

2026

GERMANY RESHAPES ITS INTELLIGENCE APPARATUS



• PAX[®] •
CONSULTING

Pax Consulting

27-10-2026

Index

1. INTRODUCTION 2

2. MAIN TOPICS ADDRESSED 3

2.1 Controversial topics. 3

2.2 Expert voices..... 10

3. COMPARISON WITH OTHER EU INTELLIGENCE ACTS..... 14

4. CONCLUSIONS 28

SOURCE REGISTER 31

1. INTRODUCTION

Germany is facing an important change which involves the intelligence agencies of the country. Germany counts on the security service (BfV) and the external intelligence agency (BND). The BND is also in charge of SIGINT. At the same time there is a military counterintelligence agency (MAD).

The BND has always had an important presence abroad and has been an important partner for the European intelligence agencies. **Despite its size and human resources, the BND has always been limited by legal constraints.** It has always been painful to organise combined operations with the BND, due to difficulties created by legal limitations imposed by legislation. The BND was very much appreciated by its technical capabilities more than the traditional tradecraft.

The BfV was very much focused on the control of far right and far left movements.

The BND was very prolific in terms of producing a great deal of papers which were really flooding organisms such as the European Union Intelligence and Situation Centre (EU INTCEN). **Its analysis capabilities were outstanding although its human assets were scarce.** A country with a population of 80 million citizens and the financial leading force of the EU was not at the spearhead of the intelligence environment.

The BND miserably failed in detecting the Russian invasion. Anti-Americanism sentiment was at the heart of the failing forecast because it fogged its analysis.

After Chancellor Merz won the elections, the intelligence apparatus started to be reshuffled. At the helm of the BND, he appointed the former German Ambassador to Ukraine, Martin Jäger, which is a declaration of intentions.



In addition to that appointment, he moved the former vice president of the BND, **Philipp Wolff**, to become the coordinator of intelligence affairs at the chancellery. In that post, he leads and oversees the profound changes in the intelligence environment in Germany, required to improve its capabilities and play the role at the heart of the EU that Germany deserves and its expected leadership.

The proposed text (over 600 pages) is being discussed at the *Budestag*. **The bill has not been passed yet.** It's being quite controversial and there will be changes to the text. But in general, we can get an idea of the changes.

The act deals mainly with the BND and the BfV. The MAD is marginally affected by the text.

2. MAIN TOPICS ADDRESSED

As mentioned above, legal constraints were painful for joint operations to be carried out. In a world where cooperation is key in order to prevent all types of transnational threats –and nowadays almost every threat is transnational– , working with the BND was slow and agencies were ready to receive limited cooperation.

Asking for additional information on any topic to the BND was expected to be delayed and limited. The internal process to clear the shared information required to be audited at several instances and approved by the management.

As some members of European intelligence agencies put it, dealing with the BND was a fire-and-forget issue. You requested something but you had to forget about it until the BND decided to react, to avoid frustration.

In the end, some kind of sclerosis settled down in the DNA of the agency. **The act pretends to remove the hurdles that hamper the flow of activity.**

But it also shows that the German political elite is aware of the importance of the tasks addressed by the intelligence agencies when decision making is at stake.

2.1 Controversial topics.

Main topics that have raised awareness among political parties are:

Controversial capability	BfV – domestic constitutional protection	BND – foreign intelligence	MAD – military counterintelligence
1. Covert sabotage, deception and alteration of information	New. §§59–62 authorise specified covert protective measures: impairing instruments, altering/blocking communications , providing	New. §§49–51 authorise active intervention against specified foreign-power threats, principally abroad, with restricted domestic	No equivalent general regime added. Existing §§17 and 21 concern narrowly defined cyberattack investigatio

	false information and deleting/falsifying threat-related data. This is the closest Stasi-method comparison in the proposal.	action. Separate cyber-defence intervention powers also appear.	n and provider assistance/removal of attack tools; they are not the BfV/BND's broader sabotage/deception regimes.
2. Full intrusion into private computers and phones	New express framework. §§25–26 distinguish full private-system intrusion from bounded access, with different thresholds. Full intrusion carries stronger danger, necessity and subsidiarity requirements.	Expanded. §§37–39 extend the specific intrusion framework beyond foreigners abroad to Germans and persons in Germany, subject to differentiated conditions and domestic cross-border requirements.	No equivalent new full remote-search regime added. Existing §16 covers specified consensual inspection or media already in MAD custody; §17 permits limited extraction of cyberattack traces.
3. Covert home entry and dwelling surveillance	New express entry provisions and revised surveillance rules. §§16(6), 27 and 60(4). Dwelling surveillance requires Federal Administrative Court approval;	Recast/differentiated. §29 regulates dwelling surveillance, with additional safeguards for homes in Germany and German nationals' homes abroad. §97(6) provides the	Existing dwelling-surveillance power retained. Current §11, with judicial authorisation under §§22 and 45, is not materially expanded by Article 5.

