Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

The new German model of intelligence operations

The German federal government has approved a reform of intelligence legislation that will grant the Federal Intelligence Service (BND) and the Federal Office for the Protection of the Constitution (BfV) significantly broader powers to operate in the digital sphere. The proposal still has to pass the Bundestag, but the direction of the reform is clear.

In strictly defined cases, the BND would be able to penetrate information systems linked to an attack on Germany, copy or delete data, and disable digital assets used in the operation. The BfV would gain wider powers for surveillance and digital investigations within the country.

Berlin is attempting to change how the country responds to operations by foreign intelligence services. The previous model relied largely on detecting threats, collecting data, and forwarding assessments to political leaders, the police, or other competent institutions.

Under the new proposal, when the legal requirements are met, the services would be allowed to participate in terminating the operation itself.

This is particularly important in cyberspace, where a few hours can determine whether an attack remains an attempt or turns into serious disruption of a state institution, a military network, or critical infrastructure.

From surveillance to disrupting attacks

The biggest change concerns active operations in digital systems. The BND would be able to access infrastructure used for a serious operation against Germany and take measures to hinder or stop the attack.

The proposal also includes broader powers to access digital communications, conduct online searches, and use state spyware.

Telecommunications companies, digital platforms, and certain other private entities would, in specified circumstances, be required to provide the data needed for such operations.

> The German government is trying to develop the capability to act in situations where traditional monitoring is no longer sufficient

These powers are not intended as a licence for German cyber attacks abroad. Any serious intervention would require a legal basis, a clearly defined target, and a justification that the measure is necessary and proportionate to the threat.

The German government is trying to develop the capability to act in situations where traditional monitoring is no longer sufficient.

If the services detect that an attack on German systems is being prepared and have the technical means to disrupt it, future legislation should specify when they are permitted to do so.

Security pressure has become tangible

The reform follows several years of increased Russian and other foreign intelligence activity targeting Germany. German institutions publicly warn of cyberattacks, espionage, sabotage, covert procurement of technology and reconnaissance of critical infrastructure.

In July, Germany and France supported the EU's attribution of a long-running cyber campaign to the Turla group, which European institutions have linked to Russia's Federal Security Service, the FSB. Berlin then summoned the Russian ambassador for talks.

> The government spoke openly about the need for the BND to reduce its dependence on foreign intelligence capabilities

For the German services, such an environment creates an operational problem that can no longer be solved simply by exchanging information with partners.

During the summer, the government spoke openly about the need for the BND to reduce its dependence on foreign intelligence capabilities and to match the capacities of leading European services.

This does not mean that Berlin will abandon intensive cooperation with its allies. It means that it wants its own capacity for situations in which the speed of response, the sensitivity of the source or political responsibility leave too little scope to wait for others to do the work.

German history continues to impose constraints

The expansion of state powers in Germany carries a different weight from that in most other Western countries. The post-war security system was designed with strict limitations, precisely because the country had lived through the Nazi repressive apparatus and, after reunification, had direct experience of the East German Stasi.

The separation of police and intelligence functions, judicial control and parliamentary oversight has remained an important part of the German institutional model.

> The BfV operates within German society

That is why the parliamentary debate will be much more intense about the BfV than about the BND. The foreign service works against foreign states, their agencies and threats originating outside the country.

The BfV operates within German society. Wider access to devices, communications and digital systems takes on a very different political significance when the target is someone living in Germany.

The opposition therefore already draws a clear distinction between the need for the BND to receive more funds for work against foreign operations and the risk that the domestic service will be given excessive scope for secret surveillance.

The Constitutional Court set a short deadline

The government is not initiating the reform solely because of the changed security environment.

In 2024, the Federal Constitutional Court ruled that part of the existing rules on the strategic monitoring of international communications, including the monitoring of cyber threats, was not sufficiently aligned with the constitutional protection of the secrecy of telecommunications.

In 2024, the Constitutional Court ruled that part of the existing rules on the strategic monitoring of international communications was not sufficiently aligned with the constitutional protection of the secrecy of telecommunications

The court has temporarily left the problematic provisions in force, but by 31 December 2026 at the latest the Bundestag must adopt a new legal solution.

