Statement by Dr. Sven Herpig, Lead Cybersecurity & Emerging Threats at interface – Tech analysis and policy ideas for Europe e.V. (formerly: Stiftung Neue Verantwortung), within the framework of the participation of leading associations, expert circles and associations onDraft bill from the Federal Ministry of the Interior (BMI) for a "Law to Strengthen Cybersecurity"

Contact

Dr. Sven Herpig

Lead Cybersecurity & Emerging Threats

interface – Tech analysis and policy ideas for Europe e.V.

Email: sherpig@interface-eu.org

Github:https://github.com/z-edian/publications

Summary

The draft bill significantly expands intrusive cyber defense powers. At the same time, key structural problems remain unresolved:

- Fragmented responsibilities,
- Lack of governance for intrusive tools,
- Insufficient strengthening of resilience.

Without coordination mechanisms and transparency standards, there is a risk of loss of effectiveness and legal uncertainties.

1. Preliminary remarks

The present draft bill[1]This section addresses the topic of "cyber defense," also known as "active cyber defense," "threat prevention in cyberspace," or "hackback." Interface defines this term as measures in which one or more states jointly order or carry out (intrusive) technical interventions to neutralize, mitigate, or attribute a current, specific cyber operation or campaign.[2]The instruments mentioned in the draft bill, for example in BKAG-E §62e, are directed against the integrity, confidentiality and availability of information technology systems for the proactive defense against malicious cyber activities, including those of third parties according to BKAG-E §62e (3), and thus fall under this definition.

The political and technical discourse on this form of cyber defense has been ongoing for almost ten years.[3], without any significant progress – apart from BSIG §7b and §7c. The reasons for this are both superficially conducted debates and deliberate obfuscation, such as the reinterpretation of the term "hackback".[4]Previous initiatives – such as the proposal by the President of the Federal Police Headquarters, Dr. Dieter Romann, within the framework of the restructuring of the Federal Police Act 2024 – also[5]failed. Parallel to the expansions of intrusive cyber defense powers planned by the Federal Ministry of the Interior (BMI) for the Federal Criminal Police Office (BKA) and the Federal Police (BPol), similar competencies are to be created for the Federal Intelligence Service (BND) in the future.[6]

Before expanding powers for active cyber defense, the associated risks must first be clearly identified. Unintended collateral damage and the potential proliferation of the tools used can

[1] Federal Ministry of the Interior (2026): Draft law to strengthen cybersecurity
[2] Sven Herpig (2023): Active Cyber Defense – Toward Operational Norms
[3] Sven Herpig et al. (2020): Active Cyber Defense/Hackback in Germany
[4] Sven Herpig (2022): Active cyber defense instead of hackback?
[5] Dieter Romann (2024): Written statement by the President of the Federal Police Headquarters, Dr. Dieter Romann, for the public hearing on April 22, 2024, regarding the draft law for the restructuring of the Federal Police Act (Bundestag printed matter 20/10406).
[6] Thorsten Wetzling (2026): Germany's Reform of Foreign & Military Intelligence

quickly escalate the situation. Misallocations of power could also lead to measures being directed against compromised third-party infrastructure or uninvolved operators – with the risk of diplomatic or legal conflicts in third countries. While such measures can enhance national cybersecurity with careful selection and consideration, and robust safeguards, it is crucial that they are consistently integrated into existing security culture, IT architecture, and strategic concepts. Without this integration, an imbalance between operational power and actual security impact is likely – a problem that has already become apparent in similar discussions about highly invasive cyber powers.

Open, nuanced technical and political debates about use cases, criteria, and safeguards are essential. Only in this way will incurring costs for attackers not become a mere symbolic demonstration of state capability. In practice, active cyber defense measures will only constitute a small part of the portfolio that strengthens cybersecurity; IT security and resilience will remain the central pillars of national security in cyberspace.[7]

Against this backdrop, the German government should limit intrusive measures to the necessary minimum and concentrate on non-intrusive, threat-independent, scalable, and sustainable steps to protect its own IT infrastructure. If this proves insufficient in individual cases, responsible implementation requires choosing the least intrusive and escalating countermeasures (e.g., a walled garden order instead of "covert intrusion into the information technology systems of victims"). These measures must be efficient, effective, and proportionate. At the same time, the economic, political, security, and societal damage of inaction must outweigh the costs incurred by active cyber defense.[8]

[7] Sven Herpig (2021): Active Cyber Defense Operations – Assessment and Safeguards
[8] Sven Herpig (2023): Active Cyber Defense – Toward Operational Norms

