The Shadow War State: How Hybrid Conflict Is Rewriting Germany's Postwar Security Doctrine.

Vladimir Tsakanyan, Ph.D. · Center for Cyber Diplomacy and International Security

October 12, 2026

Germany built its intelligence system around the lessons of dictatorship and the separation of state powers. Eight decades later, cyber operations, sabotage and foreign interference are testing whether that architecture can protect a democracy against threats operating between peace and war.

By Vladimir Tsakanyan, Ph.D. Center for Cyber Diplomacy and International Security (CCD-IS)

The Return of an Uncomfortable Question

Germany is confronting a security dilemma rooted in its own history.

On October 12, 2026, Interior Minister Alexander Dobrindt warned that the country faces a shadow conflict whose objectives extend beyond those associated with the Cold War. Speaking at a Federal Office for the Protection of the Constitution (BfV) conference in Berlin, he described a threat environment intended to destabilize German society and argued that the country's intelligence services require stronger capabilities.

His warning came as Germany's parliament continued examining legislation intended to modernize the legal authorities of its intelligence agencies.

The immediate context includes alleged foreign sabotage, cyber operations, espionage, disinformation and threats to critical infrastructure. German officials have repeatedly identified Russia as a principal source of hybrid threats, particularly since Moscow's full-scale invasion of Ukraine in 2022.

Russia disputes Western allegations of responsibility.

But the significance of Germany's current debate extends beyond any individual foreign adversary.

It concerns a fundamental question of democratic security:

Can a state preserve the constitutional limitations established to prevent the abuse of intelligence power while giving its institutions the operational capabilities needed to confront

persistent threats below the threshold of war?

For Germany, this is not an abstract institutional debate.

It reaches directly into the foundations of the postwar republic.

The Intelligence System Germany Deliberately Built

Germany's modern intelligence architecture cannot be understood without the experience of National Socialism.

The Nazi regime demonstrated the dangers of concentrating political surveillance, police authority and coercive power within institutions operating without meaningful democratic accountability.

After 1945, the emerging West German state developed a constitutional framework intended to prevent the recurrence of such abuses.

The Basic Law of 1949 established fundamental rights, constitutional limitations and mechanisms for controlling state authority.

The intelligence system reflected this philosophy.

The BfV was established to protect the constitutional order against threats including extremism and espionage.

The Federal Intelligence Service (BND), created in 1956, became responsible principally for foreign intelligence.

The Military Counterintelligence Service developed a separate responsibility for threats affecting the armed forces.

These institutions operated within different legal mandates and oversight arrangements.

An especially important principle was the separation of police and intelligence functions, commonly associated with the Trennungsgebot.

The distinction was not merely administrative.

It reflected the conviction that collecting intelligence and exercising coercive police powers should not be combined without safeguards.

Germany's security architecture was therefore deliberately more restrictive in important respects than those of several major allies.

Its limitations were part of its democratic design.

The Cold War Reinforced the Constitutional Model

During the Cold War, West Germany occupied one of the most strategically sensitive positions in Europe.

It stood at the dividing line between NATO and the Warsaw Pact.

Its territory hosted major military forces, intelligence facilities and critical communications infrastructure.

Espionage was a persistent feature of the divided German state.

The East German Ministry for State Security, or Stasi, developed an extensive apparatus of domestic surveillance and foreign intelligence.

West German intelligence institutions operated under the constant pressure of Soviet-bloc intelligence activities.

Yet the Federal Republic did not abandon the constitutional principles underpinning its security institutions.

Instead, its political system attempted to balance effective counterintelligence with judicial oversight, parliamentary supervision and legal limitations.

The experience of German reunification in 1990 further reinforced public awareness of the dangers of uncontrolled surveillance.

Access to Stasi archives exposed the extraordinary reach of East Germany's intelligence apparatus.

The resulting historical memory helped sustain a political culture skeptical of expansive state surveillance.

This legacy remains central to the current reform debate.

The Threat Has Changed Its Form

The security environment confronting Germany in 2026 differs substantially from the Cold War.

Traditional espionage remains important.

But hostile activity increasingly combines multiple instruments.

Cyber intrusions can target government networks.