	protective entry uses the specified UKRat route.	relevant judicial route.	No equivalent new protective-entry regime is added.
4. Telecommunications interception and access to encrypted communications	Recast and differentiated . §22 regulates interception; §§25–26 govern relevant IT access. Source interception itself already existed through G10.	Reorganised and expanded in specified respects. §§30–35 restructure strategic/targeted interception and domestic-data exceptions. This is not a general permission to intercept all domestic communications.	Directly affected, principally recast. New §§18–18a replace G10 incorporation with detailed interception and carrier-assistance rules. Source interception of ongoing and specified post-order stored communications is expressly reproduced; it is not wholly new.
5. AI profiling, predictive assessments and biometric searching	New express powers/framework. §§8 and 37 regulate biometric matching, data linkage, personality/behavioural profiles and predictions. Specified analysis can concern people previously lacking an	New express powers/framework. §5 and §§52–53 regulate biometrics, adaptive AI and intrusive analytical products, with differentiated safeguards, particularly for Germans/persons in Germany.	No equivalent detailed new regime added. Existing §4(3) already permits specified automated public-source collection. Article 5 does not

	individual investigation trigger.		transplant the BfV/BND profiling provisions into MADG.
6. Live CCTV access and vehicle-location information	Expanded. §§11 and 15 establish broader commercial-data access, including vehicle telemetry, and compulsory access to specified external CCTV feeds and recordings.	Expanded. §§11–16 provide public/private CCTV access and broader provider duties, including vehicle-related information.	Partly already existing. Vehicle-manufacturer location requests exist under current §20. Own-premises CCTV exists under §25. No comparable new compulsory external live-CCTV regime is added here.
7. Recruiting 16–17-year-old informants	New exception. §18 permits leadership-approved adolescent recruitment where indispensable for specified especially serious extremist threats, with additional care requirements.	New exception within revised source rules. §23 allows exceptional adolescent recruitment under its stated conditions.	Already existing. Current §13 already permits leadership-approved recruitment from age 16 under higher thresholds. This proposal does not introduce that exception.
8. Recruiting parliamentary members	Ordinary extremist-source exclusion remains. §18	Expanded recruitment flexibility. §23 permits specified	Existing exclusion retained. Current §13(1), no.4

or their staff	retains the exclusion. The distinct counterespionage position should not be confused with a newly introduced general exception.	leadership-approved exceptions concerning parliamentary members/staff, making this particularly sensitive institutionally.	excludes parliamentary members/staff; Article 5 does not change it.
9. Physical force, searches, seizure and limited holding	Expanded in specified contexts. §28 adds operational protection; §§63–65 revise premises/protective powers. Some premises searches, force and drone countermeasures already existed.	Expanded protective powers. §§104–124 include security areas, identity checks, limited holding/search/seizure and force. These are restricted protective powers, not a general political-arrest mandate.	Existing powers retained. §§25–26 already provide premises checks/searches, seizure, device examination and specified physical force/restraint. Article 5 does not comparably enlarge them.
10. Longer dossiers and children's data	Expanded. §§36–40 remove the equivalent blanket under-14 database prohibition and lengthen certain retention periods, while retaining necessity/deletion duties and child-specific safeguards.	Expanded/revised. §§55–56 provide child-specific rules and a general periodic review interval of up to 15 years, with exemptions. That interval is not a universal deletion deadline.	No equivalent general expansion added here. Article 5 principally supplies interception-specific processing rules, including review under new §18(6); it does not

			transplant the BfV/BND general retention regimes.
11. Oversight, urgency, notification and ability to challenge operations	Substantially changed. §69 transfers broad operational legal/privacy supervision to UKRat. Prior review expands for specified measures, alongside urgency provisions and notification exceptions.	Substantially changed. §§97–103 and UKRatG redistribute review, notification and redress. UKRat’s remit expands, while particular access/reporting restrictions remain controversial.	Partly changed. New §22(1a) transfers prior review of §18 mail/interpersonal interception to UKRat; §§23 and 46 change notification decisions and supervision of §18-derived data. Other MAD supervision remains with courts/BfDI.
12. Emergency suspension or relaxation of safeguards	New comprehensive regime. §75 relaxes specified authorisation, notice, documentation, data-management and control requirements during formal tension/defence conditions.	New comprehensive regime. §§125–133 provide differentiated defence, tension and special-finding arrangements, with major derogations from ordinary safeguards.	Already existing. Current §52 already contains emergency derogations, including conditional relaxation of most judicial authorisation requirements and independent privacy control.

			Article 5 leaves §52 unchanged.
13. Removing the ordinary prohibition on deliberately targeting life/bodily integrity	No equivalent derogation. This does not mean BfV officers can never use potentially lethal protective force; that is a separate legal question.	BND-specific exceptional change. §129(4) disapplies §51(3)'s prohibition only in a declared state of defence. It does not establish an ordinary peacetime killing power.	No equivalent amendment. The BND provision is not extended to MAD.