2. Criticism

2.1 Parallel structures jeopardize effectiveness

As already emphasized in the preliminary remarks, the existing security architecture is crucial for the effectiveness and efficiency of planned cyber defense measures. However, the current draft bill proposes an expansion of powers without addressing the known shortcomings of Germany's cybersecurity architecture.[9]

In addition to the existing powers of state police forces in the area of cybersecurity, the competencies of the Federal Office for Information Security (BSI) and the Federal Intelligence Service (BND) (parallel through the draft Federal Intelligence Service Act - BNDG-E) are to be expanded, those of the Federal Criminal Police Office (BKA) significantly broadened, and new competencies created for the Federal Police. However, the draft legislation provides neither binding agreements nor conflict resolution mechanisms or coordinated processes. Even if such mechanisms were provided, an operational platform where all relevant authorities are represented and could coordinate is currently lacking. Without a formalized coordination process, all of the aforementioned authorities could, in the future, conduct active cyber defense measures in parallel – largely independently of one another or with only limited coordination mechanisms.

To make matters worse, the state's handling of vulnerabilities that might be necessary for certain cyber defense operations remains unclear. Germany currently lacks a transparent procedure for the government's decision on whether to withhold or disclose vulnerabilities.[10]Risks and legal gray areas therefore persist.[11]The planned parallel structure of an active cyber defense system, comprised of the Federal Criminal Police Office (BKA), the Federal Office for Information Security (BSI), the Federal Police, and the federal states, creates several operational pillars without clear prioritization or coordination rules with the BSI as the central federal cybersecurity authority. This is reminiscent of a similar approach taken with the

[9] Sven Herpig (2023): Statement by Dr. Sven Herpig, Head of Cybersecurity Policy and Resilience at the Stiftung Neue Verantwortung e. V. (SNV), for the public hearing of the Committee on Digital Affairs of the German Bundestag on January 25, 2023 on the topic of "Cybersecurity - Responsibilities and Instruments in the Federal Republic of Germany" and Federal Court of Auditors (2025): Report pursuant to Section 88 Paragraph 2 of the Federal Budget Code on cybersecurity

[10] Sven Herpig (2018): Vulnerability Management for Greater Security – How the State Should Regulate the Handling of Zero-Day Vulnerabilities

[11] Sven Herpig (2023): Statement by Dr. Sven Herpig, Head of Cybersecurity Policy and Resilience at the Stiftung Neue Verantwortung e. V. (SNV), for the public hearing of the Committee on Digital Affairs of the German Bundestag on January 25, 2023 on the topic of "Cybersecurity - Responsibilities and Instruments in the Federal Republic of Germany" and Sven Herpig (2025): Written statement by Dr. Sven Herpig, interface, dated October 8, 2025 – Public Hearing – Draft Bill of the Federal Government: Draft of a Law for the Implementation of the NIS-2 Directive and for the Regulation of Essential Principles of Information Security Management in the Federal Administration, BT-Drucksache 21/1501

security laws at the end of 2019. At that time, Dr. Ulf Buermeyer and I concluded: “Instead of granting further authorities far-reaching powers, the solution should rather consist of defining responsibilities more clearly and ending the current coexistence and often even conflict between security authorities. Instead, the expansion of security legislation, with its sometimes massive infringements on the fundamental rights of citizens, is being pushed forward [...]”.[12]

The planned approach threatens to fragment resources, dilute responsibilities, and significantly reduce the overall effectiveness of cyber defense for national security.

2.2 Powers instead of resilience

As emphasized in the preamble, open and nuanced technical and political debates about use cases, criteria, and safeguards are essential. Only in this way will incurring costs for attackers not become a mere symbolic demonstration of state power. In practice, active cyber defense measures will only constitute a small part of the measures that strengthen cybersecurity overall; IT security and resilience remain the central pillars.

These pillars are strengthened, among other things, by the expanded powers of the BSI (Federal Office for Information Security). According to Section 11, Paragraph 1, Sentence 1 of the draft BSIG (Federal Office for Information Security Act), the BSI is authorized to act "to search for and identify impairments to the security and functionality of information technology systems." These so-called threat hunting operations[13]The draft legislation proposes that the BSI (Federal Office for Information Security) should be able to carry out three activities per year based on the personnel positions proposed. Even if personnel from incident response are also deployed for these activities, this is insufficient to justify the expansion of its powers. The draft legislation should provide significantly more positions for incident response and threat hunting in order to substantially strengthen IT security and resilience. At the same time, the BSI should examine the strategic expansion of its operational capabilities and strategically reallocate internal staff to operational areas.