Sabotage can disrupt transport or energy infrastructure.

Disinformation campaigns can attempt to undermine confidence in democratic institutions.

Drones can threaten airports, logistics facilities and military-related infrastructure.

Covert actors can operate through criminal networks or intermediaries.

These methods can be combined without a formal declaration of war.

That combination is generally described as hybrid activity.

The concept is not entirely new.

States have long used espionage, subversion, propaganda and sabotage.

What has changed is the technological environment in which these activities occur.

Digital connectivity allows disruption to move across borders rapidly.

Commercial infrastructure can become a strategic target.

The distinction between civilian and military systems has become increasingly difficult to maintain.

And attribution can remain uncertain long after an incident has occurred.

The result is a security environment in which a country may experience persistent hostile pressure without entering a legally recognized armed conflict.

The Strategic Problem of the Threshold

Modern deterrence relies partly on identifying actions that justify a response.

An armed invasion is comparatively clear.

A cyber intrusion is not.

A drone discovered near an airport may represent reconnaissance, intimidation, criminal activity or preparation for sabotage.

An unexplained infrastructure failure may be accidental or deliberate.

A disinformation campaign may involve foreign coordination, domestic political actors or both.

The strategic challenge is therefore not simply detecting hostile activity.

It is determining when individual incidents form part of a coordinated campaign.

This distinction matters because different legal and institutional authorities apply to different threats.

Police investigate crimes.

Intelligence agencies gather information.

Military institutions prepare for armed conflict.

Diplomatic authorities manage international responses.

Cybersecurity agencies protect networks.

Hybrid operations exploit the boundaries between these responsibilities.

The state must coordinate across them without eliminating the legal distinctions that justify their existence.

The Leipzig Incident and the Politics of Attribution

Germany's concerns intensified following an attempted attack involving an explosives-carrying drone near Leipzig/Halle Airport in August 2026.

German authorities attributed the incident to Russian-linked operatives.

Moscow rejected the allegation.

The incident became a focal point in Berlin's argument that hybrid threats were becoming more dangerous and potentially more violent.

Its political significance extended beyond the immediate security risk.

An attack against an airport potentially affects civilian aviation, logistics, military support operations and international transportation.

It therefore occupies several categories of national security simultaneously.

The incident also demonstrates the importance of attribution.

Governments must distinguish technical evidence, intelligence assessments and publicly established facts.

An allegation of foreign state involvement may justify diplomatic measures, investigations or security precautions.

But it does not automatically resolve questions of individual criminal responsibility or establish the legal threshold for military action.

In a democracy, the quality of evidence matters as much as the urgency of response.

From Observation to Active Defense

Germany's intelligence-reform debate is partly about the distinction between observing threats and actively disrupting them.

Traditional intelligence functions emphasize collecting, analyzing and communicating information.

Active defensive measures may involve more direct intervention against threatening systems or activities.

In cyberspace, that distinction can become difficult.

A security agency may detect malicious infrastructure.

But should it be authorized to interfere with that infrastructure?

Should it be able to penetrate a computer system to prevent an attack?

What happens if the system is located abroad?

Who authorizes the operation?

Which institution is accountable if an intervention causes unintended damage?

These questions sit at the intersection of intelligence law, cybersecurity policy, constitutional rights and international law.

The German government's proposed reforms seek to strengthen intelligence capabilities in response to an evolving threat environment.

But the legislation remains under parliamentary consideration.

Proposed authorities must not be confused with powers already enacted.

October 12: The Constitutional Disagreement Becomes Visible

The Bundestag's October 12 hearing revealed the central tension.

Some legal experts argued that the proposed intelligence reforms contain excessively broad provisions, particularly concerning strategic intelligence collection, data retention and the conditions governing access to collected information.

Others considered important portions of the proposed framework constitutionally defensible and welcomed clearer statutory thresholds and oversight arrangements.

The disagreement is significant.

It shows that Germany's debate is not simply between those who recognize security threats and those who deny them.

Rather, it concerns the design of lawful security institutions.

How broad should intelligence collection be?

When does data analysis become an intrusion into fundamental rights?

Which authorities require independent approval?