The table can be summarized as follows:

For the **BfV** (Germany's domestic intelligence agency), the biggest worry is that its combined powers start to look like those of a secret police force. Beyond intruding into people's private lives and building detailed personal profiles, the agency can secretly step in to interfere with someone's activities under the label of "protection," such as quietly disrupting an event or warning third parties. Because these interventions happen entirely behind the scenes, the person affected often has no idea the agency is involved, making it nearly impossible to discover the operation or challenge it in court.

For the **BND** (Germany's foreign intelligence agency), the central controversy comes down to how far its powers are being stretched both abroad and at home. Instead of just passively gathering information overseas, the agency is moving toward taking active, hands-on operations abroad, while also being granted specific permissions to operate and collect data inside Germany despite being a foreign spy service. Additionally, the law includes extreme exceptions for a military "state of defence," which would drastically strip away normal legal limits and privacy safeguards during a wartime emergency.

For the **MAD** (Germany's military intelligence service), the actual changes in this proposal focus on wiretapping communications, forcing phone and internet companies to assist with surveillance, and

updating how the agency is supervised. The agency already holds other controversial powers—such as recruiting minors under 18 as informants, tracking people, and stepping in with emergency or protective measures—and while those existing capabilities still deserve tough scrutiny, they are already on the books and should not be mistaken for new powers created by this reform.

2.2 Expert voices

Some relevant individuals related to the German intelligence community have been vocal regarding the following topics:

Person / connection / date / stance	Specific criticism	Change advocated / qualification / primary source
Hans-Georg Maaßen Former BfV president (2012–2018), speaking personally. Statement 11 October; hearing 12 October 2026. Opposes the draft's fundamental direction.	Expanded BfV powers would compound an overly political observation mandate, public stigmatisation and executive dependency. Objects to active domestic measures, minor-source exceptions and weakened emergency safeguards.	First restrict the BfV to terrorism, sabotage and espionage; protect lawful political activity; prohibit party/political-person monitoring and political publicity; provide institutionally independent leadership. Retain separate G 10 protection and delete specified BfV intervention/minor-source provisions. His allegations of political misuse are attributed views. Written testimony 21(4)233F, especially printedpp 4,14–15,31–35; official PDF adds cover page Author PDFpp 4–5,14–15,31–35;

		official PDF physicalpp 5–6,15–16,32–36
Markus Löffelmann HS Bund, BND/intelligence-training department; security-law professor. Statement 8 October; hearing 12 October 2026. Calls reform overdue but raises substantial objections.	Automated OSINT/biometrics need clearer, higher thresholds. Active BND capabilities leave too much to executive definition and basic-order review. Emergency activation, lost oversight/documenta tion and defence- case powers raise constitutional risks.	Specify intrusive automated- collection thresholds; require parliamentary decisions on new active capabilities and operation-level review; strengthen emergency legitimacy/time limits and preserve meaningful rights/control. Raise the threshold for deliberately collecting purely domestic communications. This is personal expert testimony, not an official BND position. Written testimony 21(4)233A Printedpp 3–4,32–33,37–38,42–46 (official PDF physicalpp 4–5,33–34,38–39,43–47)
Gerhard Conrad Former senior BND officer and former EU INTCEN director; GKND board member. Paper 20 September; web publication 21 September 2026. Strong supporter with	The response is late; complex interlocking law could hinder speed and legal certainty. UKRat expansion needs personnel/equipment and may delay practical implementation.	Implement promptly with workable instructions and decision schemes, trained personnel and adequately resourced oversight. These are implementation objections, not opposition to active powers. The operative statutory text, rather than

practical reservations.		his interpretation of emergency exceptions, governs Table 1. GKND statement on the BNDG draft, 20 September 2026 PDFpp 3–4 (late response/practical complexity), p 8 (UKRat resources)
Jan-Hendrik Dietrich MISS programme head, HS Bund; CISS co-director, University of the Bundeswehr Munich. October 2026 written evidence and 12 October hearing. Supporter with institutional reservations.	UKRat's mixed judicial/administrative leadership, subordination of administrative control, political consent over internal rules, presumptive urgency and qualification routes may impair independent expert scrutiny.	Separate control functions under appropriate full-time judicial/administrative leadership; remove subordination/political approval of internal rules; revise urgency and strengthen relevant expertise, including deleting the ex-G 10 eligibility route. His criticism concerns design, not rejection of stronger lawful capabilities. Written testimony 21(4)233E Printedpp 5–10 (official PDF physicalpp 6–11)
Gunter Warg HS Bund intelligence-training professor. Statement 9 October; hearing 12 October 2026.	Vehicle telemetry can create intrusive movement/personality profiles at low thresholds without prior independent review. Safeguards for openly obtained	Require stronger telemetry safeguards and UKRat precontrol; extend private-IT processing restrictions to openly obtained device data;

Supports the overall BfV structure with specific reservations.	private-device data are incomplete; training needs are understated.	clarify preliminary-check deletion and finance additional teaching/training. Support for the general architecture should not obscure these targeted criticisms. Written testimony 21(4)233C Printedpp 14–18 (official PDF physicalpp 15–19)
Erich Schmidt-Eenboom Intelligence author/researcher, Forschungsinstitut für Friedenspolitik . External analyst, not a former service chief. Original ntv interview 23 September 2026.	Offensive BND teams may be penetrated by Russian counterintelligence ; unilateral cyber operations risk escalation. Building BND military-style structures may duplicate existing capabilities.	Concentrate the BND on foreign technical/human intelligence; use existing military special forces for military operations and coordinate cyber responses with allies. These operational judgments are his assessments, not independently established comparative findings. Original interview by Lea Verstl,ntv Web interview questions 1–9

Criticism focuses on **preserving the democratic behaviour of the agencies above any other consideration**, being very vocal against any capability which remotely resembles the ways of the GESTAPO (law enforcement agency with intelligence mandate) or the STASI (intelligence agency with law enforcement mandate). Two different historical times which haunt the German nation in its roots.