Against the backdrop of the German government's political promises to reduce bureaucracy and exercise fiscal discipline, the planned expansion of approximately 300 positions by 2030 for highly invasive, personnel-intensive, and only in exceptional cases necessary active cyber defense measures at the Federal Criminal Police Office (BKA) and the Federal Police (BPol), as outlined in the draft legislation and accompanying personnel plans, appears politically and strategically questionable. This is especially true because it remains unclear what concrete

[12] Ulf Buermeyer and Sven Herpig (2019):Constantly introducing new security laws doesn't help.
[13] Sven Herpig (2022): Cybersecurity policy: German lack of ideas?

increase in sustainable cybersecurity this will achieve. Tom Uren, a former employee of the Australian Department of Defence, recently wrote: “Even very effective takedowns and disruptive cyber operations are speed bumps rather than roadblocks. They slow adversaries, but don't stop them.”[14]Against this background, the approach of the draft law is contradictory. Regarding the empirically proven challenges of IT infrastructure in Germany: In its audit report in the summer of 2025, the Federal Court of Auditors described the central and decentralized systems of the federal administration as "still deficient".[15]He recommended strengthening standard measures for IT security and resilience – he didn't say a word about the need for active cyber defense.

The planned expansions of active cyber defense powers are disproportionate given limited personnel resources and a lack of coordination, and they do not address the actual shortcomings in IT security and resilience. Effective protection instead requires strengthening standardized security measures andoperationally capable structures at the operators of the federal IT systems and at the BSI.

2.3 Legal uncertainty and fragmentation

With the allocation of primarily intrusive cyber defense powers to the Federal Criminal Police Office (BKA), a central question has repeatedly arisen in the political process in recent years: constitutional jurisdiction. Public safety is fundamentally the responsibility of the individual states, with the federal government only able to exercise its own powers under specific conditions. Against this backdrop, the necessity of amending the Basic Law (Germany's constitution) should such powers be transferred to the BKA has been emphasized repeatedly.

After the 2025 federal elections, it became clear that the federal government would not achieve the required two-thirds majority in parliament. Instead, it sought ways to circumvent this obstacle. One approach was to distribute the powers among the Federal Police (BPol), the Federal Office for Information Security (BSI), the Federal Intelligence Service (BND), and the Federal Criminal Police Office (BKA). The planned amendments to the Federal Police Act (BPolG), the Federal Office for Information Security Act (BSIG), and the Federal Intelligence Service Act (BNDG) are implemented only at the level of ordinary legislation. However, this "strategy" leads to a significant fragmentation of responsibilities, creates overlaps, and hinders a coherent and efficient cyber defense at the federal level.

[14] Tom Uren (2026): Srsly Risky Biz: Trump's Cyber Strategy... Great, Amazing, The Best Yet
[15] Federal Court of Auditors (2025): Report pursuant to Section 88 Paragraph 2 of the Federal Budget Code on cybersecurity

Even with regard to the amendments to the Federal Criminal Police Office Act (BKAG), the draft bill refers only to changes within the constitutional framework. However, Sections 62c–62e of the draft BKAG grant the Federal Criminal Police Office far-reaching powers: from prohibiting the operation of information technology systems and rerouting and blocking data traffic to intervening in systems by collecting, deleting, or altering data – in each case even without the knowledge of those affected. These measures are not conceived as isolated exceptional instruments, but are systematically integrated into general threat prevention and are linked to comparatively open-ended offenses such as "serious" IT threats or cases of foreign and security policy significance (Section 3a BKAG-E). This is also reflected in the high personnel requirement of over 250 positions by 2030. Even though additional judicial hurdles are foreseen for interventions in private systems, the scope of application is structurally broad. Presenting this as a mere minor correction thus underestimates the qualitative expansion of state intervention powers in the digital sphere. Given the intensity of the proposed measures and their potential scope, the question arises whether an open debate on fundamental constitutional principles – including the question of amending the Basic Law – should be conducted instead of treating the new regulation as a mere adjustment. Furthermore, it appears doubtful that the intervention thresholds stipulated in the draft law meet the requirements established by the Federal Constitutional Court in its jurisprudence regarding interventions in information technology systems or the protection of telecommunications secrecy.

