ORION FORUM

Governing the Breach: Cyber Crisis Response in Germany and the United States

SEPTEMBER 16, 2026

Introduction

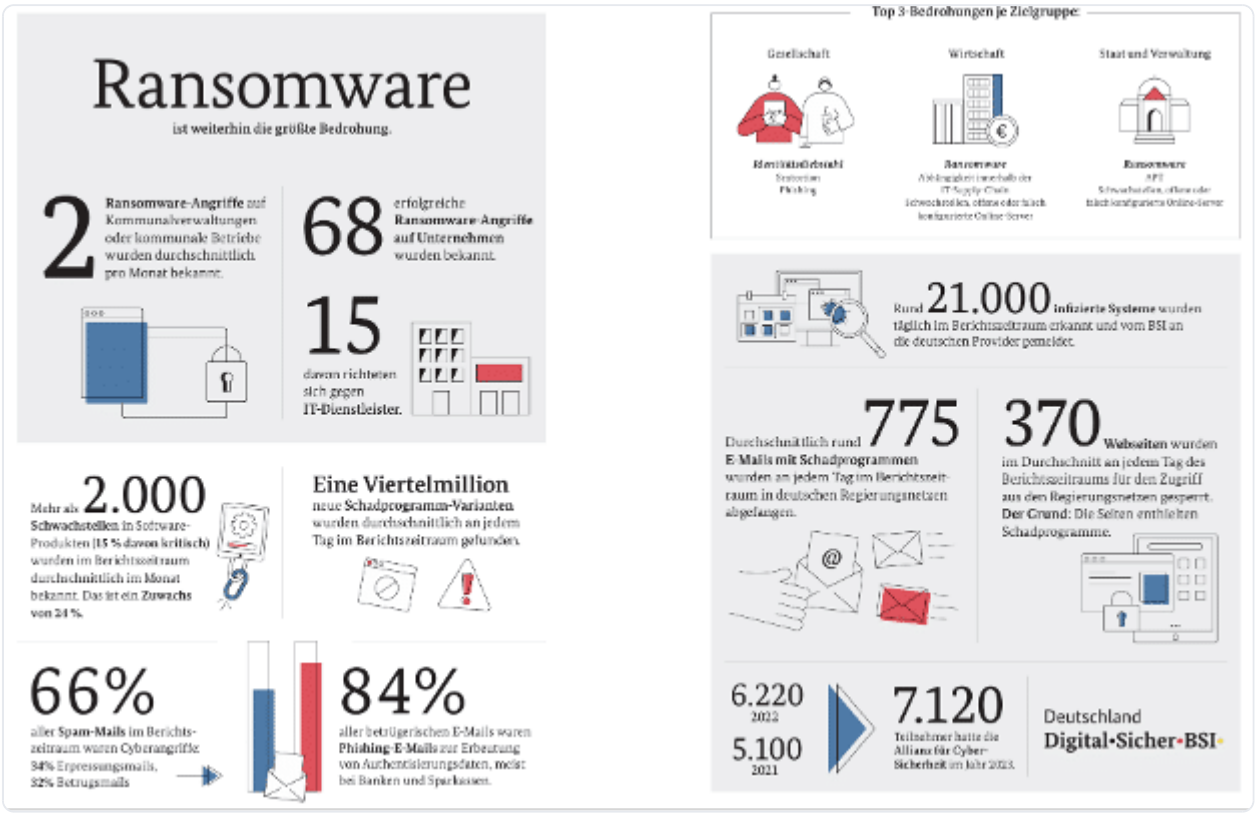
In December 2024, a cyberattack against the U.S. Department of the Treasury did not begin inside the Treasury. A Chinese state-sponsored actor gained access through a compromised third-party cybersecurity provider. The incident exposed a fundamental problem of modern cyber governance: governments are increasingly responsible for protecting digital infrastructure they do not entirely control. The vulnerability was not simply a technical weakness; it was a governance problem involving a federal agency, a private technology provider, cybersecurity authorities, law enforcement, and intelligence organizations.

