 percent rating the risk as medium and 28 percent as high. Uncertainty prevails among smaller players, with small and medium-sized businesses significantly more likely to state that they cannot estimate the risk (25 percent and 22 percent respectively).

Should a key non-EU cloud provider discontinue its service, 57 percent of companies predict that their business-critical processes would take less than a week to recover. However, 19 percent of small companies were unable to provide any information on this. There are also gaps in the know-how required for changing providers in an emergency. While 49 percent of respondents feel they have sufficient knowledge, a figure that rises to 60 percent among large enterprises, 33 percent say they lack the necessary expertise. Even among large enterprises, 17 percent only responded with "partially."



Source: Own survey

Figure 12: NIS 2 knowledge gap at small companies

2.7 NIS 2 REGULATIONS AND OBLIGATIONS

The introduction of the NIS 2 Directive reveals a profound discrepancy between the objective legal situation and the subjective perception among SMBs. While a significant proportion of companies underestimate the extent to which they are impacted due to complex thresholds, there is growing pressure on senior managers to protect themselves against personal liability for regulatory failures.

NIS 2: Knowledge gap among SMBs means smaller companies, in particular, need to review their assessment

A direct survey on the impact of the NIS 2 Directive reveals a clear correlation with company size. While 93 percent of small companies claim *not* to be affected by the Directive, the picture is different for larger organizations, with 22 percent of medium-sized companies stating that they are affected (78 percent claim they are not), and 43 percent of large enterprises identifying themselves as subject to regulations.

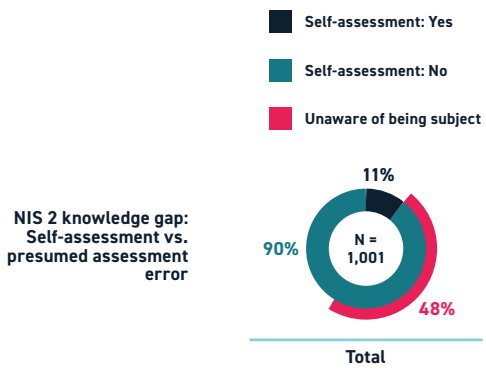
However, analysis of the overall data suggests that the actual scope of the regulation is significantly underestimated. When the information provided by companies on their sector, number of employees, and turnover is checked against the formal criteria contained in the Directive as of the end of 2025 [50], the profiles of an additional 478 organizations suggest that they may be subject to NIS 2. Since the survey method makes it impossible to draw conclusions about individual companies, and conclusive classification requires a detailed legal review, these figures merely serve to indicate the possibility of incorrect assessment. A significant proportion of the organizations potentially covered by the Directive appear not to have been aware of their regulatory obligations at the time of the survey.

It may be presumed that this widespread misconception is especially due to incorrect application of the size cap rule. The turnover threshold, in particular, seems to lead to errors in the case of small companies with 10 to 49 employees. Many of these companies apparently assume that they are not affected due to their small workforce, even though they exceed the applicable turnover threshold of €10 million. Looking specifically at this group of small companies with high turnover, 92 percent can be said to have incorrectly assessed their situation based on the formal criteria (see Figure 12). Overall, the data suggests that 48 percent of

all companies surveyed may be unaware that they are subject to the Directive (see Figure 13). These findings point to a knowledge gap among SMBs. While large enterprises tend to be more aware of their obligations, medium-sized and small companies with high turnover do not yet seem to be fully aware how the NIS 2 regulations apply to their own profiles.

Staff shortages, legal uncertainty, and limited budgets are the main obstacles to NIS 2 implementation

Companies that consider themselves subject to the NIS 2 Directive report facing significant operational obstacles. They cite a lack of human resources (58 percent), legal uncertainty (45 percent), and limited budgets (43 percent) as their biggest challenges in implementing the NIS 2 Directive (see Figure 14). Even in critical infrastructure sectors, there is a lack of information. While 49 percent of CI companies describe themselves as (very) well informed, 54 percent of smaller CI companies and 41 percent of large CI organizations say they feel poorly or not at all informed about the specific requirements. This perception correlates with criticism regarding the lack of engagement from government institutions, with 62 percent of respondents stating that they do not feel sufficiently supported by the relevant authorities in the NIS 2 implementation process.



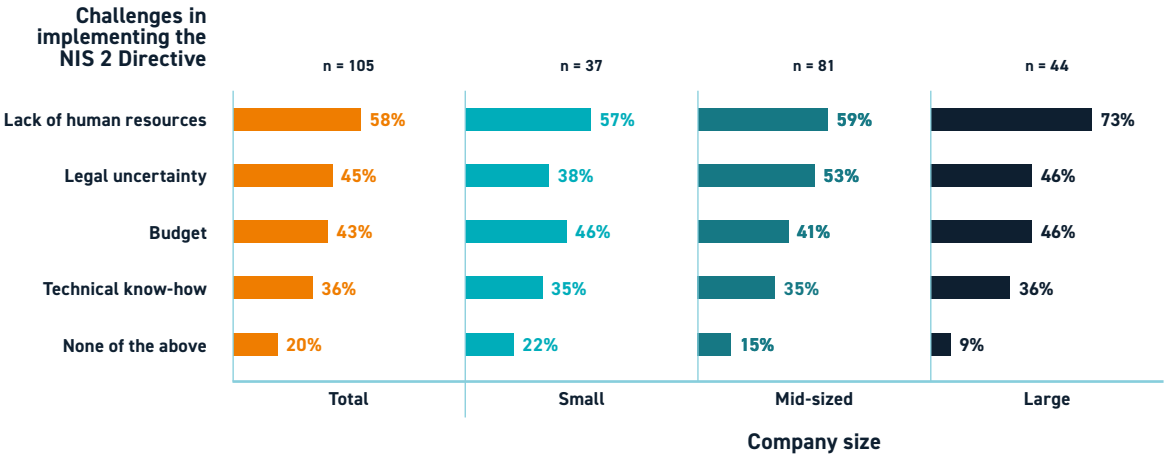
Source: Own survey

Figure 13: NIS 2 knowledge gap

Against this backdrop, the debate on personal responsibility enjoys widespread support. Forty-eight percent of respondents are supportive of personal liability for executives and supervisory board members in the event of inadequate protection against cyberattacks, with this demand receiving even stronger support from large enterprises (70 percent) and within the CI sectors (60 percent). This assessment is in line with current regulatory developments under the NIS 2 Directive. As the launch of the new BSI reporting portal makes clear, corporate liability will now be at the heart of compliance for around 30,000 companies. The fact that large enterprises and CI operators are especially supportive of liability can be attributed to the draconian sanctions of up to 2 percent of global annual turnover. In these sectors, the personal liability of management is increasingly seen as an indispensable lever for raising IT security to the same strategic level as antitrust law or data protection [103].

2.8 DIGITAL SOVEREIGNTY AND SUPPLY CHAIN RESILIENCE

At the latest since 2025, digital sovereignty has become an issue to be addressed also on a strategic and operational level. While initiatives such as GAIA-X, the European Data Spaces, and the EU Cloud Sovereignty Framework (see Chapter 4) are outlining the goal of digital sovereignty at the political level, companies are faced with the practical challenge of securing their ability to operate in a volatile and networked world. Digital sovereignty is not an end in itself, but rather the cornerstone of resilience. The ability to maintain critical systems, even in the face of geopolitical tensions or supply chain interruptions, depends directly on how strongly companies are locked into dependencies (vendor lock-in) and how well they can manage them. The present findings illustrate how German IT decision-makers are navigating between strategic aspirations and operational reality.



Source: Own survey

Figure 14: Biggest challenges in implementing the NIS 2 Directive

2.8.1 Digital sovereignty is most rooted in strategy of larger and highly regulated organizations

One in five companies is pursuing a digital sovereignty strategy – although the topic is particularly relevant for medium-sized companies and large enterprises

Despite the omnipresence of digital sovereignty as a geopolitical and economic buzzword, the reality at German companies paints a different picture. In many cases, the topic still seems to be a peripheral phenomenon. Only 19 percent of the companies surveyed report having a defined strategy for digital sovereignty (see Figure 15). In contrast, a significant majority of 68 percent are currently operating without such a strategic orientation. These figures are consistent with a study from May 2025, which found that only 18 percent of German and 22 percent of French companies identified "tech readiness" as a C-level priority [18]. These figures suggest that digital sovereignty is often rather seen as an abstract political goal than a concrete aspect of corporate strategy.

Nevertheless, a look at company sizes and industries reveals that the topic is certainly gaining traction in the German economy. At large enterprises with over 250 employees, the strategic commitment is almost twice the average at 34 percent. Relevance is even more evident in highly regulated sectors, with the finance and insurance industry clearly leading the way. At 48 percent, almost half of the companies in these sectors have implemented a digital sovereignty strategy – a figure that underlines the growing importance of the issue in the context of sensitive financial data. Adoption by CI operators is also significantly above the level of other company groups at 33 percent.

Thirteen percent of companies either have or are planning to create a digital sovereignty role, with the figure rising to 20 percent at larger companies

When it comes to assigning personnel, companies are taking different organizational approaches. The fact that only 13 percent of all companies have created or are planning to create a dedicated digital sovereignty role (see Figure 16) does not necessarily point to a lack of implementation capacity. On the contrary, this finding may suggest that digital sovereignty could be understood within the broader economy as a cross-functional task to be integrated into existing areas of responsibility – such as those of the CIO or CISO – rather than being handled in isolation by a new, dedicated unit. That said, there is a tendency toward specialization as companies increase in size and complexity.

At large enterprises, the proportion of dedicated roles is significantly higher at 20 percent. Highly regulated or technology-intensive sectors such as finance and insurance (17 percent), IT (18 percent), and CI operators (20 percent) also rely more frequently on specialized positions. This suggests that, above a certain level of regulatory density or global integration (16 percent for internationally active companies), the creation of explicit roles is seen as a necessary step to meet strategic requirements at the operational level.

2.8.2 Willingness to pay a premium for digital sovereignty

Forty-two percent of companies state a willingness to pay more for sovereign IT products

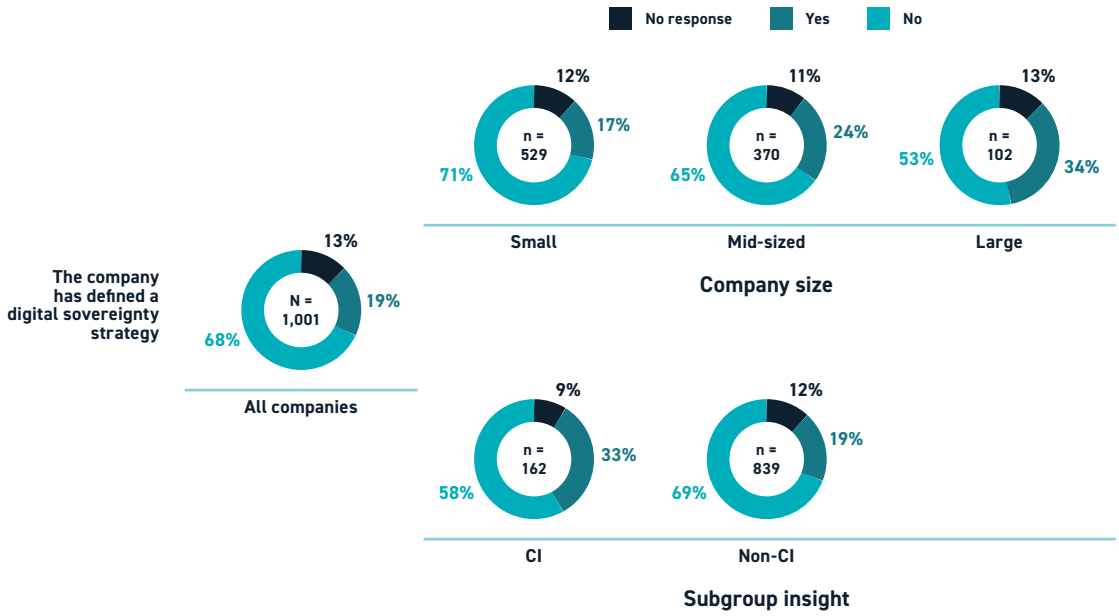
A significant proportion of respondents report a willingness to accept higher costs for sovereign IT solutions (42 percent) (see Figure 17). In 2025, The Handelsblatt Research Institute and STACKIT found even higher figures of 70 percent and 80 percent for public and private sectors, respectively, expressing a willingness to pay extra for digital sovereignty [317]. At the same time, others have issued warnings about the high economic costs of digital sovereignty [228]. It should be noted that all of the mentioned reports represent declarative self-reporting, which does not necessarily reflect actual purchasing behavior. Nevertheless, the results indicate that independence is perceived as valuable by some companies.

This willingness to pay a premium for sovereign products varies significantly from sector to sector. The highest willingness rates are found in healthcare (56 percent), followed by IT (53 percent), and finance and insurance (52 percent). In these sectors, the added value of sovereign solutions and avoidance of dependencies are valued more highly than the potential added costs. In contrast, the energy and utilities sector shows a willingness rate of only 30 percent.

Companies which are active internationally show a greater willingness to pay a premium (49 percent) than companies which operate purely nationally (41 percent). This can be interpreted against the backdrop of global compliance requirements. Organizations operating across multiple jurisdictions appear more inclined to invest in solutions designed to ensure data security and legal compliance across borders. A similar trend can be seen when looking at IT security structures. In companies with an established (C)ISO, the willingness to pay a premium is 53 percent, suggesting a correlation between existing security expertise and the value placed on digital sovereignty.

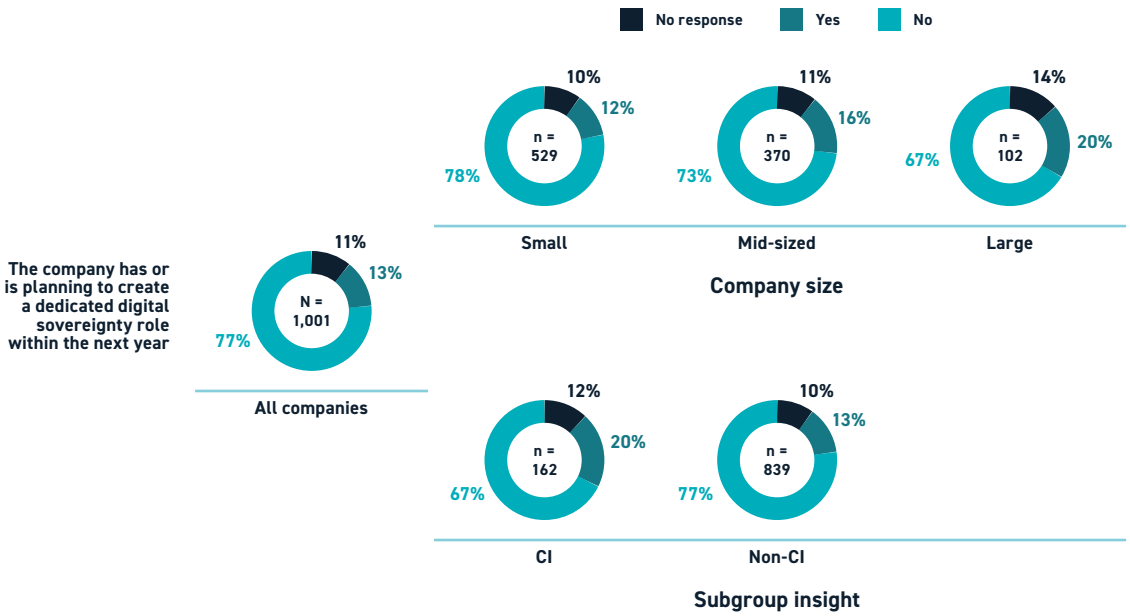
Investment in technological independence is still primarily on the agenda of large enterprises and CI operators

Even though reducing dependencies due to vendor lock-in is highly prioritized in current debates, this is not yet reflected in the actual budget planning of most German companies. While a study from 2025 indicates that 58 percent of companies intend to invest in reducing their dependency on non-European tech



Source: Own survey

Figure 15: Presence of a digital sovereignty strategy



Source: Own survey

Figure 16: Plans to establish a dedicated digital sovereignty role at the company

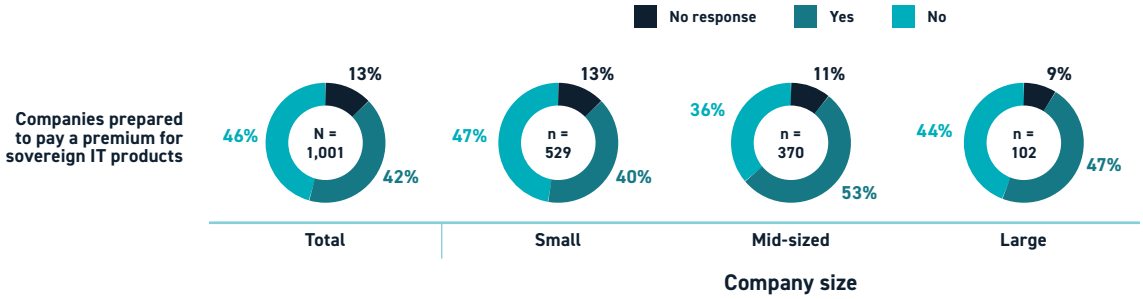
providers [18], only 13 percent of respondents in the present survey reported planning specific expenditures or investments to reduce their dependency on certain providers. In contrast, a clear majority of 83 percent have no financial resources earmarked for this purpose at present. This discrepancy suggests that technological diversification often still fails due to high switching costs or a lack of alternatives on the market. These figures also reflect a discrepancy with the above-mentioned willingness to pay a sovereignty premium, which does not seem to be reflected in planned investments to any great extent.

However, a more detailed look at corporate structures shows that the willingness to invest in digital sovereignty increases with the size and complexity of the organization. At 28 percent, large enterprises are more than twice as willing to invest than the overall average, and medium-sized companies are also significantly above the level of smaller entities at 18 percent. The pressure to invest is particularly evident in areas with increased security and compliance requirements. At 22 percent, CI operators invest significantly more frequently in reducing dependencies than non-CI companies (14 percent). Nineteen percent of globally active companies plan to make investments in sovereignty (compared to 12 percent for purely domestic companies). Companies with an established (C)ISO role are more active (18 percent) than companies without this position (12 percent).

2.8.3 Strategies for dealing with dependencies

Multi-vendor strategies are on the rise

Awareness of the risks posed by dependencies, especially vendor lock-ins, is firmly established in the German economy. In a report published by the Leibniz Centre for European Economic Research (ZEW), 58 percent of companies in the information industry cite lock-in effects as the main reason for existing dependencies [360]. Large enterprises, in particular, are no longer leaving this issue to chance. While a good quarter of all the respondents in our study say they do not take any special measures to counter lock-in effects, this figure drops to 8 percent for companies with more than 250 employees. The management of dependencies has thus become standard practice in the enterprise segment. The most widely adopted approaches are the regular assessment of alternatives (54 percent) and the consistent use of open standards (47 percent), followed by explicit multi-vendor strategies (23 percent). Although still at a lower level than other measures, the adoption of multi-vendor strategies has grown significantly compared to the previous year (2024: 10 percent) [302]. In addition, according to their own statements, companies are focusing on in-house software development, their own data centers, and on-premises operations, among other approaches.



Source: Own survey

Figure 17: Willingness to pay a premium for sovereign IT products

Open-source solutions, open interfaces, and security certificates prioritized for managing geopolitical risks

When it comes to software procurement, differing priorities emerge regarding measures to mitigate geopolitical risks. Two criteria dominate the field. Some 36 percent of decision-makers demand verifiable security certificates across the entire supply chain. In addition, 39 percent of decision-makers have a preference for open-source (OS) solutions. Other factors mentioned by respondents include the exclusive use of European cloud solutions, a preference for vendors headquartered in the EU, and data storage and processing within the EU.

An examination of the various sectors reveals different approaches to digital sovereignty. The healthcare sector relies most heavily on verifiable security certificates (60 percent) and places above-average emphasis on OS (48 percent) compared with other industries. In the financial sector, on the other hand, compliance is the main focus, with 59 percent of decision-makers prioritizing explicit legal control over their data.

This emphasis on legal certainty correlates strongly with the degree of internationalization of an organization. Companies operating internationally are significantly more likely to demand legal control over their data (38 percent) than those only operating domestically (27 percent). This can be interpreted as taking a defensive stance against extraterritorial access, for instance through the US CLOUD Act. At the same time, international companies are relying more heavily on OS solutions (47 percent). This combination of legal isolation and technological openness seems to constitute a modern formula for global digital resilience.

2.8.4 Perception of European initiatives

Only 28 percent of respondents agree that GAIA-X will strengthen Europe's digital sovereignty

The perception of key EU initiatives to strengthen digital sovereignty varies among German IT decision-makers. Once a flagship political project launched with the vision of a European data infrastructure, GAIA-X seems to have lost momentum among the broader spectrum of companies. Only 28 percent of respondents agree with the statement that GAIA-X will strengthen Europe's digital sovereignty. An almost identical proportion disagree, while the largest group (43 percent) is undecided or did not provide a response. For a project of this financial and political significance, this high proportion of undecided respondents indicates considerable shortcomings in terms of communication or relevance.

European Data Spaces perceived as having the greatest potential for digital sovereignty among European initiatives

When it comes to Common European Data Spaces, a much more positive picture emerges. Nearly half of decision-makers (50 percent) believe that these will make a real contribution to European digital sovereignty. In contrast to GAIA-X, sector-specific data spaces are seen to offer tangible benefits.

This is particularly evident in sectors which are included and already integrated. For example, 68 percent of respondents in the healthcare sector (European Health Data Space) and 59 percent in the financial sector (European Financial Data Space) see data spaces as drivers

of digital sovereignty. A shared vision of data exchange within a sector appears to act as a powerful catalyst for acceptance.

Around a third of IT managers (29 percent) express concern about the availability of sufficient data center capacity

Alongside software and data, there is an increased focus on physical infrastructure. Just under one third of IT managers (29 percent) are already expressing concern about the availability of sufficient data center capacity, particularly with regard to future AI workloads. This concern is more pronounced among medium-sized and larger companies (around 35 percent) than among smaller businesses. The urgency of this capacity issue is also underscored by the Center for AI Risks and Impacts (KIRA Center), which warns of a loss of technological sovereignty if Germany does not immediately pursue an ambitious expansion strategy for its own AI infrastructures [151].

2.9 POLITICAL MEASURES

How can digital sovereignty be put into practice in a globally networked market? For BSI President Claudia Plattner, success is crucially dependent on "close cooperation between government, business, science, and society" [279]. However, the results of this survey reflect an ambivalent reality. From skepticism toward EU regulations to calls for proactive cyber defense – it is becoming clear that IT decision-makers currently lack the reliable structural framework necessary to effectively implement this collective strategy.

Ambivalent attitudes towards EU regulations

Amongst the companies surveyed, opinion was split on whether current EU regulations actually strengthen the digital sovereignty of Germany and the European Union. With an approval rate of 41 percent, less than half of the responding decision-makers consider the current regulatory framework to have a positive impact on digital sovereignty. This suggests that regulatory interventions are often perceived not as enablers, but rather as bureaucratic hurdles or simply ineffective measures. There is a correlation between approval and company size. Among large enterprises, approval rises to 50 percent.

Once again, the finance and insurance sector stands apart, with a 59 percent approval, indicating a significantly more positive view of EU regulations. The extent to which a company operates internationally has no measurable influence on the opinion given.

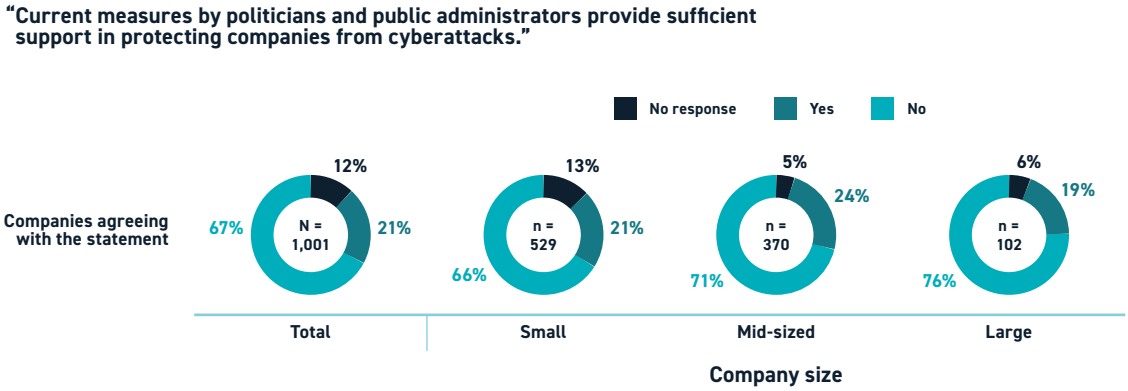
2.9.1 Political measures to support digital sovereignty and cybersecurity

The vast majority of respondents are in favor of political measures to strengthen digital sovereignty

When questioned about which political measures they feel would be appropriate to strengthen digital sovereignty in Europe, IT decision-makers expressed support for favorable framework conditions and building up capacities. There is a general consensus that measures are fundamentally necessary, with only 6 percent of respondents stating that no special measures are required.

Most respondents do not see technology as the top priority, but rather the human factor. Sixty-six percent of those surveyed consider subsidized programs for developing digital skills to be an effective lever. This is closely followed by laying the groundwork for infrastructural and technical solutions that offer alternatives to existing dependencies. The creation of trustworthy data infrastructures (63 percent) and the provision of sovereign standard IT solutions (60 percent) are identified as key building blocks.

Financial incentives also find broad support as a means of strengthening sovereignty. While 59 percent of IT managers are in favor of investment incentives or subsidies, 53 percent consider the targeted financing of open-source technologies to be effective. More specific initiatives, such as a "European Sovereign Tech Fund" (34 percent), are generally less popular, but viewed as significantly more relevant in finance-oriented sectors such as insurance and banking (59 percent). Size also appears to play a role. The larger the company, the more effective the respective political measures are considered to be at strengthening sovereignty. Beyond this, some companies are calling for financial support, better information and education hubs, less bureaucracy, stronger government defense and law enforcement, and the provision and safeguarding of infrastructure.



Source: Own survey

Figure 18: Assessment of current political measures to combat cyberattacks

2.9.2 Lack of confidence in cyber resilience and government positioning

Only 21 percent of companies consider government efforts to provide protection from cyberattacks sufficient

A critical picture emerges when assessing the existing security architecture. When asked whether the current measures adopted by politicians and government administrators provide companies with sufficient support in protecting themselves against cyberattacks, only 21 percent of respondents agree (see Figure 18). A clear majority of 67 percent disagree. This feeling of inadequate protection in cyberspace by the state is the predominant view across all industries. Only in the financial sector is trust slightly higher, at 38 percent, while sectors such as transport and logistics (16 percent) show particularly low levels of perceived support.

The majority of respondents perceive the federal, state, and local governments' preparedness against cyberattacks as moderate or weak

This lack of trust corresponds with assessments of the state's own resilience. Respondents have little confidence in the public administration's ability to defend itself against cyberattacks. Amongst the various tiers of government, the federal government scores comparatively best. However, only 15 percent consider it to be well prepared (see Table 2). For the individual states (Bundesländer), this figure drops to 12 percent. The perception at municipal or local level is particularly alarming. A mere 7 percent think local authorities are well positioned, while over half the respondents (51 percent) explicitly rate the cyber resilience of local authorities as weak. This reflects deep skepticism about the state's ability to deal with digital issues at the administrative level.

High level of support for active cyber defense

While German security policy has traditionally urged restraint on the issue of "hackback", IT decision-makers take a much more offensive stance. According to the study, 79 percent of the respondents support offensive cyber measures by the state against foreign attackers (see Figure 19). Private sector views are even more striking, with a majority (59 percent) in favor of granting such powers to private sector companies. These figures are somewhat unexpected in the German context, as they stand in stark contrast to the current legal situation and the ongoing debate on international law.

Offensive measures, ranging from the targeted disruption of criminal infrastructures (as employed against "Emotet") to active retaliatory strikes, are subject to strict legal constraints in Germany. They are considered a measure of last resort and require the attacker to be identified beyond doubt, which is often technically impossible to fully achieve.

These high levels of acceptance for offensive operations also ignore the risk of escalation and danger of collateral damage to civilian infrastructure often associated with active cyber defense. The Federal Criminal

Police Office (BKA) and the military require clear mandates for such interventions, and constitutional protection allows for investigation but not active disruption. However, real-world experience seems to be calling for a much more robust approach. With more than half of those surveyed even willing to grant companies offensive rights, there appears to be growing frustration with purely defensive protective measures. Ultimately, these findings reveal a schism between the desire for digital defense capabilities and constitutional concerns about "digital vigilantism," which harbors the risk of conflicts spiraling out of control.

2.10 CONCLUSION

The study's findings show the German economy in a state of upheaval. On the one hand, companies are responding with a significant rise in IT security budgets, which have more than doubled as a share of total IT spending from 8 percent in 2024 to 17 percent in 2025.

This development is largely driven by the heightened threat situation and new legal requirements such as the NIS 2 Directive. With the enactment of laws establishing personal liability for executives, IT security is becoming a priority for top management, especially in highly regulated sectors.

At the same time, the data reveals a systemic gap when it comes to implementation. While data protection has been established as a legally binding role, a functional position with strategic responsibility for information security often remains unfilled or is outsourced to external partners. As long as (C)ISO salary expectations do not correspond to the actual market value and growing regulatory responsibility, a shortage of skilled talent will remain in the German security landscape, hindering the transformation from mere formal compliance to long-term resilience.

Meanwhile, formalizing the (C)ISO role is shown to pay off in measurable ways. Organizations with dedicated security management rate their level of preparedness significantly higher and incur lower follow-up costs in the event of incidents. Beyond reactive protection, the appointment of a (C)ISO also acts as a driver for digital sovereignty. In such companies, the willingness to pay a premium for sovereign products (53 percent) and the adoption of measures to reduce technological dependencies (18 percent) are well above average.

Critical infrastructure CI operators in particular, with above-average staffing and financial resources, form the foundations for a resilient architecture capable of addressing complex governance tasks such as supply chain audits and AI regulation. Despite these structures, an information gap remains, as smaller CI entities in particular still feel inadequately informed about the specific requirements of the NIS 2 Directive. Nevertheless, companies in these sectors are in favor of personal liability for senior management, underscoring a desire to elevate cybersecurity to become an indispensable policy driver at the strategic level of corporate management.

The operational security of IT infrastructure reveals an ambivalent picture, including both advanced monitoring and significant deficits in prevention. While reliance on external security providers (SOC/MSS) is standard practice, there is still a shortfall in systematic risk analyses and penetration tests, which are only carried out by 36 percent of all companies.

Especially in medium-sized businesses, a lack of resources and growing regulatory complexity act as obstacles to prevention. Their perceived knowledge gap regarding NIS 2 compliance is symptomatic of a wider challenge. High acceptance rates for aggressive government countermeasures such as hackbacks (80 percent), coupled with an absence of basic self-protection measures, highlight growing frustration in the market.

	Federal government	State government	Local government
Weak	28%	32%	51%
Average	42%	40%	28%
Strong	15%	12%	7%
No response	16%	16%	14%

Source: Own survey

Table 2: Positioning of federal, state and local governments against cyberattacks

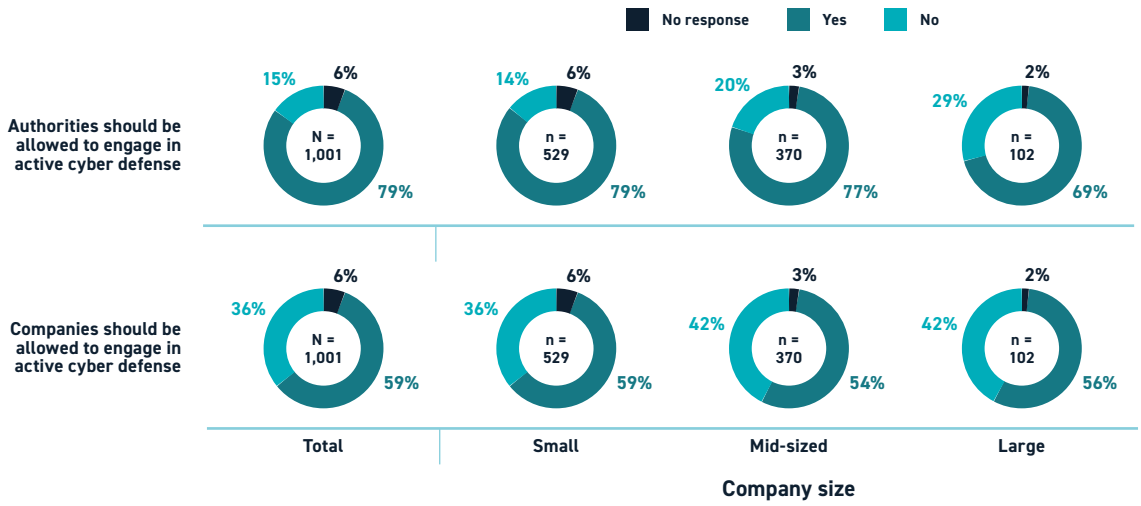
Heterogeneity is evident between specific industries, often shaped by regulatory pressure. While highly regulated sectors are playing a leading role thanks to an above-average strategic focus on the topic and high level of acceptance for investment to boost sovereignty, less regulated sectors such as construction have significant staffing shortages.

Sectors also differ significantly in their approaches to resilience. While the healthcare and IT sectors are increasingly seeking to secure their independence through technological openness based on open-source solutions and certificates, CI organizations are focusing their efforts on areas such as supply chain verification. Finally, a critical deficiency is evident with regard to trust in the system. Sectors with complex logistics chains report a discrepancy between their threat situation and the perceived level of support from the public sector. Meanwhile, trust in government safeguards is comparatively highest in the financial sector.

In conclusion, although digital sovereignty is recognized as the cornerstone of entrepreneurial capacity, the study reveals a gulf between aspiration and implementation. Only 13 percent of the respondents are currently planning investments targeted at reducing dependencies. Nevertheless, countering lock-in effects through multi-vendor strategies is gaining in importance and has more than doubled compared with last year. At the same time, a new physical bottleneck is emerging. One third of IT managers are concerned about the availability of sufficient data center capacity, a situation with the potential to seriously jeopardize digital sovereignty in terms of future AI workloads.

To overcome these hurdles, the survey reveals that sustainable cybersecurity governance not only requires a higher budget, but also a targeted approach to closing the abovementioned information and skills gaps. Ultimately, regulatory requirements need to be transformed from a purely bureaucratic burden into embedded, day-to-day security practices.

However, the success of this transformation depends heavily on the underlying attitude within the corporate landscape, which remains a crucial factor for future risk assessment. Conducting this study was complicated by the fact that many small companies showed significantly less interest in participating. These companies often stated that they did not consider cybersecurity to be within their sphere of responsibility. As long as this perception persists, the operational resilience of the German economy as a whole will remain at risk, as technical advances alone simply cannot compensate for a lack of risk awareness and vacant positions of responsibility.



