About the Article

Germany faces escalating cyber threats from state and non-state actors, targeting businesses and critical infrastructure. Ferdinand Gehringer argues that Germany's cybersecurity framework is outdated and inefficient, requiring urgent reforms. He advocates for a stronger, independent BSI, enhanced public-private partnerships, streamlined cyber defense structures, and better legal frameworks for digital forensics. Strengthening education and training is crucial for building long-term cyber resilience.

About the Author

Ferdinand Gehringer is a security policy advisor at the Konrad Adenauer Foundation, a lawyer, and a certified mediator. He advises members of the German Bundestag and the European Parliament, as well as international organizations and governments, primarily on cyber and information security, hybrid threats, and the protection of critical infrastructure

In the past 12 months, approximately 81 percent of German companies have been affected by data theft, digital industrial espionage, or sabotage (Bitkom, 2024). Concurrently, the warnings issued by the Federal Office for the Protection of the Constitution and the Federal Intelligence Service regarding cyber activities from states such as Russia, China, and Iran have intensified annually (BfV, 2025; PC-SPEZIALIST, 2024). The 2024 Situation Report by the Federal Office for Information Security (BSI) describes the situation as alarming, with Germany being a primary target (BSI, 2024). Given the increasing risk of major digital disruptions, as well as (digital) sabotage and espionage, it is imperative that Germany responds to developments in cyberspace and enhances its cyber capabilities.

Escalating Threats in Cyberspace

The cyber threat landscape has deteriorated significantly in recent years. Cyberspace has evolved into a complex and dynamic environment where various actors pursue different objectives. While cyberattacks were previously often opportunistic, they have now become more targeted and technologically sophisticated. The use of artificial intelligence (AI) and machine learning has significantly increased the effectiveness and sophistication of these attacks (BSI, 2024).

The Convergence of State and Non-State Actors

Cyber actors can broadly be categorized into state and non-state groups, though distinguishing between them has become increasingly challenging. Non-state actors frequently operate on behalf of state actors, executing their strategic objectives. State actors include national governments, as well as their military and intelligence agencies. These entities leverage cyberspace for espionage, sabotage, and the pursuit of geopolitical interests. The United States, Israel, China, Russia, Iran, and North Korea are particularly active in cyberspace and possess advanced cyber capabilities (CISA, 2021).

Non-state actors encompass criminal organizations, hacker groups, and individuals (Chaudhury, 2021). These actors typically pursue financial gains through ransomware attacks or ideological motives, as seen in hacktivism. Frequently, non-state actors are contracted by state entities for specific objectives, receiving financial compensation or state approval for their (criminal) activities in return (Maurer, 2016, p. 383f.). Cybercrime groups are often highly organized and structured similarly to corporate entities. They maintain a hierarchical structure, with leadership overseeing operations while specialized members execute tasks such as malware development, phishing, or data exfiltration. Payments are sometimes issued monthly, akin to conventional employment contracts. These groups employ sophisticated technologies and infrastructures to support their illicit activities, generating substantial revenue through ransomware attacks, the sale of stolen data, and fraud. To safeguard their identities and evade law enforcement, they utilize encryption techniques, anonymization services, and cryptocurrencies (Sancho & Fuentes, 2023). This level of organization makes cybercrime groups a significant threat to businesses and governments worldwide. One particularly notable example is the ransomware group „LockBit," which carried out numerous attacks on businesses worldwide in 2022 and 2023. Operating as a Ransomware-as-a-Service (RaaS), LockBit recruits affiliates to conduct ransomware attacks using its proprietary tools and infrastructure. These attacks result in the encryption of data on compromised systems, with victims being extorted for ransom payments to regain access to their files (CISA, 2023). A case in point is the 2022 attack on the DAX-listed company Continental, which suffered significant financial losses and required several weeks to restore its systems. LockBit affiliates have targeted companies globally, spanning industries such as financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing, and transportation (BlackFog, 2025).

Critical Infrastructure as a Target

Globally, cyberattacks frequently aim to disrupt critical infrastructure, inflict economic damage, or foster political instability. A prominent example is the Russian cyberattack on Ukraine's power grid in 2015 (Süddeutsche, 2016). The extensive Russian military aggression against Ukraine has demonstrated the integral role of cyberattacks in modern warfare, with Russian state-sponsored hackers repeatedly attempting to destabilize Ukrainian infrastructure through DDoS attacks. Notably, in the early stages of the war, these attacks targeted Ukraine's critical infrastructure alongside conventional military operations.

The Geopoliticization of Cyberspace

Digital demobilization poses a substantial challenge, as cyberspace has become a battleground for geopolitical conflicts. Real-world political events manifest in cyberspace, where their implications and consequences are increasingly severe. Cyber operations are now integral to modern military strategies and hybrid warfare.Simultaneously, non-state groups and hacktivists exploit cyberattacks to advance ideological and political agendas.