Major cyberattacks increasingly function as crises of governance rather than isolated cybersecurity incidents. State-sponsored operations can simultaneously threaten national security, democratic institutions, economic stability, and public confidence, forcing governments to make rapid decisions under significant uncertainty. As Boin et al. (2018) argue, crises test governments' ability to coordinate competing institutions, make decisions under uncertainty, communicate effectively, and maintain public confidence.

Germany and the United States offer useful comparative cases because both are democratic allies with advanced cybersecurity capabilities but use different approaches to cyber crisis governance. Germany relies on a more structured, federal, government-led model that emphasizes institutional responsibility and evidence-based attribution. The U.S. relies on a more decentralized whole-of-government model in which federal agencies, intelligence organizations, law enforcement, and private-sector partners contribute specialized capabilities.

This paper examines four state-sponsored cyber incidents targeting political and government institutions in Germany and the U.S. The comparison demonstrates that effective cyber crisis governance depends less on choosing between centralized and decentralized systems than on combining clear institutional responsibility, flexible coordination, credible attribution, private-sector integration, and institutional learning. Germany demonstrates the value of structured coordination and evidentiary rigor, while the U.S. demonstrates the advantages of operational flexibility and public-private integration.

Background: Cyber Crisis Governance as a Policy Challenge



Source: Federal Office for Information Security (BSI), The State of IT Security in Germany 2025, analyzing ransomware threats and incidents affecting organizations in Germany.

Cyberattacks rarely remain technical problems. Modern campaigns can target political parties, government agencies, critical infrastructure, and private companies to obtain intelligence, influence political processes, or undermine public trust. As Buchanan argues, cyber operations have become a routine component of geopolitical competition. Because many occur below the

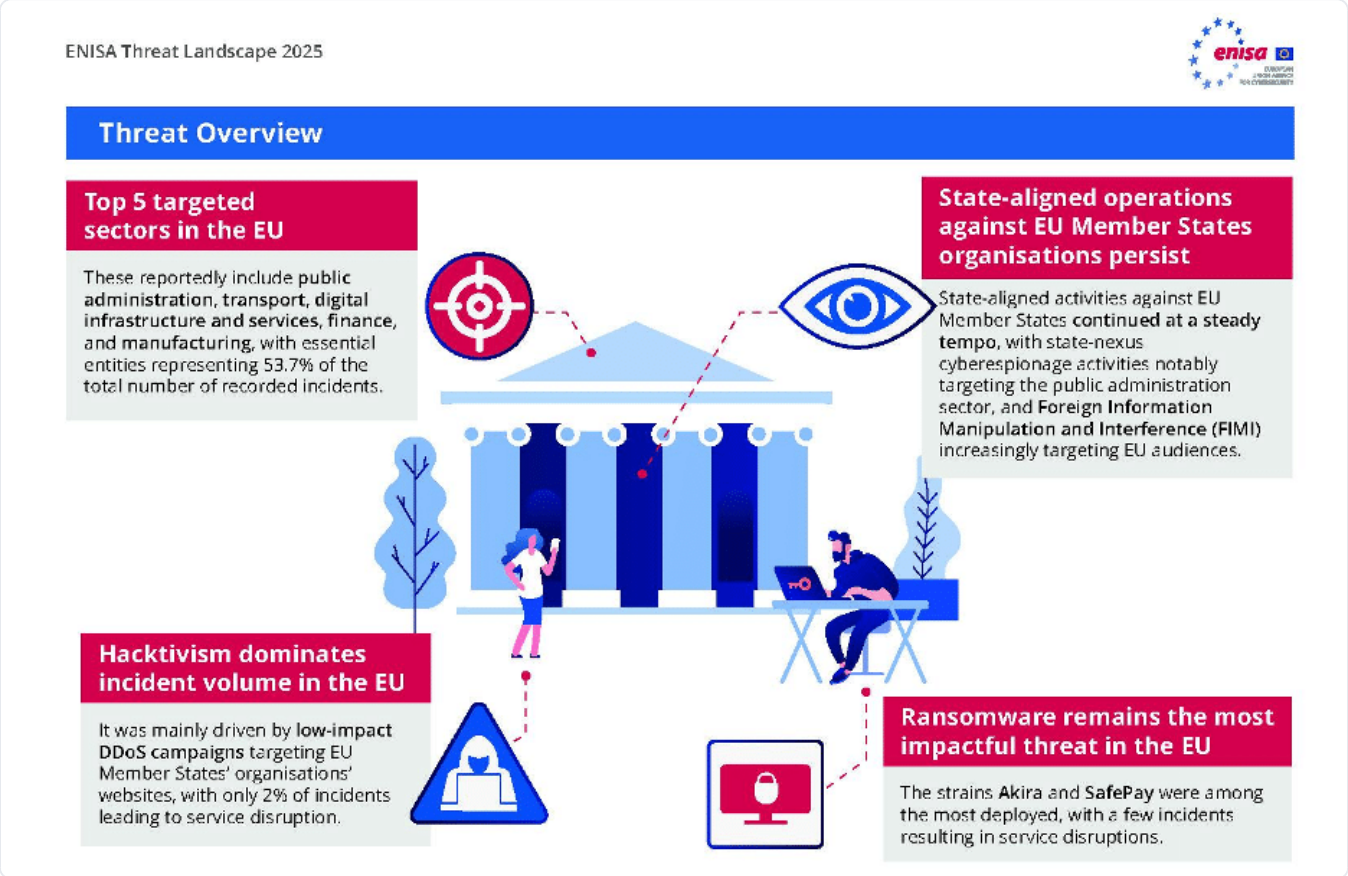
threshold of armed conflict, governments must combine technical defense with diplomatic, legal, intelligence, and political responses. The central governance challenge is therefore not simply whether a government can defend its networks, but whether its institutions can coordinate these different responses when responsibility, information, and authority are distributed across multiple actors.