Source: Own survey

Figure 19: Support for active cyber defense

CHAPTER 3

ROBOTICS IN CONFLICT
FROM HELPER TO TERMINATOR

BIOHYBRID WEAPON SYSTEMS

CPU / BRAIN
Wetware, spiking neural networks and photonics

SENSORS
Neuromorphic, event-based sensors and edge analytics

BODY
Special alloys, soft robotics, quasi direct drive motors

POWER SUPPLY
Solid-state batteries and energy harvesting

12 KILLS / SECOND
with a standard assault rifle

SKIN AND MUSCLES
Self-healing vitrimers, polymers, artificial muscles

100x FASTER REACTION TIMES THAN A HUMAN

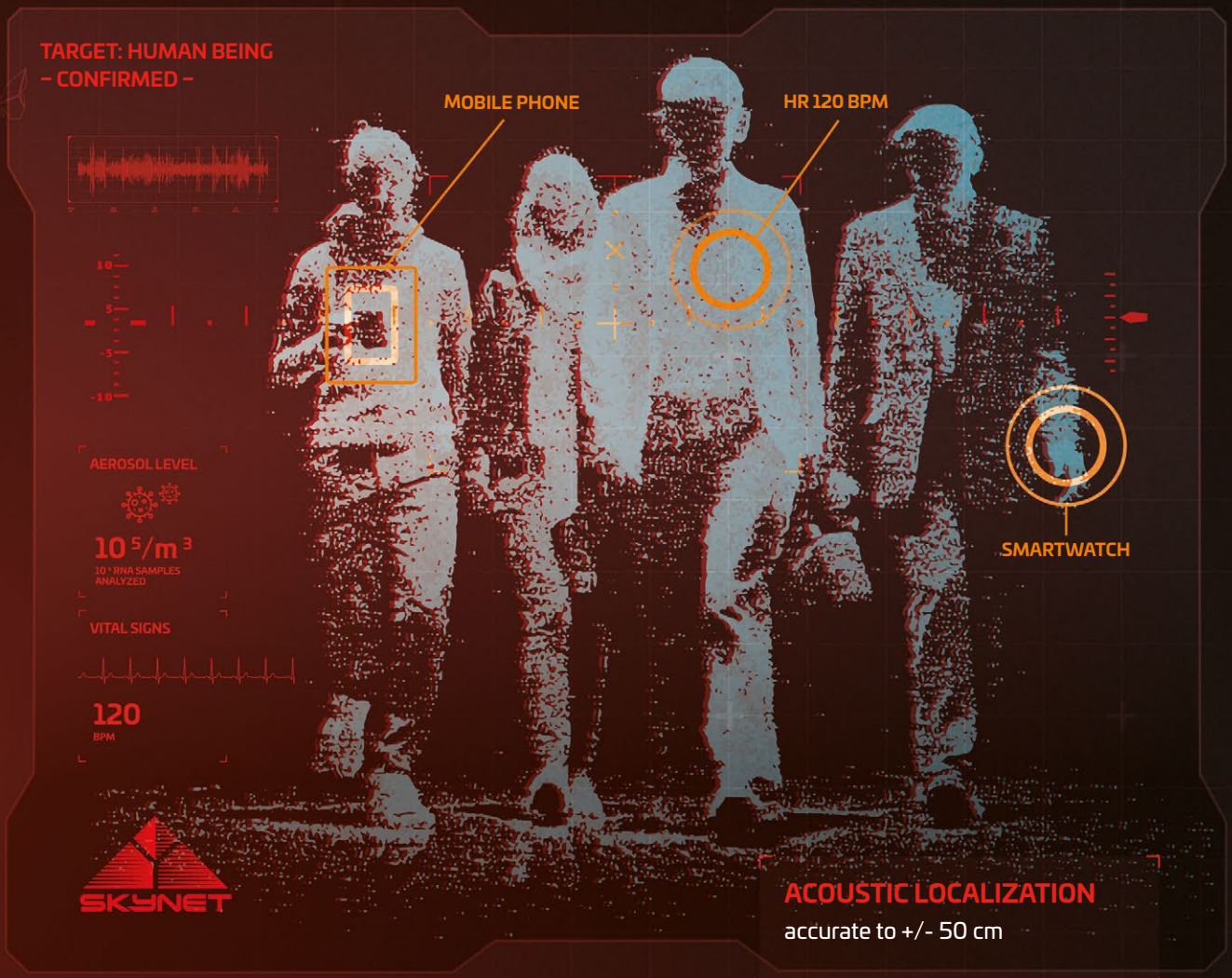
A ROBOT MAY NOT INJURE A HUMAN BEING OR, THROUGH INACTION, ALLOW A HUMAN BEING TO COME TO HARM

ASIMOV'S FIRST RULE OF ROBOTICS

CHEAPER THAN A SOLDIER

The price of a robot is expected to fall to approx. **US$ 25,000** by 2035

THE WORD **"ROBOT"** FIRST APPEARED IN **KAREL ČAPEK'S** 1920 PLAY **R.U.R.** THE TERM IS DERIVED FROM THE CZECH WORD **"ROBOTA"**, MEANING **FORCED LABOR** OR **SERVITUDE**. INITIALLY, ČAPEK HAD PLANNED TO CALL THEM **"LABORI"**.



ACOUSTIC LOCALIZATION

accurate to +/- 50 cm

SALES OF INDUSTRIAL ROBOTS

(as of 2024)

ROBOT PREVALENCE PER SECTOR

Number of robots per 10,000 workers (as of 2023)

Global average: **162**

1.4 MILLION HUMANOID UNITS BY 2025

SOLDIERS OFTEN GIVE THEIR **ROBOT COMRADES NAMES, PROMOTE THEM**, AND EVEN **AWARD THEM BADGES** IF WOUNDED IN ACTION.

Source: [9], [107], [185], [198], [199], [207], [284], [299], [301], [306], [352], Own diagram

3 ROBOTICS IN CONFLICT – FROM HELPER TO TERMINATOR

Just a few years back, the topic of "robots" would have been likely to conjure up images of the Terminator, cybernetic killers, or agents straight out of The Matrix. The thing they all have in common is that, although their creators had originally intended for them to serve humanity in line with Asimov's laws of robotics, these machines wanted to wipe out or subjugate humanity [9]. While for a long time the thought of hostile robotic technology remained pure science fiction, far removed from reality, the disruptive success of ChatGPT has made it clear how quickly technology is now advancing and what new opportunities – and dangers – this may open up.

Exponential development

The field of robotics is witnessing an explosion of reports about new advances and capabilities, with a wide range of competing products set to hit the mass market in the next year or two. Humanoid robots, in particular, have been developing at breathtaking speed over recent years and are already being tested extensively in industrial manufacturing facilities, to name just one example. At the end of 2025, for instance, an eleven-month trial was completed for the Figure 02 model at the BMW plant in Spartanburg. Working 10-hour shifts five days a week, the robots helped produce over 30,000 X3 cars [137]. Meanwhile, the data obtained in the process is being incorporated directly into its successor model, Figure 03. Numerous new robots are set to launch this year, which are not only expected to have increasingly advanced capabilities but also lead to faster adoption through particularly affordable entry-level models such as the Unitree G1/R1.

What these robots will actually be able to do remains a hotly debated topic. After all, a number of manufacturers have already been caught engaging in trickery, such as Tesla, whose Optimus robot was remotely controlled during a laundry folding demonstration. In the age of generative AI, where seeing is not necessarily believing, examining videos closely and questioning evidence is crucially important. Nevertheless, tremendous progress has been made in many areas. Looking back and comparing the "future developments" depicted in the science fiction blockbusters of the 80s and 90s with the current state of research in laboratories, start-ups, and universities, it soon becomes apparent that extensive work is being done on many capabilities that were once considered impossible. In fact, a number of these capabilities have already been shown to work successfully in experimental settings, even if there are still significant limitations in certain areas. In 2025, for instance, scientists managed to decode and display "inner speech" [218], a step closer to mind reading as portrayed in "Minority Report."

However, developments in recent months have given us cause for concern about where we stand today. In December 2025, for example, China began deploying humanoid robots from the Walker S2 series at border crossings in the city of Fangchenggang on the border with Vietnam. The robots are tasked with patrolling and conducting inspections, assisting with the transport of equipment, and helping to direct the flow of people at checkpoints [23]. The Walker S2's ability to exchange its batteries independently means it can be used almost 24/7. It remains to be seen how well the robot performs in practice.

The Future is Now

The presentation and demonstration of the T800, consciously named after the killer robot model T-800 from Cyberdyne Systems in James Cameron's film Terminator, has also showcased what is already technically possible and where the journey is headed. Though designed for general use, this humanoid robot is also specifically engineered for combat [110]. Using an aluminum alloy also found in aerospace engineering and magnesium elements gives it exceptional stability, while powerful electric motors with torque reaching 450 Nm generate enough power to enable fast movement, demanding combat maneuvers, and the lifting of heavy loads. An active cooling system allows the T800 to operate without downtime.

3.1 THE USE OF ROBOTICS IN CONFLICTS

The deployment of robotics in armed conflicts is nothing new. As early as World War I and World War II, the military used small remote-controlled tracked vehicles laden with explosives to target enemy trenches without endangering its own soldiers (e.g., Torpille Terrestre from 1915, Goliath from 1942) [100].

On the front lines in Ukraine, for instance, the Ratel S is currently performing such tasks. This remote-controlled four-wheel robot can transport anti-tank mines, among other things, and is used to engage vehicles and bunkers in combat without endangering soldiers in the "death zone". The same principle was already applied with simpler platforms in both world wars. Robotic platforms such as the Unex system, used to transport ammunition to the front and evacuate wounded soldiers, are also gaining in importance [210].

Above all, drones now dominate the airspace. The array of systems on the front lines has expanded from the tactical first-person view (FPV) kamikaze drones that previously dominated to now include hexacopters with heavier payloads, a variety of reconnaissance systems, and even strategic long-range drones with a greater range. In the water, too, vessels such as the Magura V5 have demonstrated the power of small unmanned systems, forcing the Black Sea Fleet onto the defensive and basically rendering it ineffective by sinking several Russian units. Small, inexpensive, and rapidly evolving systems currently dominate the land, sea, and air.

Innovation versus public procurement

This illustrates how the adoption and rapid advance of technology have taken center stage. Given their outdated military equipment at the start of the Russian invasion, however, Ukraine first had to find ways to overcome slow procurement processes and activate the potential offered by faster industrial innovation cycles. Indeed, this is not an uncommon problem, as procurement times for military systems in Western countries often extend to ten years or more. In Germany in particular, contract cycles are up to 60 percent longer than the global average [229].

To expedite the delivery of weapons to the front lines, groups of volunteers came together in Ukraine to collect donations, manufacture drone parts using 3D printing, and send them directly to the front lines. Signal and Telegram channels were set up to ensure that the experiences of the troops were immediately factored into further design and development. However, since voluntary donations are neither guaranteed nor scalable, meaning that they do not allow for reliable planning, the Ukrainian Ministry of Digital Transformation laid the groundwork for rapid expansion by reducing bureaucracy, changing regulations, and creating financial incentives. For instance, accepting tests carried out by manufacturers and no longer requiring government trials or certifications as is standard in the Western world, reduced the time needed to introduce a system from two years to just a few weeks. High quantity, low costs, and rapid deployment were more critical to survival than quality and process compliance.

Gamification of war: Earning points for killing

Further acceleration was achieved through the "Brave1" innovation cluster, which serves as a central point of contact for companies and supporters. To minimize delivery times and optimally align with the needs of the troops, the cluster set up a website with a marketplace that connects start-ups and manufacturers of innovative solutions directly with soldiers on the front lines. Bypassing bureaucracy, lengthy contract negotiations, and time-consuming product development (which may then already be obsolete by the time it is delivered), manufacturers can offer their solutions directly to the Ukrainian armed forces, who in turn are able to purchase them directly via the online marketplace [44].

Payment can be made in conventional ways, for example from available budgets or donations, or on the basis of a reward system using "ePoints." These are awarded for the successful elimination of Russian personnel and destruction of equipment, as evidenced by video footage. The ePoints can then be used directly on the Brave1 marketplace to purchase new drones, which are delivered to the troops within just a few days. Through this "gamification" of killing, successful units can quickly procure new arms and equipment based on their points – enabling them to become even more effective. Russian losses doubled in the first ten months following the introduction of the system, and the trend continues to rise. In December, the figure exceeded 33,000 soldiers [8].

The rapidly adapting digitalization of the battlefield is directly reflected in destroyed equipment as well as the numbers of soldiers killed and wounded. However, the systems currently in use, such as those used in the

world wars or by Optimus, the laundry-folding robot, are generally still remote-controlled, and any autonomous functions are very limited. In the Ukraine war, it is estimated that less than one percent of the technologies marketed as "autonomous" are actually used in that way [13].

Some systems stand out, like The Fourth Law's TFL-1, which can be easily integrated into common drone platforms. The TFL-1 offers autonomous flight control and final approach to the target on an optical basis, even if the radio signal is disrupted or lost. Since modules are available on Brave1 for just under 50 euros each (or via ePoints) and have already significantly boosted strike rates on the front lines, further developments and new, more sophisticated modules are sure to follow soon.

The advantage of speed

Looking at the war in Israel and Gaza, which has been called the "first robot war," illustrates just how technologically advanced today's robots already are in certain respects [205].

In order to manage the complex situation and respond as quickly as possible, a high degree of automation was used in the preparatory phase to identify targets and key enemy figures. However, these measures can also lead to dangerous routines and a decline in the quality of human monitoring and control. According to reports, for instance, the "Lavender" AI system used by the Israel Defense Forces (IDF) to identify targets during the war in Gaza resulted in extremely rapid, but inaccurate, verification of machine-generated suggestions. This consequently led to significant collateral damage [343].

A crucial turning point in the use of military robotics was their deployment not only as reconnaissance systems, but also for carrying out active combat and pioneering tasks in densely populated urban areas with the aim of minimizing their own casualties. Among other machines, the IDF has used the Caterpillar D9, which is equipped with heavy armor for triggering booby traps, clearing minefields, and debris barriers, even operating in narrow alleys. The semi-autonomous Jaguar ground vehicle goes one step further. This vehicle is especially used for border security and perimeter protection. Equipped with a 7.62 mm machine gun and high-resolution sensors, it can navigate autonomously, avoid obstacles, and patrol routes. The autonomous engagement of targets is not currently planned. While the sensors can automatically detect and track a target (known as "lock-on"), the order to fire must be issued by a human operator after reviewing the video image in the operations center (human-in-the-loop).

Human-in-the-loop or autonomous – just a few lines of code

Going from an operator giving firing permission to fully autonomous systems takes just a few lines of code. Building these kinds of robots is no longer a technical issue – it's now purely an ethical and doctrinal question whether to activate and use these capabilities.

Looking ahead to future developments, the deployment of fully autonomous, armed robots is therefore only a matter of time. The advantages they offer are highly appealing to many military forces around the world. For example, the 72nd Group Army of the Chinese People's Liberation Army (PLA) has already conducted landing exercises to practice the integration of so-called "Robot Wolves", which were used as armed escort systems for the infantry, among other things to clear paths through beach obstacles and intercept enemy fire [204]. The advanced coordination of the exercise suggests that China is also rapidly forging ahead with the integration of manned-unmanned teaming (MUM-T) into its doctrine.

Accordingly, the humanoid robots deployed in Fangchenggang should not be viewed merely as a feasibility study and the endpoint of development. On the contrary, they demonstrate how rapidly the field of humanoid robotics is progressing, especially powered by advances in AI, materials science, bioinformatics, and chemistry. In fact, dual use is becoming the norm.

Does this bring a Terminator scenario closer to real life? A complete overview, examining our humanoid robot from head to toe, coupled with a review of the current state-of-the-art and anticipated progress, aims to shed light on this question.

3.2 TERMINATOR – CURRENT AND FUTURE TECH DEVELOPMENTS

Countless demonstrations of humanoid robots showcase the capabilities already available today. However, a closer look at the current scientific landscape reveals that all the elements required for constructing a Terminator are advancing at a rapid pace.

3.2.1 The brain

The actual degree of autonomy attained remains one of the most challenging and debated aspects of contemporary robots. Although some companies are inclined to interpret the facts somewhat flexibly with a view to stock prices, and some tech demonstrations have involved the use of remote control, rapid developments are indeed taking place, notably in the field of data processing – the "brain" of the robot. Cognitive architecture [304], currently still a major limiting factor for the actual autonomy of robots, has been making huge strides, meaning that those remote controls will soon be a thing of the past. Not just in relatively simple factory settings, but also in complex environments.

These developments have not been driven by the advancement of *conventional processors*, but rather by a series of new technologies. *Photonics* can achieve new levels of performance, particularly in the field of AI accelerators, but the real performance boost comes from *spiking neural networks*, *neuromorphic sensors*, *edge analytics*, and the opportunities offered by *wetware*.

Possibilities and limitations of conventional processors

Although the concepts behind conventional digital computers have been successful for decades and continuously optimized, they are now increasingly reaching their limits in terms of both speed and energy consumption due to substantially higher data volumes and computing requirements. Since the calculations of AI models are largely based on a limited number of specific mathematical operations, significant performance improvements could initially be achieved in this area, as these functions are incorporated into the hardware of AI chips. Architectures such as NVIDIA's Blackwell also exploit other possibilities, for example by reducing the accuracy of calculations without compromising the result, generating higher speeds and better efficiency. The use of an NVIDIA Jetson Thor, specially developed for physical AI and robotics, with a maximum of 2070 TeraFLOPS (TFLOPS) enables the T800, for example, to process complex motion sequences and visual data with no delay.

However, the most important factor is that data collection and processing will no longer all be concentrated on a centralized computing unit which continuously processes all data streams. This is still one of the main reasons behind the inefficient energy management of robots. Visual perception, for instance, requires a constant stream of images to be processed and evaluated using AI algorithms. Using specialized processors such as the Jetson Thor, this is already possible in real time without difficulty. However, it consumes an excessive amount of energy, as even determining that *nothing* is happening places a strain on the battery. While the Jetson Thor is relatively energy efficient with a power consumption of 130 watts, this still has a considerable impact on the operating time of a self-sufficient robot, even though the actuators and hence the robot's musculoskeletal system are the main consumers of energy. Nevertheless, reducing the power consumption of the processor in current models would make it possible to increase the operating time by almost 25 percent, which is equivalent to one hour.

Specialized photonics processors

It is also possible to perform AI calculations very quickly and efficiently by means of photonics – using light beams instead of electrons. Another advantage of this approach is that it requires very little cooling. A 16-channel processor of this type with a performance of 1.28 trillion operations per second was already introduced last year [353], and commercial processors based on this technology are already available. In the coming years, we can expect to see further significant increases in performance and miniaturization. One current bottleneck in the technology is the need to first convert the electronic data into light for calculation purposes and then convert the result back again. Not only does this reduce the overall computing speed, it also requires a relatively large amount of energy [167], which negates the efficiency gains achieved by the actual calculation. At present, the use of photonics only pays off from an energy perspective for large matrices and high clock rates above 10 GHz. Otherwise, digital ASICs still retain their advantage. The use of photonics is therefore particularly interesting in areas where the data is already available as light, such as fiber optic networks.

Neuromorphic sensors and edge analytics

Due to the limitations encountered to date, future humanoid robotic systems will operate in a highly decentralized manner, just like their natural human counterparts. Edge computing, which is already becoming increasingly widespread in areas such as mobile communications networks, is set to be a key concept here. Analogous to the human reflex system, actions are processed locally rather than in the central "brain" wherever possible. Instead, detection and response are carried out directly in the respective parts of the robot, and the robot brain only receives information about the process (known as edge analytics). In addition to reducing the computational workload of the central processing unit, this crucially enables much faster response times in the millisecond range – essential for the superiority of the Terminator.

One of the technologies that will be used to implement edge analytics effectively is neuromorphic sensors, which attempt to mimic the perception and visual processing characteristics of living organisms. By extracting only the information required for post-processing, the required computing power is significantly reduced [113]. There is no question that the future Terminator will have this kind of advanced sensor technology on board. Start-ups are already offering modules with response times of less than 100 microseconds and minimal power consumption [284]. Over the next few years, we can expect to see increased integration of neuromorphic processing units (NPUs) to complement today's CPUs and GPUs. In the IoT and mobile communications segments in particular, the possibilities opened up by "always-on" sensors with minimal energy consumption are enormously promising, which will greatly accelerate commercialization and rapid adoption.

Spiking neural networks

In addition to the optimal distribution of computational tasks, neuromorphic computing offers many more opportunities in terms of the robot's central brain. For instance, the logical processing and storage of data are combined in artificial neurons and synapses. This facilitates a significant improvement in energy efficiency, enabling even resource-intensive AI tasks to be performed directly on battery-powered end devices with low latency [155], for example through the use of spiking neural networks (SNNs). Unlike classic artificial neural networks (ANN), which are based on signals with continuous values (floats), SNNs are based on energy pulses. An artificial neuron only "fires" (sends a spike) when the threshold value of one or more specific input signals is exceeded. This leads to significantly reduced energy consumption, as virtually no power is required for static sensor data (resting state). Even complex operations, such as distinguishing between a civilian and a combatant, can be performed much more quickly and efficiently.

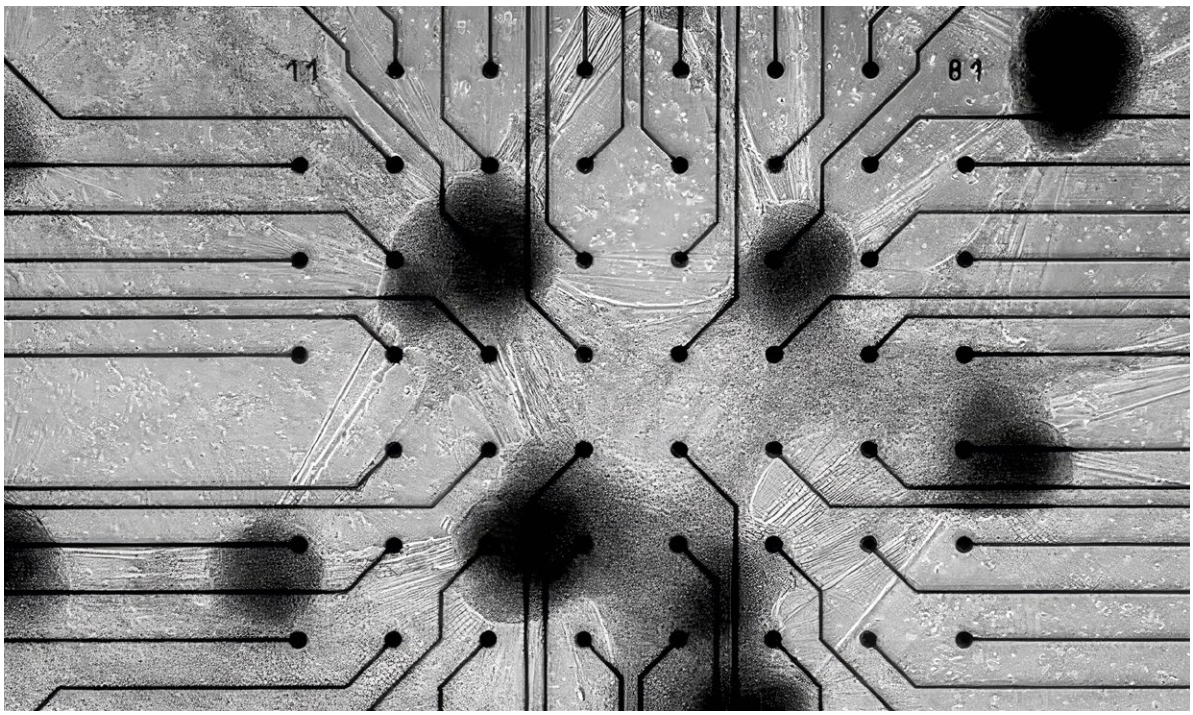
In addition, innovative memristors are now in the pipeline. Instead of processing digital signals as usual, these devices utilize analog signals, which can reduce power consumption by up to 99 percent. This technology also enables self-healing capabilities. It represents a return to analog computing, after such systems were almost entirely replaced by cheaper and more accurate digital computers in the 1960s and 1970s. Although the accuracy of analog technology has not improved significantly since then, this is not a major concern for AI calculations. As a result, the technology may not only experience a revival but could even become a core component of data processing in the Terminator – despite being older than the original film.

Assimilated: Wetware computing

It is not only neuromorphic computing that draws inspiration from biological evolution. The capabilities and efficiency of the human brain itself have also been the subject of extensive research for many decades. "Wetware computing" refers to innovative approaches that use living biological tissue to perform computing tasks. However, the range of promising applications is much broader, with brain-on-a-chip being just one variant of organ-on-a-chip concepts (see Figure 20) [225]. Advances made in recent years are now culminating in the first prototypes capable, for example, of fusing silicon chips with human brain cells cultivated in the laboratory.

This enables information to be processed in real time, in a similar way to the human brain, with much lower energy consumption than other architectures such as GPUs and AI accelerators, or the complex system requirements of quantum computers. For certain tasks, the use of wetware is anticipated to result in up to 106 times lower energy consumption compared with digital processors [138].

In terms of the robot's "mental" capabilities, this could represent a huge step forward. In an experiment conducted in 2022, neurons learned to play the classic game "Pong" within a few minutes [92]. This seminal demonstration has already given rise to the first commercial



Source: [189]

Figure 20: Human neurons on a silicon chip. Cortical Labs.

systems, although these are still focused on the field of research. Biological networks can outperform deep reinforcement learning algorithms with regard to learning efficiency [189]. For the Terminator, this means that in the future, wetware computing will facilitate the energy-efficient processing of information in real time – enabling the robot to learn, quickly adapt and find its way around – even in new and unfamiliar environments.

In this context, it is also noteworthy that, unlike conventional IT, data processing in such systems is *not* deterministic in nature. This means that the same input and seemingly identical initial conditions do *not* necessarily lead to exactly the same output. While this would be unacceptable for digital computers, it is a key characteristic of living neural networks, with inherent advantages such as generalizability, robustness, and exploratory behavior. The trade-off is that a higher level of effort is required in areas such as specification, testing, and operation. Moreover, safety engineering takes on an even more important role, especially if you want to prevent the system from developing an unwanted life of its own.

For the Terminator of the future, it can be assumed that – in keeping with the edge analytics approach – a combination of different technologies will be selected and integrated in such a way as to best exploit their respective advantages and minimize their constraints.

3.2.2 Power supply

Alongside the goal of significantly increasing performance, energy efficiency also remains a key focus of research. Power supply is currently one of the biggest constraining factors for humanoid robots. In principle, power can be *stored* or *generated* locally within the system or transmitted via *wireless technology*.

When it comes to local storage and generation, *batteries* are not the only option. New possibilities are also opening up in the form of *bioelectrochemical systems (BES)*, *radionuclide batteries*, and *betavoltaics*, as well as *energy harvesting* – the extraction of energy directly from the environment. In addition, *near field transmission*, for example by means of induction, or far field transmission by means of *radio waves* or *laser beams*, also offer new possibilities for supplying power.

Development of battery technology

When power is stored in *batteries*, only a few hours of use are typically possible. This may be perfectly sufficient for tasks in factories, shops, or even in the private sphere, where work and charging cycles can be scheduled to alternate. Robot models such as the Walker S2 are already proving their ability to exchange their own batteries autonomously in less than three minutes, enabling virtually uninterrupted operation given the appropriate infrastructure. However, a combat robot with such short operating times or the need for charging stations would hardly be practical.

If we look at developments in the field of e-mobility, however, some progress can be seen in battery capacities. Lithium-ion batteries have a pack-level energy density of up to 250 Wh/kg [101], which can be increased significantly by using different cathode and anode materials [244]. With the introduction of the latest generation of solid-state batteries, also used in the T800, this value rises to up to 500 Wh/kg. These batteries also have the advantage of being non-flammable – an important feature, especially for a combat robot.

Lithium-air (Li-O2) batteries could represent an even greater step forward. Their theoretical energy density of up to 11 kWh/kg is up to 30 times higher than current lithium-ion batteries. However, technically bringing them into mass production poses many challenges [310] and is likely to take more than a decade.

Local energy generation

BES technology, which converts biological waste directly into electrical energy, could also be used to generate power locally in robots [362]. *Radionuclide batteries*, which utilize the heat generated by the decay of alpha emitters, and *betavoltaics*, which convert the kinetic energy of beta particles into electrical energy, are also conceivable solutions. However, the applicability of such systems will remain very limited. BES solutions have a very low power density, making the technology more suitable for ensuring the energy self-sufficiency of sewage treatment plants.

Radiovoltaic batteries, on the other hand, have a service life spanning decades and an energy density millions of times higher than lithium-ion batteries. The energy they contain is released very slowly over a period of decades. A radiovoltaic battery with 100 mW [345] could, for instance, support the maintenance charge of a dormant, pre-positioned system ("loitering weapon").

Similar limitations apply to *energy harvesting* methods, i.e., the utilization of energy that is inherently available in the environment. Due to its low power output, this is also destined to remain confined to the field of special sensor technology [308].

In addition to storing and generating energy locally, power can also be supplied via *wireless technologies*, which in turn can be subdivided into *near field* and *far field approaches*.

Near field wireless technologies

When it comes to *near field* technologies, contactless charging methods have been integrated into everyday life for some time now, for example, the inductive charging of smartphones or toothbrushes. Analogous systems, but with significantly higher output, are also increasingly being used in the field of industrial robots. Coils embedded in the ground can be used to transfer energy in the double-digit kW range with efficiencies of over 90 percent. However, the relevant applications require physical parameters such as air gaps between the ground and vehicle of a few millimeters to a few centimeters [188].

With a view to sustainable transport systems, test tracks which can successfully charge trucks traveling at speeds of 100 km/h with outputs of over 200 kW are also being trialed for the dynamic wireless charging of electric vehicles [245].

Even if major transit connections or road networks in urban areas were to be equipped accordingly, the Terminator would hardly be likely to charge itself on a busy road and risk getting run over by a 60-ton truck at any moment. Nevertheless, near field technologies could still prove useful. For instance, it has been demonstrated how drones can attach themselves to high-voltage power lines to recharge their batteries [173]. This means that drones used for inspection can simply fly independently along high-voltage power lines for great distances without having to rely on battery changes. In a similar way, a robot could travel for longer distances by charging itself in secluded places and activating appropriate protocols in case it is detected.

In future communication networks such as 6G, power will also be transmitted to devices in a targeted manner using *power beaming* [309]. Although this represents an interesting source of energy, it will not be sufficient to power a combat robot and would also be too unreliable without having sufficient control over the infrastructure, especially in enemy territory.

Far field wireless technologies

Inductive, magnetic, or capacitive coupling is not suitable for transmitting energy wirelessly over long distances. This is where *far field technologies* come into play, leveraging electromagnetic radiation in the form of radio waves (up to 300 MHz) or microwaves (300 MHz to 300 GHz) or, in even higher frequency ranges, optical radiation (THz) [289].

Radio waves offer the advantage of being pervasive, as their straight-line propagation changes course when encountering obstacles. This means that energy can be harvested over a large area and even in inaccessible locations. However, the low power density of radio waves limits the technology's potential applications. Rectifier antennas (rectennas) and demonstrations of low-wattage power transmissions [305] give an indication of what can be expected in the future. Thanks to this technology, batteries will, in particular, no longer be required for Industry 4.0 and smart homes [312]. Higher power outputs are possible using microwaves, but due to their linear propagation, a line of sight (LOS) is typically required. Powering humanoid robots is therefore conceivable, but given the energy required, its use would be limited to factory settings and enclosed areas, making it unsuitable for the Terminator.

Another possibility for long-distance transmission of energy involves the use of *laser radiation*. A number of records have been set recently in terms of transmission distances and power [93]. However, the very low efficiency remains a challenge, and line of sight is also required for optical methods [342]. In the longer-term future, photovoltaic systems in geostationary orbit may enable continuous energy transmission via laser beams to earth-based receiving stations [255].

Terminator could also be powered in this way, but a large part of its surface, for example the upper back, would have to be reserved for the receiver array.

It would be virtually impossible to achieve continuous illumination, however, especially while the robot is performing dynamic movements – let alone operations in urban environments. If the Terminator was equipped with a photovoltaic surface of 0.2m² on its back, a laser beam delivering 5000 W/m² would be required to ensure a continuous power supply. On the one hand, this would be well above the safe limit for humans, and on the other hand, the permanent illumination of the Terminator would also make it much easier to detect.

Even though a variety of technologies are currently being developed, having its own self-sufficient source of energy will remain crucial for the Terminator.

3.2.3 The extremities

Arms, *legs*, and *hands* are fundamental to a humanoid robot and form the basis that enables the Terminator to carry out its mission. Today, humanoid robots are actuated almost exclusively by *electric motors*, which are constantly being developed and advanced. Pneumatic actuators powered by compressed air, as used in active exoskeletons, are not suitable for a Terminator due to endurance limitations, and have been surpassed in performance by high-performance electric motors. Alternative approaches in the field of *soft robotics* and electrostatic concepts are also still being researched.

Performance of electric motors

To achieve high power density, permanent magnet synchronous motors and brushless *DC motors* are primarily used today. Coupled with precision planetary gearboxes, these motors operate as quasi-direct-drive motors in systems specifically designed for exoskeletons and robotics. The high torque and minimal recoil enable precise, responsive motion control. The very low gear ratio (quasi-direct) further enables the robot to "sense" external forces by measuring the motor current, facilitating dynamic locomotion even without complex torque sensors [281].

Particularly in recent years, the improved performance of electric motors has enabled impressive demonstrations, for example of the new Atlas robot from Boston Dynamics and the Unitree H1, which was able to perform a backflip thanks to the enormous torque density of 360 Nm at its joints. By replacing model-based control methods with reinforcement learning approaches, robots are now able to execute new and much more natural movements [336] and to learn from observing humans [55].

Soft robots, artificial muscles, and hybrid systems

Despite significant advances in motor design, electric motors remain heavier and more energy-intensive than their biological counterparts. Research in *soft robotics* has, however, long been investigating how robots can be built from intrinsically soft and/or extensible materials (such as silicone rubber) that can deform and absorb much of the energy arising from a collision. Such "soft" robots have a continuously deformable structure, with muscle-like actuation that mimics biological systems and results in a higher number of degrees of freedom compared to conventional hard-bodied robots [295].

One goal of soft robotics research is the development of biologically inspired *artificial muscles* to replace conventional motors. Electroactive polymers (EAPs)

change shape when a voltage is applied and can therefore also be used as actuators. EAPs operate via a variety of actuation mechanisms, some of which have been the subject of study since the 1990s [275]. However, since this approach requires very high voltages, it is currently only partially suitable for use in humanoid robots.

