SPOT ON

Dominik Rehbaum, Driss Köhler, Stormy-Annika Mildner, Elisabeth Nöfer

Hybrid Threats in Times of Conflicts and Wars: Establishing Democratic Resilience in the Digital Age

April 2023

The geopolitical environment and with it the threat landscape is changing rapidly. Russia's war against Ukraine marks a "Zeitenwende" in the European security order. At the same time, the systemic rivalry between democratic and autocratic regimes is intensifying. The international system is becoming increasingly conflictual, and security threats are more and more complex. One of these are hybrid threats. They range from cyberattacks and disinformation campaigns to the use of irregular armed groups and terrorist attacks. Being employed by both states and non-state actors, they can undermine democratic stability, for example by interfering with political discourse or disrupting critical infrastructure. Several recent hybrid attacks have demonstrated Germany's vulnerability. To forge democratic resilience against hybrid threats, Germany needs a comprehensive multi-stakeholder approach, including strengthening the country's cybersecurity capabilities and institutions, promoting digital literacy, as well as enhancing information sharing and cooperation among government agencies, civil society, and the private sector.

Hybrid threats are anything but new. States have relied for centuries on manipulation and coercion tactics to influence the developments in other countries. During the Cold War, both the United States and the Soviet Union deployed a range of non-conventional means to achieve their strategic objectives. While such operations have traditionally been the purview of national intelligence agencies, the rapidly accelerating digitalization and globalized economy have rendered so-called hybrid tactics faster and more affordable than ever, providing a host of new methods to manipulate adversaries and the international environment. Emerging and disruptive technologies (EDTs) such as artificial intelligence (AI) powered models have extended the scope of attacks and the level of damage, blurring the line between state and non-state actors and introducing new layers of sophistication.

The severity of hybrid threats is illustrated by Russia's war against Ukraine. Russia uses both significant conventional forces and a wide spectrum of hybrid tools, including subversive, economic, information, and diplomatic means, infiltrating networks, sowing disinformation, and disrupting critical infrastructure such as power grids or transportation systems. Be it deepfakes to manipulate decision-makers and public opinion, the 'instrumentalization' of migration movements at the EU's external border, economic coercion, or election manipulation – the risk of hybrid attacks is growing with the systemic conflict between democratic and authoritarian regimes intensifying.

The Nature of Hybrid Threats

While the term "hybrid threats" does not have a universally accepted definition and has been criticized for its lack of conceptual clarity, hybrid threats have commonly been understood as the coordinated use of various tools of power to exploit vulnerabilities of another state to pursue an overarching strategic goal. In its Joint Framework on Countering Hybrid Threats, first released in April 2016, the European Commission defines hybrid threats as "the mixture of coercive and subversive activity, conventional and unconventional methods […], which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare."

Hybrid threats can take many different forms, such as cyberattacks, economic coercion, extortion, disinformation campaigns, propaganda, and military aggression, as also stated in the German Cyber Security Strategy. The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) lists more than 40 kinds of hybrid threats across at least 13 sectors, including targeted data manipulation or cyberattacks on critical infrastructure. Also included on this list are “public opinion manipulation” and “cyberattacks,” both of which the EU referenced explicitly in its Strategic Compass on Defense and Security adopted in March 2022.

Hybrid attacks can be executed through proxies or none-state actors. Their goal is to exploit vulnerabilities in societies, economies, and institutions with the aim of destabilizing political decision-making, stirring up unrest and uncertainty, and undermining public trust in democratic institutions.

The risk of hybrid attacks is growing

As such, they are often complex, hard to detect, and characterized by vagueness. Attribution is often difficult, and responses require collaboration of various stakeholders. For governments, it is thus key to accurately identify and assess key vulnerabilities in their current security architecture and formulate an effective strategy that defends against malign foreign influence.

Germany’s Threat Environment

The national threat environment in Germany has changed considerably since Russia’s war against Ukraine. In the report on the state of IT security in Germany 2022, the Federal Office for Information Security (BSI) emphasizes that the threat in cyberspace is higher than ever. This resembles a global trend: According to data from Check Point Research (CPR) 2023 Security Report, there is a 38 percent increase in cyberattacks globally. The most affected sectors are education and research, government institutions, and healthcare. CPR also finds that cyberattacks in Germany increased by 27 percent in 2022 compared to 2021.