Cyberattacks in Germany and the United States reached record levels in 2024-2025, with ransomware, data theft, and state-linked espionage driving hundreds of billions in losses and straining crisis-response institutions. In Germany, the Federal Office for Information Security (BSI) reports €202.4 billion in cyberattack losses over the past year, with 950 reported ransomware incidents (80% targeting SMEs), though underreporting likely makes the true figure ten times higher. Public administration accounts for half of all attacks; critical infrastructure operators reported 153 significant incidents, and Germany ranks as the fourth most targeted nation globally by Advanced Persistent Threat groups. In the United States, the FBI's Internet Crime Complaint Center recorded $20.877 billion in cybercrime losses in 2025, a 26% increase from 2024, with 3,611 ransomware complaints and nearly half involving critical infrastructure. The Cybersecurity and Infrastructure Security Agency (CISA) blocked 2.62 billion malicious connections on federal networks and 371 million within critical infrastructure in 2025. The ROCCA dataset, tracking 711 core and 954 extended critical cyberattack records, shows recurring targeting of energy, healthcare, and government sectors in both countries, blurring the line between criminal extortion and geopolitical coercion.

Germany's cyber governance model is built around a relatively centralized federal structure that combines technical expertise, regulatory oversight, and intelligence capabilities. The BSI serves as the primary technical authority, while the Federal Ministry of the Interior and Community (BMI) coordinates national cybersecurity policy. Intelligence and domestic security agencies, including the Federal Intelligence Service (BND) and Federal Office for the Protection of the Constitution (BfV), address foreign cyber threats, espionage, and threats to Germany's constitutional order. This framework emphasizes administrative coordination and legal requirements, reflected in Germany's *IT-Sicherheitsgesetz* and broader EU cybersecurity rules, while relying on cooperation between government agencies and private-sector operators.

The United States takes a more decentralized approach, distributing cybersecurity responsibilities across agencies with distinct missions. CISA leads civilian cybersecurity and critical-infrastructure protection, while the Federal Bureau of Investigation (FBI) focuses on cybercrime and domestic investigations, and the National Security Agency (NSA) contributes foreign intelligence and technical capabilities. Military and national-security functions are handled through institutions such as U.S. Cyber Command and the National Security Council. This division allows agencies to draw on specialized authorities and capabilities, but also makes coordination and information sharing essential, particularly when a cyber incident crosses the boundaries between criminal activity, national security, and critical infrastructure.