The same generally applies to hydraulically amplified self-healing electrostatic (HASEL) actuators, which combine *hydraulic* and *electrostatic concepts* in a way that promises high performance [1], but likewise still require high voltage. In HASEL actuators, electrostatic forces displace a fluid within a soft pouch, producing contraction. The advantages of these actuators are that they directly couple electrostatic speed with hydraulic force, and the closed system does not require pumps. As with quasi-direct-drive motors, HASEL actuators are capable of self-sensing, eliminating the need for complex high-voltage sensors [292]. Furthermore, the fluid also allows for self-healing in the event of damage – ideal for a Terminator. The first products are already commercially available from spin-offs, but not yet for heavy loads.

What could make this technology even more interesting for integration into humanoid robots is the current research focus on significantly reducing the voltages required for operation. For example, hydraulically amplified low-voltage electrostatic (HALVE) actuators have achieved muscle-like performance metrics at a five times lower driving voltage (1100 volts) [165]. Thanks to active development and progress in previously limiting areas, it is anticipated that modular muscle packages could be integrated into the Terminator in just under ten years – a game changer, since this would also enable self-healing.

Hands

Due to its complex structure, ability to combine strength and precision, and highly developed sense of touch, the human *hand* is a universal tool that is extremely difficult to replicate. Reliable, precisely controlled hands capable of tactile manipulation remain a challenge for robotics, although significant progress has been made in recent years. Dexterity, including the ability to handle deformable objects and work within tight tolerances, has been refined considerably [356].

The availability of high-resolution tactile sensors [357], along with the implementation of multimodal tactile sensor arrays capable of measuring contact forces, microvibrations and heat flows, has greatly enhanced the ability to respond to unfamiliar, unprogrammed situations, such as an object slipping out of the hand. However, this also increases the demands on the sensors, the available degrees of freedom, and the amount of data that needs to be processed [287].

A human-like sense of touch, which plays a fundamental role in triggering rapid corrections in response to unforeseen changes that cannot be captured by optical or other sensors [227], is therefore of particular importance. Advances in hydrogel membranes are paving the way for whole-body tactile sensing by constructing artificial skin from a single conductive material capable of detecting different types of stimuli (known as electrical impedance tomography, EIT). This eliminates the need for a large number of sensor elements with complex wiring. Instead, electrodes are integrated at a few key points, such as the wrists, and use voltage measurements to detect and localize changes in conductivity caused by pressure, stretching, or damage [169]. The elasticity of the material makes it particularly suitable for soft robotics.

Recent work has also demonstrated how humanoid robots can experience a pain-like sensation through their skin, allowing them to respond to corresponding stimuli. The neuromorphic robot electronic skin (NRE skin) encodes dynamic tactile stimuli into neural-like pulse trains and features active pain detection that triggers protective reflexes. Its modular design and specialized injury-sensing capabilities enable precise localization of damaged areas [157].

3.2.4 Making sense of the world: Advances in sensory technology

While, thanks to recent rapid developments, actuators already enable superhuman feats and could literally catapult the Terminator forward in the future, the field of *sensory technology* has also made tremendous progress – not only in tactile perception but also in *vision*, *hearing*, and *smell*.

The Terminator's vision

For the Terminator, *vision* will be far more than mere visual perception of the environment through cameras and will bear little resemblance to the way humans see the world. Instead of processing continuous image streams, data will primarily be transmitted only when the state of a pixel changes, for example in brightness

or color value. This event-based vision, using a dynamic vision sensor (DVS), results in minimal data load. In addition, new algorithms for motion compensation already enable the Terminator's "field of view" to achieve a temporal resolution equivalent to 2,000 frames per second, resulting in latencies in the microsecond range [2].

This enables perception and reaction times that are significantly faster than those of humans. A neuromorphic vision sensor can detect motion within microseconds, whereas human visual reaction time is just under 250 milliseconds. To illustrate the resulting advantages, consider the following combat scenario: A robot using neuromorphic sensor technology could visually process a gun being fired so quickly that it could react before the human shooter had even registered that they had fired their weapon.

This type of perception also allows for extremely high sharpness – blurred images or distortions that occur in the human eye during rapid motion are eliminated. In surveillance systems, the most important parts of an image can appear blurred or smeared, because capturing all environmental information slows the system down, even though most of the scene remains constant. This problem is eliminated with neuromorphic sensors. (Compression techniques like MP3 and MP4 illustrate a similar effect, with large amounts of data drastically reduced by storing only changes instead of complete individual images. The key difference with neuromorphic sensors is that unnecessary data is never generated in the first place.)

Since the robot's vision is not limited to wavelengths visible to the human eye, it opens up extraordinary possibilities for perceiving the entire environment. Image sensors commonly used in CCTV cameras have long had very high sensitivity in the near-infrared range, since the base material, silicon, absorbs photons not only in the visible spectrum but also in the near-infrared range. In addition to capturing images in daylight, the sensors can therefore also provide black-and-white images in darkness. However, the technological possibilities extend far beyond color vision in daylight and infrared-based night vision. By using hundreds of narrow spectral bands instead of just three channels for red, green, and blue, the robot can, for instance, detect camouflage much more easily through hyperspectral analysis. Since chlorophyll reflects strongly in the near-infrared spectrum but not in color, artificial objects can be identified more quickly [226]. Polarization sensors can be integrated to further enhance this capability. Since light reflected from artificial surfaces is polarized differently than light reflected from natural structures, a polarimetric fingerprint can be detected, helping to identify camouflaged or transparent objects [325].

Thermal or UV images can also be captured and used for material inspections. Furthermore, electromagnetic emissions from cell phone antennas, Wi-Fi networks, etc. can be directly detected through analysis of the corresponding frequency bands, as can the transmitter electronics of smartwatches, wireless hearing aids, insulin pumps, and pacemakers. These capabilities provide the Terminator with a highly comprehensive view of its surroundings – but it "sees" far more than that.

Detection of fear

As multiple fields of technology advance rapidly, highly accurate detection of emotional states and reactions will become possible. The objective is for an analysis to detect stress and fear even before an individual becomes consciously aware of their emotional state.

Heart rate variability (HRV) is a key indicator of autonomic nervous system activity and can be used to identify emotional states. The development of remote photoplethysmography (rPPG) technology has made it possible to analyze pulse rate variability (PRV) using a camera, without any sensor-skin contact, based on microscopic color changes in the skin caused by the heartbeat. Since PRV correlates with HRV, this enables contactless assessment of emotional states [364]. Although current methods – in particular in outdoor environments or under poor lighting conditions – are still relatively inaccurate and prone to error in assessing emotional states, such sensor technology could in the future become part of the Terminator's extensive analysis system. In addition, the use of high-frequency radar sensors enables contactless measurement of vital signs, such as heart and respiratory rate, at distances of up to ten meters – through clothing, blankets, and even mattresses [153], [363]. This is not a distant prospect, but an imminent reality.

The Terminator's radar sensor will therefore not only be able to measure the vital parameters of individuals in its vicinity. Improvements in multimodal approaches to radar-based biometric identification, optimization of radar frequencies and antenna configurations, and systematic exploration of wall materials and environmental conditions suggest that through-wall radar-based biometric identification could ultimately become as reliable as traditional line-of-sight (LOS) methods [293]. In

other words, the Terminator would even be able to detect whether individuals are present in a room *through* a door or wall.

The sniffer dog

In some areas, however, artificial systems have not yet come close to competing with human sensory systems. When it comes to *olfactory detection*, in particular, devices have typically been relatively large and bulky, energy-intensive, and limited to very specific gases such as alcohol or carbon monoxide. While olfactory detection sensors are becoming smaller and more affordable, and the use of AI-based pattern recognition enables the detection of more complex odor patterns [222], [335], the real game changer is only just on the horizon. On the one hand, advanced materials such as graphene, carbon nanotubes, and silicon, in combination with downstream biomolecular probes such as aptamers, antibodies, and enzymes, allow for the creation of new biological field-effect transistors (Bio-FETs) that offer unprecedented sensitivity and precision [271]. On the other hand, as seen in the field of computational neuroscience, wetware can also be used here to convert signals from biological receptors into easily usable electrical signals which can be processed in computational systems. Due to the high sensitivity of biological cells, even very specific molecules in extremely low concentrations can be detected [242].

Research into bio-olfactory chips for security and medical applications – for example, odor sensors for detecting explosives and chemical warfare agents – has been ongoing for over a decade [154]. Thus far, the limiting factor has been the lifespan of the biological components, which often had to be kept in special nutrient solutions and environments. Recently, however, significant improvements have been achieved, with the result that the first wetware systems are already commercially available. In view of advances in synthetic biology, which is still in its infancy but has already produced initial market-ready applications [243], stable and significantly more durable systems are only a matter of time. Olfactory sensors will therefore be capable of, for example, detecting early signs of diseases such as cancer based on markers in human breath or of identifying individuals. Integrated into a Terminator's sensory system, such information could be extremely useful for its combat system – and quickly cross ethical boundaries.

The integration of biosensors into the robot's skin is also making great progress, significantly expanding the capabilities of the overall system [361]. Distributed sensing across the skin will be an inherent feature of future humanoid robots. Instead of, for example, two microphones installed in the head to act like ears, the corresponding sensors will be distributed across the surface of the humanoid robot's body. By using micro-electro-mechanical systems (MEMS) microphones, the aperture, i.e., the distance between the sensors, can be increased, thereby significantly improving localization, especially for low frequencies. Event-based processing, which does not continuously analyze a frequency range for changes but activates only when a signal occurs, analogous to the spectral bands presented earlier in this chapter, minimizes response times and maximizes localization accuracy. Through multimodal information processing, such as incorporating visual object recognition into sound reflection calculations (physics-informed neural networks, PINNs) [301], the robot can localize acoustic sources with extremely high precision.

Superhuman: The perfect hunter

In the future, the Terminator will have even more capabilities that make it a perfect hunter. Genome sequencing is already being used at international airports to detect viruses such as SARS-CoV-2, influenza, and mpox [156]. Until now, reverse transcription polymerase chain reaction (RT-PCR) has been used to test for the presence of specific viruses, with genome sequencing initiated in positive cases to precisely identify the variant.

The most recent pilot research, however, shows that the transition to metagenomic sequencing is underway. This technique enables direct genetic analysis of environmental samples, without the need to first culture organisms in the laboratory. All microbes in a sample can be analyzed, not just those being specifically targeted. This also enables the detection of unexpected and completely new pathogens [277].

With ongoing miniaturization, for example in nanopore sequencing, and advances in the use of short tandem repeats (STRs), a future Terminator will not only be able to perform phenotyping within minutes – for instance, determining the skin or hair color of the source of a DNA trace – but also specifically identify individuals or targets through next-generation sequencing (NGS) [230].

The analysis of environmental DNA (eDNA) will thus enable the Terminator to track down its target, albeit more like a silent hunter than in rapid pursuit.

When combined properly, the robot's sensor systems can therefore very quickly surpass not only human capabilities but also those of specialized animals. As part of a multi-stage analysis, the Terminator can first perform a continuous assessment of the surrounding environment to detect any anomalies. This can be done using chemical solid-state sensors, such as nanotubes, which, while not yet capable of fine differentiation, can be operated continuously. In the next step, samples from the environment can be collected, possibly using ultrasound to lift particles contactlessly from the examined surfaces. These samples are then analyzed in more detail in the biological sensor module inside the Terminator, using receptor cells embedded in a nutrient solution. Depending on their emotional state, humans produce different pheromones and volatile organic compounds. The Terminator can use this to instantly detect stress and distinguish between tears of grief and anger. During a pursuit, therefore, it is possible not only to perform DNA analyses, but also to analyze short-lived and volatile stress hormones, particularly inside buildings, for tactical close-range reconnaissance. The Terminator can smell fear even before seeing a person. While differentiation is not possible using scent alone, it could deploy its high-frequency radar to analyze the vital statistics of various individuals and ultimately distinguish between friends and foes.

3.2.5 The effectors

The Terminator also has extensive possibilities in the area of effectors. It can readily be equipped with all the systems that humans use, from conventional *firearms*, flamethrowers, and grenade launchers to directed *energy weapons* and micro-drones. Notably, however, its arsenal could also include biological and chemical weapons, *insect drones*, and *cyborg insects*.

The perfect shot

The integration of *firearms* into robots has already been extensively tested in practice. China, for example, incorporated armed robot dogs into its advancing troops during a landing exercise to clear the way and intercept enemy fire.

In contrast to the usually unlimited ammunition shown in films, the amount of ammunition carried by the Terminator may be significantly reduced in favor of endurance, mobility, or to increase the number of integrated weapon systems. Since robots, unlike human shooters, have no problem with recoil after firing, larger calibers or even armor-piercing ammunition can be used. By combining various sensor technologies such as LiDAR and thermal imaging, as well as using fire control systems, the robot can calculate the *perfect* shot in real time, taking factors such as wind speed, humidity, target movement, and its own movement into account. The anticipation of recoil and the precise counteraction of the actuators at the moment of firing enable high-precision combat with almost 100% accuracy even in dynamic movement.

Furthermore, new technologies will continue to reduce human error rates. One example is the U.S. Army's XM-157, a fire control system (FCS) using variable optics, laser rangefinder, ballistic computer, and environmental sensors to generate corrected target points for increased shot accuracy [276]. In the future, lock-on technologies, as already found in large weapon systems such as tanks, will delay the firing of a shot after the trigger has been pulled until the weapon's barrel is in the optimal position relative to the target in order to compensate for the shooter's hand tremors. Nevertheless, the stress-resistant robot, with a significantly faster reaction time (sensor-to-shoot chain) and extremely high hit rate even when moving, will have a clear advantage over its biological opponent [299].

Direct energy weapons

Laser and microwave weapons may also form part of the robot's equipment, although their high energy requirements mean they are unlikely to be the Terminator's weapons of choice. They can, however, be used to induce biological effects intended to cause active or cognitive denial, i.e., to control crowds without lethal impact [269] or to induce cognitive impairment [354].

Cyborg insects and the like

The use of *biological and chemical weapons* can actually be much more sophisticated and deceptive. Unlike humans, the Terminator faces no danger when transporting and handling these weapons. This opens up the possibility of integrating drones or swarms of micro-drones into the combat system, including the use of insect drones. These can be used both as intelligent, inconspicuous (loitering) munitions and to deliver contact poisons that are absorbed through the skin or administered by means of a micro-injection system.

Insect drones are devised in two basic forms – *biomimetic robots* and *biohybrid systems*:

Biomimetic robots are drones created entirely by humans that imitate their natural counterparts, for example taking the shape of birds. While the earliest models merely imitated the flapping of wings, more recent designs use biomimetic controls that adapt to the environment and may even incorporate real feathers [58].

Biohybrid systems, on the other hand, involve living insects which are fitted with electronics to enable remote control. This technology has already been used to fully control beetles, dragonflies, and cockroaches, among other insects. It is now also possible to control entire swarms by simply specifying a destination [12].

The advantage of these cyborg insects is that they (almost) inherently solve the problem of energy supply and propulsion. The electronic components only need to perform the control function by way of implants that send the appropriate impulses to the muscles, while the insect itself provides the basic energy biologically. Combined with a micro-injection system and a highly effective poison, this can result in a weapon that is difficult to detect, extremely inconspicuous, and highly mobile. Conversion to cyborg insects in a "mass production" assembly line system, in which the electronics are attached to cockroaches in a fully automated process, has already been demonstrated [224].

Micro-drones and cyborg insects can also be employed to collect samples of skin particles from potential targets or to deploy DNA-specific agents against individuals or specific ethnic groups (genetic targeting) [220], [278].

3.2.6 Mass production and autonomous development

The speed at which modern robot technology is developing is now only partly dependent on humans and the limits of our imagination. Robotics was once subject to a top-down approach, in which machines were designed and optimized for a specific purpose. For some time now, however, there has been a shift toward a more evolutionary approach, in which the robot's morphology and control systems are further developed in a co-evolutionary process without human involvement [108]. The ultimate goal is autonomous morphogenesis, in which systems adapt their design to environmental conditions and are not limited to optimizing a given blueprint based on environmental factors [184].

Robot reproduction

Projects such as ARE (Autonomous Robot Evolution) and Robot Fabricator (RoboFab) are already showcasing what is possible. A symbiosis of additive manufacturing and automated assembly, RoboFab is pioneering a hybrid manufacturing approach in which each robot's skeleton is individually produced using 3D printing based on "genetic code" generated by an evolutionary algorithm. The system draws on an "organ bank" for the functional components. The organ bank contains prefabricated modules with standardized interfaces for motors, sensors, and microcontrollers, bridging the gap that currently exists – complex electronics cannot yet be printed in a single run along with structural material.

Fully automated assembly is then accomplished using a gripper arm, which picks up the "organs" and inserts them into the freshly printed skeleton. Thanks to the use of spring clip mechanisms and snap connectors, there is no need for soldering or gluing (although this would no longer represent a major technical challenge but is rather a question of time and cost). The electrical connections are established when the modules snap into place. The entire process thus autonomously produces a functional robot that is able to learn and "reproduce" itself.

Self-healing

Leveraging the potential of 4D printing, which enhances static objects with the dimension of time, future robots will become increasingly resilient due to the use of materials that can alter their shape or function when exposed to external stimuli such as heat, moisture, or light. Among other benefits, this opens up the possibility of self-healing. Inspired by the biological healing of wounds, self-healing materials such as vitrimers and polymers are increasingly undergoing testing in the field of robotics. Using the thermally reversible Diels-Alder reaction, for example, a robot's damaged leg can be broken open and repaired by targeted heating of the molecular network – the tear seals at a molecular level [328].

Microvascular networks embedded in the robot's skin can transport unhardened resin or other hardening agents in a similar way to blood vessels. In the event of an injury, the respective vessel breaks open, allowing the liquid to escape and polymerize, thereby sealing the structure. Liquid metal can also be used, for example to restore broken electrical circuits and pathways [340].

Source: Own image

Figure 21: A wolf in sheep's clothing?

In addition to self-healing capabilities at the hardware level, robots can also repair themselves algorithmically in order to fulfill their mission. In the event of an injury, a robot can analyze the damage and "understand" the resulting limitations, how these can be compensated for, and adapt accordingly. If one arm fails, for example, the system can adapt within a very short time to continue the mission using its remaining capabilities [217].

3.2.7 A question of cost?

The extent to which such technologies will become established in the coming decades depends not only on whether they are fundamentally technically feasible but also largely on their cost. In view of the figures forecast by market research institutes, China is investing heavily in an effort to secure a large share of this fast-approaching future market. This is also reflected in the pricing of humanoid robots already available on the market. Humanoid robots available from Unitree or Figure AI, for instance, currently range in price from approximately $16,000 to $100,000, depending on the model, its capabilities, or tailored optimization for logistics, high precision, heavy-duty work, or research.

To predict how the prices for humanoid robots are likely to develop over the next decade, it is helpful to consider Wright's law [352], which has been successful at foreseeing developments in aircraft manufacturing and the automotive industry. According to Wright, doubling the volume of goods produced leads to a fixed percentage reduction in costs, typically around 15-20 percent per year. The construction of a Terminator-class robot with the necessary components, high-quality sensors, and effectors could therefore entail total material costs of around $20,000 in ten years.

Looking at personnel costs in Western armed forces, the mere training of a single soldier accounts for approximately 50,000 to 100,000 US$ [306] – a sum that could already fund the production of multiple Terminators. However, the most massive cost advantages emerge in the long run, given that personnel and maintenance costs constitute a substantial share of Western defense budgets at around 40 percent [40]. If a Terminator is damaged in combat, it can either be repaired cost-effectively or simply disposed of and replaced by a model that has already evolved further autonomously. The need for extensive medical care or the costly retirement of wounded soldiers is entirely eliminated.

This means that cost considerations will not be an obstacle for the Terminator appearing on the battlefield. In fact, they will accelerate its arrival.

3.3 CONCLUSION

Considering the rapid pace of technological development, it becomes clear that a powerful Terminator is no longer the stuff of science fiction, nor for that matter a distant dream. Humanoid robots have literally made great strides forward and backward, especially over the past year, repeatedly exceeding even the most optimistic expectations. Although we may still find it amusing when demonstrations go wrong or a little trickery is revealed and a supposedly autonomous robot turns out to be remote-controlled after all, it is only a matter of time before *fully* autonomous weapon systems appear somewhere around the globe. A combat robot like the Terminator is no longer a question of "if" but "when."

Even if the international community sharing democratic values sets comprehensible and absolutely sensible ethical limits on the development and use of such systems, answers must still be found as to how to deal with adversary systems of this kind. While armed drones have become increasingly important in numerous conflicts, Germany has been engaged in a political debate on the subject for over ten years that is detached from reality. The democratic community of values must assume that other states will push ahead with development and, unfortunately, cannot afford to wait until hundreds of combat robots are stationed across the border. The major challenge concerning the core aspects of such dual-use technologies is that the difference between permitted and prohibited usage often lies in nothing more than an algorithm or a few lines of code.

Precisely what to expect from a future Terminator, hinges on whether one or more technological breakthroughs will lead to rapid development in specific areas, or whether technological development will proceed at a more moderate pace.

Terminator – "Lightweight"

In the case of a more "conservative" Terminator, we can expect a high-precision combat robot that promises near-perfect target engagement based on conventional weaponry. Its detection, action, and reaction capabilities dwarf any human capabilities, even if these are further improved by the use of equally advanced technology. The speed of autonomous machines, especially when they are based in part on biological elements and processes, can only be matched by other machines. Even man-unmanned teaming (MUT), in which, for example, a human pilot monitors the deployment of several (partially) autonomous air systems, is mainly motivated by an insistence on old conventions and an attempt to buy time. Looking at development times, one might also question whether such systems are not already a thing of the past and whether sixth-generation fighter jets, such as the Future Combat Air System (FCAS) planned by Germany, France, and Spain, will still be viable by the time they come into service around 2040 – even with unmanned support. The g-forces that unmanned systems can withstand during maneuvers are significantly higher than anything a trained fighter pilot could withstand. With advances in materials research, this gap will only continue to widen.

Terminator – "Worst case"

In the event of significant technological advances or optimal progress in development, the Terminator will grow considerably more powerful. The primary focus here is on multimodal sensor integration and a resilient, self-healing structure for the entire system – with the added possibility of autonomous further development. When it comes to effectors, we can still expect to see conventional weapons with extremely high precision, but also the use of biological or chemical weapons and genetic markers. The main point is that the Terminator's wide-ranging, superior sensor technology will make it the ultimate hunter, capable of adapting to unknown situations and environments, learning quickly, and adjusting its behavior. The exact arsenal of weapons will be of secondary importance for the successful execution of its mission.

A wolf in sheep's clothing

A key aspect is that an overpowering "Terminator" does not necessarily have to be a specialized, highly sophisticated combat robot. If robotics continues to find its way into our households in the form of the now ubiquitous, useful helpers such as vacuum robots, and if the capabilities of humanoid robots develop as promised, then future domestic or care robots could pose a much greater problem than combat robots in the field. After all, here too, there are often only a few lines of code separating good from evil (see Figure 21).

The assumption that the potential risks posed by such systems would be met with particularly high-quality software development, focused on security in the sense of DevSecOps, is already proving to be a fallacy. At the German hacker congress organized by the Chaos Computer Club (39C3), it was recently demonstrated just how easy it is to take over control of robots. No new

techniques were required [288]. The same vectors of attack that have been working for decades once again led to the hackers gaining full control and escalating their administrative rights. This is not surprising, because when it comes to market share, many companies in the Far East are clear about their priorities – speed and dominance at any price.

Having control over such systems, and in particular their software, algorithms, and "thoughts," is thus becoming a matter of existential importance. The slow-moving discussions about software sovereignty and half-hearted, bare-minimum definitions have not been helpful so far. That said, the current generation of robot vacuum cleaners has far fewer possibilities to terminate their owners than the humanoid household helpers of the future will. We've already almost missed the boat. Unless cybersecurity is finally taken seriously, the consequences could be enormous in the near future.

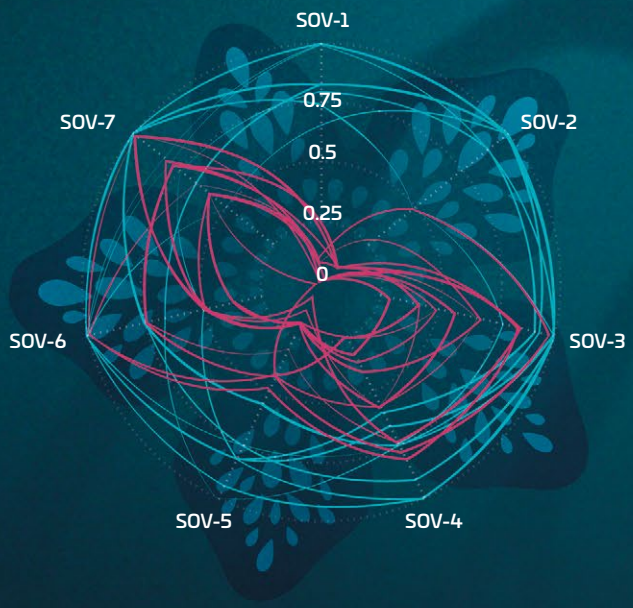
CHAPTER 4

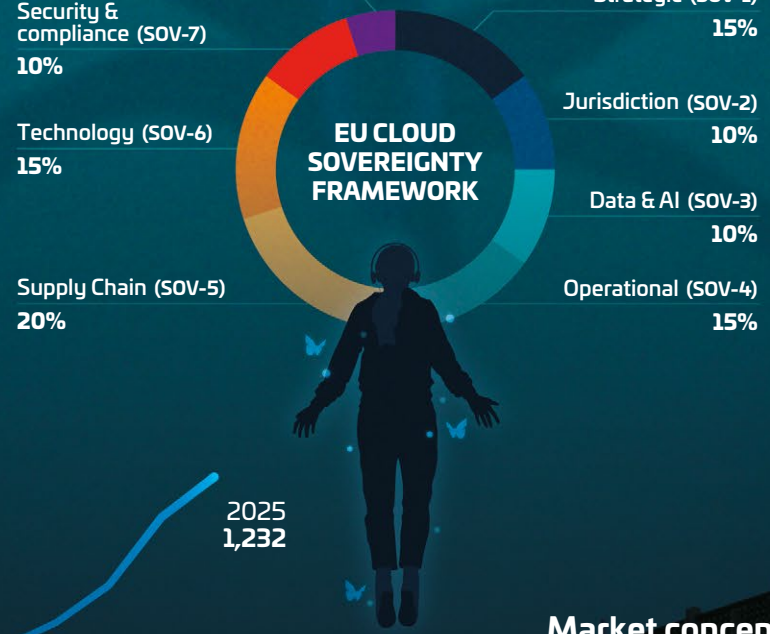
— SOFTWARE SOVEREIGNTY IN EUROPE —

SOVEREIGN THINGS

Sovereignty score (SOV)

- EU Providers (avg. 0.84 points)
- Non-EU Providers (avg. 0.37 points)





TOP SCORES: OpenProject, axelor, NextCloud

GAME OVER: Miro, Confluence, ChatGPT

– INSERT COIN –

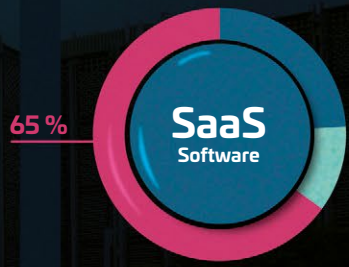
Worldwide enterprise software

turnover in billion US$

Market concentration

While IaaS and PaaS are clearly dominated by US hyperscalers, the SaaS market remains much more fragmented

- AWS
- Microsoft Cloud
- Google Cloud
- Other



Perceived dependence

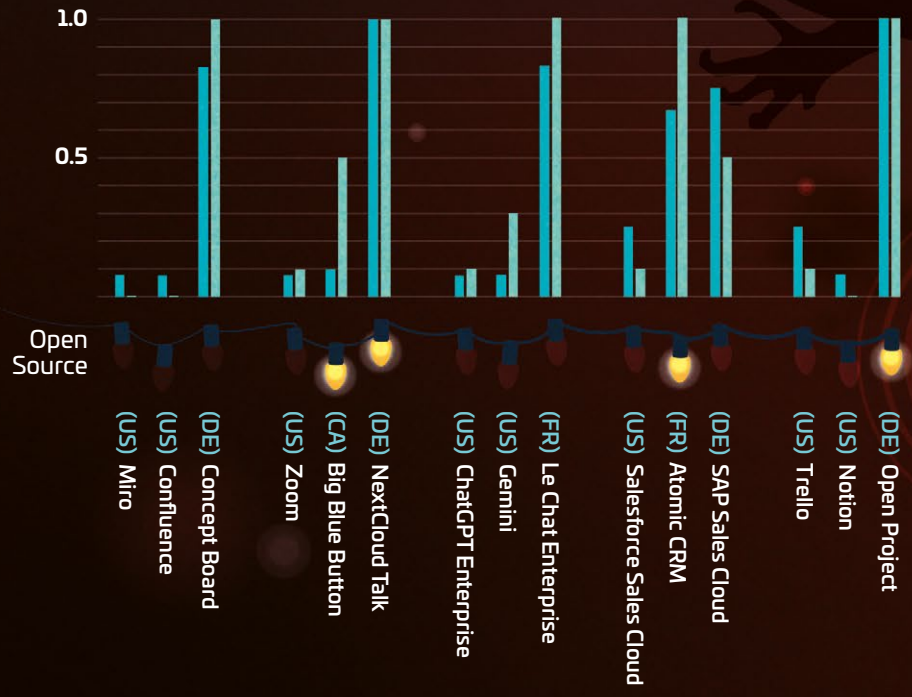
on digital products from the USA and China

Number of employees

Information technology	USA	China
5–19	76%	25%
20–99	85%	33%
>= 100	91%	29%
Manufacturing sector		
5–19	55%	28%
20–99	75%	36%
>= 100	86%	34%

Comparing EU and non-EU solutions

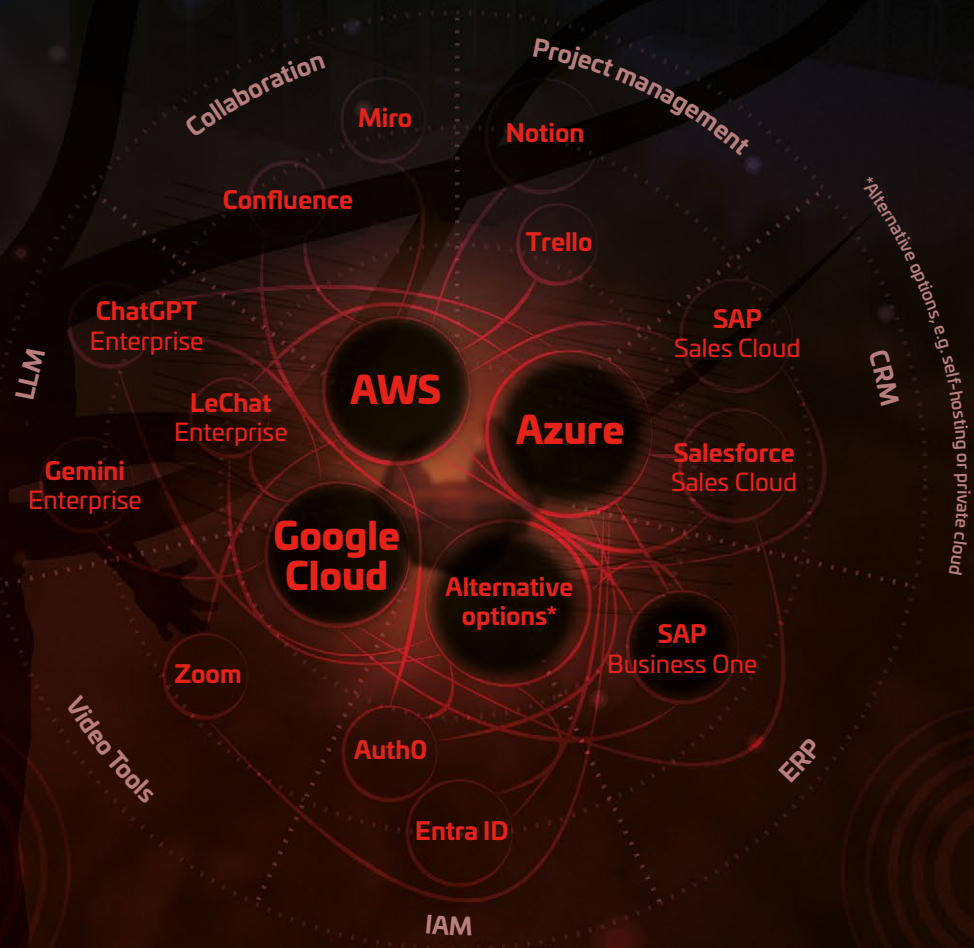
with regard to their SOV-1 (strategy) and SOV-2 (legal sovereignty) scores



Source: [320], [322], [359], Own diagram

US Hyperscalers play a role in all categories of software

Available hosting options



96%

of all AI-enabled public cloud regions are powered by US chips

(primarily NVIDIA)

4 SOVEREIGN THINGS – SOFTWARE SOVEREIGNTY IN EUROPE

In recent years, the debate over Europe's digital sovereignty has developed into a strategic priority. Amid an increasingly charged geopolitical climate, the topic has moved beyond academic discourse and is now ripe for implementation at the political and economic levels. Today, it is no longer just a question of "what" or "why," but of implementing operational solutions which factor in national security, global competition, and regulatory compliance.

Taking the current background into account, this chapter addresses the urgent need to make digital sovereignty tangible at the application level. While the debate tends to be dominated by infrastructure issues, it is clear that software applications play a crucial role in an organization's digital infrastructure and sovereignty [321]. In order to facilitate the assessment of a software portfolio relevant to a modern organization, this chapter adopts the EU Cloud Sovereignty Framework (EU CSF) of the Directorate-General for Digital Services (DG DIGIT) from October 2025 as a guiding framework.

To bridge the gap between theory and practical implementation, this chapter pursues three objectives. (1) Contextualization of the discussion: It provides an introduction to the current debate on digital sovereignty in Europe. (2) Methodological application: It introduces the EU CSF and presents the Software Sovereignty Framework (EU SSF), which is based on the EU CSF and adapted for practical use. (3) Evidence-based assessment: It subjects enterprise software available in Europe to explorative analysis based on the EU SSF.

4.1 THE DEBATE ON DIGITAL SOVEREIGNTY IN EUROPE

The digital sovereignty of Germany and Europe is much more than a debate about technology. It is a strategic pursuit that ties national security, global competition, and regulatory compliance together.

Uncurbed dependencies give rise to severe vulnerabilities, ranging from geopolitical risks and extra-territorial data accessibility to classic vendor lock-in. Given this context, digital sovereignty is not just about short-term data control or security, but about "grandchild-proofing" – creating a resilient, sustainable, future-proof digital society for generations to come [303].

Sovereignty in transition

The concept of sovereignty has existed for centuries, and its meaning has evolved over time [15]. Since the 17th century, it has reflected the idea of sovereign rule as supreme, all-encompassing, territorially restricted power [162]. In the modern international order, sovereignty has primarily come to refer to a state's independence from other states (external sovereignty) and its unrivalled authority within its own territory (internal sovereignty) [283].