How should intelligence agencies be prevented from assuming functions belonging to police institutions?

What standards of judicial review should apply?

These questions cannot be answered through threat assessments alone.

They require constitutional judgment.

The Digital Surveillance Problem

Cybersecurity has transformed the practical meaning of intelligence collection.

During much of the twentieth century, surveillance was constrained partly by physical and organizational limitations.

Collecting information required personnel, equipment and operational resources.

Digital systems have reduced many of those barriers.

Large volumes of communications data can be collected, retained and analyzed.

Artificial intelligence can identify patterns across datasets.

Automated systems can generate behavioral assessments.

Location data can reveal personal movements.

Metadata can expose relationships even when message contents remain encrypted.

Consequently, modern intelligence reform must address not only what information agencies may collect, but also what they may infer from it.

A database containing individually unremarkable records may produce highly sensitive conclusions when subjected to advanced analysis.

This creates a constitutional challenge that earlier intelligence legislation was not designed to confront at the same scale.

The distinction between collecting data and generating knowledge about individuals is becoming increasingly important.

Germany's Security Debate Is Also an AI Governance Debate

Artificial intelligence adds another dimension.

AI systems can support the identification of cyber threats, suspicious behavior and potential foreign interference.

They may improve intelligence analysis and accelerate the detection of coordinated activity.

But they can also produce errors.

A statistical association is not proof of hostile intent.

An automated risk assessment is not a criminal conviction.

An AI-generated behavioral profile is not equivalent to independently verified intelligence.

Security agencies must therefore distinguish between analytical assistance and authoritative decision-making.

Human accountability remains essential.

Germany's current legislative debate may become an important test of how democratic intelligence systems regulate AI-enabled analysis.

The issue is not whether intelligence agencies should use modern technology.

It is how the law should constrain its use.

The European Dimension

Germany is not confronting these problems alone.

European governments have increasingly described sabotage, cyberattacks, information manipulation and threats to critical infrastructure as interconnected security challenges.

The European Union has developed instruments for responding to malicious cyber activity, including diplomatic coordination and restrictive measures.

NATO has strengthened its attention to resilience and hybrid threats.

European governments are also improving cooperation among civilian, military and intelligence institutions.

But national sovereignty remains central to intelligence operations.

Intelligence agencies answer primarily to national governments.

Their legal powers differ.

Their oversight systems differ.

Their willingness to share sensitive information varies.

Hybrid threats expose the costs of these differences.

An operation may begin in one jurisdiction, use infrastructure in another and target systems in a third.

Effective defense requires international coordination.

Yet coordination must coexist with national constitutional obligations.

Germany's reforms therefore have implications beyond Berlin.

They may influence the evolving relationship between national intelligence authorities and European security cooperation.

The Cyber Diplomacy Dimension

Cyber diplomacy has traditionally emphasized international norms, responsible state behavior, confidence-building measures and the application of international law to cyberspace.

Germany's current debate illustrates another dimension.

Domestic institutional design affects international cyber strategy.

A government cannot respond to foreign cyber threats solely through diplomatic declarations.

It requires technical capabilities, intelligence assessments, legal authorities and mechanisms for coordinating national institutions.

At the same time, expanding those capabilities can create international risks.

An active cyber operation directed at infrastructure abroad may raise questions of sovereignty.

A disruptive measure may affect third-party systems.

Misattribution may produce diplomatic escalation.

An operation intended to prevent harm may be interpreted by another state as hostile interference.

Thus, intelligence reform and cyber diplomacy cannot be treated as separate fields.

The powers granted domestically shape the actions a state may undertake internationally.

The Danger of Strategic Overreaction

There is a further risk.

A government facing genuine foreign threats may gradually normalize extraordinary security measures.

Powers introduced in response to one adversary can remain available after the immediate threat changes.

Authorities justified by external security concerns may eventually be used in domestic contexts.

This does not mean that stronger intelligence capabilities are inherently illegitimate.

It means that legal safeguards must be designed for the institution's entire future, not merely the present crisis.

German constitutional history makes this particularly important.

The lessons of the twentieth century do not require intelligence agencies to remain technologically ineffective.