The planned transfer of intrusive cyber defense powers to the Federal Criminal Police Office (BKA) and the expansion of intervention options without an open constitutional debate will lead to a fragmentation of responsibilities and considerable legal uncertainty. Given the scope and intensity of these measures, a fundamental discussion about their constitutional legitimacy is urgently needed.

2.4 Unclear Transparency and Governance

As already emphasized in the preliminary remarks, transparent and effective safeguards are indispensable when security authorities are granted new intrusive powers.[16]However, the current draft bill does not explicitly specify such protective mechanisms.

It remains unclear, in particular, according to which standards and from which sources the Federal Criminal Police Office (BKA) and the Federal Police procure vulnerabilities, exploits, or other technical tools for intrusive cyber defense operations, and how these are subsequently to

[16] Sven Herpig (2018): A Framework for Government Hacking in Criminal Investigations

be managed. Given the considerable risks and the problematic market structure for such capabilities, a significantly higher degree of transparency and regulation would be necessary.[17]

Furthermore, there is a lack of systematic transparency regarding orders, permits, and measures actually implemented. A reporting system analogous to the statistics of the Federal Office of Justice on telecommunications surveillance could remedy this.[18]In particular for measures pursuant to BPolG-E § 41a (7) or BKAG-E § 62f (4), such documentation would be necessary in order to be able to assess the frequency of application, effectiveness and proportionality afterwards.

Since certain measures may be carried out without the knowledge of those affected—such as covert interventions pursuant to Section 62e of the draft Federal Criminal Police Office Act (BKAG-E)—subsequent individual legal recourse is structurally impossible. To compensate for this deficiency, independent oversight mechanisms should be established, for example, by the Federal Commissioner for Data Protection and Freedom of Information (BfDI). Such institutional oversight enables effective review of the measures without jeopardizing the success of the investigation by prematurely disclosing them to potentially involved parties.

Finally, the integrity of the chain of evidence is of central importance in police operations – including in the digital realm. Particularly in light of expanded powers to delete or alter data, such as those stipulated in Section 62e of the draft Federal Criminal Police Office Act (BKAG-E), clear technical standards and governance mechanisms are needed to ensure the traceability and admissibility of digital evidence in court. Such regulations are currently lacking in the draft bill.

The draft legislation expands intrusive cyber defense powers without simultaneously establishing the necessary safeguards, transparency, and governance mechanisms. Significant regulatory and transparency gaps exist, particularly regarding the handling of vulnerabilities, the documentation of operational measures, and the safeguarding of digital evidence. Without appropriate standards, legal uncertainties and risks to transparency, oversight, and the admissibility of evidence in court are likely.

[17] Foreign, Commonwealth & Development Office (2025): The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities and Sven Herpig (2018): A Framework for Government Hacking in Criminal Investigations

[18] Federal Office of Justice (2025): Statistics on telecommunications surveillance for the year 2023 published

3. Recommendations

Introduce systematic evaluation: Every cyber defense measure should document measurable security gains. This allows for transparent justification of political and operational decisions. Only on this basis can effectiveness and necessity be realistically assessed.

Proportionate measures: Intrusive interventions should be limited to the necessary minimum. Efficiency, effectiveness, and escalation risk must be examined, risks of collateral damage and tool proliferation assessed, and the costs of active cyber defense weighed against the risks of inaction.

To create constitutional clarity: Responsibilities between the federal government and the states must be clearly defined. This requires an open and fundamental debate about the powers of the Federal Criminal Police Office (BKA) and, if necessary, an amendment to the Basic Law (Constitution).

Establish an operational platform: All relevant authorities must be able to plan and coordinate operational measures on a common level. This is the only way to avoid duplication of structures and achieve efficiency gains.

Ensure coordination: Uniform coordination and conflict resolution mechanisms between the Federal Criminal Police Office (BKA), the Federal Police (BPol), the Federal Office for Information Security (BSI), the Federal Intelligence Service (BND), and the state police forces are necessary. This clarifies responsibilities and prevents fragmented procedures.

Increase personnel capacity: The BSI's threat hunting and incident response teams should be significantly expanded. At the same time, operational capabilities must be strategically strengthened to effectively enhance IT security and resilience.

Strengthening transparency and safeguards: For intrusive cyber defense powers, clear rules should be established for the procurement, use, and management of vulnerabilities, exploits, and technical tools, and a regular reporting system for ordered, approved, and implemented measures should be implemented. In addition, binding technical standards and governance mechanisms are needed to ensure the integrity of digital evidence and its admissibility in court; where applicable, relevant guidance should be included in the legislative consequences.