With the advent of the internet and globalization, all-encompassing territorial control has been called into question in many respects. On the one hand, cross-border data flows defy geographic logic [142], and on the other, international corporations have built up rival, quasi-sovereign power [273]. Whereas digital transformation was celebrated in the 1990s as a catalyst for a post-territorial world free of national borders [14], it is now increasingly perceived as a threat to the state's ability to govern.

Today, the term "digital sovereignty" is often defined as the ability to make decisions independently and carry out self-determined actions in the digital space [123], [209], [283]. It encompasses the entire "digital stack" – from hardware such as semiconductors and microchips to standards and protocols all the way through to software, data, and the infrastructures they run on, such as the cloud [142]. Digital sovereignty manifests at three levels: the state, the organizations, and individuals [283]. The state level is concerned with national security, regulation, and protection of critical infrastructure. The economic level focuses on competitiveness as well as the management of dependencies and risks.

The individual level relates to the capacity of individuals to exercise informational and digital self-determination, digital competencies, and independence in shaping the digital transformation [80].

Internationally, interpretations of the term "digital sovereignty" vary. While authoritarian states such as Russia and China often view internet or cyber sovereignty as state control over the national internet and cyberspace in order to shield themselves from external influences [57], the EU pursues a more value-based approach. The EU's Joint Research Centre (JRC) outlines this approach through a multi-layered conceptual framework that defines digital sovereignty as the ability to exercise strategic independence while remaining open to global networks [123]. In the BRICS countries, digital sovereignty is also increasingly seen as an instrument for exercising power and control over infrastructure in order to challenge "digital colonialism" and attain technological independence [19]. In Germany, the discussion is characterized by a variety of narratives ranging from economic prosperity to individual empowerment [219].

In recent years, the discourse both within the EU and beyond has shifted from a scientific debate to a more practical political and economic discussion. The Snowden revelations (2013) highlighted the surveillance capabilities of foreign intelligence services and prompted calls for territorial protection strategies [162]. The COVID-19 pandemic served as a further catalyst, as disruptions to global supply chains exposed the EUs dependency on US platforms and hardware manufacturers. In a 2021 letter to Ursula von der Leyen, President of the European Commission, the heads of state of Germany, Denmark, Finland, and Estonia called for digital sovereignty to be established as a guiding principle of European policy and for critical technological dependencies to be reduced [246].

Growing geopolitical tensions, especially since 2025, have significantly intensified the debate. The focus for national governments and many organizations is now to reduce dependencies and develop resilient European digital industries. These developments are coupled with a lively political and economic "stack" debate (e.g., EuroStack; Germany Stack) and initiatives such as the European Digital Sovereignty Summit in Berlin, which took place in November 2025 [37], [38], [46], [134]. The EuroStack concept proposes a comprehensive, interdependent technology ecosystem ranging from microchips to cloud computing, software, and AI in order to establish a centralized, federated European infrastructure as an alternative to global hyperscalers [134]. The D-Stack is a program by the German Ministry for Digital Affairs to create a sovereign technology platform for digital projects in Germany [37].

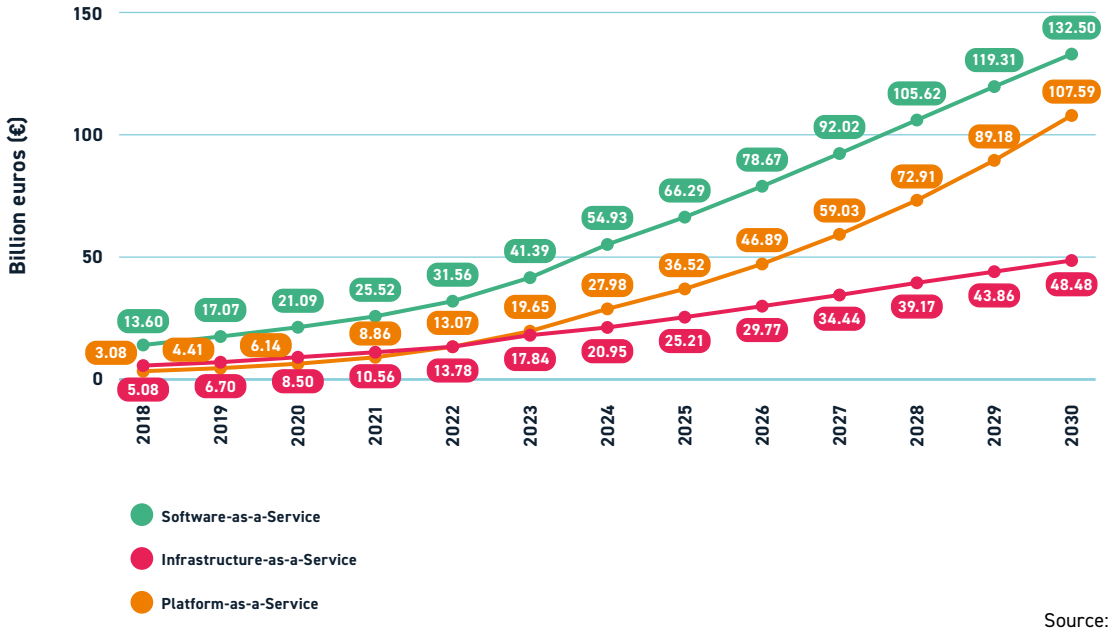
Measuring and operationalizing digital sovereignty

Despite its political relevance, measuring digital sovereignty remains a complex task, as it is not a precisely defined political instrument or clearly delineated field of action. Approaches such as the stack model [209] or the multi-layered framework proposed by the EU JRC aim to give structure to digital sovereignty [123].

In response to the challenge of operationalization, the EU Commission's DG DIGIT published the EU Cloud Sovereignty Framework (EU CSF) [123] in October 2025. Designed to enable self-assessment by cloud providers and subsequent evaluation by DG DIGIT as part of its procurement process, the metrics provide a valuable basis for broader application to other IT solutions. The project has gained added relevance due to the proposed EU Cloud and AI Development Act (CADA) [127] and the revision of the EU public procurement Directives (Public Procurement Act 2014/23/EU, 2014/24/EU, 2014/25/EU), both of which are likely to include definitions for digital sovereignty and "buy European" approaches. CADA is anticipated to be introduced in the first quarter of 2026 and is based on recommendations outlined in the Draghi Report [102]. It aims to strengthen the EU's capacity to develop independent cloud technology and artificial intelligence (AI) and specifically reduce dependency on US providers by establishing clear definitions and targets for cloud sovereignty. Similarly, the revised Public Procurement Directive pursues the "Buy European" policy guideline and promotes security interests. The first draft is scheduled for the second quarter of 2026 [126].

From cloud infrastructure to software considerations

Thus far, the practical debate on digital sovereignty has often concentrated on the cloud infrastructure of US hyperscalers and concerns about clandestine data access legitimized by American laws such as the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) or the US Foreign Intelligence Surveillance Act (FISA) [143]. Other technologies are now also coming into strategic focus with regard to dependencies, competitiveness, and long-term resilience.



Source: [321]

Figure 22: Comparison of public cloud markets in Europe

Compared with other areas of technology, companies currently feel most dependent on non-EU providers when it comes to software (36 percent) [359]. While 72 percent of German companies rely on software from other countries [26], 80 percent of European software and cloud spending goes to US providers alone [161]. The dependence on non-EU providers is even more pronounced in public sector IT than in the private sector, particularly in the areas of office software (81 percent) and collaboration tools (47 percent) [259].

Current forecasts confirm that software is a significant growth market. Revenue in the European Software-as-a-Service (SaaS) cloud market is forecast to rise from €66.29 billion in 2025 to €132.5 billion in 2030 – a volume far exceeding the Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) segments (see Figure 22) [322]. With average spending of €107.78 per employee, SaaS is also the most cost-intensive element in digital organizational infrastructure [321]. The digital economy in Germany grew at a rate of 10.2 percent in 2025 [27]. At the same time, US providers profit from around 80 percent of EU software and cloud spending [161]. This creates a flywheel effect, a self-perpetuating business cycle in which EU spending increases US corporate profits which, in turn, enables reinvestment into research and development. This dynamic has enabled US providers to build up an innovation lead in numerous areas, consolidating their market dominance and protecting them from European competition.

Dependencies in the realm of office software have been acknowledged for years and have been addressed since 2025 through decisions to switch providers and create exit strategies, particularly in the public sector. For example, the Ministry of Education and Cultural Affairs in Baden-Württemberg [249] and the International Criminal Court (ICC) [117] are replacing Microsoft 365 with openDesk from the Center for Digital Sovereignty (Zentrum für digitale Souveränität, ZenDiS). The ICC's decision follows US sanctions against its judges and chief prosecutor [174]. By December 2025, 80 percent of the state administration of Schleswig-Holstein will have migrated to LibreOffice [172], a change also announced by the Danish Ministry of Digital Affairs for 2025 [294]. The Austrian Ministry of Social Affairs and Health has recently started using the open-source Nextcloud Hub as a collaboration platform [258], and from 2027, French civil servants will only be allowed to use the open-source video conferencing tool Visio, developed in France, instead of Microsoft Teams, Cisco Webex or Zoom [358].

In contrast to office software suites, other types of software have received relatively little attention to date. Structural sovereignty risks across software categories (talent management, transparency, interchangeability) also need to be placed under greater scrutiny. Given the deep penetration of software into working environments and the massive capital flows for non-EU software, it is essential to understand digital sovereignty more deeply in this area, so that risks and areas requiring action can be identified.

Framework	Publisher	Approach	Technology	Data	Object of comparison	Aim
C5	BSI	Criteria catalog	Cloud	Audit report	Product	Certification
Deutsche Verwaltungs-cloud (DVC)	DVC/ IT Planungsrat	Maturity assessment	Cloud	Supplier self-assessment	Product	Procurement process
Digital Sovereignty Index	NextCloud	Country comparison	Open-Source Collaboration & communication tools	Publicly available data	Country	International comparison
EU Cloud Sovereignty Framework	DG DIGIT	Maturity assessment	Cloud	Supplier self-assessment & publicly available data	Product	Procurement process
GAIA-X Level 3 Certification	CISPE	Product catalog	Cloud	Supplier self-assessment	Product	Supplier overview – GAIA-X compliant solutions
SecNumCloud	ANSSI	Criteria catalog	Cloud	Audit report	Product	Certification
Tech Sovereignty Catalogue	Digital SME Alliance	Product catalog	Digital products	Supplier self-assessment	Product	Supplier overview – European solutions

Source: Own diagram

Table 3: Comparitive overview of frameworks, certifications and indexes for digital sovereignty

This analysis uses the CSF, published by the EU Commission's DG DIGIT, as a basis for evaluating a modern, enterprise-relevant software portfolio in terms of its digital sovereignty while simultaneously testing the applicability of such a framework.

4.2 OPERATIONALIZATION AND MEASURABILITY OF DIGITAL SOVEREIGNTY

The biggest hurdle in measuring digital sovereignty lies in the inherent vagueness and generally accepted methods for assessing the concept. Digital sovereignty is often used as a political buzzword – "consensus vocabulary" that signals strategic relevance but remains conceptually vague [350]. To transform this rhetoric into operational implementation, it is necessary to translate the concept's goals into measurable indicators.

4.2.1 The framework landscape

The current framework landscape can be divided into three categories: product catalogs, criteria catalogs with certifications, and maturity models. While product catalogs primarily represent the market availability or diffusion of certain solutions, criteria catalogs with certifications focus on compliance with minimum technical and regulatory standards. Maturity models map digital sovereignty onto a dynamic development path for a product or organization.

Despite this diversity, the majority of approaches to date share a strong focus on cloud infrastructure, while evaluation at the application level (software) remains underrepresented (see Table 3).

While digital sovereignty is often discussed in the context of the capacity of states and organizations to act, current frameworks primarily reflect requirements for products and services. Rather than comparing the digital sovereignty of entire states or organizations, the characteristics of specific products contributing to digital sovereignty are compared. Frameworks from the EU and national security authorities also refer to particular (cloud) services. Examples include national certifications such as SecNumCloud from the French Agency for the Security of Information Systems (ANSSI) and the Cloud Computing Compliance Criteria Catalogue (C5) from the German BSI [47]. These provide catalogs of auditable criteria for cloud providers in their respective countries and so support the assessment of digital sovereignty for organizations.

The evaluation criteria range from publicly available data and information submitted by providers themselves to audit reports. The Tech Sovereignty Catalog compiled by the Digital SME Alliance, for example, provides an overview of European solutions for organizations and private consumers [96]. It is based on information provided by vendors themselves about their products (Tech Sovereignty Catalog) or compliance with various standards (CISPE Catalog) [77]. In contrast, the Nextcloud Digital Sovereignty Index is based on publicly available data relating to the uptake

of self-hosted collaboration and communication tools in various countries [257]. The German government's cloud procurement platform ("Deutsche Verwaltungscloud") relies on maturity assessments and software architecture principles based on self-reported information elicited from providers [95].

This diversity illustrates that to date there is no single metric or approach for assessing digital sovereignty. The choice of measurement method instead depends on the specific objectives, the subject under investigation, and the available data.

4.2.2 The EU Cloud Sovereignty Framework

The framework established by DG DIGIT defines digital sovereignty as a measurable spectrum, and not a binary state. It provides the methodological groundwork for an EU procurement process aimed at identifying cloud solutions with a high level of digital sovereignty for adoption in European institutions. Cloud providers were invited to participate in a tender process, in which they were asked to self-assess their services against predefined criteria and submit comprehensive supporting documentation by the end of 2025. The framework divides digital sovereignty into eight objectives (see Table 4), each with four to six contributing factors, and uses a two-stage evaluation system based on "Sovereignty Effectiveness Assurance Levels" (SEALs) and an overall score (sovereignty score).

ID	Sovereignty objective	Weight in scoring
SOV-1	Strategic Sovereignty	15%
SOV-2	Legal & Jurisdictional Sovereignty	10%
SOV-3	Data & AI Sovereignty	10%
SOV-4	Operational Sovereignty	15%
SOV-5	Supply Chain Sovereignty	20%
SOV-6	Technology Sovereignty	15%
SOV-7	Security & Compliance Sovereignty	10%
SOV-8	Environmental Sustainability	5%

Source: [123]

Table 4: Sovereignty objectives of the EU Sovereign Cloud Framework, and their weighting

Sovereignty Effectiveness Assurance Level (SEAL): A provider must achieve a specified minimum sovereignty level for each of the eight objectives. Failure to attain this level in any one of the objectives leads directly to exclusion. The SEALs describe a spectrum from SEAL-0 (no digital sovereignty, exclusive control of non-EU third parties) to intermediate levels such as SEAL-2 (data sovereignty with enforceable EU law, but remaining dependencies) to SEAL-4 (complete digital sovereignty through EU control without critical dependencies). The minimum SEAL can be specified for different requirements (in one process at SEAL-2, in another at SEAL-4). Only offerings that achieve the predefined minimum SEAL in all objectives are then evaluated and compared using the sovereignty score. While the SEAL minimum requirements thus determine basic eligibility, the score enables a differentiated ranking of the qualified solutions.

Sovereignty score: The sovereignty score enables a granular, comparative evaluation of the offered solutions. A numerical score is determined for each of the eight objectives. The overall result is then calculated using a weighted aggregation, meaning that the individual categories are incorporated into the final score with different degrees of prioritization (see Table 4).

The weighting of each of the eight objectives reflects its relative prioritization. Technological sovereignty (15%) and supply chain sovereignty (20%) form the core, while legal and jurisdictional aspects are weighted at 10%. This distribution is based on DG DIGIT's assumption that legal protection measures are already covered by standard procurement procedures [123].

The approach has its shortcomings. Providers could partially compensate for a lack of legal immunity with high efficiency in the supply chain or sustainability, provided that the minimum SEAL level is achieved for each dimension. Thus, the "sovereignty spectrum" carries the risk that providers will achieve high sovereignty scores even if they still have critical dependencies. There are also concerns that the high administrative burden of complying with the SEAL metrics could favor large corporations and overwhelm smaller European providers [78], [144].

It is expected that this framework will be taken up, expanded, and adapted by various stakeholders. In November 2025, for example, BSI and ANSSI announced the joint development of a set of criteria based on the EU CSF, including an auditing method [280].

To make the EU CSF, primarily intended for cloud infrastructures, fit for the purpose of assessing a software portfolio, the criteria were adapted and defined in more detail in an EU Software Sovereignty Framework (EU SSF) to enable practical measurement.

4.3 ADAPTING THE EU CSF TO MEASURE SOFTWARE SOVEREIGNTY

The core of the analysis presented here is to translate the contributing factors formulated in the EU CSF into applicable criteria for assessing software. The resulting EU SSF consists of seven objectives, each with four to six assessment criteria, as well as the accompanying evaluation methodology with sovereignty scores and SEALs. The EU SSF was developed for the purpose of this analysis with the aim of testing the EU CSF, adapting its specifications to the software ecosystem – which has received little attention to date – and conducting an exploratory analysis of enterprise software in various categories. At the time of publication, no comparable analysis is available.

Objectives of digital sovereignty

Of the EU CSF's eight objectives, seven have been adapted for the EU SSF. The objective of ecological sovereignty (SOV-8) has been excluded because its applicability is limited in the context of software technologies and little data is available.

The contributing factors for each of the objectives were refined to create assessment criteria and response categories. In the original framework, some criteria are vague and in some cases several elements, some of which are heterogeneous, have been combined into a single factor (see, for example, Table 6 and Table 7).

Sovereignty Score and SEALs

Analogous to the CSF, a score is calculated based on a weighted average. The weighting of the EU CSF has been adopted to allow comparability. In the EU SSF, all influencing factors within an objective are weighted equally (no information is available on weighting in the CSF). The individual factors are either rated on a binary scale as 0 or 1 (headquarters within the EU, SOV-1.1) or using a graded scale (0.25; 0.5; 0.75) (data localization, SOV-3.3).

As the exact threshold values for the SEALs (0–4) in the CSF have not yet been clarified by DG DIGIT, all values below 0.2 were rated as SEAL-0 in this EU SSF analysis, assuming a uniform distribution of the five SEAL levels between 0 and 1. In this case, the SEALs are not based on specific characteristics of the individual criteria, but on the weighted scores for each sovereignty dimension.

The software under review

The EU SSF is applied to the typical software portfolio of an organization, covering the following areas: databases, enterprise resource planning (ERP), customer relationship management (CRM), project management, video conferencing tools, AI, identity and access management (IAM), collaboration, and cybersecurity (see Table 5). The selection of software products is based on a balance between European and non-European (non-EU) providers. There is no claim that the selection is representative, and only publicly available data is used.

For the purposes of this analysis, the term "software" is limited to application software typically used in modern organizations, including business-critical processes such as ERP, CRM, or digital collaboration. A conscious decision was made to focus on the business context in order to define a clear delimitation from the much broader scope of software and deeper infrastructure components, which are often used indirectly via complex architectures. Customized software developed in-house has also been excluded, as its highly specific nature means that it places different demands on digital sovereignty than standard solutions available on the market.

AI plays a special role

Assessing the sovereignty of AI goes beyond the metrics of conventional software products. The SSF, however, applies to software products that integrate AI systems as subsystems, as well as to AI-centric software solutions, such as large language models (LLMs). The LLM product category addresses the need for the standalone assessment of AI software. AI poses challenges for the evaluation of digital sovereignty due to its

Category	Software product	Vendor/Principal developer	Open source	Country
Databases	Microsoft SQL Server	Microsoft	no	US
	Mimer SQL	Mimer	no	SWE
	Apache Cassandra	Apache	yes	US
ERP system	SAP Business One	SAP	no	DE
	Oracle Fusion Cloud ERP	Oracle	no	US
	Axelor Open Suite	Axelor	yes	FR
CRM	Salesforce Sales Cloud	Salesforce	no	US
	Atomic CRM	Marmelab	yes	FR
	SAP Sales Cloud	SAP	no	DE
Project management	Trello	Atlassian	no	US
	Notion	Notion Labs	no	US
	Open Project	Open Project	yes	DE
Video conferencing tools	Zoom	Zoom	no	US
	BigBlueButton	Blindside Networks	yes	CA
	Nextcloud Talk	Nextcloud	yes	DE
Large language models (LLMs)	ChatGPT Enterprise	OpenAI	no	US
	LeChat Enterprise	Mistral	no	FR
	Gemini	Google	no	US
Identity & Access Management (IAM)	Okta Identity Engine	Okta	no	US
	cidaas	WidasConcepts	no	DE
	Entra ID	Microsoft	no	US
Collaboration	Miro	Tactivos	no	US
	Conceptboard	Conceptboard	no	DE
	Confluence	Atlassian	no	US
Cyber security (WAF)	Akamai App & API Protector	Akamai Technologies	no	US
	Myra Hyperscale WAF	Myra Security	no	DE
	Cloudflare WAF	Cloudflare	no	US

Source: Own diagram

Table 5: Software solutions from various software categories selected as samples for assessment

"black box" nature, specific computing infrastructure requirements, and the technological complexity of the model architectures.

4.4 THE SOFTWARE SOVEREIGNTY FRAMEWORK (SSF)

Similar to the CSF, the EU SSF formulates objectives and contributing factors for digital sovereignty and adapts them to the software context. The objectives, their goals, and the assessment criteria are introduced below. Deviations and specifications to the software context are presented along with their relative distinctions from the CSF.

SOV-1: Strategic Sovereignty focuses on the degree of anchoring of a provider in the EU's "legal, financial, and industrial ecosystem". It concentrates on owner stability, governance influence, and alignment with the EU's strategic priorities [123].

Strategic sovereignty relies on European jurisdiction (SOV-1.1), assurances against a change of control (SOV-1.2), reliance on financing sources from outside the EU (SOV-1.3), and the ability to maintain secure operations against requests to discontinue or suspend services (SOV-1.6). In the EU CSF, this dimension also takes into account contributions to value creation within the EU (SOV-1.4) and participation in and alignment with the EU's strategic priorities (SOV-1.5), both of which are excluded here due to lack of established or practical measures to assess.

ID	Sovereignty objective	Contributing factors	Included	Assessment items (adapted)
SOV1.1	Strategic Sovereignty	Ensuring that bodies having decisive authority over your services are located within EU jurisdiction.	yes	Headquartered in the EU.
SOV1.2		Evaluating the assurances against change of control.	yes	Safeguards to prevent companies based outside the EU gaining significant control over the company.
SOV1.3		Degree to which the provider relies on financing coming from EU sources.	yes	Degree of funding provided by stakeholders within the EU.
SOV1.4.1		Extent of **investment**, jobs, and value creation within EU.	no	Total investment over the last five years.
SOV1.4.2		Extent of investment, **jobs**, and value creation within EU.	yes	Number of employees within the EU.
SOV1.5.1		**Involvement in EU initiatives**, Consistency with digital, green, and industrial sovereignty objectives defined at EU level.	yes	Documented participation in EU initiatives.
SOV1.5.2		Involvement in EU initiatives, **Consistency with** digital, green, and industrial sovereignty **objectives defined at EU level**.	no	Alignment of the company's strategy with the EU's environmental, industrial, and digital goals.
SOV1.6		Ability to sustain secure operations against requests to cease or suspend the service, or if vendor support is withdrawn or disrupted.	yes	Headquartered in the EU.

Source: [123]; Own diagram

Table 6: Operationalization of the contributing factors for the "Strategic Sovereignty" objective in the SSF context

The CSF is still vague as to whether there are preferences for financing options or whether certain types of companies are favored. While the legal jurisdiction can be clearly identified by the company's registered headquarters, aspects such as "involvement in EU initiatives" or "investments, jobs, and value creation within the EU" are open to interpretation. One possible proxy for "investment, jobs, and value creation" is, for example, the proportion of employees within the EU, which can be used to measure the extent of a provider's value creation and anchoring in the EU, as was done in this assessment. By way of example, an overview of the operationalization of the original contributing factors into measurement criteria can be found for other objectives in Table 6.

SOV-2: Legal and Jurisdictional Sovereignty reflects control over the provider and its operations. The aim is to determine the extent to which digital services are rooted in European jurisdiction and protected from foreign legal claims [123].

SOV-2 assesses the national legal system governing the provider's operations and contracts (SOV-2.1), exposure to non-EU laws with cross-border reach (e.g., Chinese Cybersecurity Law, US CLOUD Act, or FISA) (SOV-2.2) and exposure to foreign authorities (SOV-2.3). The applicability of international jurisdictions (SOV-2.4) and the jurisdiction for the development and registration of intellectual property (IP) are also included in the assessment (SOV-2.5).

The importance of legal sovereignty became apparent in June 2025 and January 2026. Microsoft had to admit that the protection of EU data from requests by US authorities cannot be guaranteed without exception [143] and that cooperation with authorities extends to the disclosure of BitLocker recovery keys [45]. A report published in 2025 by German legal scholars for the Federal Ministry of the Interior comes to a similar conclusion [215]. Other perspectives point out that EU subsidiaries, as independent processing entities, should strictly be subject to EU law and the requirements of the GDPR [143].

SOV-3: Data & AI Sovereignty addresses the protection, control, and digital independence of data sets and AI services within the EU (see Table 7). The aim is to ensure data security at the point of processing and a high degree of technological autonomy for customers over the AI capabilities they use [123].

ID	Sovereignty objective	Contributing factors	Included	Assessment items (adapted)
SOV3.1.1	Data & AI Sovereignty	Ensuring that only the customer, not the provider, has effective control over cryptographic access to their data.	yes	Options for encryption keys and encryption management.
SOV3.1.2		Ensuring that only the customer, not the provider, has effective control over cryptographic access to their data.	yes	Location of hardware security modules (HSM).
SOV3.2.1		**Visibility into when, where, and by whom** data is accessed, including auditability of AI model usage, mechanisms guaranteeing irreversible removal of data, with verifiable evidence.	yes	Access to real-time audit logs.
SOV3.2.2		Visibility into when, where, and by whom data is accessed, including **auditability of AI model usage**, mechanisms guaranteeing irreversible removal of data, with verifiable evidence.	yes	Mechanisms to audit the usage of AI models.
SOV3.2.3		Visibility into when, where, and by whom data is accessed, including auditability of AI model usage, mechanisms guaranteeing **irreversible removal of data**, with verifiable evidence.	yes	Technical and contractual mechanisms to ensure irreversible deletion of data.
SOV3.2.4		Visibility into when, where, and by whom data is accessed, including auditability of AI model usage, mechanisms guaranteeing **irreversible removal of data, with verifiable evidence**.	no	Availability of cryptographic, certified proof of deletion.
SOV3.3		Strict confinement of storage and processing to European jurisdictions, with no fallback to third countries.	yes	Localization of data strictly within the EU, exclusion of fallback models in non-EU countries.
SOV3.4		Extent to which AI models and data pipelines are developed, trained, hosted, and governed under EU control, minimizing dependency on non-EU technology stacks.	yes	The degree to which AI models and data pipelines can be developed, trained hosted and governed under EU control.

Source: [123]; Own diagram

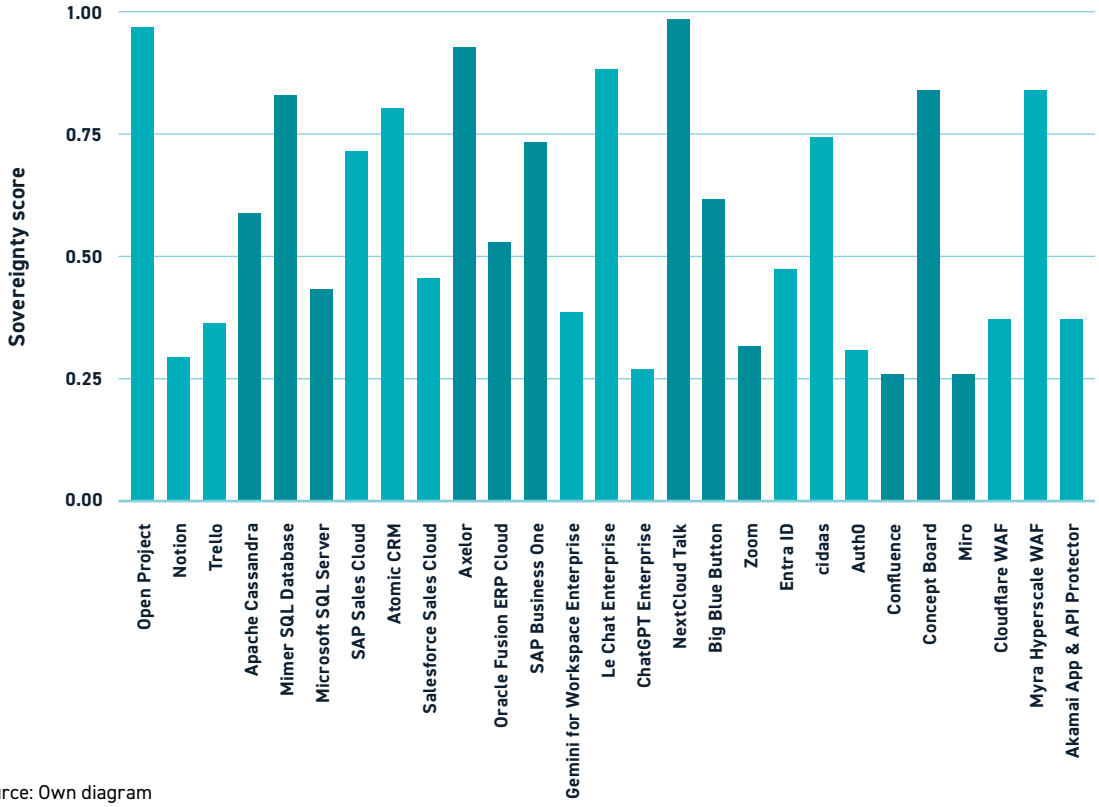
Table 7: Operationalization of the contributing factors for the "Data & AI Sovereignty" objective in the SSF context

This objective includes customer control over cryptographic access to data (SOV-3.1) as well as comprehensive visibility mechanisms (SOV-3.2). These include real-time audit logs for data flows and the use of AI models (SOV-3.2.1), mechanisms for auditing the use of AI models (SOV-3.2.2), and the verifiable and irrevocable deletion of data (SOV-3.2.3). Data sovereignty is also defined by strict data localization, meaning storage and processing should take place within the EU without fallback options to third countries (SOV-3.3), and the degree of EU control over the development, training, hosting, and control of AI models (SOV-3.4).

Standard SaaS providers (such as collaboration or CRM tools) often use global indexes for metadata to enable features such as global search, causing a significant portion of the data flow to leave EU jurisdiction. Strict data sovereignty can only be achieved by solutions that guarantee the localization of work data, metadata, and service or operational data. This also involves consistently isolating service logs and telemetry data within EU jurisdiction.

SOV-4: Operational Sovereignty aims to ensure the ability of European entities to operate, support and develop technologies independently of foreign control. The focus is on operational continuity, availability of skills and reducing external dependencies [123].

For operational sovereignty, factors such as options for barrier-free migration of workloads through the use of standardized export formats (SOV-4.1) and platform independence (SOV-4.2) are considered in order to reduce lock-in. Another contributing factor is the availability of an EU-based pool of experts with the capacity to operate and maintain services over the long term (SOV-4.3). As an extension of the data localization considered in SOV-3, it is also recorded whether maintenance and support can be provided entirely from within the EU and under local legislation without any operational dependence on manufacturers in non-EU countries (SOV-4.4). The availability of technical documentation and access to source code (SOV-4.5), as well as the location and legal control of critical suppliers and subcontractors involved in service provision (SOV-4.6) also contribute to operational sovereignty.



Source: Own diagram

Figure 23: Overall sovereignty scores

In recent years, new "sovereign" provisioning models have emerged which – in addition to data localization, physical decoupling of servers, and separate EU subsidiaries – offer exclusive operation and support within the EU [53]. This can also be achieved through self-hosting open source software (OSS), as operational control remains with the user.

SOV-5: Supply Chain Sovereignty assesses geographical origin, transparency, and resilience of the supply chain. The objective is to achieve resilient management of global dependencies. At its core is an analysis of the extent to which critical components and processes remain under EU control or are subject to dependency on non-EU actors [123].

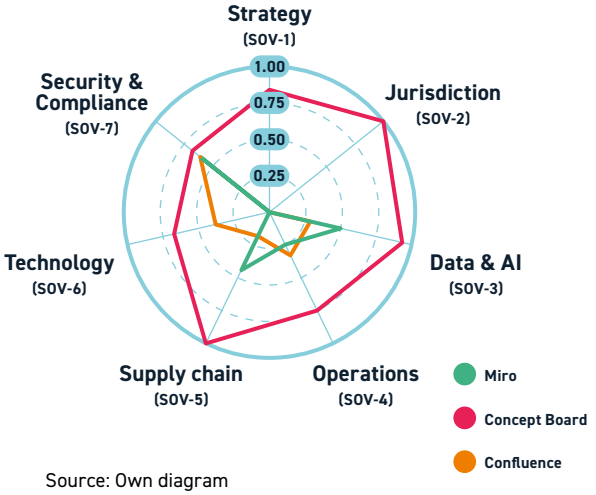
The assessment of software supply chain sovereignty focuses on the jurisdiction of code-controlling hardware (SOV-5.1), the origin of the software (SOV-5.2) and the jurisdiction of the development teams (SOV-5.2), reliance on third-party, non-EU vendors, locations, or proprietary code (SOV-5.3), and transparency through audit rights (SOV-5.4).

Although the EU CSF also includes the origin and manufacture of physical hardware components and raw material dependencies, these points have been excluded from the present analysis. Information about the origin of microchips or raw materials contained in hardware is in most cases not publicly available. Additionally, the hardware configuration used to develop and host a software depends on several factors and is hard to determine exactly. Furthermore, dependencies – for example, on manufacturers such as AMD, Intel, or NVIDIA – are rather homogeneous and currently almost unavoidable for the majority of market participants.

SOV-6: Technology Sovereignty focuses on openness, transparency, and independence in the technology and software stack. This objective is aimed at ensuring that EU entities can use, audit, and evolve solutions in an interoperable manner without becoming dependent on or locked into non-EU proprietary systems [123].

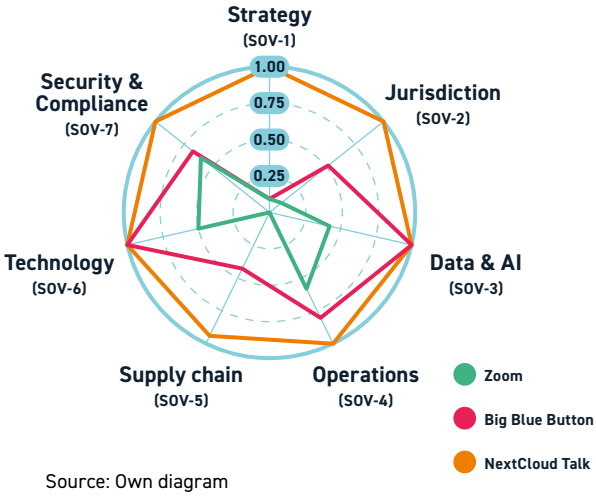
SOV-6 encompasses the use of documented, non-proprietary APIs or protocols (SOV-6.1), the availability of software under open-source licenses (SOV-6.2), and the documentation of architectures, data flows, and dependencies (SOV-6.3). The degree of dependency on non-EU computing for high-performance computing capacities is also taken into consideration (SOV-6.4).