3. COMPARISON WITH OTHER EU INTELLIGENCE ACTS

The EU intelligence agencies have a distinctive role different from the one played by law enforcement agencies. This is the result of a historical evolution but also the translation of the political separation of powers to the world of security. And it is vital for the preservation of the functioning of liberal democracies. It's key to maintain this strict divide to keep Western democracies far from turning gradually into Russia, Cuba or Iran among others.

In political polarised times as the current ones, keeping this in mind is pivotal because intelligence agencies and law enforcement agencies will push in that direction. We can see this move, still gentle, in the acceptance of prospective investigations by intelligence agencies in The Netherlands for instance, where a referendum was held –Dutch population rejected the move– but it was disregarded after minor changes to the law to grant those powers to the Dutch intelligence community. Dutch government –at the time led by the current NATO Secretary General, Mark Rutte– passed a bill that allowed AIVD and MIVD to carry out prospective investigations¹. Just, “let's see what we find there” suffices to open an investigation. **Dutch police already enjoyed partly these powers.**

These movements push other agencies (not only in the intelligence environment but also in the law enforcement) in Europe to long for the same capabilities as their partners, just to compete with the same powers. It's a human feature, difficult to contain, to tame. It requires vision, imagination and innovation to perform better with less. And it is not effortless. Oversight becomes critical.

The comparison of the new proposed German act with the British and Spanish intelligence acts, broadly speaking, equals the capabilities to theirs. The British enjoy, loosely speaking, more room to act in some areas than the Spaniards but both agencies revolve around the same

¹ The Dutch referendum of **21 March 2018** concerned intelligence-service powers under the Wiv 2017. It produced an advisory rejection: **49.44% against, 46.53% in favour and 4.03% blank**, with **51.54% turnout**. Following additional safeguards announced on 6 April, the law's main provisions entered into force on **1 May 2018** under Rutte. Police exploratory investigations under Article 126gg of the Code of Criminal Procedure had already been authorised from **1 February 2000**, while specified terrorism-related powers based on indications rather than reasonable suspicion took effect on **1 February 2007**; both predated Rutte's premiership. ([Electoral Council](#); [government response](#); [police legislation](#); [Public Prosecution Service](#)).

principles and controls. The new German act brings the German services to the very same room.

The Spanish CNI is an integral service. It means that **the CNI acts as security service, external service and signal and cyber intelligence service**. In the UK the signal and cyber intelligence service, the GCHQ, is an independent agency. As they represent a different architecture the comparison seems relevant.

The comparison CNI-German intelligence community:

Domain	Proposed German framework	Spanish CNI framework	Assessment
Active disruption and interference	BfV §§59–62 permit specified covert protective measures, including interference with threat instruments, communications and data. BND §§49–51 permit active measures against qualifying foreign-power threats, including constrained domestic action. Necessity, proportionality and additional conditions apply. D1 pp 60–63, 127–129.	CNI may prevent, detect and enable neutralisation of specified threats. This is a broad functional mandate. The act does not expressly enumerate the German catalogue of covert impairment, deception and data alteration; specific action remains subject to legal authorization. ES1 arts 2, 4(b); PDF pp 4–5.	Germany has a clearer and more extensive express statutory basis for these active methods. This is a major expansion relative to Germany's present framework. Spanish statutory silence does not establish that every analogous CNI operation is unavailable or unlawful.
Approval before	The draft generally requires	Home inviolability and	The German urgency provisions

intrusive action	independent approval for specified serious intrusions. UKRatG §31 permits immediate execution where delay would defeat or substantially obstruct the purpose, with immediate submission and subsequent review. Special home-surveillance provisions involve the Federal Administrative Court and also contain an urgency route. D1 UKRatG §31 pp 204–205; BVerfSchG §34 pp 41–42; BNDG §97.	communications secrecy require prior authorisation by the designated Supreme Court magistrate on a reasoned written application. The ordinary decision deadline is 72 hours, reduced to 24 hours for justified urgency. That urgency rule does not permit CNI to begin before approval. ES1 art 12; ES2 sole article 1–3.	confer greater freedom to commence covered action before independent confirmation. The German normal approval rules still matter. Spain's prior-judge requirement covers the specified rights; it is not prior judicial approval of every covert method.
Duration and renewal	BfV: listed interception up to one year; full private IT intrusion six months; dwelling surveillance one month. BND: strategic orders up to 36 months; §37(2) private IT intrusion	The special judge may authorise home interference for up to 24 hours and communications interference for up to three months, renewable for equal periods where necessary. These are	Germany reduces renewal frequency for some comparable communications measures. Its 36-month strategic regime has no directly equivalent detailed rule in these