These institutional differences become particularly important when cyberattacks target politically sensitive institutions or government systems. In such crises, governments must determine who is responsible, assess incomplete evidence, coordinate agencies with overlapping authorities, work with private-sector providers, and decide when and how to publicly attribute an attack. The following cases examine how Germany and the United States navigated these challenges through responses to such cyber operations. Together, they illustrate how different governance structures shape attribution, coordination, public-private cooperation, and the speed and effectiveness of crisis response.



Source: European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025, which analyzes major cybersecurity threats and trends observed across Europe.

Cyberattacks Targeting Government and Political Institutions

Germany: Russian Cyber Operation Against the SPD

In May 2024, the German government publicly attributed a cyber espionage campaign targeting the Social Democratic Party (SPD) to Russia's military intelligence organization APT28, also known as Fancy Bear. German authorities determined that attackers exploited the Microsoft Outlook vulnerability CVE-2023-23397 to compromise email accounts belonging to SPD officials and other German organizations. According to Germany's Federal Foreign Office, the operation formed part of a broader Russian intelligence campaign targeting democratic institutions across Europe.

The response demonstrated Germany's structured approach to cyber crisis governance. The BSI, BfV, BND, BKA, and relevant federal ministries contributed to the investigation and

response. Following forensic analysis and intelligence review, Germany publicly attributed the operation to Russia, summoned the Russian ambassador, and coordinated diplomatic responses with EU and NATO partners. However, this highly coordinated approach also revealed a potential limitation: the need to integrate technical, intelligence, and political assessments can make the response process lengthy. Germany discovered the attack in 2023 but did not publicly attribute it to Russia until May 2024. While the extended process strengthened the evidentiary basis for attribution, it also delayed the government's ability to move from identifying the intrusion to taking an immediate coordinated political and diplomatic response.

Germany: Federal Office for Cartography and Geodesy Cyberattack

Germany's Federal Office for Cartography and Geodesy (BKG), which provides official geospatial information to government agencies and critical infrastructure operators, was targeted by a cyber espionage operation in 2021. The attackers compromised devices belonging to private individuals and companies and used them to conceal their access to the BKG's network. They successfully gained access to parts of the BKG's systems, although German authorities have not publicly disclosed what information, if any, was taken.

The response involved an extensive investigation by the BfV and BSI, with other government agencies contributing to the national attribution process. Nearly three years after the attack, Germany publicly attributed the operation to Chinese state actors and summoned the Chinese ambassador. However, the government still did not publicly identify a specific Chinese intelligence service, hacking group, or individual responsible for the operation. The case therefore illustrates a trade-off in cyber crisis governance: extensive technical and intelligence investigations can produce a credible attribution to a state, but attribution may still fall short of identifying the specific actors responsible. This limits the government's ability to pursue more targeted forms of accountability while demonstrating the difficulty of translating cyber intelligence into concrete political consequences.

United States: Russian Cyber Operations Against Democratic Institutions

In July 2018, the U.S. Department of Justice indicted 12 GRU officers for conducting a coordinated cyber campaign against the Democratic National Committee, Democratic Congressional Campaign Committee, and Hillary Clinton's presidential campaign. The FBI was notified of the DNC intrusion in June 2016. Within months, the U.S. publicly attributed the campaign to Russia, and by January 2017, the intelligence community had publicly identified the GRU's role. According to the indictment two years later, Russian intelligence officers used spear-phishing and malware to gain access to political networks, steal documents and communications, and release stolen information through online personas and platforms such as WikiLeaks. Russian actors also targeted state election officials and election infrastructure.

The U.S. response demonstrated its distributed but expansive governance model. The FBI, DOJ, DHS, NSA, and broader intelligence community contributed to a response combining criminal indictments, intelligence assessments, public attribution, diplomatic measures, and election-security initiatives. The case illustrates the advantage of distributed capabilities: they were able to indict the individuals much quicker. However, this structure also created coordination challenges. Agencies operated under different mandates and priorities, making communication and information sharing essential to prevent duplicated efforts or gaps in the response. At the same time, agencies had to share relevant information while protecting sensitive intelligence, sources, and methods, limiting how much information could be exchanged across institutions. The U.S. model therefore presents a tradeoff: distributing responsibilities allows multiple institutions to respond quickly, but without effective coordination, overlapping authorities can lead to duplicated efforts and inefficient use of government resources.