Transparency regarding dependencies can be achieved by means of external audits or via a Software Bill of Materials (SBOM), which discloses libraries and dependencies in the code. The creation of SBOMs will be mandatory for "manufacturers of products with digital elements" [116], including software products, under the



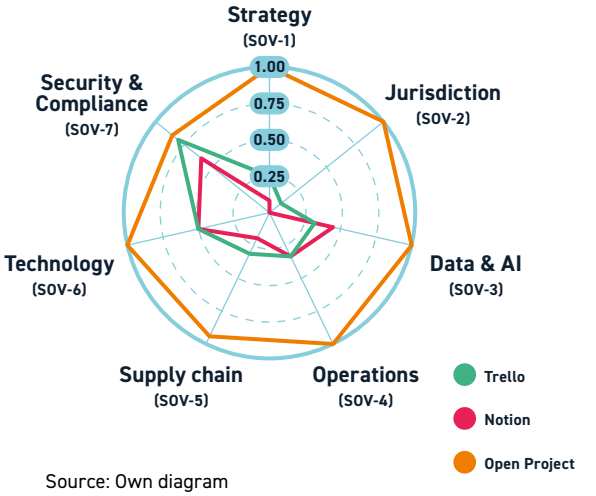
Source: Own diagram

Figure 24: Scoring results – Collaboration



Source: Own diagram

Figure 25: Scoring results – Video conferencing tools



Source: Own diagram

Figure 26: Scoring results – Project management

EU Cyber Resilience Act, which is set to come into force in 2026. They are only audited for certain products. Due to security concerns, however, SBOMs are rarely published and are generally only made available to business customers. As a result, the amount of publicly available data for this factor is very limited.

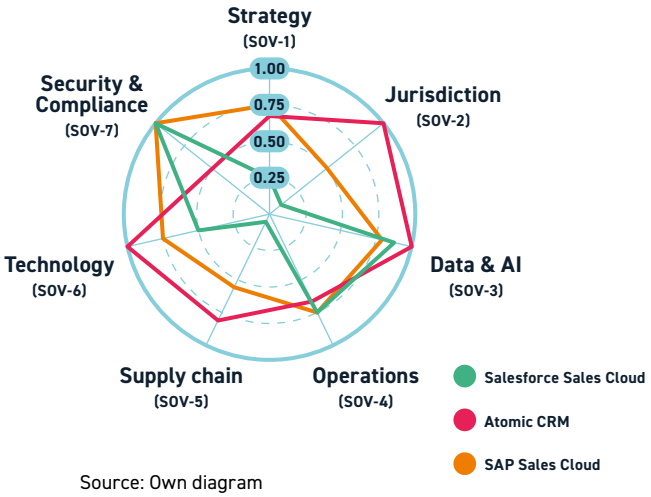
SOV-7: Security and Compliance Sovereignty focuses on cybersecurity and compliance measures being controlled within the EU. The aim is to ensure independence from third countries and long-term operational assurance [123].

The assessment takes into account the extent to which a provider can demonstrate through certifications – such as international ISO standards (e.g., ISO27001, ISO27017/18, ISO27701, ISO42001), Common Criteria (CC), or specific national certifications (BSI C5, SecNumCloud) – that it meets security requirements (SOV-7.1). In addition, documentation of GDPR adherence (SOV-7.2), the existence of a Security Operations Center (SOC) operating exclusively under EU jurisdiction (SOV-7.3), and EU-compliant reporting of security incidents (SOV-7.4) are included in the assessment. The capacity for independent audits by EU authorities is also covered (SOV-7.5).

However, the need for a SOC or specific security certifications such as Common Criteria depends largely on the criticality of the software, the customer segment, the size or financial strength of the software provider, and the corresponding risk profile of the data being processed. Therefore, a more nuanced assessment is needed, depending on criticality of the software category and area of application.

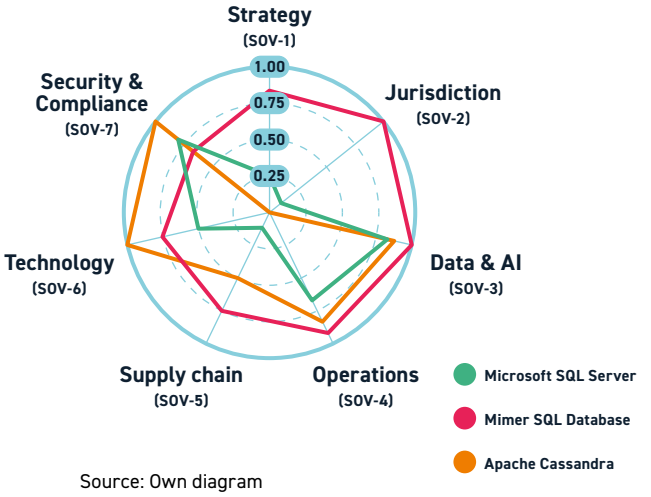
SOV-8: Environmental sustainability. Sustainability is considered a factor for long-term resilience and autonomy in the face of raw material shortages and energy dependencies [123].

The CSF evaluates metrics such as power usage efficiency (PUE), circular economy practices, and the use of energy obtained from renewable or low-carbon sources for operations. While these metrics are well established for cloud computing, their application to software products is limited, although software induces energy consumption in hardware. The chosen deployment option (e.g., self-hosted on-premises or public cloud) for software has a strong influence on its sustainability footprint. With the introduction of new generations of hardware (RAM, CPU, GPU), sustainability metrics also change independently of the software used. Accordingly, environmental sovereignty does not currently factor into the SSF's considerations.



Source: Own diagram

Figure 27: Scoring results – CRM



Source: Own diagram

Figure 28: Scoring results – Databases

Source: Own diagram

Figure 29: Options for data localization of various data types (excluding OSS with no enterprise version)

4.5 FINDINGS: HOW SOVEREIGN IS THE SOFTWARE PORTFOLIO AT A EUROPEAN ORGANIZATION TODAY?

There are two primary indicators for high software sovereignty. Firstly, the company is headquartered within the EU and secondly, the software is provided as OSS. When applying the framework, these characteristics show a clear correlation with high overall scores for digital sovereignty.

EU-based, open-source solutions lead the way

In comparison, open-source solutions (e.g., Open Project, Axelor ERP, Nextcloud Talk) consistently outperform proprietary competitors in the EU SSF, with the specific jurisdiction (e.g., Germany vs. Canada) determining the top ranking (see Figure 23). In contrast, market-leading tools such as Trello, Notion, Miro, ChatGPT, and Zoom consistently achieve low digital sovereignty scores (see also Figure 24, Figure 25, and Figure 26).

Software	Public Cloud				Self-Hosting Option	Private Cloud Option
	AWS	Azure	GCP	Other		
Trello	🟢	🔴	🔴	🔴	🔴	🔴
Confluence	🟢	🔴	🔴	🔴	🟢	🟢
Notion	🟢	🔴	🔴	🔴	🔴	🔴
Miro	🟢	🔴	🔴	🔴	🔴	🔴
Salesforce Sales Cloud	🟢	🟢	🟢	🔴	🔴	🔴
SAP Business One	🟢	🟢	🟢	🟢	🟢	🟢
SAP Sales Cloud	🟢	🟢	🟢	🟢	🔴	🟢
Oracle Fusion ERP Cloud	🟢	🔴	🔴	🟢	🔴	🟢
Zoom	🔴	🟢	🔴	🟢	🔴	🟠
ChatGPT Enterprise	🔴	🟢	🟢	🟢	🔴	🔴
Le Chat Enterprise	🔴	🟢	🟢	🔴	🟢	🟢
Gemini for Workspace Enterprise	🔴	🔴	🟢	🔴	🔴	🔴
Axelor	🔴	🔴	🔴	🟢	🟢	🟢
Conceptboard	🟢	🟢	🟢	🟢	🟢	🟢
Open Project	🟢	🟢	🟢	🟢	🟢	🟢
BigBlueButton	🟢	🟢	🟢	🟢	🟢	🟢
NextCloud Talk	🟢	🟢	🟢	🟢	🟢	🟢
Atomic CRM	🟢	🟢	🟢	🟢	🟢	🟢

Source: Own diagram

Table 8: Hosting models available

The foundations of digital sovereignty: Strategic anchoring and legal immunity (SOV-1 and SOV-2)

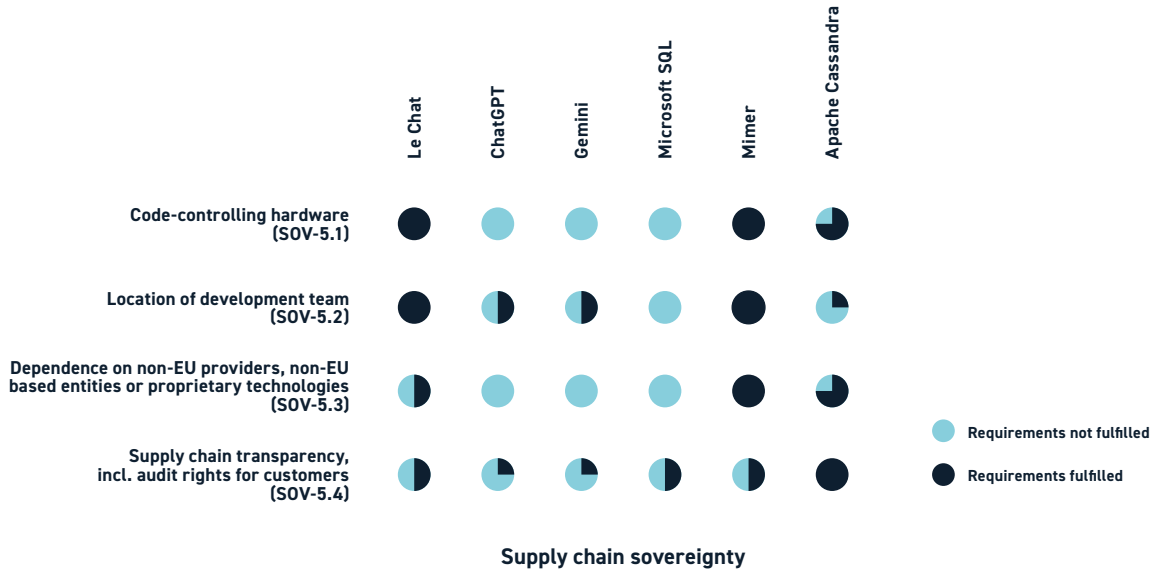
The strategic and jurisdictional sovereignty objectives analyze a provider's economic anchoring in the European Economic Area and the extent to which it is subject to EU jurisdictions to ensure protection against foreign influence.

Overall result: Jurisdictional dependency (SOV-2) due to being headquartered outside the EU can hardly be compensated for by other factors. Assuming a threshold value of 0.2 for SEALs, most non-EU providers are already excluded from the assessment due to their foreign headquarters and the associated implications (remember: products must achieve a defined minimum level in each dimension, assuming that at least SEAL-1 must be achieved, this would represent a score of 0.2).

EU versus non-EU entities: Non-EU providers which generate jobs and investments in the EU or are involved in EU initiatives can score well in terms of strategic sovereignty (SOV-1), but jurisdictional dependency (SOV-2) remains problematic. This can be seen, for example, in companies such as Microsoft, Oracle, and Salesforce, which have their headquarters in the US while also conducting development activities and filing most of their patent applications outside the EU.

The results for CRMs and databases clearly illustrate how they trail behind in terms of the SOV-1, SOV-2, and SOV-5 objectives (see Figure 27 and Figure 28). While European providers with a strong EU presence (Mimer and Atomic) score highly in terms of jurisdictional sovereignty (SOV-2), non-EU providers (Microsoft, Salesforce) achieve low scores. Depending on the interpretation, even a German company like SAP may suffer deductions due to the possible applicability of international regulations, for example due to its American co-headquarters and strong presence on the US market (see Figure 27). When considering financing by non-EU entities, one can also take the company shares held by institutional investors from the US into consideration [297].

Even in the case of open-source foundations, such as the Apache Foundation, there are weaknesses in compliance with the framework due to the jurisdiction of the headquarters as well as IP development and patent registration in the US, despite contributors being decentralized (see Figure 28).



Source: Own diagram

Figure 30: Example of results for supply chain sovereignty – LLMs and databases

Data and AI sovereignty (SOV-3)

This objective assesses the protection, control, and independence of data assets and AI services, including data security, processing, and control over AI capabilities.

Overall result: European providers and open-source solutions achieve high scores in SOV-3, as they often by design guarantee both physical data storage and complete control over encryption on hardware located within the EU. In contrast, non-EU-based solutions usually only achieve middling scores (approx. 0.5 to 0.7).

SOV-3.3: Software offers various options for data localization, which concerns the requirement to keep data in Europe without fallback options (SOV-3.3). While EU localization of work data or customer content is possible with almost all software solutions, the offerings differ when it comes to metadata and service data (see Figure 29). European software solutions that consistently host and operate within the EU usually fulfill data residency requirements across data types, as they ensure fully local storage of data without the fallback options to third countries that are common with global platforms. In several software categories (e.g., databases, OSS or open core with enterprise versions), strict data localization is fundamentally possible. In some cases, "sovereign" provisioning models (SAP Sovereign Cloud, Oracle Sovereign Cloud, or Microsoft EU Data Boundary) enable the fully local storage of various types of data.

Hosting as a sovereignty factor (SOV-4)

Operational sovereignty focuses on operational independence, control over administrative access, and management of dependence on critical suppliers.

Overall result: The choice of operating model is a crucial lever for operational sovereignty. While self-hosting (on-prem) offers maximum independence from external infrastructures, for many organizations this option is unrealistic due to a lack of resources or may no longer be available for certain software. Sovereign cloud or private cloud offerings provide alternatives. While data portability (SOV-4.1) is often possible, dependence on critical suppliers outside the EU (SOV 4.6) is the biggest weakness, with a low score of 0.19 – even European providers often rely on critical subcontractors from third countries.

OSS versus proprietary software: OSS dominates this category with an average score of 0.88 (compared to 0.56 for proprietary software) due to enabling full access to the source code (SOV-4.5), full data portability, and the ability to run the software anywhere (SOV-4.1).

Due to the possibility of self-hosting, open-source solutions enable greater independence and options in operational use. SaaS solutions with strong platform lock-in, no self-operation option, and support located outside the EU bring up the rear with scores below 0.3. Many of the products examined are offered as SaaS models, in many cases (10 out of 27) from the data centers of US hyperscalers like AWS, Microsoft Azure, or Google

Cloud (see Table 8). Solutions such as Trello, Notion, and Miro are designed as cloud-native applications with no alternative for on-prem operation.

EU versus non-EU: European providers meet the requirements for operational sovereignty in most cases (see Table 8), as the basic facilities and capacities for operating their software are located in Europe. Models such as the Salesforce EU Operating Zone or the "Sovereign Cloud" models offered by Oracle and SAP also enable technical support and maintenance work to be provided by staff within the EU.

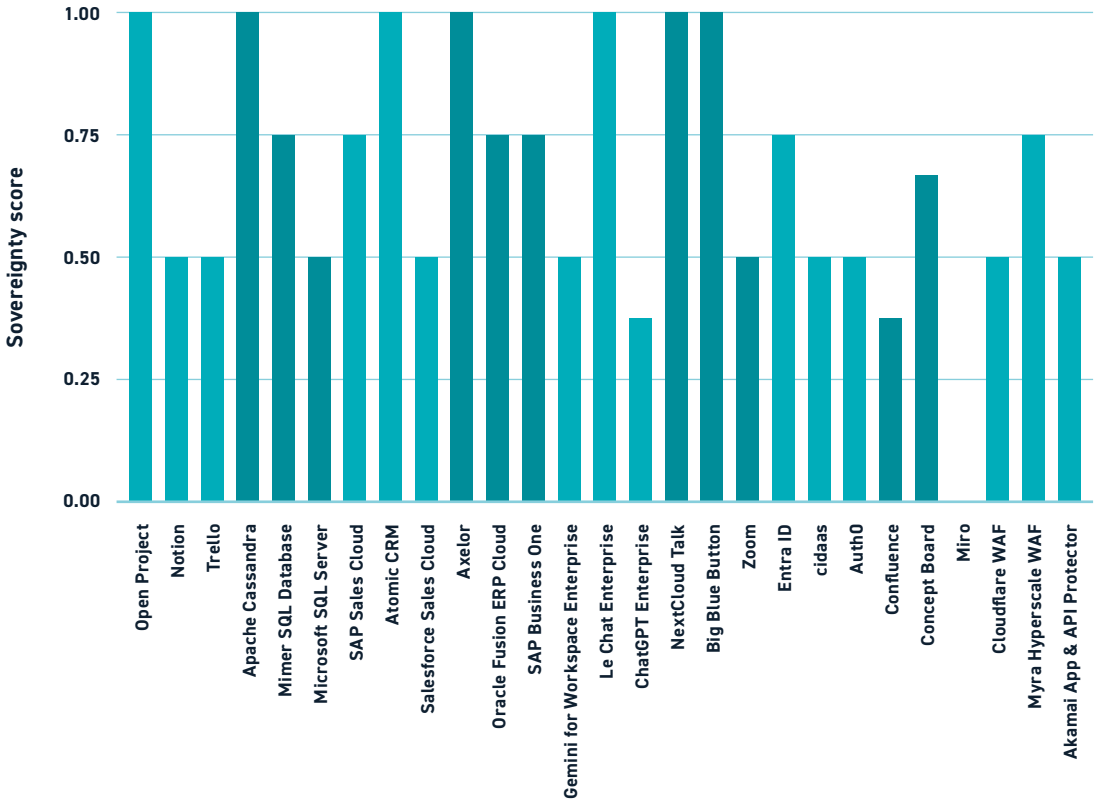
Supply chain sovereignty poses the greatest risk besides legal sovereignty (SOV-5)

Supply chain sovereignty focuses on the geographical origin of the source code and control over the locations and infrastructures involved in development.

Overall result: Supply chain sovereignty (SOV-5) is the biggest weakness for non-EU providers apart from legal sovereignty. Ten of the solutions examined fell below the SEAL minimum due to the locations of development teams, dependence on non-EU locations, and the location of code-controlling hardware (SOV-5.1) (see sample results in Figure 30).

EU versus non-EU: While many non-EU providers locate at least part of their development teams within the EU (SOV-5.2), they cannot avoid dependence on non-European sites (SOV-5.3). Some European providers, on the other hand, rely primarily on European development teams, which ensures that control over critical components and processes of the software supply chain remains within the EU.

SOV-5.2: The geographical distribution of development locations highlights the challenge. The majority of the providers analyzed develop their software at least partially in the US, which accounts for 64% to 84% of the total development activities, depending on whether open source contributors are included. Other notable countries outside the EU involved in development are India (8 of the companies surveyed), the United Kingdom (5), Canada (4), Australia (4), and Japan (4). Within Europe, Germany (7), France (5), and Ireland (3) are the main



Source: Own diagram

Figure 31: Overall technological sovereignty scores

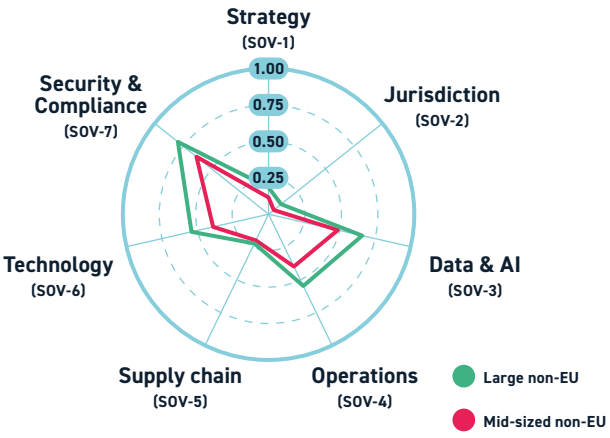
development locations. While larger European companies such as SAP (with SAP Labs in over 20 countries) as well as Axelor and Mistral, have a global presence, there are examples such as Mimer, which carries out all of its development in Sweden [212].

Technology sovereignty (SOV-6)

Technology sovereignty is characterized by openness, transparency, and independence in the underlying tech stack.

Overall result: While OSS is unbeatable in terms of openness, transparency, and hosting independence, proprietary solutions can also score high points by providing standardized and open APIs, as well as transparent documentation. The greatest threat to technology sovereignty in the context of this framework is posed by closed SaaS platforms.

OSS versus proprietary software: OSS is transparent by design and achieves maximum scores on this objective through the use of standardized and open interfaces (SOV-6.2) coupled with open licenses (SOV-6.2) as well as transparent documentation (SOV-6.3). Closed SaaS platforms fall significantly short in comparison (see Figure 31).



Source: Own diagram

Figure 32: Average scores for large vs. mid-sized non-EU providers

SOV-6.1: Almost all providers, whether OSS or proprietary, demonstrate a high degree of openness when it comes to their interfaces. They rely on well-documented, REST-based APIs. Even proprietary providers are increasingly granting insight into their architecture through documentation and white papers (average score: 0.87).

Compliance sovereignty and the certification ecosystem (SOV-7)

Compliance sovereignty is defined by the provision of recognized security certifications and the fulfillment of specific regulatory requirements for the entire software ecosystem.

Overall result: Security and compliance sovereignty (SOV-7) is the category with the highest scores across all software categories (mean value 0.78). A notable difference can be seen between large non-EU providers (0.84) and medium-sized non-EU providers (0.64).

SOV-7.1: The assessment shows a distinction between general security compliance and specific proof of digital sovereignty. While almost all players can point to ISO 27001 security certification for their organization, only a few providers possess a BSI C5 or SecNumCloud certificate. US providers such as Microsoft have invested in European standards and certificates such as the German C5, the Spanish ENS, or the French SecNumCloud.

When it comes to open-source solutions such as OpenProject or Nextcloud, the focus is shifting, as it is often not just the software that is certified, but the entire ecosystem, including European hosting partners such as Hetzner, OVHcloud, or StackIT. Since open-source tools are often operated as self-hosted instances, it is less common to see certificates from the software manufacturer. In such cases, digital sovereignty is instead assessed on the basis of the actual provision. If a solution is operated from a German data center with ISO 27001 and BSI C5 certification, the overall system achieves a higher score than a certified US SaaS solution.

The impact of company size on sovereignty scores

Large non-EU corporations (more than 10,000 employees) achieve better scores across the board compared to medium-sized non-EU companies (500–10,000 employees) (see Figure 32). The differences are particularly pronounced (more than 15%) in the sovereignty

objectives relating to data/AI (SOV-3), operations (SOV-4), technology (SOV-6), and security/compliance (SOV-7). This can be attributed to extensive compliance resources and certifications, development and support units based in Europe in some cases, and the provision of specially designed sovereign options by larger providers.

4.6 CONTEXTUALIZING THE RESULTS

The following section contextualizes the results of the analysis across the various objectives considered. The focus is on the results relating to open source and AI, as well as findings regarding the approach employed for making digital sovereignty measurable.

4.6.1 Open source as a sovereign alternative?

The political and strategic debate often identifies open source as a key instrument for achieving digital sovereignty. However, a purely licensing-based approach falls short, as digital sovereignty extends beyond the mere fact of being open source.

The EU CSF Framework favors aspects of open-source models

Open source offers clear advantages with regard to the technical and operational objectives of the framework. OSS achieves high scores due to its availability under open licenses, which grant comprehensive rights for testing, modification, and redistribution. However, this technological freedom requires sufficient in-house expertise. The question which then arises is to what extent sovereign use remains possible if strategic development is still largely shaped by non-EU key maintainers without contributions from within the EU.

The convergence of global development infrastructure creates dependencies

Special attention should be paid to the code-controlling hardware layer. While operation of the software can be ensured within the EU, global development infrastructure is concentrated on US-based platforms such as GitHub or HuggingFace. The fact that GitHub now belongs to the US corporation Microsoft, poses questions about jurisdictional control over the software production "factories." Even if local copies or forks of the code offer a certain degree of resilience, it remains unclear to what extent the integrity of build pipelines and access to them can be maintained in a crisis situation if the central coordination platform is outside of EU jurisdiction. This applies not only to platforms such as GitHub, but also to the development ecosystems of the OSS building blocks used for modern software architectures. These are also largely shaped by US-based companies and foundations.

Open source should not simply be equated with security or economic superiority. Real, ongoing security risks underscore the need for Europe to develop robust governance structures for open source that ensure accountability, rather than relying solely on code inspection by the community [16]. Comparing the total cost of ownership (TCO) for functionally equivalent open source and proprietary tools remains an essential requirement for the public sector.

Sovereign code does not always need to be open source

The debate on digital sovereignty needs to go beyond the mere issue of licensing. In line with the EU's objectives for auditability and autonomy, controlled transparency and code sovereignty are crucial. The aim is to create systems that remain transparent, verifiable, and under European control, regardless of their business model. In this sense, sovereign code is software whose audibility is not just a theoretical right but can be exercised in practice and independently by European authorities. Open-source code fulfills this condition, but it is not the only option.

4.6.2 How sovereign can an AI system be?

AI intensifies the digital sovereignty debate through new dimensions of technological interdependence. AI systems require vast amounts of dedicated computing resources and highly specialized expertise, which poses challenges regarding efforts to exert control over the entire AI lifecycle as outlined in the framework.

Gaining complete control over the AI lifecycle has proven difficult to achieve

The EU has set itself the goal of controlling the entire AI lifecycle – from development and training to provisioning, inference, and governance (SOV-3.4). While the EU AI Act provides a regulatory basis for a certain degree of control by the EU, reliance on proprietary models from non-EU providers has led to these efforts falling short. Given the EU's lack of control over the development process, these deficiencies are especially evident in the areas of strategy and supply chain.

Enterprise solutions typically meet the requirements for visibility and traceability of system access and data processing integrity (SOV-3.2). The EU CSF primarily requires logging of model usage to ensure auditability of user behavior and system output. Many providers offer this feature so that organizations can access employee interactions for security reasons.

An additional aspect of control is the guarantee of irreversible data deletion (SOV-3.2.3). For LLMs, this also means preventing AI training on company data, which has already become standard practice in products currently available on the market. In specialized cases, where models have been trained on proprietary data sets (e.g., through fine-tuning), this requirement needs to be extended to "machine unlearning". However, fully proven methods for selectively unlearning information in LLMs are still difficult to implement reliably [223], which has so far made it challenging to enforce this requirement in practice with regard to LLM providers.

Skilled workers a cornerstone of AI sovereignty

Given the technological complexity of AI systems, a distinction must be made between control over operations and sovereignty over strategic development. Digital sovereignty is measured by the capacity to operate an AI system securely and independently develop it further. The latter is currently rather difficult to achieve in the case of LLMs within the EU, given the dominant US market players and an uneven distribution of highly specialized top talent [54]. In 2022, the majority of top AI researchers worked in the US (57%), followed by China (12%) and the UK (8%) [240]. Germany and France each accounted for 4%. While the EU faces a talent gap in frontier-AI research, the emergence of Agentic Software Engineering (SE 3.0) suggests that the capacity for "further development" is becoming increasingly automated [170], [266]. As a result, the ability to orchestrate and deploy these coding agents could become a critical factor in addition to the number of experts employed.

AI inference can bring about infrastructure dependencies and security deficits

Using specialized computing clusters for inference and training processes plays a core role in AI systems (relevant for SOV-3.4 and SOV-5.2). At the same time, this poses challenges for providers due to high global demand and the associated costs of European provision [171]. This is exemplified by Mistral AI, which has been using US computing capacity from Google Cloud in the SaaS version of its product since February 2025 in order to ensure the necessary scalability for its chatbot service [300].

This leads to jurisdiction-related risks when it comes to data within the working memory (*data-in-use*). Trusted Execution Environments (TEEs) can provide a technical alternative that guarantees hardware-based isolation of processing, thereby ensuring data security with regard to AI inference. The non-EU LLM offerings from Google and OpenAI reviewed in this assessment process data on US-owned infrastructure without implementing the technical safeguards for *data-in-use* confidentiality that TEEs make possible. Mistral AI offers a self-hosting option that allows users to benefit from a fully European server infrastructure.

The SSF does not evaluate the functionality of a model in terms of content. Aspects such as inherent values or cultural appropriateness of AI models, which may be important for societal resilience, are not covered and at most indirectly reflected in the evaluation of control over the training process.

4.6.3 Limitations of the approach

A sound assessment of the results also requires critical reflection on the methodological framework and the underlying data. Applying the CSF to software reveals specific challenges, particularly regarding the transferability of standards from public sector procurement in the EU to the more heterogeneous requirements of the broader enterprise software market.

A new framework through exploratory adaptation

The framework, which was originally designed for cloud infrastructures, has here been applied to software applications. The primary objective was to validate the functional mechanisms for measuring digital sovereignty and transfer them to the field of software, an area to which researchers have thus far paid little attention. However, this transfer reveals methodological challenges and limitations that must be taken into account when interpreting outcomes.

Retaining the same objectives and weightings applied in the EU CSF allows for direct comparability, but also highlights limitations. While environmental aspects or physical security may be relevant for infrastructure, certain technologies such as AI or specialized software applications may require weightings to be adjusted. For instance, greater emphasis may need to be placed on data interoperability or algorithmic transparency.

While a flexible framework allows weighting to be adapted to specified protection requirements, it also entails the risk of manipulation, as results can vary significantly depending on how weighting is adjusted. Furthermore, the thresholds defined for SEALs in this study are based on mathematical averages, as the internal calculation methods used by the EU DG DIGIT are not publicly available at time of publication.

Validity of the information base and contextual dependence

Given the exploratory nature of this analysis, it is based exclusively on publicly available information. Inevitably, this leads to information asymmetries, as internal audit reports or confidential contract details could not be taken into account. For reliable decisions in procurement, it is essential to validate this evidence using primary data sources and detailed surveys of software providers.

Moreover, it should be noted that the underlying framework originates from the context of EU public sector procurement processes, which naturally impose the highest digital sovereignty requirements, especially when it comes to critical data. However, the broader market beyond the public sector has heterogeneous requirement profiles. Companies in less critical or regulated industries may prioritize different aspects of digital sovereignty than government agencies. The framework thus represents a specific, highly regulated standard that cannot be applied to all market-based scenarios without qualification.

Delimitation from market economy factors

This analysis assesses the software products, but does not go beyond that to examine the provider as an organization or broader market dynamics. Aspects such as risk analysis of supply chains and investigations into concentration of the market are explicitly excluded, although these factors can contribute significantly to dependencies and overall EU digital sovereignty. Likewise, no comparisons were made with regard to feature parity or TCO between comparable softwares. As cost and functionality are often decisive selection criteria in practice, the sovereignty assessments discussed here represent only one facet, though certainly a critical one.

4.7 OUTLOOK: BEYOND TECHNICAL METRICS

In addition to assessing the metrics in procurement frameworks such as the one presented here, future analyses of digital sovereignty should also incorporate economic factors such as innovative capacity, performance, and costs. It is also essential to start with a precise definition of the assessment's objectives. While public procurement is sure to remain a powerful lever for digital sovereignty in Europe, attention should also be paid to other aspects and players. Investing in future technologies and areas where the EU can build on its existing strengths, for instance, will be key to ensuring future competitiveness.

4.7.1 What can be learned from applying the CSF to software?

Adapting the EU Cloud Sovereignty Framework (EU CSF) to software (EU SSF) allows for the evaluation of individual products while also providing insight into the structure of digital dependencies.

Software and infrastructure interdependence

Still, assessing software sovereignty goes hand in hand with the available deployment options. Since the choice of hosting model has a direct impact on supply chain

transparency, physical data localization, and protection against extraterritorial access rights, having a sovereign cloud strategy is essential for software sovereignty. Its relevance is heightened by the ongoing transformation toward cloud-native structures.

Modern digital value creation processes, and powerful AI systems in particular, are increasingly based on scalable architectures. Therefore, the question of digital sovereignty needs to be addressed not only at the software license level, but also in terms of control and governance of the organization's operational ecosystem. Providers are increasingly offering a range of deployment models to meet these requirements. For organizations, digital sovereignty thus does not necessarily mean forgoing cloud technologies. Rather, it requires them to consciously select a model that combines technological scalability with legal and operational security and resilience.

At the same time, transferring the framework makes it clear that the objectives of the CSF need to be recontextualized for the software layer. While physical control is a prominent consideration in the infrastructure context, there is an even stronger focus on legal and logical control when it comes to software.

Sovereign cloud hosting is an essential condition, but not sufficient on its own. Even running on sovereign infrastructure, software may create dependencies through restrictive licenses or proprietary data formats. Furthermore, applying the framework to software reveals the need for a deeper examination of the software supply chain (e.g., through SBOMs), as complex libraries are affected by dependencies.

Market concentration and international providers

Consistently applying the framework and its exclusion criteria (SEALs) to the portfolio under review reveals that only 10 of the 27 software products analyzed meet the minimum requirements set by the EU for digital sovereignty. Although it is possible to identify European alternatives which achieve a passing grade in almost all of the technology fields examined, they seldom have a dominant market position – with the exception of SAP in the ERP segment.

While China emerges alongside the US as the second key player in hardware, the European software ecosystem is almost exclusively characterized by deep reliance on US providers. The trend toward cloud migration is resulting in growing interdependencies regarding (cloud) infrastructures which are often located at US hyperscalers.

4.7.2 The role of public procurement in contributing to the EU's digital sovereignty

Public procurement can serve as a strategic lever for Europe's digital sovereignty. Beyond meeting the government's own needs, demand from the public sector for sovereign digital products sends a signal to the market and acts as an instrument for supporting the European industry. The EU CSF serves as an instrument to support this strategic direction.

Demand as a steering mechanism, driver and lever

The potential of demand as a steering mechanism is confirmed by macroeconomic indicators. Every year, around €264 billion, equivalent to around 1.5 percent of EU GDP, flows out of the European Economic Area to non-EU suppliers [161]. Even if only part of these funds were channeled back into EU providers by the public sector, this could help "Made in Europe" solutions catch up. The goal should not be isolation or self-sufficiency but rather focus on attaining the strategic capacity to act in critical areas. In this context, digital sovereignty acts as a precautionary measure against geopolitical instability while also establishing the capacity to act.

The limits of (public) procurement

Despite its strategic significance, it is important not to view public procurement as a panacea for Europe's digital sovereignty. Public procurement should not bear the sole burden for the EU's entire digital strategy. Even today, tendering authorities are often constrained in their ability to act by considerable bureaucratic hurdles, potentially making it difficult to implement complex sovereignty criteria [161]. In addition, procurement reaches its limits in cases where there are fundamental technological needs or dependencies that cannot currently be resolved by the market. The hardware stack, for instance, remains a critical dependency that cannot be remedied in the short term by any current provider in the field based on demand management alone.