Germany's current cybersecurity architecture is insufficiently aligned with existing threats and proves inefficient.

Strengthening Germany's Cyber Capabilities

To effectively respond to developments in cyberspace, Germany must enhance its cyber capabilities. The country's current cybersecurity architecture is insufficiently aligned with existing threats and proves inefficient. Redundant structures at federal and state levels, along with unclear jurisdictional responsibilities among various institutions, exacerbate the issue. Small and medium-sized enterprises (SMEs) and operators of critical infrastructures (KRITIS) face particular challenges in this regard, especially concerning the upcoming implementation of the European NIS2 Directive (European Parliament, 2022) and the Cyber Resilience Act (European Parliament, 2024).

A Central Role for the BSI

The Federal Office for Information Security (BSI) should assume a more central and independent role, particularly in advisory and certification functions. To meet future challenges, the BSI must receive additional personnel and financial resources. Simultaneously, the interests of federal states and municipalities must be equitably considered when restructuring cybersecurity frameworks.

Cybersecurity as a Collective Responsibility

Cybersecurity is a shared responsibility among all stakeholders. Beyond government agencies, the private IT security sector must be more actively involved. Germany possesses a robust base of SMEs specializing in IT security services, which could significantly contribute to strengthening cybersecurity while alleviating the burden on public institutions such as the BSI. Establishing a resilient public-private partnership is crucial, supported by targeted incentives such as tax benefits for companies investing in cybersecurity or funding programs for innovative security solutions.

Optimizing Cyber Defense

Germany's current cyber defense mechanisms are inadequate for addressing the existing threat landscape. The Federal Criminal Police Office (BKA) should be designated as the central authority for cyber threat prevention due to its well-developed and scalable structures. Furthermore, the National Cyber Defense Center (C-AZ) should be upgraded and placed under the jurisdiction of the Federal Chancellery, with stronger involvement from federal states. A nationwide real-time cyber threat intelligence

system, maintained at the C-AZ and accessible to all relevant stakeholders, is essential.

Enhancing Digital Forensic Capabilities

Germany's prosecution authorities must also be adequately equipped for the digital transformation. Cybercrime is escalating, with cybercriminal groups becoming increasingly sophisticated. Legal frameworks should be revised to enable secure confiscation of digital attack infrastructures such as servers and IT networks. Additionally, a reform of cybercrime laws is necessary. Notably, ethical security researchers should no longer face prosecution for identifying and mitigating security vulnerabilities. Establishing an official register for security researchers would provide them with greater legal clarity. For non-researchers, voluntarily reporting vulnerabilities to the BSI, the Federal Commissioner for Data Protection and Freedom of Information, the Federal Ministry of Justice, or Central Cybercrime Contact Points (ZAC) could yield mitigating legal benefits.

Strengthening Cybersecurity Education and Training

These reforms alone will not render Germany fully cyber-capable. Future crises cannot be entirely prevented. Therefore, alongside a more robust cybersecurity education and training framework for the general population, regular cybersecurity exercises should be conducted to enhance preparedness and resilience.

Strengthening Digital Sovereignty

Germany must also place greater emphasis on strengthening its digital sovereignty. This includes not only diversifying risks and reducing dependencies but also promoting sustainable and secure digitalization based on the principle of „Security by Design." According to a survey by Bitkom, four-fifths of German companies view their digital dependence on the USA and China as problematic. The dependency is particularly high in the areas of semiconductors and end devices: 83 percent of companies consider Germany to be highly dependent on third parties. This dependence poses a significant risk, as many companies see no way to counteract political pressure on their foreign business partners (Bitkom, 2025). National and European innovations should be promoted more intensively, and investments should be strengthened. Start-ups must be supported in product development in the German market and encouraged to compete in international markets such as the USA or Israel. For the federal administration, state institutions, municipalities, and critical infrastructures, this means relying on uniform digital solutions „Made in Germany." A first step could be the development of a national cloud infrastructure and a German cloud solution.

Germany Must Act Quickly

To address developments in cyberspace, the increasingly professionalized state and non-state actors, and the growing damage potential, several adjustments must be made. Germany is currently not sufficiently prepared. Successfully tackling these challenges requires close cooperation between the government, society, and the economy. The key issues and necessary measures are clear: adapting the cybersecurity architecture, strengthening the Federal Office for Information Security (BSI), building an effective cyber defense, improving education, and promoting digital sovereignty. Only in this way can hostile actors in cyberspace be stopped and Germany become cyber-capable."

References

Bitkom. (2024). Wirtschaftsschutzstudie 2024. Abgerufen von https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf (zuletzt aufgerufen am 24.01.2025).

Bitkom. (2025). Deutschlands digitale Abhängigkeit steigt. Abgerufen von https://www.bitkom.org/Presse/Presseinformation/Deutschlands-digitale-Abhaengigkeit-steigt (zuletzt aufgerufen am 24.01.2025).