This gives the reform two tasks that are difficult to reconcile: the services should gain greater operational capabilities, while the law must at the same time define more precisely when they are used, who approves them, and who monitors their legality.

The independent control council, which already oversees some of the most sensitive activities of the BND, should be given a more prominent role in reviewing the new measures. How effective this control will be in practice will be one of the key questions for the final text of the law.

Who decides when the intervention starts

The most sensitive part of the reform will be the boundary between intelligence assessment and operational decision-making.

While the service is monitoring the adversary's infrastructure, responsibility is relatively clear. The moment it decides to delete data, disable a server or disrupt the operation of a system, the consequences extend beyond traditional intelligence work. A diplomatic dispute, material damage or the reaction of another state may follow.

The law will therefore have to specify which measures the BND can authorise within its own chain of command and which require a decision at the political level or by an independent oversight body.

> In the event of a failed assessment, the German government will need to be able to explain who made the decision

That boundary is also important for accountability. In the event of a failed assessment, the German government will need to be able to explain who made the decision, on what data, and with what legal authority. Germany must therefore clearly determine who can approve such an operation and on what basis.

Speed is important, but the decision to enter someone else's system, delete data or stop the operation of infrastructure must rest on a precise legal basis and clearly defined responsibility for the consequences.

The biggest problem is reliable attribution

Cyber operations have one weakness that the law cannot remove: it is often difficult to determine with certainty who actually controls the infrastructure from which an attack originates.

A server may be located in one country, rented through a company in another and compromised without the owner's knowledge. An attacker can use someone else's network, commercial cloud services or third-party computers.

The decision to disable such a system therefore requires a much higher security threshold than the assessment that a particular country is probably behind the campaign.

> Intervention could be interpreted as an unacceptable state cyber operation

The wrong intervention can damage other people's property, destroy evidence needed for subsequent criminal proceedings or cause a dispute with the state on whose territory the infrastructure is located. In more serious cases, it could be interpreted as an unacceptable state cyber operation.

The BND will therefore need to develop a process in which technical attribution, intelligence and legal assessments are verified before an operation moves from surveillance to active interference.

Parliament decides how far services can go

The parliamentary procedure will almost certainly change certain thresholds and processes. The most sensitive powers of the BfV will be subject to detailed discussion, and some measures may require a prior court

decision or the approval of an independent supervisory body.

However, it is unlikely that the Bundestag will revert the reform to its starting point. The constitutional deadline expires at the end of the year, and the political consensus that the German services must be more capable of responding to foreign operations is much broader than support for the current government.

> If the new law is adopted in roughly its current form, the BND could, in such a situation, gain scope to react before damage occurs

The first practical test is unlikely to be a major operation deep inside a foreign government's network. A much more realistic scenario is an ongoing attack on a German state institution, military system or critical infrastructure, in which the service has sufficiently robust data on the origin and the technical infrastructure through which the attack is conducted.

If the new law is adopted in roughly its current form, the BND could, in such a situation, gain scope to react before damage occurs.

Germany is entering a new phase of intelligence work

Germany has already recognised the need for more technologically capable services. The hard part is yet to come: determining how far the BND and BfV can go when they move from surveillance to active intervention, what level of hard evidence is required before a cyber operation, and who controls decisions taken in secret.

If the Bundestag leaves the thresholds for intervention unclear, the first contested case will quickly end up in the courts

The most likely outcome is that the BND will gain broader operational powers abroad, under a more complex system of legal approval and oversight, while the BfV receives a narrower package of new capabilities than the government's proposal currently envisages.

Berlin will try to retain two things at once: the ability to stop a serious operation by a foreign power, and the institutional brakes that have limited the power of the German services for decades.

If that model works, Germany will move closer to its British and French partners in its ability to respond to cyber and hybrid operations, while maintaining tighter domestic controls.

If Parliament leaves the thresholds for intervention unclear, the first contested case will quickly end up in the courts.

The real scope of the August reform will become evident only when the BND receives a case in which there is sufficiently strong evidence of an attack and the technical capacity to stop it. Only then will it be clear how much Berlin has really changed the way its foreign intelligence services operate.