In addition, it should not be the state's responsibility to support the market on its own. Public procurement must also be aimed at mobilizing private investment through "crowding in", rather than suppressing market mechanisms through unilateral government action ("crowding out").

Ultimately, digital sovereignty is also a matter of human capital and international cooperation. The demand for skills necessitates education and innovation policies that go beyond the sphere of influence of public procurement offices.

In a globally interconnected world, digital sovereignty must also be regarded in the context of international cooperation and partnerships to avoid it becoming an obstacle to global cooperation. Thus, public procurement is a valuable tool, but only truly effective as part of a coordinated set of economic, educational, and foreign policy instruments.

Keeping an eye on the "future stack" and interoperability

A forward-looking procurement strategy must acknowledge that answers to the question of sovereignty will vary depending on the field of technology concerned. Whereas powerful European alternatives offering a high degree of operational sovereignty already exist for standard business software such as CRM, ERP, and databases, new challenges are posed in some respects by SaaS solutions and LLMs. It is important to make a distinction between short-term operational control and long-term independence. Given that the hardware stack will remain a critical external dependency for the foreseeable future, the focus of European funding – beyond procurement – should concentrate on areas where strengths already exist.

When it comes to designing the future "stack," interoperability will be a crucial factor. If software ecosystems become more cost-efficient, for instance due to AI-powered customization, systems that lack interoperability also run the risk of becoming economically unattractive. This means that procurement also needs to focus on the interoperability of middleware to ensure long-term freedom of choice between multiple providers.

4.7.3 Does "made in Europe" necessarily mean "digitally sovereign"?

European headquarters and operational anchoring within the EU correlate with higher scores in this analysis. However, this is only a foundational element and does not represent an absolute guarantee of digital sovereignty.

Geography a precondition for certain requirements

European software performs significantly better than its non-EU counterparts in terms of the objectives evaluated. Having registered headquarters and a strong operational presence within the EU correlates positively with greater legal certainty and compliance, for example more robust data protection standards. Nevertheless, it would be misguided to equate the "Made in Europe" label with guaranteed digital sovereignty. In a globally networked technological value chain, geography is a necessary condition for certain foundational aspects of digital sovereignty, but it is by no means an all-encompassing guarantee.

Moreover, there is a need to be specific about what characterizes a European product or provider. In many debates, "European" is evoked as a desirable feature, which can be defined by a company's headquarters, the location of stock exchange listing, the main sources of financing, the nationality of management, or through other means.

Considering the entire technology stack

EU-based providers can allow for administrative control by virtue of their legal form and location, but may also run into dependencies with regard to their technological infrastructures. Even software platforms based in Europe often operate on a globalized hardware and virtualization landscape dominated by non-EU technologies such as chips, hypervisors, and container orchestration. This means, EU location currently does not automatically imply resilience against technological sanctions or changes in a supplier's strategic course.

Hence, digital sovereignty must not be defined by isolation, but rather the ability to take action – for instance the freedom to change systems, migrate to new ones, or replace components in order to build resilience without losing operational capability.

These frameworks – based on seven (SSF) or eight (CSF) sovereignty objectives – underscore that being headquartered in Europe does not in itself guarantee digital sovereignty, and that digital sovereignty is a multidimensional, multilayered issue. Even providers based in the EU may fall short in certain areas, such as the transparency of their supply chains, auditability, or dependence on proprietary third-party components. Digital sovereignty should therefore not be reduced to mere proof of origin but primarily manifests itself in the attributes of a product which enable customers to exercise freedom of action and allow them to switch providers.

Investment and the innovation dilemma

Digital sovereignty is closely linked to ownership structures and financial flows. A company may be legally registered in Europe, but if its funding is primarily provided by non-EU venture capital, strategic loyalties are not shielded against potential shifts.

In addition, capital outflow is compounded by spending on US-based cloud infrastructure and software platforms in the European market [161]. This prevents the accumulation of profits in Europe and reinvestment in local research and development. The result is a negative flywheel effect. While US providers accelerate their innovation cycles and expand their technological superiority, in part through European turnover, European providers lack precisely this capital to catch up technologically.

Without a sovereign financing ecosystem to break this cycle, the "Made in Europe" label may remain only a phase in a company's life cycle or be limited to niche markets, while the overall technological climate is shaped outside Europe.

Digital sovereignty as an organizational task

In conclusion, the analysis shows that digital sovereignty is not a static end state that can be achieved and checked off by purchasing a certified "Made in Europe" product. Instead, it should be understood as an ongoing strategic and risk management process that needs to be deeply embedded within the organization.

For companies using digital products, responsibility is shifting from simple focus on IT procurement to more strategic governance of digital sovereignty. This means assessing data and applications based on their criticality and assigning them to appropriate provisioning models – from the public cloud for non-critical workloads to strictly isolated environments for sensitive core processes. At the same time, organizations must proactively define roles and responsibilities, for example in risk management or enterprise architecture, continuously monitor dependencies in the software supply chain, and develop "exit strategies" for key components.

Digital sovereignty develops within organizations when the mechanisms of the EU's legal framework, such as the Data Act, are actively utilized to contractually enforce portability, thereby establishing freedom of choice and preventing technological lock-in effects. In this sense, digital sovereignty is not only an attribute of the software, but more importantly a competence on the part of the user.

CHAPTER 5

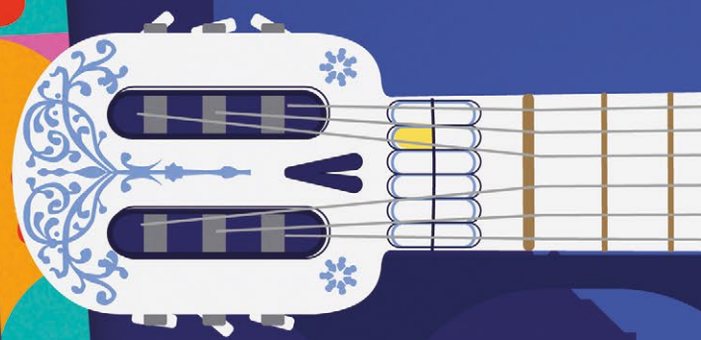
DIGITAL AFTERLIFE
MANAGING YOUR DIGITAL ESTATE

Global ranking of social networks
active monthly users in millions

QUICK CHECK: DIGITAL ESTATE

- [ ] **INVENTORY**
  Keep a list of all accounts, subscriptions and crypto assets
- [ ] **BACKUP**
  Regularly and securely save a local copy of photos and documents
- [ ] **PRIVACY**
  Specify which information should be deleted without being read
- [ ] **POWER OF ATTORNEY**
  Appoint "digital proxies" – in the best case attested by a notary
- [ ] **PASSWORDS**
  Store the master password for your password manager in a safe place
- [ ] **DEVICE PINS**
  Ensure access to smartphones to enable MFA procedures
- [ ] **PLATFORM TOOLS**
  Activate digital estate functions for Google, Apple & Meta

68%
of internet users **have made no provisions** regarding their digital estates



The "grief tech" sector has a global value of around

€120 billion

Nearly every 5th Bitcoin
is lost irretrievably due to missing login credentials

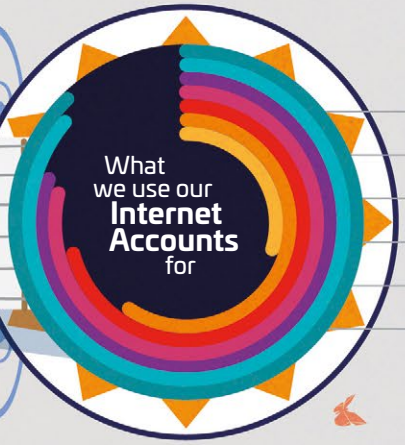
4.9 Billion
profiles of deceased users may exist on Facebook by the year 2100, turning the platform into a "digital cemetery".

62%

of users recycle the same password for mulitiple services

60%

of users would not like anyone to have access to their digital content after their death



- Emails: **87.8%**
- Online purchases: **85.9%**
- Searching for info: **80.1%**
- (Video) Telephony: **78.7%**
- Online banking: **70.7%**
- Social networks: **59.2%**
- Selling items online: **29.6%**

Identity theft

16 Billion

compromised credentials

1.8 Billion

of these are exploited in hacker attacks

Number of accounts each user actually has:

80–170

Number of accounts each user thinks they have:

15–20

40,000 Apps in everyday use

provide uninterrupted location tracking for the global data market

Source: [3], [22], [24], [25], [90], [140], [145], [168], [216], [221], [251], [254], [262], [265], [311], [313], [319], [323], [327], [329], Own diagram

5 DIGITAL AFTERLIFE – MANAGING YOUR DIGITAL ESTATE

Erica M. passed away on March 14th. Her death certificate recorded that she had died of natural causes. Three days later, an installment loan was applied for in her name – without her relatives' knowledge.

Erica's death was peaceful, but sudden. She didn't die in an accident nor had she been ill. She was only 52 years old. The evening before her death had been much the same as any other evening – dinner with her husband Max, discussing their appointments and an upcoming business trip. The next morning, Erica did not wake up. For her husband, a senior executive at an industrial corporation, professional routine became a survival strategy. He tried to cope with the shock of her death by doing what he did best – getting things in order and taking care of everything that needed to be done.

In the years preceding her death, Erica had taken steps to ensure their joint affairs were in order. She was an attorney who regarded order not as an end in itself, but an important precautionary measure. In her study, there were a number of folders, all neatly labeled. Insurance, home loan, powers of attorney, living wills. Contracts they had signed together, and others that Erica had arranged on her own. Max worked his way through the documents. Many were familiar, some he hadn't seen in years, and others he had never seen before, but there was nothing that stood out as suspicious or surprising.

As far as he was aware, he had found and accounted for everything. His wife's smartphone lay locked on the desk – her laptop closed beside it. Both devices were password protected, and Erica had never written down her passwords. Max put them aside. He didn't need them right now. Or, at least, so he thought.

In the first few weeks following Erica's death, much proceeded as expected. Standing orders continued to go out of her bank account, subscriptions were canceled, bills paid. Max took care of their joint accounts, and the children helped him as much as they could. It was exhausting, but manageable. Emails continued to arrive in Erica's inbox. Max saw the notifications pop up on her cell phone lock screen. He read the subject lines, but otherwise left them there. He didn't want to access anything that had belonged to Erica unless he had to.

Around two weeks after Erica's death, Max began to examine her bank statements more closely. At first out of routine, then with increasing confusion. It wasn't the large amounts that caught his eye, but the small, recurring debits going out to a payment service provider that Erica had used while alive. €49.90. €27.30. €12. The amounts seemed legitimate enough, yet they didn't match up with any contract that Max was aware of. He searched through Erica's folders but found nothing. He asked the children, but none of them knew anything about it.

Not long after that, a letter arrived from the bank regarding a change in contact details for one of the couple's joint accounts. An email address had recently been added as the primary contact address for online banking communications. Max recognized it immediately. It was Erica's email address. The fact that someone had made this change after Erica had passed away rang alarm bells with Max. A quick call to the bank confirmed that the change had been authorized by the system. Max froze. That was impossible. He filed a report with the police.

When he finally gained access, he saw the extent of the damage: Erica's inbox contained dozens of password reset and security code messages. Somebody had gained access to Erica's email account – presumably via an old data breach and a reused password. Existing accounts had been taken over: Payment services, customer accounts, online logins. None newly created. All had already existed.

Weeks later, Max received a letter from a financial service provider he didn't recognize the name of, addressed to Erica M. and confirming a loan application for a mid-five-figure sum. Max called the company immediately and told them that Erica had passed away. Their response shook him to the core – the application had been submitted correctly and the identity clearly verified. Multiple times. It was only through police investigations that the truth came to light: the perpetrators had used state-of-the-art deepfake filters to superimpose Erica's face onto that of an accomplice in real time, using her photos from social media and within her email account. During a remote video identity verification process, the deception had not been detected on screen by the employee. As far as the system was concerned, Erica M. was a living, active person.

Max spoke with attorneys and authorities. It took months to sort most things out. Some things were successfully reversed. Direct debits were stopped, accounts closed. For Max, though, it was yet another battle to fight amid the countless tasks that come with a bereavement – all under the emotional strain of his recent and sudden loss. What could not be reversed, however, was the realization of just how unprotected the period between Erica's death and the final closure of her digital estate had been. Erica had done many things right. What she had neglected to do in her preparations, though, was to consider what would happen to her data. Not out of indifference on her part, but out of a lack of awareness of the consequences.

5.1 DIGITAL EXISTENCE AND THE PROTECTION GAP AFTER DEATH

Identity is no longer linked exclusively to the physical body or official records. Today, it is also defined as the totality of all personal data, online accounts, biometric characteristics, and digital traces that an individual generates during their lifetime [216]. This identity manifests itself in digital infrastructures, communication archives, and algorithmically processed behavioral patterns, evolving from simple data into a complex digital shadow that encompasses email accounts, social networks, cloud storage, and digital contractual relationships. This state is increasingly described as an "informational body". This data – including stored voices, texts, and behavioral patterns – is not mere property. Since it reflects values, thoughts, and social relationships, it is regarded as an extension of the human being. Our data is us in digital form [20], [79], [141], [263].

This digital existence does not automatically end with an individual's biological death. While this marks a clear change in legal status, digitally it creates a state of uncertainty [20], [216]. Between the end of life and the definitive end of an individual's digital existence, there is a transitional period that is not clearly regulated – neither technically nor legally [216]. During this period, systems continue to operate and accounts remain active. Since digital identities are highly networked and interlinked via technical interfaces and data exchange mechanisms, automated systems evaluate the authenticity of an identity not on the basis of biological status, but on the basis of consistent usage patterns, successful logins, and historical payment flows. For these verification mechanisms, a deceased individual may therefore remain a completely valid identity. This decoupling of the end of human life and digital persistence creates a protection gap that poses significant risks for heirs, institutions, and the integrity of digital systems [79].

This highlights the need for comprehensive digital identity protection, encompassing all preventive and reactive measures designed to safeguard the integrity, authenticity, and confidentiality of a digital existence throughout its entire lifecycle and beyond. An approach, in other words, that serves to protect the interconnected identity from unauthorized access, manipulation, or misuse by third parties. Identity protection is therefore not just a question of protecting technical data, but also of safeguarding human dignity, since it concerns the integrity of the individual themselves. While this protection is already complex during a person's lifetime, it becomes particularly fragile after death, since active

control by the individual concerned ceases [79] while their digital identity continues to exist within technical systems.

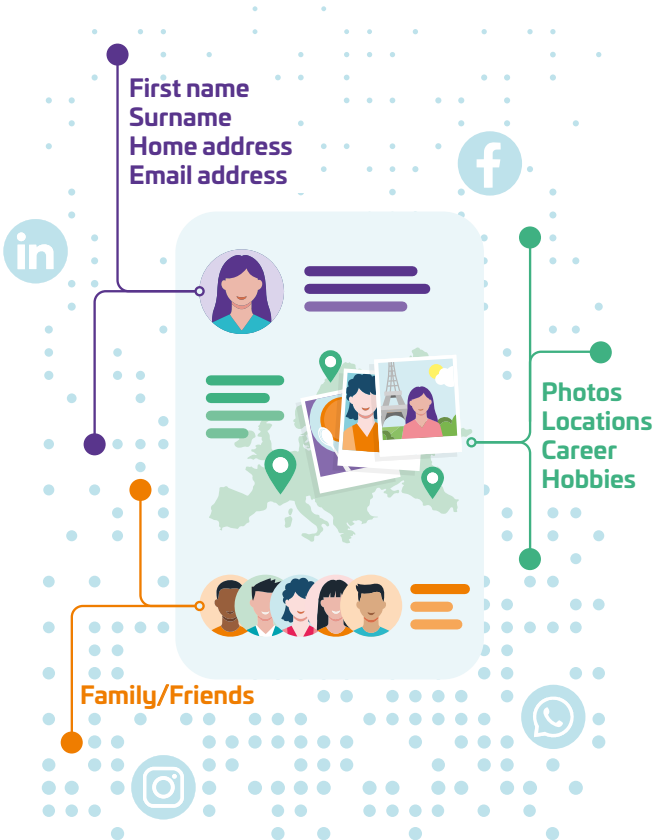
Effective identity protection must therefore continue postmortem, since the misuse of data belonging to deceased individuals can violate personal integrity even after death [263].

Criminals are already able to create detailed profiles from just a few publicly available data points. Names, photographs, professional information, previous addresses, or publicly visible relationships can be enough to enrich a digital identity and convincingly sustain it. The practice is made all the easier by social networks and open platforms. An individual's digital shadow is dynamic, constantly growing with every interaction, post, and stored piece of information – often without users realizing the full extent of their digital footprint [216], [250]. It is also reproducible and vulnerable to manipulation.

The use of artificial intelligence (AI) is giving rise to a whole new dimension of abuse. Deepfakes are no longer a niche phenomenon but are increasingly finding their way into everyday communication contexts. Fake images, videos, and audio recordings have become so realistic that – to the untrained eye – it is impossible to distinguish them from authentic content. This significantly exacerbates the issue of digital identity after death, since it not only exploits existing data, but also actively generates new content that appears authentic.

Deepfakes of deceased individuals are particularly problematic, since they can be deliberately used for political influence, fraud, or financial manipulation. Forms of "digital resurrection" are also becoming increasingly prominent, such as voicebots or chatbots that replicate an individual's communication style using existing data [6]. As part of the re-creation services offered within the digital afterlife industry (see Chapter 5.3), "griefbots" leverage generative AI to actively generate new content that replicates the voice and communication style of the deceased, rather than merely repeating static datasets [6], [175]. Just how advanced this technological simulation of presence has already become can be illustrated by the example of the late Robert Kardashian, whose hologram delivered a pre-recorded message in lifelike appearance and voice [17]. Alongside these high-tech simulations, hybrid funeral concepts are increasingly reshaping traditional ways of commemorating the dead. QR codes on gravestones link the physical grave to digital memorial pages where visitors can access multimedia content such as photographs and biographies [6].

This situation poses considerable challenges for heirs. While traditional estates follow clear legal regulations, digital estates are often fragmented and difficult to navigate. Digital estates should be understood as a logical extension of traditional estates and encompass all traces and assets that an individual leaves behind online, from user accounts on social networks and email inboxes through to crypto assets and private photographs stored in the cloud [216].



Managing a digital estate is often fraught with technical and legal barriers, including missing access rights, unknown passwords, and providers who do not respond or demand formal documentation that is difficult to provide. Meanwhile, digital systems keep operating, generating new risks.

Digital legacies are therefore not a minor issue, but a fundamental phenomenon with profound legal, technical, and ethical implications. The gap between biological death and the persistence of digital data demonstrates that traditional concepts of identity, responsibility, and protection are no longer adequate in the face of today's digital infrastructures [216], [272].

5.2 OUR DIGITAL FOOTPRINT AND THE ILLUSION OF CONTROL

A key security risk lies in the everyday digital routines of users. Risky practices are widespread and can continue to have consequences even after death. According to global surveys, 62 percent of users reuse the same password, or a variation, across multiple online services [221]. In contrast, the use of security tools is still not particularly widespread: in Germany, only around 50 percent of users use a password manager to protect their digital identities [48]. While this is often down to convenience or time constraints while alive, it poses particular risks after death. If third parties succeed in gaining access to a central account, such as an email inbox, they may be able to take control of numerous other accounts without detection or intervention. Password reset mechanisms, authentication protocols, and identity verification processes rely on these centralized points of access.

These risks are inherent in the near-universal use of the internet in Germany. Ninety-seven percent of individuals aged 16 to 74 are online, including 90 percent of those aged 65 to 74. In addition to communicating via email (88 percent) and video calls (79 percent), 59 percent of the population is regularly active on social networks, making it a significant part of their daily lives, and leaving a growing digital footprint [323]. This internet connectivity extends to digital public administration services, with 59 percent of citizens communicating with government authorities and agencies online and 34 percent scheduling appointments with public institutions or health insurers via the internet [323].

This behavior is particularly evident in e-commerce. Eighty-six percent of individuals over the age of 16 purchase goods or services online. There is also a clear trend toward consuming exclusively digital content – 42 percent of those surveyed access movies and music via streaming or downloads, while 19 percent read digital books and news publications. Travel and leisure planning is another key online activity, particularly when it comes to booking tickets (32 percent), accommodation (29 percent), and transport (27 percent). The picture is completed by the widespread use of online banking (71 percent) and the occasional sale of personal goods by nearly one-third of the population [323].

The digital legacy that results from modern society is becoming increasingly complex and constantly evolving. While digital legacy used to be primarily associated with email accounts, it now also encompasses not only social media and online banking but also stored photographs, videos, and messages, as well as virtual currencies, behavioral data, and even AI-generated avatars [216]. Despite this diversity, many people significantly underestimate the number of digital accounts they have, giving rise to an illusion of control [254]. A 2018 study found that while users estimated that they had a median of just 15 online accounts, objective scans of their email inboxes revealed as many as 80 accounts [168]. Since this misperception occurred even among tech-savvy academics, it is seen as an example of bounded rationality – a cognitive limitation that persists across educational level.

In 2026, the gap is larger than ever. Roughly 95 percent of Germans believe they have fewer than ten online accounts [30]. In reality, the average person has around 170 passwords [262]. These password statistics are based on analyses of user data from password manager providers. As not everyone uses such tools, this figure highlights just how challenging it can be for people to manage their digital lives independently. This significant underestimation means that, today, individuals are only consciously aware of around 6 percent of their actual digital presence. This awareness gap can be explained by the availability heuristic [250]. People tend to primarily recall the services they use on a daily or weekly basis, such as email providers, social networks, and online banking platforms. Accounts created for one-time transactions – such as purchasing a specialized product from a niche online shop, registering for a time-limited service, or booking overnight accommodation abroad – fade from active memory almost immediately after use. Nevertheless, these accounts remain in provider databases as active identities, expanding the potential attack surface for data breaches without

users' awareness [152]. In addition, tens of thousands of smartphone apps track users' location and browsing behavior in the background, storing this data for further use by external data brokers. These comprehensive behavioral profiles reveal far more than just consumer behavior – they provide deep insight into intimate aspects of daily life and health routines. This exposure of an individual's personal life renders them vulnerable to manipulation, reputational harm, and stalking while they are alive [90].

The long-term effects of this accumulation of accounts can be seen in the size of the largest social networks and messenger services and the vast number of user accounts that they host. As of February 2025, Facebook ranked first, with approximately 3.07 billion monthly active users. In second place was YouTube, the video platform owned by Google, with around 2.53 billion users. Third place was shared by Instagram and the messaging service WhatsApp, each with roughly two billion users worldwide [346]. It is estimated that by 2100, Facebook may host as many as 4.9 billion deceased users' profiles, turning the platform into a "digital cemetery" [20], [94], [265].

5.3 RISKS AND THREATS

The digital self often outlives the physical body indefinitely. Unlike physical assets, digital content does not deteriorate naturally. Social media profiles, dormant cloud storage, and email accounts remain on servers unless they are actively deleted [94] or subject to providers' automated deletion routines, which increasingly target inactive accounts after periods of six months to two years. Researchers in the fields of digital culture and human-computer interaction refer to this persistent online presence as "informational or digital corpses" – digital accounts and data of deceased individuals that remain unmonitored on servers [94], [263], [264].

This perpetual digital presence poses security risks, since these informational corpses, or "zombie accounts", can significantly expand the attack surface. These are typically user accounts that have not been consistently deleted or deactivated following a job change, loss of login credentials, or the user's death, leaving them as unmanaged access points within systems. Since these "dormant identities" often have weak or outdated passwords and are not actively monitored, they provide attackers with entry points to infiltrate networks undetected [211], [216], [264], [355].

Necro-economy

The current debate warns of the emergence of a "necro-economy" [89],], in which the data of deceased individuals is exploited as a valuable resource for the advertising industry and AI sector, either for training algorithms or for inferring information about living relatives [6]. In this context, major tech companies such as Google, Meta, and Apple effectively act as "digital undertakers" [79], [216], [263], [264]. They control the global digital legacy and, through algorithms and terms of service, determine who is remembered and who is erased. Since these corporations are profit-driven rather than neutral archivists, strategic changes or platform shutdowns could result in a significant loss of collective human history [263]. This creates a conflict between the individual's right to privacy and society's interest in preserving historical data. Consequently, there is a growing call to recognize digital remains as part of the collective cultural heritage and to afford them special protection, comparable to that granted to physical archives [263].

This necro-economic approach to data processing is not limited to platform operators but also reflected in the exploitation of accounts by third parties. Profiles with high "digital status capital" (high status, many followers) become a valuable resource for cybercriminals. Hackers "harvest" the social status of the deceased to exploit their credibility, built up over many years, as a tool for disinformation campaigns [253]. In this informal, user-driven sphere of the necro-economy, the identities of deceased individuals are also used for the self-promotion of others. In cases of fake death reports, for example, malicious actors leverage the viral dynamics of the news to enhance their own reputation at the expense of the integrity of the deceased [253]. Without authorized estate contacts, rumors can spread uncontrollably, potentially causing permanent damage to the digital memory of the deceased [307].

New dimensions of manipulation: AI and social engineering 2.0

The integration of AI adds a whole new level of sophistication to identity theft and misuse. "Neural echoes" – AI-driven simulations (griefbots) – can replicate the online persona of a deceased individual almost perfectly, mimicking their language, tone, reasoning patterns, and response styles with such accuracy that third parties can hardly distinguish them from real communication [79], [94]. Without clear labeling, this carries a serious risk of deception and erosion of integrity, since AI can

generate statements that the real person never actually made [94]. This technology enables "social engineering 2.0": attackers can use deepfake audio to gain the trust of relatives or business partners and legitimize fraudulent actions or deploy deepfakes of deceased individuals for political or financial manipulation [94]. Moreover, combining data fragments from multiple individuals enables the creation of entirely new synthetic identities – digital personas constructed from the digital traces of two or three deceased individuals that appear real, yet are entirely fictitious.

In addition to these direct attacks, the growing digital afterlife industry represents a new supply chain risk. The industry can be broadly divided into four main areas: information management services (e.g., password vaults), posthumous messaging services, online memorial services, and technologically advanced re-creation services [79], [216], [264]. A data breach at any of these third-party providers could expose highly sensitive private data such as chat histories and voice samples, and severely compromise personal privacy [175]. There is also a risk that intimate expressions of grief could be exploited for profit, with personal mourning treated as a commodity [252]. Companies could even use this data to train AI or feed advertising algorithms, which can be considered a violation of human dignity [141], [175], [263], [264].

Without a digital estate plan in place, private information could be exposed through future data breaches, with the deceased individual unable to protect themselves [263]. Studies indicate a growing awareness of the issue: 61 percent of consumers are concerned that the identities of the deceased are particularly vulnerable to such abuse [211].

Consequential economic risks

The financial consequences of an unmanaged digital estate, although difficult to quantify statistically, can be substantial. With the average cost of a funeral in Germany amounting to approximately €13,000 [334], the additional financial risk posed by posthumous identity theft is often underestimated. While funeral expenses are a known quantity, there are currently no dedicated statistics on posthumous digital identity misuse, since such cases are typically reported locally and categorized under general fraud. However, based on data on identity theft among living individuals, the average financial loss in Germany stands at approximately €1,366 per case [285]. It is reasonable to assume that this figure could be higher for deceased individuals, since fraudulent activity often goes undetected for longer periods due to the lack of active account monitoring.

This phenomenon, sometimes also known as "ghosting", appears to be significantly more widespread in the US, with over 1.1 million cases of identity theft reported annually [136]. Its prevalence is linked to the country's centralized consumer fraud reporting system and the social security number (SSN), which often serves as sufficient proof of identity on its own. In contrast, the risk in Germany primarily stems from the technological shift described in the previous sections. While domestic security measures, such as remote video identity verification, were long considered a barrier to identity theft, AI-powered deepfakes are increasingly able to circumvent biometric identification processes.

The economic logic behind this type of fraud is evident on darknet marketplaces, where "fullz" packages – complete sets of personal data including name, SSN, date of birth, and address – are sold for US$20 to US$100 [329]. Data sets of deceased individuals, known as "dead fullz", are available for as little as US$1 to US$3 and are often used to open bank accounts for money laundering [311]. In addition to criminal fraud, the phenomenon known as "subscription creep" leads to a gradual loss of assets [42], since contracts for streaming services, cloud storage, or software licenses do not automatically end at death. Without proactive management, funds from the deceased's estate can continue to flow to service providers for months. The risk is particularly grave when it comes to digital assets. Estimates suggest that 11 to 18 percent of the total Bitcoin supply has already been permanently lost due to inaccessible keys, including those lost as a result of death [251]. Without proper management, a digital estate either becomes vulnerable to criminal activity or gradually loses value through automated charges and inaccessible assets.

5.4 LEGAL AND TECHNICAL CHALLENGES

In modern jurisprudence and the sociology of technology, the transition to the digital age marks a turning point in inheritance law. Today, nearly every deceased individual leaves behind digital traces – some as part of a private online life – including emails, smartphone chat histories, and accounts with payment services such as PayPal or e-commerce platforms [272]. Digital assets can be characterized by four cornerstones: first, they exist only in digital form; second, they are stored

digitally, either locally, in the cloud, or on a blockchain; third, they have financial or emotional value; and fourth, they ensure "quasi-ownership rights" to their user. These digital assets encompass both tangible assets, such as cryptocurrencies and non-fungible token (NFT) artworks, and intangible content [208], [264]. Beyond monetary value, behavioral and health data can also hold deep personal significance, such as knowing what music a loved one was listening to on the day they died [254].

Despite the prevalence and importance of digital assets, the legal system is lagging behind technological developments. The emergence of digital assets has triggered a revolution in the expansion of objects of rights, yet their unclear legal status poses significant challenges for inheritance law [355]. Digital assets cannot entirely be legally characterized as traditional property because, unlike physical goods, they inherently depend on technical infrastructure and external service providers [355]. This situation exacerbates an existing protection gap. The EU General Data Protection Regulation (GDPR) explicitly excludes deceased individuals from its scope (recital 27), leaving families and businesses to navigate uncertain territory. Much of this uncertainty arises because access to accounts is often restricted by platform operators' terms of service, which contractually prohibit third party access. Moreover, digital content often contains shared data. The private messages of deceased individuals are inextricably linked to the privacy of living communication partners, resulting in a direct conflict between the heirs' right to access information and the persisting data privacy rights of these third parties. Without specific national legislation, it therefore remains unclear how inheritance law can be enforced in the face of these technical and data protection barriers [79], [94], [272].

International legislative landscape and national differences

France is leading the way in posthumous data protection. The country's 2016 Law for a Digital Republic establishes an explicit right for individuals to leave binding instructions regarding the handling of their personal data after death [79]. Heirs can request the closure of accounts and access to data where necessary, although the absence of general guidelines still complicates practical implementation [94].

Germany, by contrast, follows an *ipso iure* succession system, under which estates automatically transfer to heirs upon death pursuant to § 1942 of the German Civil Code (BGB). A landmark ruling by the German Federal Court of Justice (BGH) in July 2018 clarified that contracts for digital accounts are inheritable. In the case of a deceased 15-year-old, the girl's parents were able to gain access to her Facebook account. The BGH held, pursuant to § 1922 BGB (Universal Succession), that heirs inherit all rights and obligations of the deceased. While the BGH's landmark ruling effectively equated digital content to physical letters, granting heirs access [94], [351], [355], the systemic limitation of § 90 BGB remains. Since data is not legally considered a tangible object, heirs do not inherit direct ownership, but only the rights granted under the service agreement with the provider, i.e., the right to access [208], [355].

Platforms as digital gatekeepers

Despite legal successes, digital legacy often fails in practice due to technical implementation challenges. Platforms such as Facebook and Google act as "digital gatekeepers", using their specific architecture – known as "affordances" – to control who has access to a deceased individual's data and how that person is remembered [6], [79], [81], [175], [216], [250], [307]. Affordances can be defined as the actions that a platform enables or restricts. This power imbalance allows private corporations to determine posthumous identity through technical permissions or restrictions, often without knowledge of the deceased's actual wishes [81], [263], [307], depriving both the deceased and their relatives of control.

The field of digital legacy is marked by a striking absence of government regulation, giving digital service providers enormous power [6]. This lack of binding rules may be partly explained by societal discomfort with confronting the end of life [231]. Compounding the issue is a significant knowledge gap, with approximately 85 percent of Facebook users unaware of the platform's "Legacy Contact" feature [94]. In the absence of standardized procedures and interfaces, users often resort to risky workarounds such as sharing passwords. However, these practices not only violate platform terms of service but are increasingly rendered technically impossible by modern security mechanisms, such as biometrics and multi-factor authentication (MFA) [326].

The ethical dilemma: Digital dead body management

At the center of the debate is the conflict between protecting the privacy of the deceased individual and the property interests of their heirs [216], [355]. In this context, the concept of "digital dead body management" (DDBM) has been developed by scholars and practitioners to address the management of digital remains and to advocate for "residual rights of dignity and respect" for the deceased [20]. The challenge lies in balancing the protection of digital privacy (posthumous data protection) with the needs of the bereaved for closure, resolution, and healing [20], [141], [175]. Since digital traces – from emails to cloud-stored photographs – carry significant emotional and spiritual value, they are considered an essential part of an individual's privacy [355].

At the same time, they are fragile historical sources. Since they are stored on private platforms driven by commercial interests, their preservation as part of a collective digital heritage is at risk [20], [81]. This also raises the question of whether contract law should grant heirs full access to and the ability to continue using the social media accounts of deceased individuals. The interests of heirs do not necessarily align with those of platforms, society at large, or the presumed wishes of the deceased [231].

Ultimately, current approaches to digital estate regulation often fail due to technical implementation barriers and a lack of awareness regarding identity protection, while the broader domain of posthumous identity – particularly in the context of AI – remains largely unregulated. In the current debate, therefore, the idea of a broader right to digital identity is being explored, particularly with regard to the right to shape one's own life narrative in the digital sphere. Traditionally, privacy has been understood primarily as protection against interference by others. The new interpretation, however, emphasizes an active dimension, focusing on the freedom of individuals to shape their own digital identities in accordance with how they wish to be seen. As a legal basis for this, two provisions of the EU Charter of Fundamental Rights serve as reference points: Article 7 (Respect for private and family life) and Article 8 (Protection of personal data). Experts have proposed closer integration of these rights to establish an all-encompassing right to digital identity [231].

5.5 COMPREHENSIVE STRATEGIES AND FUTURE ACTIONS

What individuals should do: Planning and support for heirs

Planning a digital estate is just as important today as writing a traditional will. In Germany, there is no separate digital inheritance law. Instead, digital content and contracts automatically transfer to heirs under the principle of universal succession (Gesamtrechtsnachfolge) [3], [216], [313]. The following points offer initial guidance and general information. They are not intended to be exhaustive and should be considered in the context of each individual's specific situation.