	up to twelve months, but §37(3) against Germans or persons in Germany six months. Orders are renewable. D1 BVerfSchG §33(4) p 40; BNDG §§46–48 pp 124–127.	individual authorisation periods, not lifetime limits on surveillance. ES2 sole article 2(d).	Spanish acts. The differing categories prevent a universal duration ranking.
Hacking and compelled technical access	BfV and BND receive detailed powers for forms of private IT intrusion and provider assistance. The draft expressly addresses data from transport, payment and vehicle-related services and access to camera systems, with conditions varying by method. D1 BVerfSchG §§11–15, 23–27; BNDG §§7–17, 37–39, 60.	CNI has broad collection and strategic signals functions and may request necessary public and private collaboration. The acts do not supply a comparable detailed catalogue of compelled live camera access, telemetry or graded computer-intrusion powers. Relevant home and communications interference requires judicial authority. ES1 arts 4–5, 12; ES2.	Germany gains more explicit authority and clearer statutory compulsion in named areas. This does not prove CNI lacks sophisticated hacking or other technical capabilities; sparse public regulation can itself leave important legal questions unresolved.
AI profiling and	The draft expressly regulates biometric	Ley 11/2002 predates modern AI systems and	Germany would have a more explicit and extensive

integrated data	comparisons, automated analysis, profiling and certain automated responses. These provisions primarily concern BfV and BND, with purpose and threshold requirements. They do not import the entire package into MAD. D1 BVerfSchG §§8, 37; BNDG §§5, 52–53.	contains no comparable method-specific architecture. General intelligence functions, legality and rights protections still apply. Absence of an express AI chapter is not a statutory prohibition on every automated analysis tool. ES1 arts 1–5, 12.	public basis for named analytic methods. The texts alone cannot determine whose operational data access, systems or practical analytical freedom are greater.
Coercion and protection of premises	BND §§104–124 create a detailed protective regime, including security areas, identity checks and specified detention, search, seizure and force powers. BfV also has separate agency-security powers, including restricted force and restraint; these differ from its covert-	CNI staff generally lack the status of agents of public authority, with an exception for protection of CNI personnel and installations. The act also permits service-related weapons licensing under the law. ES1 art 5(3)–(4); PDF p 5.	BND obtains more detailed express coercive authority for protective purposes. Spain already has a protection exception. Neither provision should be represented as an unrestricted domestic police mandate.

	intervention regime. D1 pp 165–177; BVerfSchG §§59–65.		
Legal protection for officers and sources	Lawfully authorised conduct can be justified under German law. The explanation of BND §51 expressly treats active-operation authority as criminal-law justification for BND and mission participants. Separate §23 source rules provide conditional justification and limited non-prosecution. Conduct outside the powers is not thereby protected. D1 BNDG §§23, 51; explanation pp 561–562.	The CNI acts contain no general liability exclusion. General criminal law nevertheless exempts conduct in lawful fulfilment of a duty or legitimate exercise of a right, profession or office. Secrecy or cover identities alone do not justify unlawful conduct. ES1 art 2; ES2; ES5 Penal Code art 20(7).	Germany codifies legal protection for authorised intervention and particular source conduct. This matters to operational confidence, but neither legality within a statutory power nor secrecy proves practical impunity. A blanket comparison of German immunity against Spanish liability would be misleading.
Secrecy oversight and remedies	UKRat provides specialised independent legality review and audit; courts and parliamentary	The act classifies extensive operational information. Congress scrutiny excludes	Spain already has substantial opacity, so weaker German accountability cannot be assumed.

	control remain relevant. The draft also contains notice, access and audit exceptions. Restrictions on source identities do not exclude all operational material from all oversight. D1 UKRatG §§13, 26, 32–38; BVerfSchG §35; BNDG §§100–103.	sources and means and protected foreign-service information. Ordinary courts, the Ombudsman and judicial review of declassification on refusals provide further controls. There is no routine post-surveillance notification mechanism. ES1 arts 5(1), 11; ES3–ES4.	Germany's independent audit architecture is an important counterweight. Secrecy and lack of notice can hinder remedies in both systems; practical effectiveness requires evidence beyond the legislation.
BND exceptional situations	BND §§125–133 permit specified derogations in tension, defence and defined urgent cases. In a declared defence case, §129(4) removes the ordinary bar on deliberately targeting life or bodily integrity in relevant active operations, and a domestic competence restriction. §132 relaxes audit and	Neither of the two public CNI acts contains a directly comparable self-contained intelligence emergency package. Spain has separate constitutional and emergency rules which these attachments do not exhaust. ES1–ES2 complete texts.	This is a particularly serious express German expansion. It applies chiefly to BND and depends on the statutory emergency trigger. It does not establish a peacetime licence to kill or prove Germany has broader wartime freedom than Spain under every

	specified approval safeguards. Other legal constraints remain. D1 pp 177–182.		applicable law.
--	--	--	-----------------