BlackFog. (2025). LockBit's 2024 Attacks – An Overview. Abgerufen von https://www.blackfog.com/lockbit-attacks-2024/ (zuletzt aufgerufen am 24.01.2025).

Booz Allen Hamilton. (2023). China's Cyberattack Strategy Explained. Abgerufen von https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html (zuletzt aufgerufen am 24.01.2025).

Bundesministerium des Innern und für Heimat (BMI). (2024). Cyberangriffe auf die SPD und auf Rüstungs-, IT- und Luftfahrtunternehmen sind APT 28 und damit dem russischen Militärgeheimdienst GRU zuzuordnen. Abgerufen von https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/05/aktuelle-Cyberangriffe.html (zuletzt aufgerufen am 24.01.2025).

Bundesministerium des Innern und für Heimat (BMI). (2024) II.

Bundesamt für Verfassungsschutz (BfV). (2025). Akteure und Angriffsmethoden.
Abgerufen von https://www.verfassungsschutz.de/DE/themen/cyberabwehr/akteure-und-angriffsmethoden/akteure-und-angriffsmethoden_node.html (zuletzt aufgerufen am 24.01.2025).

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2024). Die Lage der IT-Sicherheit in Deutschland 2024. Abgerufen von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5 (zuletzt aufgerufen am 24.01.2025).

Chaudhury, D. R. (2021, April 12). States' use of non-state actors in cyberspace. Observer Research Foundation. https://www.orfonline.org/expert-speak/states-use-of-non-state-actors-in-cyberspace (zuletzt aufgerufen am 24.01.2025).

CrowdStrike. (2024). Global Threat Report 2024. Abgerufen von https://www.crowdstrike.com/en-us/global-threat-report/ (zuletzt aufgerufen am 24.01.2025).

Cybersecurity and Infrastructure Security Agency (CISA). (2021). Nation-State Threats. Abgerufen von https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors (zuletzt aufgerufen am 24.01.2025).

Cybersecurity and Infrastructure Security Agency (CISA). (2023). Understanding Ransomware Threat Actors: LockBit. Abgerufen von https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a (zuletzt aufgerufen am 24.01.2025).

Europäisches Parlament. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Abgerufen von https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555 (zuletzt aufgerufen am 24.01.2025).

Europäisches Parlament. (2023). Cybersecurity in the EU: Threats, challenges and policy responses. Abgerufen von https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/702594/EXPO_BRI(2023)702594_EN.pdf (zuletzt aufgerufen am 24.01.2025).

Europäisches Parlament. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 14 December 2024 on measures for a high common level of cybersecurity across the Union. Abgerufen von https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847 (zuletzt aufgerufen am 24.01.2025).

Maurer, T. (2016). Cyber Proxies and the Crisis of International Relations. Journal of Conflict and Security Law, 21(3), 383-403. https://carnegie-production-assets.s3.amazonaws.com/static/files/JConflictSecurityLaw-2016-Maurer-383-403.pdf (zuletzt aufgerufen am 24.01.2025).

Merics. (2023). Cyber Security in China (II): Neue politische Führung setzt auf Stärkung der nationalen Sicherheit. Abgerufen von https://merics.org/sites/default/files/2020-05/China%20Monitor%20No%2020.pdf (zuletzt aufgerufen am 24.01.2025).

PC-SPEZIALIST. (2024). Digital Defense Report 2024: Zahl der Cyberangriffe steigt. Abgerufen von https://www.pcspezialist.de/blog/2024/11/04/digital-defense-report-2024/ (zuletzt aufgerufen am 24.01.2025).

Sancho, D., & Fuentes, M. R. (2023, April 3). Unpacking the structure of modern cybercrime organizations. Trend Micro. Abgerufen von https://www.trendmicro.com/en_us/research/23/d/unpacking-the-structure-of-modern-cybercrime-organizations--.html (zuletzt aufgerufen am 24.01.2025).

Spiegel. (2023). Vulkan Files. Abgerufen von https://www.spiegel.de/politik/deutschland/vulkan-files-enthuellungen-wie-putins-cybersoldaten-den-krieg-ins-internet-tragen-a-bb241ad9-a9c3-422e-af57-ffe59986a1d8 (zuletzt aufgerufen am 24.01.2025).

Süddeutsche Zeitung. (2016, Januar 11). Ukraine: Bundesamt geht von Hackerangriff auf ukrainisches Stromnetz aus. Süddeutsche.de. Abgerufen von https://www.sueddeutsche.de/wirtschaft/ukraine-bundesamt-geht-von-hackerangriff-auf-ukrainisches-stromnetz-aus-1.2830197 (zuletzt aufgerufen am 24.01.2025).

The Cyber Express. (2023). Hacktivist Groups Target G20 Summit. Abgerufen von https://thecyberexpress.com/g20-summit-2023-cyber-attack-infrastructure/ (zuletzt aufgerufen am 24.01.2025).