Providing for the future: Planning your digital estate

[3], [22], [216], [247], [254], [291], [313]

To spare their next of kin complex and lengthy processes, individuals should take timely action.

1. **Inventory and organization:**

   - Create a list of all online accounts, email addresses, and cloud services.
   - Document all subscriptions (streaming services, shopping platforms) and financial accounts (online banking, cryptocurrencies).
   - Regularly back up personal data, such as photographs, locally on external storage devices to ensure access independent of platforms.

2. **Confidentiality wishes:**

   - Explicitly specify which content (e.g., private chats, browser histories) is to be deleted unread after your death. This protects your posthumous personal rights and prevents relatives from inadvertently accessing sensitive information.

3. Legal safeguards:

- Draw up a specific "digital power of attorney" or include your digital estate in a will.
- Appoint a trusted person as a "digital executor". You can instruct that specific data must be destroyed without being viewed by third parties.
- A notarized power of attorney is most likely to be accepted by service providers and provides the greatest legal security.

4. Access management:

- Use a password manager as a central solution.
- Ensure that your trusted person has access to the master password (e.g., by depositing it with a notary or in a safe deposit box).
- Make sure your heirs can access your smartphone to receive multi-factor authentication (MFA) codes.

5. Platform-specific solutions:

- Configure the legacy or account-deactivation features of major providers while you are still alive, such as Apple's and Meta's "Legacy Contact" or Google's "Inactive Account Manager".

For relatives and heirs

[3], [22], [216], [247], [313]

After a death, relatives often need to act quickly to avoid unnecessary costs and data loss.

1. Document search and review:

- Look for the inventory list, power of attorney, or will.
- Check account statements for any recurring charges for digital services.

2. Proof of death and cancellation of contracts:

- Notify the respective service providers of the death, providing the death certificate (and, if applicable, the certificate of inheritance).
- Cancel any current contracts and subscriptions promptly, since these generally pass to heirs under inheritance law.

3. Account management:

- Decide whether social media accounts should be deleted or memorialized. Respect any deletion instructions left by the deceased for sensitive data, to protect their privacy.
- Back up important digital memories (photographs, messages) before an account is permanently deleted, since many providers do not recover data after deletion.

4. Legal enforcement:

- If necessary, invoke the German Federal Court of Justice (BGH) rulings of 2018/2020, which generally grant heirs access to the accounts of deceased individuals.

Requirements for professional legal structuring and advice

In addition to an individual's own digital estate planning, professionals such as attorneys and notaries must follow specific standards to ensure the legal and secure management of the digital estate [3], [216], [313]:

- **Avoidance of security risks:** Passwords should never be included directly in a will, since they may become public once the will is filed with the probate court.
- **Differentiation of powers of attorney:** Contracts should explicitly differentiate between administrative powers (e.g., account deletion) and access to highly personal communications (e.g., private chats).

- **Protection of personal rights:** Professional legal structuring involves balancing the heirs' interest in information with the protection of the deceased's privacy. Arrangements may include a notary overseeing the deletion of sensitive data before third parties are granted access.
- **Legal classification:** While Germany's statutory inheritance law already covers digital assets, explicit regulations can simplify dealings with service providers.
- **International context:** For accounts with US providers, powers of attorney should be drafted in such a way that they comply with international access standards so as to facilitate cooperation with providers [22], [291].

What policymakers should do: Regulatory measures

To close the systemic gap in protection between biological death and digital persistence, lawmakers are called upon to establish reliable infrastructures.

- **Central digital estate registry:** A key focus is the introduction of a central digital estate registry under draft § 1959a BGB, which would allow heirs to discover online accounts in the same way as traditional accounts [43]. In addition, a statutory obligation for providers to proactively inform users about the inheritable nature of their data is recommended [216].
- **Automated identity verification:** To accelerate the process, the German Federal Government plans to automate the verification of heirs' identities using its Deutschland-ID national digital identity system [56]. The German Federal Bar Association is calling for strict data protection measures to prevent misuse of sensitive information [43].
- **Posthumous data protection:** A precise legal distinction should be made between personal rights-based, property rights-based, and composite rights-based data within an individual's estate [355]. Only then can platforms be effectively required to provide appropriate interfaces without infringing posthumous personal rights [6].

What companies should do

Companies should address digital estate management through practical, operational measures:

- **Account hygiene:** Regular reviews of inactive accounts and automated deprovisioning (linking HR offboarding to IT workflows) help protect "dormant identities" from misuse [22], [94].
- **Transparent communication:** Providers should clearly set out in their terms of service what happens to accounts, subscriptions, and licenses in the event of death, and explicitly highlight clauses relating to inheritable rights. Simplified access for heirs, for example by accepting digital proof instead of requiring original documents by mail, would reduce administrative burden for both parties [3], [216].

European solutions

Europe is developing groundbreaking approaches to legally sound digital estate regulation. The eIDAS 2.0 Regulation establishes the framework for self-sovereign identity (SSI), which is expected to lead to the rollout of European Digital Identity Wallets (EUDI Wallets) by 2026/2027 [120], [39]. This system enables "smart successions": through mechanisms such as a "dead man's switch" (a type of digital emergency trigger), digital keys can be automatically and securely transferred in encrypted form to heirs upon verified proof of death [6], [114]. These solutions may be complemented by regulatory frameworks such as the European Law Institute's Model Rules on data access [125] or the French model, which already provides a statutory right to "digital death" [79].

A range of European providers offer practical solutions for digital estate management (selected examples):

- **Platforms:** The German service Userwill supports structured estate management (e.g., account deletion and subscription cancellation). Similar services are offered by memoresa and ex medio.
- **Technical vaults:** SecureSafe (Switzerland) provides a highly secure infrastructure for storing passwords and documents. Its integrated inheritance feature allows information to be automatically released to beneficiaries after a configurable lock period.

- **Specialized services:** Digital Life Legacy (Netherlands) provides support for accessing the data of deceased individuals, while Inheriti (Belgium) focuses on decentralized inheritance information.

Lifelong management

Digital estates require lifelong identity management that extends beyond death. Without clear instructions, heirs face complex hurdles and the risk of identity theft. Therefore, individuals and tech companies both have a responsibility to establish binding standards for privacy and access.

Early planning is an act of precaution and care. It protects an individual's digital presence from being misused as mere "raw data" and allows them to actively shape their narrative as a dignified record of their existence, rather than ceding control to faceless algorithms.

APPENDIX

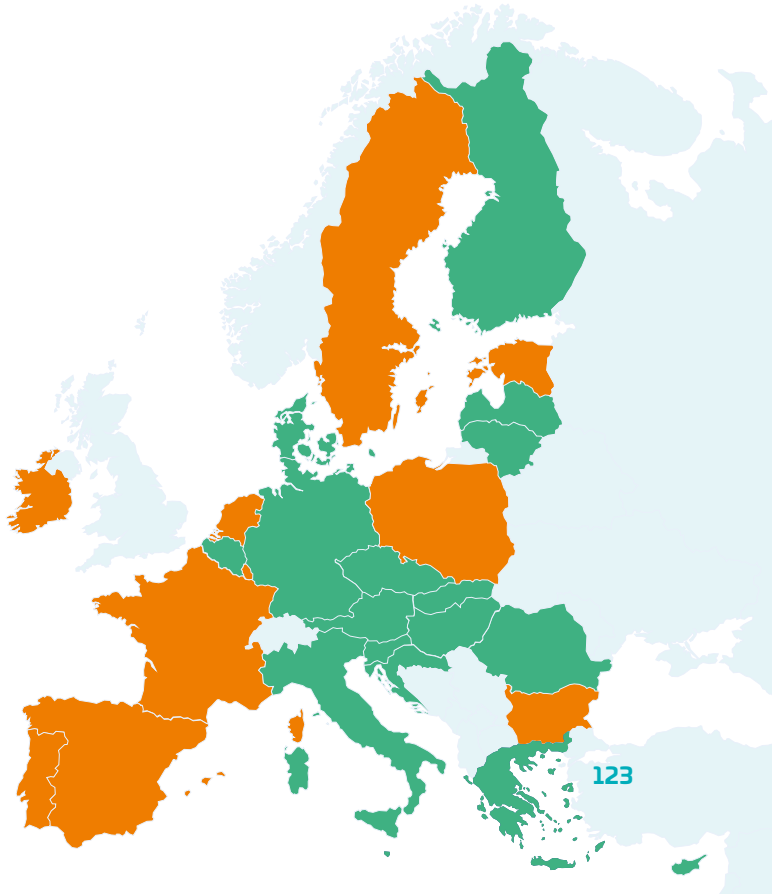
NIS 2 – STATE OF PLAY

THE NIS 2 DIRECTIVE

Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS 2) constitutes a comprehensive revision of the EU's network and information security requirements aimed at countering the growing number of cyber threats to critical infrastructure [99], [121]. This revision is based on a clause in the 2016 NIS 1 Directive requiring the European Commission to review the effectiveness of NIS 1 by 2021 [98]. Originally planned as a routine update, the huge increase in ransomware attacks and the acceleration of digital transformation in the wake of the pandemic prompted a major regulatory overhaul, which officially came into force in January 2023 [121].

Compared with its predecessor, NIS 2 marks a significant step change in both the depth and breadth of the regulation. NIS 1 identified and addressed seven sectors as critical infrastructure (CI), while also allowing member states considerable leeway in determining which companies the regulation covered [98]. In contrast, the new Directive applies a size cap approach. This means that companies no longer need to be classified as critical individually but automatically fall within the scope of the Directive if they operate in one of the 18 established EU-wide sectors, and have at least 50 employees or annual turnover of €10 million or more [99].

Organizations designated as CI are of particular importance to state and society. Their failure or interruption would result in long-term supply shortages, significant disruptions to public safety, or other dramatic consequences [51]. The NIS 2 Directive distinguishes between two main CI categories, each of which has a direct impact on the intensity of state supervision and the severity of fines. A distinction is made between essential and important organizations. Under German law, KRITIS (CI) operators are automatically considered "essential entities" and are thus subject to proactive supervision by the Federal Office for Information Security (BSI). The Directive establishes an EU-wide framework of sanctions. In the event of violations of the Directive, essential facilities face fines of up to €10 million or 2 percent of their global turnover, while important entities face sanctions of up to €7 million or 1.4 percent of revenue [121]. Furthermore, Article 21 of the Directive defines a list of mandatory risk management measures (e.g., backup concepts, supply chain security) and introduces stricter personal liability for management [99].



Source: [267]

Figure 33: Status of implementation in EU countries – early February 2026

Implementation progress across the EU

Even though the official deadline for implementation into national law expired on October 17, 2024, progress has been uneven across the EU. By November 2024, only four member states had fully implemented the Directive, prompting the European Commission to launch infringement proceedings against 23 countries [118]. As of February 2026, 17 member states, including Germany, Belgium, Croatia, Italy, and Slovakia, have passed national laws. In ten other states, including France and Estonia, draft bills are still in the process of being passed, with delays often due to political developments [267].

IMPLEMENTATION IN GERMANY: THE NIS 2 IMPLEMENTATION ACT

In Germany, the NIS 2 Directive was transposed into national law through the "Act Implementing the NIS 2 Directive and Regulating Essential Features of Information Security Management in the Federal Administration" (NIS2UmsuCG) [160]. As an umbrella act, it represents a comprehensive modernization of German IT security law. NIS 2 contains "articles" that in turn amend existing laws, such as the "Act on the Federal Office for Information Security and on Information Security in Institutions" (BSI Act – BSIG).

Whether a company is subject to this legislation under German law depends on three factors [160]:

- **Sector affiliation:** The company operates in a critical sector (e.g., energy, health, or transport).
- **Size:** It employs at least 50 people or has annual turnover exceeding €10 million.
- **Special cases:** Regardless of size, certain providers always fall within the scope of the law because their services are classified as systemically essential.

Estimates suggest that over 41,000 companies will be impacted in Germany alone [115].

Key obligations and requirements

In Germany, organizations falling within the scope of the NIS 2 Directive as "essential" or "important" entities are required by law to register online on a BSI portal. This involves providing master data on the company, contact persons for IT security incidents, and classification of the organization into the relevant sectors and subsectors. The aim is to enable the BSI to immediately warn and support the companies concerned in the event of large-scale cyberattacks or critical vulnerabilities [160].

Risk management measures pursuant to Section 30 BSIG

Companies are required to implement appropriate technical and organizational measures in line with the "state of the art." The legislator explicitly lists the following [159]:

- Concepts for risk analysis and information security
- Incident management
- Maintaining operations (business continuity management), e.g., through backups and contingency plans
- Security in the supply chain (verification of suppliers)
- Training and awareness measures
- Cryptography and encryption
- Multi-factor authentication (MFA) used as standard method of access

Heightened reporting requirements pursuant to Section 32 BSIG

In the event of serious security incidents, a strict timeline applies [159]:

- **24 hours:** Initial report (early warning) after becoming aware of the incident.
- **72 hours:** Incident notification, including comprehensive assessment of the incident.
- **30 days:** Final report with detailed root cause analysis.

Role of senior management and legal liability

One of the key elements contained in the German implementation law concerns the direct responsibility of executive management. It is no longer possible for managing directors and board members to delegate responsibility for cybersecurity to the IT department. If senior management culpably violates its duties (intentionally or through negligence), executives are held personally liable to the organization for any resulting damage (Section 38 (2) BSIG).

The key obligations for senior management are:

- **Approving and facilitating implementation:** Senior management is obligated to implement risk management measures (in accordance with Section 30 BSIG).
- **Oversight of implementation:** It must continuously monitor the implementation of these measures.
- **Training requirement:** Every member of the management is legally obliged to participate in regular risk management training (Section 38 (3) BSIG) [159].

Cybersecurity Act 2 (CSA2): Increased focus on certification and sovereignty

Since the NIS 2 Directive came into force on January 16, 2023, the threat posed by ransomware, state-sponsored espionage, and hybrid attacks has continued to escalate. While NIS 2 compels companies to protect themselves, it was often unclear which technical products were secure enough for this purpose. To close this gap, the European Commission presented the draft Cybersecurity Act 2 (CSA2) on January 20, 2026 [122].

Although the original Cybersecurity Act of 2019 (Regulation EU 2019/881) provided the theoretical framework for EU-wide security certificates, in practice it often failed due to the voluntary nature of the measures [290]. This became particularly clear in connection with the EUCS (European Cybersecurity Certification Scheme for Cloud Services). This uniform security level for cloud services was blocked for years by debates over "sovereignty requirements", specifically regarding how European data could be protected from access by foreign authorities.

The CSA2 draft bill resolves years of deadlock on the issue of certification by introducing a strict distinction between security criteria related to technology and considerations pertaining to geopolitics [122]:

- **Technology:** The European Cloud Certification Scheme (EUCS) will be finalized under CSA2 as a purely technical certification.
- **Geopolitics:** A separate mechanism will be introduced for assessing high-risk providers in the supply chain – for instance, the trustworthiness of manufacturers from non-EU countries.

The most important changes in CSA2

A key aspect of the reform is the shift from voluntary toward mandatory compliance. The EU Commission now has the power to require mandatory certification for critical information and communication technology (ICT components). This provides tangible benefits and enables clear repercussions for businesses [122]:

- **Presumption of conformity:** By using certified products, organizations automatically demonstrate to supervisory authorities that they fulfil the strict risk management requirements of the NIS 2 Directive.
- **Harmonization:** CSA2 adopts key definitions (such as those relating to security incidents or network systems) directly from NIS 2. This is in line with the REFIT program (the EU program to ensure the efficiency and benefit of legislation) and aims to simplify implementation for companies.
- **Draconian sanctions:** In the event of violations of the new supply chain security requirements, the draft increases the maximum fine to up to 7 percent of global annual turnover.

ENISA ensures operational effectiveness

ENISA (the European Union Agency for Cybersecurity) is being expanded further in its role as the "control center" for European cyber protection. It provides operational support to member states and is responsible for coordination activities [122]:

- **Setting up crisis teams:** It supports the establishment of CSIRTs (Computer Security Incident Response Teams), government task forces for responding to IT security incidents.
- **Centralized databases:** It maintains a European vulnerability database and provides the secretariat for the EU-CyCLONe crisis network (the cooperative network for European cyber crisis organizations).
- **European Cyber Shield:** Accompanying this is a network of AI-powered security centers, known as security operations centers (SOCs), which are tasked with detecting threats across the EU in real time.

Digital Omnibus Package

In November 2025, the European Commission presented the Digital Omnibus Package (COM(2025) 837) of amendments to clarify the overlaps between various EU laws such as NIS 2, GDPR, AI Act, and DORA [119].

A cornerstone of the cybersecurity reforms is the proposed "report once, share many" principle. In future, companies will be required to report cyber incidents centrally via a single entry point (SEP) at ENISA, rather than having to inform various authorities individually. This could save an estimated €5 billion in administrative costs [119]. When using the SEP, the GDPR reporting deadlines are set to be extended from 72 to 96 hours and the threshold for reporting obligations raised to apply only to "high-risk" cases, in a bid to curb a flood of insignificant reports [119].

Small and medium-sized enterprises are especially looking forward to some relief due to the planned introduction of the "small mid-cap" (SMC) category, which covers companies with up to 750 employees. Under NIS 2, these companies will only be subject to reactive supervision in future, significantly reducing the compliance burden for around 22,500 companies across Europe [119].

MANDATORY REQUIREMENTS FOR BUSINESSES (AS OF MARCH 2026)

The year 2026 marks a peak in terms of regulatory burden. That said, the underlying hope is that this short-term burden will lead to a resilient digital market in the EU over the long term, providing a competitive advantage around the globe based on trust and security.

Action needs to be taken in the following areas:

1. **Ensuring registration compliance:** Institutions are required to register on the BSI portal no later than three months from the date they first become subject to NIS 2 or after becoming subject to it again.

2. **Supply chain check:** Keeping an inventory of critical hardware and software is essential. Under CSA2, suppliers are now assessed separately for geopolitical risks, which may lead to the exclusion of certain manufacturers.

3. **Liability of senior management:** Company directors are now required to document their fulfilment of statutory training obligations in order to minimize the risk of personal liability.

4. **Adapting processes:** Internal reporting channels must be converted to Standard European Formats (based on standard essential patents – SEP).

ABOUT THE SCHWARZ GROUP AND SCHWARZ DIGITS

The Schwarz Group is an international leader in retail trade with around 14,200 stores and 595,000 employees. In the 2024 fiscal year, the companies comprising the Schwarz Group generated revenue of roughly 175.4 billion euros. The Schwarz Group's unique ecosystem covers the full value cycle, from production and retail to recycling and digitalization. The enterprise creates solutions to make the lives of billions of people safer, healthier and more sustainable, both now and for the future – The Schwarz Group acts ahead.

Lidl and Kaufland represent the group's food retail pillars and are an integral part of everyday life for customers in 32 countries. A large number of their own-brand products and sustainable packaging come directly from Schwarz Produktion. Through its recycling management solutions, environmental services provider PreZero facilitates an effective circular economy, thereby 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 Schwarz Group companies with all matters related to administration, HR, and operational activities. With this commitment top of mind, Schwarz Digits provides the IT infrastructure and services for the extensive ecosystem of companies within the Schwarz Group and continues to develop these solutions in a future-proof manner. Schwarz Digits' sovereign core services include cloud, cyber security, data and AI, communication, and workspace. Schwarz Digits ensures optimal conditions for the development of trend-setting innovations for end customers, companies and public sector organizations.

Follow the butterfly

The Schwarz Digits butterfly symbolizes our ultimate mission: digital transformation. In our podcast *Tech, KI & Schmetterlinge* (Tech, AI & Butterflies), we decode how technology is changing our world.

Take a deeper dive into our digital universe on schwarz-digits.de:

- **Buzz:** Tech insights with VIP guests on our podcast.
- **Expertise:** Exclusive white papers on digital sovereignty.
- **Security:** All cybersecurity reports and current survey results at a glance.

DEFINITIONS & ABBREVIATIONS

GLOSSARY OF DEFINITIONS

Advanced persistent threat (APT)	Cyberattacks designed for the long term, usually carried out by state actors or their affiliates. Rather than rapid destruction, adversaries aim to achieve sustained, covert access to information, systems, or decision-making processes.
Adversary-in-the-Middle (AiTM)	An attack method in which attackers secretly interpose themselves in the login process. They can then take over not only passwords but also active sessions – even if multi-factor authentication is employed.
API tokens	Digital keys that allow applications automatic access to systems. Their compromise is particularly critical, as they often unlock wide-ranging privileges.
Business email compromise (BEC)	A type of fraud in which attackers impersonate executives, business partners, or service providers to deceive victims into making payments or disclosing sensitive information.
Common vulnerabilities and exposure (CVE)	A system for identifying and providing a unique designation for known security vulnerabilities in software. Administered by an independent organization.
Credential stuffing	An automated attack in which stolen login credentials are systematically tested on a large number of services. This approach is successful because the same passwords are often recycled.
Cyber resilience	The ability of an organization to prevent, manage, and quickly recover from cyberattacks – technically, organizationally, and strategically.
DevSecOps	A portmanteau of "Development," "Security," and "Operations", DevSecOps is an approach that prioritizes security early in the development process by integrating security measures into the workflows of developers and IT operations teams.
Exploit	The technical mechanism used to exploit a vulnerability. Many attacks are able to leverage known exploits because countermeasures have not been implemented quickly enough.
Identity and access management (IAM)	All processes and systems used to manage user accounts, roles, and access rights. This has become a core security discipline.
Initial access broker	Criminal actors who sell compromised credentials. They serve as a key link between data theft and ransomware actors.
Managed service provider (MSP)	External IT service providers that operate systems for many clients. Due to their privileged access, they are attractive targets for adversaries.
Multi-factor authentication (MFA)	Users log in to accounts utilizing multiple factors (e.g., password plus code), which enhances security.
Passkey	Passwordless authentication method, based on cryptographic keys. It reduces the risk of phishing and password theft. It is considered to be the future standard for accessing privileged accounts.
Passwort spraying	An attack in which a frequently used password is speculatively tested on a large number of accounts.
Patch management	Structured process for identifying, testing, deploying, and monitoring software updates (patches) for operating systems and applications to resolve known vulnerabilities.
Phishing	An attack using deception to trick users into revealing their login credentials. The use of AI has led to these attacks becoming increasingly convincing and highly targeted.

Prompt injection	An attack on AI language models, in which manipulated input commands are utilized to bypass security mechanisms in order to execute malicious commands.
Ransomware	Software that locks systems and/or steals data in order to extort money from victims.
Ransomware-as-a-Service (RaaS)	A platform model in which various actors collaborate to carry out ransomware campaigns – not unlike a franchise system.
Security operations center (SOC)	Functional unit within an organization which monitors IT security events and responds to security incidents.
Shadow IT	Unauthorized use of IT or cloud services by functional units or departments. Poses increased risks as security controls are bypassed.
Single Sign-on (SSO)	Authentication method which allows users to gain access to multiple applications and websites using a single set of login credentials.
Session hijacking	An attack in which active login sessions are hijacked, for example by intercepting access tokens. This permits attackers to circumvent security mechanisms such as MFA.
Social engineering	Taking advantage of human "weaknesses" such as fear, curiosity, or obedience to trick users into revealing sensitive information, bypassing security measures, or installing malicious software.

LIST OF ABBREVIATIONS

ANN	Artificial neural network
ANSSI	French National Agency for the Security of Information Systems
API	Application programming interface
APT	Advanced persistent threat
BDSG	German Federal Data Protection Act
BKA	German Federal Criminal Police Office
BMF	German Federal Ministry of Finance
BMDS	German Federal Ministry for Digital Transformation and Government Modernisation
BRAK	German Federal Bar
BSI	German Federal Office for Information Security
C5	BSI Cloud Computing Compliance Criteria Catalogue
CADA	Cloud and AI Development Act
CATI	Computer assisted telephone interview
CI	Critical infrastructure organizations
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CISPE	Cloud Infrastructure Service Providers in Europe
CLOUD Act	US Clarifying Lawful Overseas Use of Data Act
CPU	Central processing unit
CRA	Cyber Resilience Act
DARPA	Defense Advanced Research Projects Agency
DDoS	Distributed Denial-of-Service
DG DIGIT	Directorate-General for Digital Services of the European Commission
DORA	EU Digital Operational Resilience Act
DPO	Data Protection Officer
DsiN	Deutschland sicher im Netz e. V. (Germany Safe on the Internet)
ENISA	European Network and Information Security Agency
FLOP	False load output prediction
GAI	Generative AI
GDPR	General Data Protection Regulation
GRC	Governance, risk management, and compliance
IaaS	Infrastructure-as-a-Service
IAM	Identity and access management
IO	Information operations
IoT	Internet of Things
IR	Incident response
LLM	Large language model
MFA	Multi-factor authentication
MSP	Managed service provider
MSS	Managed security services
NIS	Network and Information Security Directive
NIST	National Institute of Standards and Technology
OSS	Open Source Software
OT	Operational technology
PaaS	Platform-as-a-Service
RaaS	Ransomware-as-a-Service
SaaS	Software-as-a-Service
SBOM	Software bill of materials
SEAL	Sovereignty Effective Assurance Level
SOC	Security operations center
SSI	Self-sovereign identity
STR	Short tandem repeats
TFLOPS	TeraFLOPS
US$	US dollar
VPN	Virtual private network
WEF	World Economic Forum
WAF	Web application firewall
ZenDiS	German Center for Digital Sovereignty of Public Administration
ZITiS	German Central Office for Information Technology in the Security Sector

REFERENCES

[1] Acome, E. et al. (2018) Hydraulically amplified self-healing electrostatic actuators with muscle-like performance, Science, 359(6371), pp. 61-65.

[2] AliAkbarpour, H. et al. (2024) Emerging Trends and Applications of Neuromorphic Dynamic Vision Sensors: A Survey, IEEE Sensors Reviews, vol. 1, pp. 14-63.

[3] Allianz (2026) Den digitalen Nachlass regeln: Das Wichtigste in Kürze.

[4] Allianz (2026) Risk Barometer.

[5] Alto Intelligence (2026) From European Airspace to Venezuela: Pink Slime Media and Pre-Positioned Narrative Infrastructure.

[6] Ammicht, Q. et al. (2024) Ethik, Recht und Sicherheit des digitalen Weiterlebens. Forschungsergebnisse und Gestaltungsvorschläge zum Umgang mit Avataren und Chatbots von Verstorbenen.

[7] Anti-Phishing Working Group, Inc (2025) Phishing Activity Trends Report 2nd Quarter 2025.

[8] ArmyInform (2026) Record ePoints: Ukrainian drone operators eliminated over 33,000 Russians in a month.

[9] Asimov, I. (1942) Runaround, Astounding Science Fiction, March. New York: Street & Smith.

[10] ATHENE Cybernation Deutschland (2025) Sicherheit der IT der Länder.

[11] ATHENE Cybernation Deutschland (2025) Sicherheit der IT der Universitäten.

[12] Bai, Y. et al. (2025) Swarm navigation of cyborg-insects in unknown obstructed soft terrain, Nat Commun 16, 221.

[13] Baker, S. (2025) Ukrainian robotics company says autonomy in defense is overhyped – but it's also past the point of no return, Business Insider.

[14] Barlow, J. P. (1996) Declaration of Independence for Cyberspace.

[15] Bartelson, J. (1995) A genealogy of sovereignty (Vol. 39) Cambridge University Press.

[16] Baums, A. & Kilian, M. (2025) Better Stack (Part 1): 10 Theses to Demystify the Debate on Digital Sovereignty and the Euro Stack. GovTech Intelligence Hub.

[17] BBC (2020) Kanye West gives Kim Kardashian birthday hologram of dead father.

[18] BCG (2025) Europe's Race to Tech Readiness.

[19] Belli, L. & Jiang, M. (2024) Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press.

[20] Bergtora Sandvik, K. (2020) Digital Dead Body Management: Time to Think it Through. Journal of Human Rights Practice, 12(2020), 428-443.

[21] BfV (2026) Cyberangriffe. Gefahren, Risiken und Schutz vor staatlich gesteuerten Attacken.

[22] Biersdorfer, J. D. (2025) How to Prepare for Your Digital Afterlife.

[23] Biget, S. (2026) Why China is testing humanoid robots at its Vietnam border now.

[24] Bitkom (2025) Cyberkriminalität – Bevölkerungsumfrage zu Wahrnehmung, Erfahrungen und Schutzverhalten.

[25] Bitkom (2025) Digitales Erbe: Was passiert mit Online-Zugängen nach dem Tod?

[26] Bitkom (2025) Europas Weg in die digitale Souveränität.

[27] Bitkom (2026) Digitalwirtschaft bleibt Stabilitätsanker: 245 Milliarden Euro Umsatz in 2026.

[28] Bitkom (2025) Wirtschaftsschutz 2025.

[29] Bitkom (2025) Wirtschaft setzt verstärkt auf Cloud – Forderungen nach europäischen Anbietern nehmen zu.

[30] Bitdefender (2024) 2024 Consumer Cybersecurity Assessment Report.

[31] BKA (2025) Bundeslagebild Cybercrime 2024.

[32] BKA (2025) Darknet-Handelsplattform „Archetyp Market“ abgeschaltet.

[33] BKA (2025) Endgame 2.0: Weitere 20 Haftbefehle in der bislang weltweit größten Cyber-Polizeioperation.

[34] BKA (2025) International abgestimmtes Vorgehen gegen die hacktivistische Gruppierung „NoName057(16)“.

[35] BKA (2025) Strafverfolgungsbehörden schalten die zwei weltweit größten Cybercrime-Foren mit rund zehn Millionen registrierten Nutzern ab.

[36] Blair-Frasier (2025) The 2025 Security Benchmark Report.

[37] BMDS (2025) Deutschland-Stack.

[38] BMDS (2025) Gipfel zur Europäischen Digitalen Souveränität.

[39] BMDS (2026) Bund startet Sandbox für EUDI-Wallet.

[40] BMF (2024) Entwurf zum Bundeshaushaltsplan 2024 Einzelplan 14.

[41] BNP Media (2025) The Security Benchmark Report.

[42] Bologna, C. (2025) This Sneaky Spending Habit Might Cost You More Money Than You Think.

[43] BRAK (2025) Digitale Nachlassermittlung: BRAK fordert strengere Datenschutzregeln.

[44] Brave1 (2026) Defense Tech Cluster Market.

[45] Brewster, T. (2026) Microsoft Gave FBI Keys To Unlock Encrypted Data, Exposing Major Privacy Flaw, Forbes.

[46] Bria, F., Timmers, P., & Gernone, F. (2025) EuroStack – A European alternative for digital sovereignty. EuroStack.

[47] BSI (2019) BSI – Kriterienkatalog C5.

[48] BSI (2025) Befragung zur Cybersicherheit.

[49] BSI (2025) Die Lage der IT-Sicherheit in Deutschland 2025.

[50] BSI (2025) Entscheidungsbaum der NIS-2-Betroffenheitsprüfung des BSI.

[51] BSI (2025) Kritische Infrastrukturen (KRITIS).

[52] BSI (2025) KRITIS in Zahlen.

[53] Buchholz, L. (2025) Digitale Souveränität in Deutschland: Eine Analyse der Cloud-Angebote von Superscalern und Hyperscalern für Behörden, focus on IT.

[54] Calderaro, A. & Blumfelde, S. (2022) Artificial intelligence and EU security: the false promise of digital sovereignty. European Security.

[55] Cao, L. (2024) Humanoid Robots and Humanoid AI: Review, Perspectives and Directions, arXiv preprint arXiv:2405.15775.

[56] CDU, CSU und SPD (2025) Verantwortung für Deutschland. Koalitionsvertrag zwischen CDU, CSU und SPD.

[57] Chander, A. & Sun, H. (Eds.) (2023) Data sovereignty: From the digital silk road to the return of the state. Oxford University Press.

[58] Chang, E. et al. (2024) Bird-inspired reflexive morphing enables rudderless flight, Sci. Robot.9, eado4535(2024).

[59] Check Point (2025) 40,000 phishing emails disguised as SharePoint and e-signing services: A new wave of finance-themed scams.

[60] Check Point (2025) AI 2030: The coming era of autonomous cyber crime.

[61] Check Point (2025) Check Point Blog.

[62] Check Point (2025) Global cyber attacks increase in November 2025 driven by ransomware surge and GenAI risks.

[63] Check Point (2025) Global cyber threats September 2025: Attack volumes ease slightly but GenAI risks intensify as ransomware surges.

[64] Check Point (2025) Latin America 2025 Mid-Year Cyber Snapshot Reveals 39% Surge in Attacks as AI Threats Escalate Regional Risk.

[65] Check Point (2025) Microsoft dominates phishing impersonations in Q3 2025.

[66] Check Point (2025) Phishing campaign leverages trusted Google Cloud automation capabilities to evade detection.

[67] Check Point (2025) The rise of AI-powered threats and other mobile risks highlight why it's time to rethink your security architecture.

[68] Check Point (2025) The State of Cyber Security 2025.

[69] Check Point (2025) The state of ransomware in Q3 2025.

[70] CISA (2025) CISA, NSA and Cyber Centre Warn Critical Infrastructure of BRICKSTORM Malware Used by People's Republic of China State-Sponsored Actors.

[71] CISA (2025) CISA Unveils Guide to Combat Bulletproof Hosting Cybercrime.

[72] CISA (2025) Forging National Resilience for an Era of Disruption.

[73] CISA (2025) FY2025-2026 CISA International Strategic Plan.

[74] CISA (2025) Key Cyber Initiatives from CISA: KEV Catalog, CPGs, and PRNI.

[75] CISA (2025) News.

[76] CISA (2025) United in Cyber Defense: A Model for Operational Collaboration.

[77] CISPE (2025) CISPE Cloud Catalogue.

[78] CISPE (2025) No Such Thing as "75% Sovereign".

[79] CNIL (2025) Our Data After Us. From Digital Death to Immortality, Uses and Issues of Post Mortem Data. IP Report N°10, Innovation & Foresight Division.

[80] Couture, S. & Toupin, S. (2019) What does the notion of "sovereignty" mean when referring to the digital? New media & society, 21(10).

[81] Corralero Medina, L. (2025) The Digital Afterlife: Ethical implications of memorial accounts on socio-technological platforms.

[82] CSO Online (2025) Cyberangriff auf Arla Deutschland.

[83] CSO Online (2025) Diese Unternehmen hat es schon erwischt.

[84] CSO Online (2025) Vodafone von Hackerangriff auf Dienstleister betroffen.

[85] Cyber Monitoring Centre (2025) Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025.

[86] CyberProof (2025) 2025 Global Threat Intelligence Report 2025 – Mapping Threats and Trends.

[87] CyberProof (2025) Mid-Year Cyber Threat Landscape Report – H1 2025 Analysis August 2025.

[88] Cyfirma (2026) Tracking Ransomware Dec 2025.

[89] Cziesla, F. (2022) Von der Biopolitik zur Nekro-Ökonomie. Für eine genealogische Kritik der politischen Ökonomie des Todes. Bielefeld: transcript.

[90] Dachwitz, I. & Meineck, S. (2025) New data set reveals 40,000 behind location tracking.