United States: Treasury Department Third-Party Vendor Breach

In December 2024, the U.S. Department of the Treasury disclosed that a China-linked state-sponsored actor had compromised BeyondTrust, a third-party provider of remote technical support services used by Treasury. The attacker obtained a key used by BeyondTrust to secure its remote-support system, allowing access to Treasury workstations and files. The compromise occurred between September 30 and November 18, 2024, and Treasury was notified by BeyondTrust on December 8. Investigators later determined that the attackers had accessed 419 Treasury computers and at least 3,029 unclassified files, including files belonging to senior

Treasury officials. Treasury, CISA, the FBI, and other investigators worked to assess the scope of the breach and contain the intrusion. The compromised service was taken offline, and Treasury found no evidence that the attackers retained access to its systems.

The incident demonstrated a different governance challenge from the BKG case: the security of government systems can depend on organizations that the government does not directly control. Treasury's own cybersecurity measures did not prevent the intrusion because the attacker entered through a trusted third-party provider. Responding therefore required Treasury to rely on the vendor to identify and report the compromise while simultaneously working with CISA, the FBI, and other agencies to investigate its impact. The breach also raised broader questions about federal reliance on third-party technology, including whether existing contracting and security requirements adequately protect government systems. The case illustrates a tradeoff between the efficiency and specialized capabilities gained from private-sector providers and the loss of direct government control over the security of the infrastructure on which federal agencies depend.

Policy Recommendations

Cybersecurity is a constant process of catching up with an evolving threat. The cases examined in this study reveal recurring weaknesses in attribution, third-party security, interagency coordination, and information sharing. The infographic below highlights these challenges and poses key lessons that can be learned from the events.

Findings and Policy Recommendations

Five connected reforms for more resilient cyber-crisis governance in Germany and the United States.

GOVERNANCE PRIORITY	KEY LESSON	POLICY ACTIONS
1 **Build clearer coordination mechanisms** Institutionelle Koordination	Distributed institutions need clear roles and decision authority.	• Define lead/supporting agencies • Accelerate investigation-to-decision handoffs • Run regular cross-sector exercises
2 **Establish clearer attribution thresholds** Zuschriebungs- und Handlangsschwellen	Different actions need different confidence levels	• Use graduated thresholds • Permit defensive action/intelligence sharing at lower confidence • Reserve public attribution/ sanctions for higher confidence
3 **Treat private companies as part of the criss-response architecture** Staat-Wirtschaft-Kooperation	Trusted vendors can expose government systems	• Permanent public-private mechanisms • Secure reporting and technical information sharing • Clear vendor obligations for notification and forensic access
4 **Institutionalize allied coordination & strategic communication** Strategische Kommunikation	Cyber operations cross borders and collective responses improve credibility	• Rapidly share indicators and forensics • Standing allied attribution network • Coordinated credible public communication
5 **Turn incidents into institutional learning** Institutionelles Lernen	Recurring weaknesses must produce reforms	• Formal after-action reviews • Assess technical and decision-making failures • Assign agencies and deadlines for reforms

STRONGER TOGETHER. Clear coordination, proportionate action, trusted partnerships, allied resolve, and institutional learning build resilient cyber governance.

Source: Designed using an AI-powered design tool from Canva; content and analysis by the author.

***Build clearer coordination mechanisms* (*Institutionelle Koordination*)**

The first key takeaway is not that governments should centralize or decentralize cyber response, but that distributed institutions need a clear system for working together. Germany should maintain its structured coordination model while establishing procedures for moving more quickly from technical investigation to political decision-making when immediate action is necessary. The U.S. should establish standing interagency cyber-crisis frameworks that identify a lead agency, supporting agencies, and decision-making responsibilities for different types of incidents. These frameworks should be tested through regular exercises involving CISA, FBI, DOJ, the intelligence community, state and local authorities, and relevant private-sector organizations. Exercises should specifically test how agencies share sensitive information, avoid duplicating investigations, and coordinate decisions when multiple agencies have overlapping responsibilities.