The comparison between the German and British intelligence communities:

Domain	Proposed German framework	British framework	Assessment
Correct service and executive control	BND remains under the Chancellery, BfV under Interior and MAD under Defence. Foreign intelligence, domestic constitutional protection and military security remain distinct. D1 Art 1 §1; Art 2 §1; Art 5.	MI6 and GCHQ fall under the Foreign Secretary; MI5 under the Home Secretary. MI5's statutory basis is the Security Service Act 1989, absent from the attachment. MI5 has no arrest or detention power. UK1 §§1–4; UK2; UK10.	No general German advantage follows from ministerial dependence. Compare BND with MI6/GCHQ and BfV with MI5. MAD requires its own power-specific assessment.
Active foreign operations	BND receives express powers against qualifying foreign-power threats, subject to conditions, proportionality and ordinary harm	MI6's functions already include non-collection tasks relating to persons outside the British Islands. The National	No demonstrated German superiority. Explicit German drafting would authorize functions Britain already

	restrictions. UKRat approves the basic operational framework; this is not automatically approval of each individual operation. D1 BNDG §§49–51, 97(2); explanation p 560.	Cyber Force, combining GCHQ, MOD and MI6 capabilities, officially describes covert disruption of communication s and technology and influence operations. UK1 §1(1)(b); UK11.	exercises under its own legal framework. BND's UKRat approval is also a meaningful check compared with the ministerial section 7 route, although technique-specific UK controls can additionally apply.
Domestic disruption and police separation	BfV §§59–62 authorize covert intervention against specified terrorist or systematic foreign-power threats, with conditions and UKRat review. Section 59 bars direct coercion against people. Separate §§63–65 permit restricted agency-security search, restraint, seizure and force, including	MI5 protects national security and can use relevant covert-source, surveillance and investigatory powers. It lacks a general arrest power and normally works with police for coercive enforcement. The supplied ISA alone cannot establish the extent of MI5 disruption authority. UK2; UK10; UK4.	The German draft gives BfV a particularly explicit standalone intervention regime. This textual difference does not prove BfV would be freer overall than MI5. A catalogue comparison must include MI5's companion legislation and police cooperation.

	narrowly conditioned weapons use. D1 BVerfSchG §§59–65.		
Ordinary interception and hacking approval	Specified serious intrusions require UKRat or, for designated dwelling surveillance, Federal Administrative Court approval. Requirements depend on the method and target category. D1 BVerfSchG §§33–34; BNDG §§46–48, 97.	Targeted intelligence interception and equipment-interference warrants normally require an executive decision plus approval by a Judicial Commissioner, assessing necessity and proportionality. This is the double lock. It does not apply identically to every covert operation or every ISA section 7 authorisation. UK3; UK5–UK6.	Both systems impose independent control over major intrusive techniques. A general claim that Germans could act freely while Britain always needs a judge would be incorrect. Compare the precise warrant and operation.
Urgency before independent approval	UKRatG §31 permits immediate execution followed by immediate submission. Its three-working-day period runs from submission;	Urgent targeted interception and equipment interference, including bulk equipment interference, may begin without prior Judicial	Both frameworks permit some action before independent review. The German submission trigger and continuation provision may give more

	the Council can permit continuation pending a prompt decision where it has no serious legality doubts. Separate judicial urgency rules apply to designated home surveillance. D1 pp 204–205; BVerfSchG §34.	Commissioner approval. Review is due within three working days following issue; initial validity is five working days. Bulk interception requires prior approval. UK5–UK6.	flexibility than the specified UK urgent-warrant timetable. That comparison does not apply to all powers or replace separate statutory requirements.
Duration of authorisations	BfV's listed interception orders may last one year; its full private IT intrusion six months. BND strategic orders may last 36 months. Under §48(3), §37(2) private IT intrusion may last twelve months; the six-month exception concerns §37(3) against Germans or persons in Germany.	Normal targeted and bulk interception and equipment-interference warrants generally last six months, renewable. A minister-signed ISA section 7 overseas authorisation also lasts six months, renewable; its urgent senior-official route has separate five-working-day validity.	Germany allows less frequent renewal in particular categories, especially strategic collection. A longer warrant does not itself authorise a broader mission or remove necessity, proportionality, supervision or termination requirements.