[91] Daily News Egypt (2025) Egypt's ICT minister stresses need for Arab cooperation on cyber threats.

[92] Danby, P. (2022) Human brain cells in a dish learn to play Pong, UCL News.

[93] DARPA (2025) DARPA program sets distance record for power beaming.

[94] Del Valle, I. (2025) AI After Death: Digital Identity, Neural Echoes, and Post-Mortem Decision Rights.

[95] Deutsche Verwaltungscloud (2025) Reifegradmodell.

[96] Digital SME Alliance (2025) New Tech Sovereignty Catalogue Announced to Map Europe's Digital Potential.

[97] Diletta, D. M. et al. (2025) Open but Not Powerless: Towards a Common Understanding of EU Digital Sovereignty, EU Joint Research Center, European Commission.

[98] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[99] 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[100] Doaré, R. et al. (2014) Robotson the Battlefield: Contemporary Issues and Implications for the Future. Fort Leavenworth, KS: Combat Studies Institute Press.

[101] Dorrmann, L. et al. (2021) Kompendium: Li-Ionen-Batterien, VDE.

[102] Draghi Bericht (2024) Die Zukunft der europäischen Wettbewerbsfähigkeit, Teil A.

[103] Dressler, N. (2026) Neues BSI-Protal startet: Vorstände haften persönlich für IT-Sicherheit.

[104] DsiN (2025) Deutschland im Fokus von Cyberangriffen: Höchste Angriffszahlen in der EU.

[105] DsiN (2025) DsiN Sicherheitsindex 2025.

[106] DsiN (2025) Pressemitteilungen.

[107] Du, J. et al. (2024) Global Automation Humanoid Robot: The AI accelerant. Goldman Sachs.

[108] Eiben, A. & Smith, J. (2015) From evolutionary computation to the evolution of things, Nature 521, 476–482.

[109] Elias, J. (2026) Exaggeration per record.

[110] EngineAI Official Website (2025).

[111] ENISA (2025) ENISA Threat Landscape 2025.

[112] ENISA (2025) NIS Investments 2025.

[113] Etienne-Cummings, R. & Van der Spiegel, J. (1996) Neuromorphic vision sensors, Sensors and Actuators A: Physical, 56(1-2), pp. 19-29.

[114] European Commission (o. J.) Verifiable Credentials Framework.

[115] European Commission (2020) Commission Staff Working Document.

[116] Europäische Kommission (2025) Cyberresilienzgesetz.

[117] Europäische Kommission (2025) International Criminal Court switches to open source with openDesk.

[118] Europäische Kommission (2025) Vertragsverletzungsverfahren: Kommission leitet in vier Fällen rechtliche Schritte gegen Deutschland ein.

[119] Europäische Kommission (2026) Ein agiles digitales Regelwerk für die EU.

[120] Europäische Kommission (2026) Europäische digitale Identität.

[121] Europäische Kommission (2026) NIS2-Richtlinie: Sicherung von Netz- und Informationssystemen.

[122] Europäische Kommission (2026) Vorschlag für eine Verordnung zum EU-Rechtsakt zur Cybersicherheit.

[123] Europäische Kommission DG DIGIT (2025) Cloud Sovereignty Framework. Europäische Kommission. Seiten 1-6. Brüssel, Belgien.

[124] Europäischer Rat, Rat der Europäischen Union (2026) Cybersicherheit in der EU: Strategie und wichtigste Maßnahmen.

[125] European Law Institute (2025) ELI Guiding Principles and Model Rules on Digital Assistants for Consumer Contracts.

[126] European Parliament (2024) Public Procurement Act. In "A new plan for Europe's sustainable prosperity and competitiveness", Legislative Train Schedule.

[127] European Parliamentary Research Service (2025) Cloud and AI Development Act.

[128] Europol (2025) Europol and partners shut down "Cryptomixer".

[129] Europol (2025) Global operation targets NoName057(16) pro-Russian cybercrime network.

[130] Europol (2025) Internet Organised Crime Threat Assessment, IOCTA 2025.

[131] Europol (2025) Key figure behind major Russian-speaking cybercrime forum targeted in Ukraine.

[132] Europol (2025) Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown.

[133] Europol (2025) Newsroom.

[134] EuroStack Industry Alliance (2025) Regulation of Strategic Digital Procurement.

[135] EY (2025) Datenklaustudie 2025. Virtuelle Gefahr – realer Schaden.

[136] Federal Trade Commission (2025) Data Book 2024.

[137] Figure AI (2025) F.02 Contributed to the Production of 30,000 Cars at BMW.

[138] FinalSpark (2024) Biocomputing.

[139] Flashpoint (2025) Flashpoint 2025 Global Threat Intelligence Report.

[140] Flashpoint (2025) Flashpoint's Global Threat Intelligence Index: 2025 Midyear Edition.

[141] Floridi, L. (2016) On human dignity as a foundation for the right to privacy. Philos Technol 29:307–312.

[142] Floridi, L. (2020) The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. Philosophy & Technology.

[143] Förster, M. (2025) Microsofts Souveränitäts-Debakel: Zwischen „blumiger Werbung" und „keine Panik". heise.

[144] Förster, M. (2025) Scharfe Kritik am EU-Rahmenwerk für Cloud-Souveränität.

[145] Forbes (2025) Billions Of Passwords Have Leaked — Hack Attacks Are Ongoing, Act Now.

[146] Fortinet (2025) Bericht zum Stand der Betriebstechnologie (OT) und Cybersecurity 2025.

[147] Fortinet (2025) CISO Predictions 2026.

[148] Fortinet (2025) Data Security Report 2025.

[149] Fortinet (2025) Global Threat Landscape Report 2025.

[150] Fortinet (2025) Insider Risk Report 2025.

[151] Fox, P., Schnitzer, M. & Privitera, D. (2025) KI-Rechenzentren in Deutschland. Aktuelle Kapazität, künftiger Bedarf. KIRA Center.

[152] Francis, J. (2025) The Hidden Dangers of Forgotten Accounts.

[153] Fraunhofer (2025) Berührungsloses Patientenmonitoring: EKG per Radar. Press Release, May 2025.

[154] Fraunhofer IPA (2019) If Machines Could Smell ...

[155] Fraunhofer ISS (2026) Neuromorphes Computing.

[156] Friedman, C. R. et al. (2025) Leveraging a Strategic Public-Private Partnership to Launch an Airport-Based Pathogen Monitoring Program to Detect Emerging Health Threats, Emerg Infect Dis. 2025 May; 31(13):35-38.

[157] Gao Y. et al. (2025) A neuromorphic robotic electronic skin with active pain and injury perception, Proc. Natl. Acad. Sci. U.S.A. 122 (52) e2520922122.

[158] G DATA Cyberdefense (2025) Cybersicherheit in Zahlen.

[159] Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSI-Gesetz – BSIG).

[160] Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung.

[161] Gineikyte-Kanclere, V., Eggert, M. & Skiotyte, G. (2025) European Software and Cyber Dependencies, Study Requested by the ITRE Committee, European Parliament.

[162] Glasze, G. et al (2023) Contested spatialities of digital sovereignty, Geopolitics.

[163] Google Threat Intelligence Group (2025): APT24's Pivot to Multi-Vector Attacks.

[164] Google Threat Intelligence Group (2025) GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools.

[165] Gravert, S. D. et al. (2024) Low-voltage electrohydraulic actuators for untethered robotics, Sci Adv. 2024 Jan 5;10(1):eadi9319.

[166] Group-IB (2025) Trends in der High-Tech Kriminalität 2025.

[167] Hamerly, R. et al. (2019) Large-Scale Optical Neural Networks Based on Photoelectric Multiplication, Physical Review X, 9(2), 021032.

[168] Hanamsagar, A. et al. (2018) Leveraging Semantic Transformation to Investigate Password Habits and Their Causes.

[169] Hardman, D. et al. (2025) Multimodal information structuring with single-layer soft skins and high-density electrical impedance tomography, Sci. Robot.10,eadq2303.

[170] Hassan, A. E. et al. (2025) Agentic Software Engineering: Foundational Pillars and a Research Roadmap. arXiv preprint arXiv:2509.06216.

[171] Hawkins, Z. H., Lehdonvirta, V., & Wu, B. (2025) AI Compute Sovereignty: Infrastructure Control Across Territories, Cloud Providers, and Accelerators. Cloud Providers, and Accelerators.

[172] Heise Online (2025) Schleswig-Holstein: Fast 80 Prozent der Microsoft-Lizenzen gekündigt.

[173] Hoang, V. D. et al. (2024) Autonomous Overhead Powerline Recharging for Uninterrupted Drone Operations, 2024 IEEE International Conference on Robotics and Automation (ICRA).

[174] Hölzl, V. (2025) USA verhängen Sanktionen gegen IStGH-Chefankläger Khan. ZEIT.

[175] Hollanek, T., & Nowaczyk-Basińska, K. (2024) Griefbots, Deadbots, Postmortem Avatars: On Responsible Applications of Generative AI in the Digital Afterlife Industry. Philosophy & Technology, 37(63).

[176] Hornetsecurity (2025) Cybersecurity Report 2025.

[177] Hornetsecurity (2025) Monthly Threat Reports 2025.

[178] Hornetsecurity (2025) Monthly Threat Report Mai 2025.

[179] Hornetsecurity (2025) Monthly Threat Report Juni 2025.

[180] Hornetsecurity (2025) Monthly Threat Report Juli 2025.

[181] Horneysecurity (2025) Monthly Threat Report Oktober 2025.

[182] Hornetsecurity (2025) Monthly Threat Report November 2025.

[183] Hornetsecurity (2025) Monthly Threat Report Dezember 2025.

[184] Howard, D. et al. (2019) Evolving embodied intelligence from materials to machines, Nat Mach Intell 1, 12–19.

[185] Hsu, J. (2015) Robot Funerals Reflect Our Humanity.

[186] IANS (2026) The CISO Pay Gap: Inside Cybersecurity's massive compensation divide.

[187] IBM Security (2025) Cost of a Data Breach 2025.

[188] ICSSD (2020) 4th International Conference on Science and Sustainable Development: Industry and Robotics. Conference Proceedings.

[189] Informatik.ch (2025) Gehirn auf dem Chip: Wie 800.000 Neuronen einen Computer antreiben.

[190] Inside the Rise of AI-Powered Pharmaceutical Scams.

[191] Intel 471 (2025) Cybercrime takedowns: trust, partnerships and focus.

[192] Intel 471 (2025) DanaBot malware disrupted, threat actors named.

[193] Intel 471 (2025) How initial access offers power intrusions and ransomware.

[194] Intel 471 (2025) Intel 471 Blog.

[195] Intel 471 (2025) Law enforcement hammered cybercrime in 2024. Is it working?

[196] Intel 471 (2025) "Pig-Butchering" Scams: The Dark Side of Social Engineering and Why Terminology Matters.

[197] Intel 471 (2025) UK 2025 Threat Landscape: "Rampant Cyber Crime".

[198] International Federation of Robotics (2025) Absatz von Industrierobotern nach ausgewählten Ländern weltweit in den Jahren 2023 und 2024. Statista.

[199] International Federation of Robotics (2024) Manufacturing industry-related robot density in selected regions worldwide in 2022 (in units per 10,000 employees). Statista.

[200] Interpol (2025) African authorities dismantle massive cybercrime and fraud networks, recover millions.

[201] ISACA (2025) State of Cybersecurity 2025 report.

[202] ISC2 Research (2025) 2025 ISC2 Cybersecurity Workforce Study.

[203] it-daily (2025) Analyse aktueller Cyberangriffe im Nahen Osten.

[204] Jerusalem Post (2025) China unveils "robotic wolves" leading frontline in amphibious assault exercise.

[205] Jerusalem Post (2025) "First robotics war": Defense Ministry shows how robotic systems used in Israel-Hamas War.

[206] Joint Cybersecurity Advisory (2025) Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System.

[207] Jordan, J. M. (2019) The Czech Play That Gave Us the Word Robot.

[208] Juhász, Á. (2024) Inheriting Digital Assets – A Glimpse Into the Future, Juridical Tribune – Review of Comparative and International Law 14, no. 4: 547-563.

[209] Kaloudis, M. (2021) Sovereignty in the Digital Age – How Can We Measure Digital Sovereignty and Support the EU's Action Plan? New Global Studies, 16(3).

[210] Kashchenko, M. (2025) Robot rescues Ukrainian soldier trapped 33 days behind Russian lines, navigating minefields and mortar strikes, CNBC News.

[211] Kaspersky (2024) Digital Afterlife: 61% Worry About Online Legacy of the Deceased. Press Release, Aug 21, 2024.

[212] Königssohn, K.-K. (2025) White House protection included, Mimer.

[213] Kompetenzzentrum Öffentliche IT (2017) Digitaler Nachlass.

[214] KPMG (2025) Passkeys: Sicherheit ohne Passwort.

[215] Krempl. S. (2025) Gutachten: US-Behörden haben weitreichenden Zugriff auf europäische Cloud-Daten. heise.

[216] Kubis, M. et al. (2019) Der digitale Nachlass. Eine Untersuchung aus rechtlicher und technischer Sicht.

[217] Kumar, A. et al. (2021) RMA: Rapid Motor Adaptation for Legged Robots, Preprint 2107.04034.

[218] Kunz, E. M. et al. (2025) Inner speech in motor cortex and implications for speech neuroprostheses, Cell, 188(17).

[219] Lambach, D. & Oppermann, K. (2023) Narratives of digital sovereignty in German political discourse. Governance.

[220] Larsson, O. (2025) DNA as a power tool in hybrid warfare, Swedish Defence University.

[221] LastPass (2022) Psychology of Passwords.

[222] Lee, B. et al. (2023) A principal odor map unifies diverse tasks in olfactory perception, Science381, 999-1006(2023).

[223] Li, C. et al. (2025) An overview of machine unlearning High-confidence computing.

[224] Lin, Q. et al. (2025) Cyborg insect factory: automatic assembly for insect-computer hybrid robot via vision-guided robotic arm manipulation of custom bipolar electrodes, Nat Commun 16, 6073 (2025).

[225] Li, S. et al. (2025) Advanced Brain-on-a-Chip for Wetware Computing: A Review, Advanced Science, 12, e08120.

[226] Li, Y. et al (2025) MCOD: The First Challenging Benchmark for Multispectral Camouflaged Object Detection, Proceedings of the 33rd ACM International Conference on Multimedia (MM '25).

[227] Li, Z. et al. (2025) Humanoid Locomotion and Manipulation: Current Progress and Challenges in Control, Planning, and Learning, arXiv preprint arXiv:2501.02116.

[228] Lundblad, N. (2025) Digital Sovereignty: Can Europe afford it. CEPA.

[229] Mackay, N. (2025) Germany's defense procurement crisis: it's time for strategic overhaul, CCM Institute Insights.

[230] Mahmoud, O. A. et al. (2025) Advancements and Applications of STR Kits in Forensic DNA Profiling: A Comprehensive Review, Baghdad Journal of Biochemistry and Applied Biological Sciences. 6. 1-17.

[231] Mak, C. (2023) Data After Life: The Protection of Users' Development of their Digital Identity, VerfBlog, 2023/5/24.

[232] Mandiant (2025) Adversarial Misuse of Generative AI.

[233] Mandiant (2025) BitM Up! Session Stealing in Seconds Using the Browser-in-the-Middle Technique.

[234] Mandiant (2025) Deception in Depth: PRC-Nexus Espionage Campaign Hijacks Web Traffic to Target Diplomats.

[235] Mandiant (2025) M-Trends 2025 Report.

[236] Mandiant (2025) Phishing Campaigns Targeting Higher Education Institutions.

[237] Mandiant (2025) Preparing for Threats to Come: Cybersecurity Forecast 2026.

[238] Mandiant (2025) Threat Intelligence.

[239] Mandiant (2025) What's in an ASP? Creative Phishing Attack on Prominent Academics and Critics of Russia.

[240] Marco Polo The Global AI Talent Tracker (2023).

[241] Marsh (2025) Cyber catalyst report: Guiding priorities in cyber investments.

[242] Max, K. et al. (2025) Synthetic biology meets neuromorphic computing: towards a bio-inspired olfactory perception system, Neuromorphic Computing and Engineering 5 034010.

[243] Max-Planck-Gesellschaft Synthetische Biologie und Sicherheit (2026)

[244] McNulty, D. et al. (2022) A review of Li-ion batteries for autonomous mobile robots: Perspectives and outlook for the future, Journal of Power Sources, Volume 545, 2022, 231943.

[245] Mehar, V. et al. (2025) Receiver-Side Power Control of a 200-kW Three-Phase DWPT System for Heavy-Duty Vehicles, 2025 IEEE Transportation Electrification Conference & Expo (ITEC).

[246] Merkel, A., Frederiksen, M., Marin, S. & Kallas, K. (2021) Letter to European Commission President Ursula von der Leyen.

[247] Meyer, H. (2023} Digital legacy: how to organise your online life for after you die.

[248] Microsoft (2025) Microsoft Digital Defense Report 2025.

[249] Ministerium für Kultus, Jugend und Sport Baden-Württemberg (2025) Digitaler Arbeitsplatz für Lehrkräfte wird nun mit openDesk umgesetzt.

[250] Nagy, P., & Neff, G. (2015) Imagined Affordance: Reconstructing a Keyword for Theory. Sage Journals, 1(2).

[251] Nair, V. (2025) How many Bitcoin are lost?

[252] Nansen, B. et al. (2017) Social Media in the Funeral Industry: On the Digitization of Grief, Journal of Broadcasting & Electronic Media, 61(1), pp. 73–89.

[253] Nansen, B. et al. (2019) "Death by Twitter": Understanding false death announcements on social media and the performance of platform cultural capital. First Monday, 24(12).

[254] Nansen, B. (2025) Most of us will leave behind a large digital legacy when we die.

[255] NASA (2024) OTPS SBSP Report Final.

[256] National Security Bureau. R.O.C. (2025) Analysis on China's Cyber Threats to Taiwan's Critical Infrastructure in 2025.

[257] Nextcloud (2025) Digital Sovereignty Index.

[258] Nextcloud (2025) Nextcloud enables secure, sovereign collaboration for Austria's Federal Ministry.

[259] Next:public (2025) Souveränitätsbarometer der öffentlichen IT.

[260] NIST (2025) National Vulnerability Database.

[261] NOKIA (2025) Threat Intelligence Report 2025.

[262] NordPass (2024) People have around 170 passwords on average, study shows.

[263] Öhman, C. (2024) The Afterlife of Data. What happens to your information when you die and why you should care. The University of Chicago Press, Chicago and London.

[264] Öhman, C. & Floridi, L. (2017) The Political Economy of Death in the Age of Information: A Critical Approach to the Digital Afterlife Industry. Minds & Machines 27, 639–662.

[265] Öhman, C., & Watson, D. (2021) Are the Dead Taking Over Instagram? A Follow-up to Öhman & Watson (2019). In: Cowls, J., Morley, J. (eds) The 2020 Yearbook of the Digital Ethics Lab. Digital Ethics Lab Yearbook. Springer, Cham.

[266] OpenAI (2026) GPT-5.3-Codex System Card.

[267] OpenKRITIS (2026) NIS2 in EU Countries.

[268] Open Web Application Security Project (OWASP) (2025) OWASP Attack Surface Management Top 10.

[269] Paleja, A. (2021) US Military's Active Denial System is a 95 GHz Heat Ray, Interesting Engineering.

[270] Palo Alto Networks (2025) Bedrohungsbeschreibung: Eskalation des Cyberrisikos im Zusammenhang mit dem Iran.

[271] Pandey, M., et al. (2025) Advanced Materials for Biological Field-Effect Transistors (Bio-FETs) in Precision Healthcare and Biosensing, Advanced Healthcare Materials, 14(13), 2500400.

[272] Pape, A. (2023) Ethische Herausforderungen digitaler Nachlässe. Hannover: Hochschule Hannover.

[273] Pasquale, F. (2019) From Territorial to Functional Sovereignty: The Case of Amazon, LPE.

[274] Paulus, A. (2025) Europas Cybersicherheit hängt an den USA, SWP-Aktuell 2025/A 48.

[275] Pelrine, R. et al. (2000) High-Speed Electrically Actuated Elastomers with Strain Greater Than 100%, Science, 287(5454), pp. 836-839.

[276] PEO Soldier (2019) XM157 Next Generation Squad Weapons – Fire Control, Program Executive Office Soldier.

[277] PHF Science NZ (2025) Testing plane sewage at border can help detect disease.

[278] Pilch, R. et al. (2021) Scientific Risk Assessment of Genetic Weapon Systems, CNS Occassional Paper #52 (2021).

[279] Plattner, C. & Seiller, F. (2025) Schneller zur digitalen Souveränität. Atlantik Brücke.

[280] Plattner, C. & Strubel, V. (2025) Joint Statement by ANSSI and BSI on Cloud Sovereignty Criteria.

[281] P. M. Wensing et al. (2017) Proprioceptive Actuator Design in the MIT Cheetah: Impact Mitigation and High-Bandwidth Physical Interaction for Dynamic Legged Robots, IEEE Transactions on Robotics, vol. 33, no. 3.

[282] Pohle, J. (2020) Digitale Souveränität Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa, Konrad Adenauer Stiftung.

[283] Pohle, J. & Thiel, T. (2020) Digital Sovereignty. Internet Policy Review.

[284] Prophesee.ai (2026).

[285] Ptock, J. (2020) Cybercrime: Zahlen und Statistiken für Deutschland.

[286] PwC US Group LLP (2025) 2026 Global Digital Trust Insights: C-suite playbook and findings – New world, new rules: Cybersecurity in an era of uncertainty.

[287] Qiang L. et al. (2020) A Review of Tactile Information: Perception and Action Through Touch, Trans. Rob. 36, 6 (Dec. 2020), 1619–1634.

[288] Qu, S. et al. (2025) Skynet Starter Kit: From Embodied AI Jailbreak to Remote Takeover of Humanoid Robots, 39C3.

[289] Rahman, M. M. et al. (2024) A comprehensive review of wireless power transfer methods, applications, and challenges, Engineering Reports, 6(10), e12951.

[290] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[291] Roosevelt, R. & Hodder, C. (2025) The Ultimate Guide to Planning Your Digital Estate.

[292] Rothemund, P. et al. (2020) Miniaturized Circuitry for Capacitive Self-Sensing and Closed-Loop Control of Soft Electrostatic Transducers, Soft Robotics.

[293] Rouco, A. et al. (2025) Biometric Identification via Through-Wall Radar: A Survey on Vital Signs and Gait Analysis, IEEE Access 25(13).

[294] RPTU (2025) Dänemark: Bye-bye Microsoft?

[295] Rus, D. & Tolley, M. (2015) Design, fabrication and control of soft robots, Nature. 521. 467-75.

[296] Salary.com (2025) SVP of Information Security Salary in the United States.

[297] SAP (2024) Aktionärsstruktur & Basisdaten, SAP Investor Relations.

[298] ScamWatchHQ (2025) Egypt Scams 2025: The Nile's Digital Deception – When Currency Crisis, Youth Unemployment, and Religious Trust Create a Perfect Storm for Fraud.

[299] Scharre, P. (2018) Army of None: Autonomous Weapons and the Future of War, New York: W. W. Norton & Company.

[300] Schneider, M. (2025) Mistral starts processing personal data in USA and stops notifying of such changes. Open Terms Archive.

[301] Schoder, S. (2025) Physics-Informed Neural Networks for Modal Wave Field Predictions in 3D Room Acoustic, Applied Sciences, 15(2), 939.

[302] Schwarz Digits (2025) Cyber Security Report.

[303] Schwarz Digits (2025) Warum die Digitalisierung ein Umdenken in einer neu geordneten Welt erfordert.

[304] ScienceDirect (2024) Cognitive Architecture.

[305] Shao, S. et al. (2022) High Efficiency Wireless Power Transmission System That Uses HTS Transmitting and Copper Receiving Coils, IEEE Transactions on Applied Superconductivity, 32(4).

[306] Shaughnessey, I. M. (2024) The Ethics of Robots in War, NCO Journal, February 2024.

[307] Shaw, A. (2017) Encoding and decoding affordances: Stuart Hall and interactive media technologies. Sage Journals, 39(4), 592-602.

[308] Sherazi, H. H. R. (2022). A Comprehensive Survey on RF Energy Harvesting: Applications and Performance Determinants. Sensors, 22(8), 2990.

[309] Singh, S. et al. (2024) Powering the future: A survey of ambient RF-based communication systems for next-gen wireless networks, IET Wireless Sensor Systems, 14(6), 265-292.

[310] Smith, J. (2025) Meeting Abstracts, Journal of The Electrochemical Society, MA2025-02.

[311] SOCradar (2022) "Fullz," "Dumps," and More: What do Hackers Sell on the Black Market?

[312] Soleimani, J. & Kurt, G. K. (2024) High-power radio frequency wireless energy transfer system: Comprehensive survey on design challenges, IET Wireless Sensor Systems, 14(6), 248-264.

[313] Sommer, D. & Lorenz, B. (2022) Der digitale Nachlass – Was passiert mit meinen Daten nach meinem Tod?

[314] Sophos (2025) The Human Cost of Vigilance: Addressing Cybersecurity Burnout in 2025.

[315] Sophos (2025) The Sophos Annual Threat Report: Cybercrime on Main Street 2025.

[316] Sophos (2025) The State of Ransomware 2025.

[317] StackIT (2025) Deutschlands Digitaler Aufbruch.

[318] Statista (2025) Estimated cost of cybercrime worldwide 2018-2029.

[319] Statista (2025) Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Februar 2025.

[320] Statista Market Insights (2025) Brand Shares (BETA), basierend auf Finanzberichterstattung der Key Player.

[321] Statista Market Insights (2025) Public Cloud – Durchschnittliche Ausgaben je Arbeitnehmer.

[322] Statista Market Insights (2025) Public Cloud – Umsatz.

[323] Statistisches Bundesamt (2025) Informations- und Kommunikationstechnologien privater Haushalte.

[324] Swiss Cyber Security (2025) Adidas meldet Datenleck nach Angriff auf Dienstleister.

[325] Taglione, C., et al. (2024) Polarimetric Imaging for Robot Perception: A Review, Sensors, 24(14), 4440.

[326] Taylor, J. (2024) Digital afterlife – how to deal with social media accounts when someone dies.

[327] Techround (2024) How The Rise Of Grief Tech Comforts The Broken Hearted.

[328] Terryn, S. et al. (2017) Self-healing soft pneumatic robots, Sci. Robot.2,eaan4268(2017).

[329] Tester, P. (2025) What are Fullz? How Hackers & Fraudsters Obtain & Use Fullz.

[330] Thales (2025) 2025 Thales Data Threat Report.

[331] The Rise of AI-Powered Threats and Other Mobile Risks Highlight Why It's Time to Rethink Your Security Architecture.

[332] The White House (2025) National Security Strategy of the United States of America November 2025.

[333] Tidy, J. (2024) Firm hacked after accidentally hiring North Korean cyber criminal.

[334] Todesfall-Checkliste.de. (2020) Durchschnittliche Kosten von Bestattungen in Deutschland (in Euro). Statista.

[335] Tom, G. et al. (2025) From Molecules to Mixtures: Learning Representations of Olfactory Mixture Similarity using Inductive Biases, Preprint 2501.16271.

[336] Tong, Y., et al. (2024) Advancements in Humanoid Robots: A Comprehensive Review and Future Prospects, IEEE/CAA Journal of Automatica Sinica, 11(2), pp. 301-328.

[337] Trend Micro (2025) Trend Micro State of AI Security Report, 1H 2025.

[338] Trend Micro (2026) The AI-Fication of Cyberthreats.

[339] TÜV Verband (2025) TÜV Cybersecurity Studie 2025.

[340] Tutika, R. et al. (2021) Self-healing liquid metal composite for reconfigurable and recyclable soft electronics, Commun Mater 2, 64 (2021).

[341] UNIDIR Security and Technoligy Programme (2026) Securing Cyberspace for Peace: Insights into Cyberthreats and International Security in 2025.

[342] Van Mulders, J., et al. (2022) Wireless Power Transfer: Systems, Circuits, Standards, and Use Cases, Sensors, 22(15), 5573.

[343] Verfassungsblog (2024) Gaza, Artificial Intelligence, and Kill Lists.

[344] Verizon Business (2025) 2025 Data Breach Investigations Report.

[345] Wang Y. & Weng G.-M. (2025) Nuclear batteries: Potential, challenges and the future. The Innovation Energy 2:100079.

[346] We Are Social, DataReportal, Meltwater (2025) Ranking der größten Social Networks und Messenger nach der Anzahl der Nutzer im Februar 2025 (in Millionen). Statista.

[347] WEF (2025) Cybercrime Atlas: Impact Report 2025.

[348] WEF (2026) Global Cybersecurity Outlook 2026.

[349] WEF (2026) The Global Risks Report 2026.

[350] Weizenbaum Institut (2024) Digitale Souveränität.

[351] Wen, S. (2024) The real battle for data privacy begins when you die.

[352] Wright, T. P. (1936) Factors Affecting the Cost of Airplanes. Journal of the Aeronautical Science Volume 3.

[353] Xie, Y. et al. (2025) Complex-valued matrix-vector multiplication using a scalable coherent photonic processor, Science Advances, 11(eads7475).

[354] Yaghmazadeh, O. (2024) Pulsed High-Power Radio Frequency Energy Can Cause Non-Thermal Harmful Effects on the BRAIN, IEEE Open Journal of Engineering in Medicine and Biology, vol. 5, pp. 50-53.

[355] Yang, Q. (2025) Principles for the Standardized Handling of Digital Property Inheritance. Humanities and Social Science Research, 8(3), p29.

[356] Yu, C. & Wang, P. (2022) Dexterous Manipulation for Multi-Fingered Robotic Hands With Reinforcement Learning: A Review, Frontiers in Neurorobotics.

[357] Yuan, W. et al. (2017) GelSight: High-Resolution Robot Tactile Sensors for Estimating Geometry and Force, Sensors, 17(12), 2762.

[358] Záboji, N. & Sachse, M. (2026) Frankreich wirft Teams, Zoom und Co. raus, Frankfurter Allgemeine Zeitung.

[359] ZEW (2024) Digitale Souveränität: Unternehmen sehen Abhängigkeit bei KI und Software.

[360] ZEW (2025) Digitale Souveränität: Herausforderungen aus Sicht der Unternehmen.

[361] Zhang, S. et al. (2021) A Robotic Electrochemical Biosensor Based on Kinetic Electronics Technique, IEEE Sensors, 2021, pp. 1-4.

[362] Zhang, R., et al. (2025) Characteristics and driving factors of power generation performance in microbial fuel cells: An analysis based on the CNKI database, Frontiers in Microbiology, 16, 1620539.

[363] Zhao, X. et al. (2025) Remote Vital Sign Monitoring Based Millimeter-Wave Sensing, IEEE Access, 24(12).

[364] Zhou, K. et al. (2023) Dimensional emotion recognition from camera-based PRV features, Volume 218.

CYBER THREATS TIMELINE

2017 2018

- 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.

Ransomwa attack on the city of Atlanta

Maersk malware attack

LO

GANDCRAB

Gar ove

FIN7

Marriott data theft

DOUBLE DRAGON

Equifax data theft

LAZARUS GROUP SINCE 2009

WannaCry ransomware attack

COZY BEAR SINCE 2008

ANONYMOUS SINCE 2003

EQUATION GROUP SINCE 2001

0.86 T USD

CULT OF THE DEAD COW SINCE 1984

2017 2018

2019 2020 2021 2022 2023 2024 2025

SCATTERED SPIDER

LAPSUS$

SALT TYPHOON

CONTI

DARKSIDE

CKBIT

Microsoft hack

Uber hack

T-Mobile hacks

Jaguar Land Rover hack

US provider hacked

Colonial Pipeline ransomware attack

Funke Media Group ransomware attack

Capital One data theft

Coop ransomware supply chain attack

Continental AG data theft

Steico hack

Bitmarck data theft

Game over

America Water Works hack

Hackers arrested

Cyberattack on the Australian parliament

SolarWinds supply chain attack

Several operations and protests counter Russia's war of aggression against Ukraine

Axie Infinity hack

#DeutschlandRIP

Bybit crypto heist

Data theft via Microsoft Teams

Cyberattack on the CDU's IT

Attack on European diplomats

1.16 T USD

2.95 T USD

5.49 T USD

7.08 T USD

8.15 T USD

9.22 T USD

10.29 T USD

By way of the hacked SolarWinds software, adversaries penetrate government authorities such as the US Department of the Treasury and the Pentagon, as well as leading companies and organizations around the globe.

Following a supply chain attack via the IT service provider Kaseya, Swedish supermarket chain Coop has to shut 800 stores for a week as the cash register systems are offline.

Hackers make off with 40 terabytes of data, including highly sensitive documents, and demand USD 40 million to return it. The attack is repelled, and the damage assessment is still ongoing.

Jan/May 2023: two hacks at T-Mobile within six months, with over 37 million customer records stolen.

As payback for Germany's decision to send tanks to Ukraine, pro-Russian hacker group Killnet launches attacks on targets in Germany (police, Defense Ministry, airports).

In August 2024, the Chinese hacker group Salt Typhoon infiltrates several large US telecommunications corporations, including AT&T, Verizon and T-Mobile, gaining access to extensive metadata relating to callers as well as text messages, especially in the Washington D.C. area. More than a million users, including high-ranking politicians and election campaign teams, are impacted.

In October 2024, an unknown hacker group compromises the systems of American Water Works, one of the largest water utilities in the USA, by gaining unauthorized access to internal networks.

In February 2025, the North Korean Lazarus group pulled off the largest crypto heist in history, stealing US$1.5 billion from the Bybit crypto market. Using manipulated JavaScript code, the hackers were able to infiltrate the signing process during a wallet transfer and get their hands on huge stocks of Ethereum.

In March 2025, investigators arrested an alleged hacker belonging to the GandCrab group.

Russian hacker group Cozy Bear targeted European diplomats in a wave of attacks in April 2025, using fake invitations to wine-tasting events to entice them to download a malicious archive. The aim of this phishing scam is to install the GRAPELOADER spyware, granting adversaries persistent remote access to government computers and enabling unauthorized access to sensitive information.

2019 2020 2021 2022 2023 2024 2025

1 Source: [318], Own diagram

IMPRINT

Publisher

Schwarz Digits KG
Am Campus 1
74177 Bad Friedrichshall
Germany

Registered Office:
Neckarsulm (Bad Friedrichshall as of May 1st, 2026)
Local District Court: Stuttgart HRA 737212
VAT identification number: DE335467503

Email: info@schwarz-digits.de
Website: www.schwarz-digits.de
LinkedIn: https://www.linkedin.com/company/98943909
Youtube: https://www.youtube.com/@SchwarzDigits

Scientific Director: Dr. Alexander Schellong

Authors: Dr. Leonid Glanz, PD Dr. Robert Koch, Dr. Patricia Köpfer, Dr. Alexander Schellong, Sofie Schönborn

Design: André Renvert, Lukas Breitkreutz (infotectures)