In connection with Russia’s war against Ukraine, there has been an accumulation of smaller incidents and hacktivism campaigns with collateral damage in cyber-sabotage. The cyberattack on the KA-SAT satellite network segment in Central and Eastern Europe on October 24, 2022, for instance, has led to the failure of about 5,800 German wind turbines connected with the network. In addition to cyberattacks, Germany has also experienced disinformation campaigns and economic coercion related to the Nord Stream 2 gas pipeline project in the months leading up to Russia’s war against Ukraine. The attempted poisoning of Russian activist and opposition leader Alexei Navalny, who was treated in the Charité – Universitätsmedizin Berlin, serves as another example to illustrate the intrusion by foreign agents. The series of explosions rupturing the Nord Stream 1 and 2 gas pipelines in September 2022 and the shutdown of rail traffic in northern Germany due to sabotage in October 2022 add to the examples of how hybrid attacks can endanger critical infrastructure.

In response to Russia’s war against Ukraine and the dramatically worsening security landscape, German Chancellor Olaf Scholz attested a Zeitenwende, which since then has become the defining paradigm for Germany’s foreign and security policy. With a €100 billion special fund and lasting raise in defense spending, the government sought to strengthen defense capabilities to counter vulnerabilities on a myriad of security issues. This includes security challenges in the digital domain. In this regard, a “Cyber-Zeitenwende” is not only a matter of national defense. It includes economic competitiveness and social cohesion and thus requires a comprehensive and collaborative approach that involves all relevant stakeholders from the public and private sectors, as well as civil society and public administration.

Mapping the Actors to Counter Hybrid Threats

Despite growing awareness, Germany continues to grapple with countering hybrid threats effectively. This has structural and individual reasons. Against this backdrop, three dimensions dominate Germany’s response to hybrid threats.

Public Administration: The issue of countering hybrid threats has been on the government’s agenda for some time. Already in the 2016 White Book on Security Policy and the Future of the German Armed Forces, the government underlined the importance of hybrid analytical capability and defense capacity to counter hybrid threats. The concept Civil Defense in 2016 further identified hybrid threats among the most significant challenges to Germany. Public administration plays thus a key role in coordinating and funding responses to hybrid threats. Despite heightened awareness and new strategic angles, such as the Cyber Security Strategy for Germany of 2021, concrete actions and implementation have remained insufficient. High-profile cyberattacks on German entities, for example by the Russian hacker group “Snake” on German parliamentarians, the military and several embassies in 2018 or a cyberattack on a hospital in Düsseldorf in 2020, illustrate this finding. In its report on the Cyber Security Strategy for Germany 2021, the German Federal Audit Office criticizes considerable technical errors in the implementation of the strategy, for example inadequate definition of targets and indicators or insufficient involvement of key players in the cybersecurity landscape. Moreover, it remains unclear how the strategy will be integrated into the European framework and how the German government will ensure complementarity of the two strategies. Building on the mapping of Germany’s cybersecurity architecture by the Stiftung Neue Verantwortung (SNV), structural challenges such as fragmented responsibilities and competencies among federal actors continue to prevail. This is not least due to the plethora of actors, often operating in silos with sometimes incompatible approaches. A comprehensive legal framework with a common platform for information exchange and cooperation is still lacking, while insufficient resources both at the state and municipality level impair the ability to prevent and detect cybersecurity threats.

Civil Society: Functioning democracies depend on well-informed citizens. Although false information and manipulation of public opinion have long played a central role in hybrid tactics, digitalization has radically transformed the handling of information. The proliferation of AI-based content generation tools such as ChatGPT have not only reduced manipulation costs but also amplified the speed and sophistication of disinformation campaigns. Consequently, media and information literacy among the population is ever more important for resilience against hybrid threats. As the Internet overtakes television as the most used news source, according to the Reuters Digital News Report, social media has emerged among the most widely used source of news content online. At the same time, a study by the SNV in 2021 found that only 43 percent of the interviewees recognized a (fictive) post Facebook containing false information as such, whereas 33 percent incorrectly categorized this as “information”. In times of rampant malicious information campaigns in digital spaces, high susceptibility to false and misleading information renders both individuals and democratic societies vulnerable.