	D1 BVerfSchG §33(4); BNDG §§37, 47–48.	UK1 §7(5)–(8); UK5–UK6.	
Bulk collection and AI	BND strategic collection and BND/BfV automated analysis, biometrics and profiling are expanded or made more explicit. Some automated defensive responses are expressly addressed. D1 BNDG §§30–35, 52–53; BVerfSchG §§8, 37.	The IPA already provides targeted and bulk powers. Its amended Part 7A covers datasets attracting low or no reasonable expectation of privacy: agency heads authorise, with Judicial Commissioner category or individual approval. A dataset inside an approved category needs no fresh individual approval. The code permits machine-learning development. UK3; UK7.	No general German advantage is established. Britain already has extensive collection and analytic powers and streamlined approval for some datasets. Data categories, privacy thresholds and actual access must be matched before ranking reach.
Express protection from UK liability abroad	BND §51 authorises active measures. Its explanatory memorandum says this also justifies covered conduct under criminal law, including conduct by	ISA §7(1)–(4) expressly excludes UK criminal and civil liability for conduct covered by a valid overseas authorisation. It can cover specified	Both systems can protect conduct within valid authority. Britain states the UK civil/criminal exclusion expressly; Germany uses substantive operational

	mission participants and assisting third parties. Sources used for these operations can be covered by §51 without reliance on §23. D1 BNDG §51; explanation pp 561–562.	acts, classes of acts or operations and persons. Conditions include proper functions, necessity, reasonable consequences and safeguards. UK1 §7; PDF pp 7–9.	powers and justification . Wording alone cannot rank protection. Neither creates immunity for acts outside its scope or changes host-country law. [UK12]
Sources authorised to commit crimes	BND §23 provides conditional source justification and limited discretionary non-prosecution. BfV and MAD have their own source provisions; the BND overseas rule must not be transferred to them. D1 BNDG §23; BVerfSchG §§18–19; Art 5 and MADG source rules.	RIPA §29B permits authorisation of specified criminal conduct connected with a covert source. Section 27 gives lawfulness only within the entitlement and authorisation . Necessity, proportionality, non-criminal alternatives and Human Rights Act requirements apply. UK4 §§27, 29B.	Britain already supplies substantive legal protection in this sensitive field. Neither regime creates unrestricted immunity for all source activity. No German superiority follows simply from a German justification clause.
Assisting overseas wrongdoing	No general German immunity should be inferred from	National Security Act 2023 §30 inserted Serious Crime	This additional, limited British protection

	liaison cooperation or a statutory intelligence mission. Each applicable justification, offence, individual act and legal constraint must be examined. D1 BNDG §§23, 49–51 and cooperation framework.	Act 2007 §50A: a defence to specified extraterritorial encouraging or assisting offences for conduct necessary to proper intelligence functions, subject to arrangements and evidential requirements. It is not a defence to every offence. UK13.	further undermines a blanket ranking of Germany as more legally immune. The exact offence, authority and defence determine protection; the statutory mission alone does not justify every act.
Oversight notice and enforceable remedies	UKRat supplies independent control, audit and review mechanisms. Notice and access exist for specified measures with exceptions. Ordinary judicial remedies must be considered separately; UKRat is not simply a substitute label for an ordinary court. D1 UKRatG §§26, 32–38;	IPCO oversees powers; the IPT can award compensation, quash authorisations and require records destroyed, with qualified appeals. IPA §231 notification concerns serious harmful errors, not every lawful surveillance target. Parliamentary ISC scrutiny also has operational and executive	Neither system can be described as free of accountability. Britain has concrete judicial remedies; Germany has important independent controls. Both restrict disclosure. Actual impunity requires evidence of how investigation, disclosure and sanctions work in practice.

	BVerfSchG §35; BNDG §§100–103.	secrecy filters. UK8–UK9; UK3 §231; UK6.	
Defence and emergency provisions	BND §§125–133 contain express derogations. In declared defence, §129(4) disapplies the ordinary deliberate life/body- targeting prohibition for relevant active measures; §132 removes specified review safeguards. It does not abolish every court control or proportionali ty. D1 pp 177–182.	ISA 1994 contains no directly matching self- contained emergency chapter. British military operations, emergency powers and the full body of public and international law extend beyond that act. Overseas authorisation under §7 remains a separate ordinary framework. UK1 complete text.	The German chapter is a serious additional source of latitude within its triggers. The supplied statutes cannot support a complete comparison of wartime force or a conclusion that Germany gains a uniquely unrestricted power to kill.

4. CONCLUSIONS

As stated before, German intelligence community needed an update and be released of the self-imposed chains which were limiting its capabilities.

Although the bill will suffer some changes, the German intelligence community will be in better shape to compete and develop its capabilities which will take them to higher levels of performance. **The German governments will count on better insights to make better decisions.**

German intelligence community will get **better access to exclusive information which will provide it with self-reliance and independence.**

But it will not happen overnight. The bill will allow fresh air into the room, but **it will take time and some failures** before the enriched air will be naturally accepted by the lungs. Lungs will have to adjust to new capabilities and how to manage them as well as the proactivity will require adjustments to new responsibilities and dangers which the services will face for the first time.

Intelligence is not a science. It is a tradecraft which means it is learnt by doing. Recruiting assets, carrying out surveillance, building up a front company as a cover, to name a few, can only be perfected by doing. Any agency requires time to master the tradecraft. In the meantime, failures happen. And this tradecraft must be constantly updated, or you will find yourself out of the business. **To play in the premier league requires constant training, investment, innovation and determination.**

The bill is just the first step to introduce the German intelligence community into a thrilling world in constant movement.