***Establish clearer attribution thresholds* (*Staat-Wirtschaft-Kooperation*)**

Governments should also establish different thresholds for different types of action rather than treating attribution as a single decision. A lower threshold could authorize immediate defensive measures and intelligence sharing, while higher confidence would be required for public attribution, criminal charges, sanctions, or diplomatic action. Germany could use high-confidence intelligence assessments to reduce delays in protecting systems and warning partners while investigators continue building the evidentiary case. The United States should similarly standardize thresholds for sharing attribution-related intelligence to improve coordination across agencies.

***Treat private companies as part of the crisis-response architecture* (*Zuschreibung staatlicher Verantwortung*)**

The U.S. Treasury breach demonstrates that government cybersecurity can depend on the security of privately operated technology. The Treasury's own systems were compromised through a trusted third-party provider, showing that agencies cannot protect government

networks by securing their own systems alone. Both the United States and Germany should therefore establish permanent public-private response mechanisms before a crisis occurs. These should include standardized procedures for reporting significant incidents, secure channels for sharing technical and threat information, joint exercises with major government contractors and critical infrastructure operators, and stronger cybersecurity requirements for vendors with access to government systems. Contracts for sensitive government services should also clearly define responsibilities for breach notification, forensic access, incident response, and information sharing.

Institutionalize allied coordination & strategic communication (Strategische Kommunikation)

Cyberattacks rarely remain within a single country's borders, making allied coordination essential to an effective response. According to "A Need for Informed Policy Against Critical Cyberattacks: The ROCCA Project," China and Russia accounted for 458, or 48 %, of the 954 critical cyberattacks recorded in the ROCCA dataset between 2005 and 2025. NATO itself experiences hundreds of cyber incidents each month, highlighting the scale of the threat facing the Alliance. Germany's response to the SPD attack demonstrates the value of coordinating with EU and NATO partners, but considering the scale of the threat, NATO could play a more visible role in responding to state-sponsored operations from Russia, China, and other major adversaries. The United States should also work with NATO allies to establish a standing attribution network for rapidly sharing technical indicators, intelligence, and forensic findings. NATO could coordinate collective defensive measures and, when evidence is sufficiently strong, communicate allied assessments publicly. Clear procedures for evidence-sharing and public communication would allow allies to respond collectively rather than treating major cyberattacks as isolated national incidents, strengthening deterrence and raising the costs for states targeting the Alliance.

Turn incidents into institutional learning (Institutionelles Lernen)

Cybersecurity is a constant process of catching up with an evolving threat. The cases examined in this study reveal recurring weaknesses in attribution, third-party security, interagency coordination, and information sharing. Governments should require formal after-action reviews following significant state-sponsored cyber incidents. These reviews should

examine more than the technical cause of a breach. They should assess who made key decisions, how information moved between agencies, how long attribution took, where information-sharing barriers emerged, how private companies and foreign partners were involved, and whether existing authorities were sufficient. Each review must be actionable, producing specific recommendations with assigned agencies and deadlines. The goal should be to ensure that every major cyber incident leaves governments better prepared for the next one.

Conclusion

The cases in Germany and the United States show that the hardest part of a major cyberattack is often not detecting the intrusion but deciding what to do once it is discovered. Governments must determine who is responsible, coordinate agencies with different authorities, work with private companies and foreign partners, and act even when important information remains uncertain. Germany's structured approach can strengthen credibility but slow decision-making, while the U.S. model can mobilize diverse capabilities quickly, but risks duplicated efforts. These tradeoffs will become more difficult as attackers increasingly exploit the connections between government agencies, private companies, and international networks. Governments will need to treat each cyber incident as an opportunity to improve the institutions responsible for the next response. The objective is not to build a system that never fails (a realistic goal for neither Germany nor the United States) but one that can identify its weaknesses, adapt to new threats, and respond more effectively the next time they are exploited.