They require that intelligence effectiveness remain subject to democratic law.

The objective should be capability without unchecked authority.

The Limits of the Shadow War Concept

The language of shadow conflict can help governments communicate complex threats.

But it also carries risks.

If every cyber incident, infrastructure failure or controversial political narrative is treated as part of a hostile campaign, the concept becomes analytically weak.

Not every cyberattack is state-sponsored.

Not every act of sabotage is foreign-directed.

Not every misleading narrative constitutes an organized influence operation.

And not every security incident should trigger intelligence intervention.

Effective policy requires disciplined classification.

Authorities should distinguish confirmed operations from suspected activity.

They should identify the confidence level of attribution.

They should separate strategic assessments from criminal evidence.

They should recognize alternative explanations where credible.

Without these distinctions, hybrid-threat analysis can become an overly broad justification for state power.

The credibility of democratic security institutions depends on maintaining them.

The Real Transformation: Security Between Peace and War

Germany's experience reveals a larger international transformation.

The institutional boundaries separating peacetime security from wartime defense are becoming less effective at describing contemporary threats.

Cyber operations may produce strategic effects without military force.

Sabotage may disrupt critical infrastructure without territorial occupation.

Foreign interference may undermine institutions without an overt attack.

Intelligence agencies increasingly operate in the space between traditional law enforcement and national defense.

This does not make those distinctions obsolete.

It makes them more important to define.

The central institutional challenge is creating coordination without allowing responsibilities to become legally indistinguishable.

Germany's postwar constitutional architecture was built to prevent the concentration of coercive power.

The emerging security environment requires that architecture to become more capable without abandoning its foundational logic.

What a Sustainable Reform Would Require

A durable intelligence reform should be judged by more than the number of new authorities it grants.

It should establish clear legal thresholds for intrusive operations.

It should distinguish intelligence collection from active intervention.

It should preserve meaningful independent oversight.

It should define the circumstances in which agencies may access sensitive digital information.

It should regulate AI-assisted intelligence analysis.

It should maintain accountability for operations affecting foreign systems.

And it should provide mechanisms for reviewing whether exceptional authorities remain necessary.

These principles are not obstacles to national security.

They are conditions for legitimate national security.

A system that is operationally powerful but constitutionally unstable may ultimately weaken public confidence in the institutions it is intended to strengthen.

Bottom Line Assessment

Germany's intelligence-reform debate marks a significant moment in the evolution of European security.

The country is confronting a threat environment in which cyber operations, sabotage, espionage and foreign interference can create strategic effects without conventional warfare.

Its political leadership argues that intelligence institutions must become more capable.

Its constitutional tradition demands that those capabilities remain limited, accountable and legally defined.

Both concerns are legitimate.

The strategic challenge is not choosing between security and constitutional democracy.

It is determining how a constitutional democracy can remain secure under conditions its original institutional architecture did not fully anticipate.

Germany's historical experience gives the debate unusual importance.

Few major Western states have built such a substantial portion of their security identity around the deliberate limitation of intelligence power.

Few now face such visible pressure to reconsider the practical consequences of those limitations.

The outcome may influence how other European democracies approach intelligence reform, cyber defense and hybrid-threat response.

The deeper lesson extends beyond Germany.

Modern states increasingly face adversarial activity that falls between traditional categories of crime, espionage and war.

Their institutions must adapt.

But adaptation should not mean abandoning the principles that make those institutions legitimate.

Germany's postwar republic was founded on the proposition that state power must remain constrained even when security is at stake.

The shadow conflict of the twenty-first century is testing whether that proposition can survive a more technologically complex threat environment.

The defining measure of Germany's intelligence reform will not simply be whether the state becomes more powerful. It will be whether the state becomes more capable while remaining constitutionally accountable.

Vladimir Tsakanyan, Ph.D. Center for Cyber Diplomacy and International Security (CCD-IS)

Sources and links

[1] Vladimir Tsakanyan, Ph.D.

https://cybercenter.space/vladimir-tsakanyan/

Read the original article online

https://cybercenter.space/2026/10/12/the-shadow-war-state-how-hybrid-conflict-is-rewriting-germanys-post war-security-doctrine/