Having said this, mentioning the recruitment of teenagers in such a bill might be considered unnecessary. In the same vein, the validity of providing false information to participants in a threat or falsify stored information for purposes of that threat might ruffle the feathers of lawmakers.

Candidly speaking, every intelligence agency does all of it. A minor might be key in some cases (think of a youngster with hacking capabilities or a teenager recruited to infiltrate a far-right group). False information provided to an asset of the GRU is a regular way to play in the counterintelligence ground. **It all is done to counter threats with the goal of gathering information.**

But, what's the benefit of exposing intelligence tradecraft in a law? Perhaps the difference is that, once these practices are expressly codified in law, they acquire a legal basis that can be invoked and used in court. And that's where conflict arises because intelligence tradecraft would be confounded with law enforcement powers.

Most citizens are honest, hardworking and do not cross the line to commit a crime. Therefore, they don't feel they are affected by this kind of nuances. However, if one day they are affected, it will be too late to react. What today is legal, a different government may consider it unlawful. And those granted powers which seemed irrelevant to a law-abiding citizen, suddenly are turned against him. It is in the law, and courts only administer and interpret it.

It all relies on the good faith and intentions of those who manage these powers but it's a matter of statistics that among those chosen there will be rotten apples.

As Martin Luther King put it: **"Injustice anywhere is a threat to justice everywhere."**

The Dutch experience in 2018 warrants close scrutiny. The concern lies not only in the powers granted to the intelligence services, but also in the political process through which the referendum result was marginalised and ultimately set aside. Parliament approved measures that voters had rejected, raising broader questions about democratic legitimacy and institutional accountability.

Western democracies often assume that civil liberties are secure by default. They are not: **their protection depends on maintaining rigorous legal, political and institutional safeguards.**

Concerns about the excess of powers granted to the services are legitimate and should always be on the table. Oversight on the services, political and financial, is pivotal to keep services at bay. Human nature cannot be ignored. Western societies must be candid, bold and sincere if genuinely intend to avoid mistakes of the past.



SOURCE REGISTER

- D1** [Supplied German reform draft](#) GE-ND-Reform.pdf, 732 pages. Section references concern the proposed acts, not present law. Physical PDF page numbers are used throughout.
- D2** [Official German parliamentary version and proceedings](#) BT 21/7868 and first reading of 24 September 2026. Different pagination from the supplied draft.
- ES1** [Supplied Spanish CNI Act](#) Spain intel service.pdf, 10 pages; Ley 11/2002, last consolidation update 15 June 2021. Current BOE text checked.
- ES2** [Spanish prior judicial control](#) LO 2/2002, sole article. Prior authorization, decision deadlines, warrant periods and destruction of unrelated material.
- ES3** [Spanish oversight information supplied to the Venice Commission](#) Country information on spyware, including ex-post judicial remedies and notification. A contributor compilation, not a judicial determination.
- ES4** [Spanish Ombudsman review](#) 18 May 2022; the review verified prior judicial authorization in the 18 cases examined. This does not establish the legality of every alleged spyware case.
- ES5** [Spanish general criminal justification](#) Penal Code article 20(7), lawful fulfilment of duties and legitimate exercise of rights, professions or public office.
- UK1** [Supplied Intelligence Services Act 1994](#) UK Intel service.pdf, 16 pages, consolidation as at 25 June 2026; especially §§1–7. Section 7 current text checked separately.
- UK2** [Security Service Act 1989](#) Statutory functions and control of MI5, read with the current investigatory framework.
- UK3** [Investigatory Powers Act 2016](#) Consolidated framework, including 2024 amendments and Part 7A.
- UK4** [Covert source criminal conduct rules](#) RIPA 2000 §§27 and 29B, as amended by the CHIS Criminal Conduct Act 2021.
- UK5** [Interception of communications code](#) June 2025; targeted and bulk warrants, approval, urgency and duration.
- UK6** [Equipment interference code](#) June 2025; especially §§5.83–5.85, 5.99–5.100, 6.30–6.39, 6.49–6.56 and 9.29–9.32.

UK7 [Bulk personal datasets code](#) June 2025; datasets with low or no reasonable expectation of privacy, especially §§4.1–4.9 and 4.25.

UK8 [Investigatory Powers Tribunal procedures and remedies](#) Official account of complaints, compensation, quashing, destruction and appeals.

UK9 [Justice and Security Act 2013](#) ISC functions and executive information filters; §§1–3 and Schedule 1.

UK10 [MI5 official questions and answers](#) Ministerial responsibility, operational role and absence of arrest or detention powers.

UK11 [National Cyber Force operational account](#) Responsible Cyber Power in Practice, 4 April 2023. Institutional account of disruption and influence, not independent proof of every operation.

UK12 [Intelligence Services Commissioner annual report 2014](#) Printed p 23; overseas authorization does not alter host-country law. Applicable Human Rights Act requirements remain relevant.

UK13 [National Security Act 2023 section 30](#) Inserts Serious Crime Act 2007 §50A, a limited defence for identified encouraging or assisting offences.