Private Sector: As companies increasingly rely on digital infrastructure and automated processes to provide products and services, they become more vulnerable to hybrid threats. A study by the German business association Bitkom found that 84 percent of the German companies surveyed across all industries had been the victim of cybertheft, espionage, or sabotage in 2022. However, companies are often still afraid of notifying attacks due to a fear of loss of reputation. According to a Kaspersky survey in 2022, two-thirds of decision-makers in companies in Germany assume that customer confidence is lost in the event of successful cyberattacks, while a clear majority is certain that their reputation would be affected. Moreover, vital questions arise regarding the protection of critical infrastructure, where the responsibility lies primarily with private owners and operators. For instance, both the EU and the German government struggle to effectively protect internet nodes and submarine cables.

Building Resilience: Next Steps to Address Hybrid Threats against Germany

Building on the third Cyber Strategy in 2021 and the Digital Strategy in 2022, the German government seeks to strengthen Germany’s security infrastructure and civil society’s resilience against hybrid threats. The planned National Security Strategy, which is currently in the inter-ministerial consolidation process, is also likely to address hybrid threats.

To effectively counter hybrid threats, a whole-of-society approach with concrete implementation steps is needed.

Societal Resilience: Public awareness and media literacy must be bolstered to forge societal resilience against hybrid threats, for example by promoting local journalism and supporting source verification skills among citizens. A specific focus should be laid on countering disinformation campaigns through digital literacy and transparency of online sources.

Improving digital literacy is paramount

The special task force of the inter-ministerial working group on hybrid threats on the situation in Russia and Ukraine provides a useful starting point and should be better positioned to expand its geographical focus. In addition to supporting educational initiatives, the focus should be put on enhancing situational awareness and early warning capacity to ensure reliable communication and information sharing.

Institutional Framework: In the spirit of the Zeitenwende, Germany should promote a strategic culture that includes the willingness and ability to prioritize security issues. An updated institutional framework should clarify the roles and responsibilities of different actors and define the conditions and limitations for such measures together with a range of stakeholders from civil society, academia, and the private sector. It should specifically incorporate technical and administrative cooperation between the federal government and the states, with a clear division of responsibilities and detailed protocols for emergency situations that require rapid responses.

Critical Infrastructure: Ukraine's dependency on the SpaceX Starlink system has demonstrated the importance of infrastructure and communication systems. Relying on private-public cooperation, the German government should establish backup IT and communication systems, for example through so-called data embassies. A data embassy, which is a server resource owned and maintained by a nation-state outside its territorial boundaries, is a tool to ensure the survival of a government's critical database in a situation where governing from within the country's borders is no longer possible due to, for instance, an attack or a natural disaster. Furthermore, it should enhance its support for small and medium-sized enterprises to bolster their cybersecurity capacity. The physical and digital protection of critical infrastructure such as submarine cables is another important component to bolstering resilience against hybrid threats. In doing so, the government should support companies to adopt a proactive and collaborative approach that involves enhancing cyber resilience, protecting their critical infrastructure, and sharing best practices. This requires recognition from both parties that the emergence of hybrid threats creates a co-dependency between the public and the private sector.

International Environment: Germany's alignment with European initiatives and tools remains key. The EU has already adopted tools against information manipulation and foreign interference such as the Cyber Diplomacy Toolbox and the Strategic Compass. Other initiatives such as the EU Hybrid Rapid Response Team provide expert assistance to member states. Germany should support the implementation of the EU Hybrid Toolbox to enable fast and coherent responses to hybrid threats across internal and external security divisions beyond the capabilities of member states. Participating in joint exercises and training activities not only contributes to a global cybersecurity agenda but supports a coherent policy framework on hybrid threats. Finally, Germany should continue to reach out to middle-ground states to build global cyber norms and enhance international accountability.

Given the increasingly conflictual international environment, hybrid threats are likely to continue to grow. To effectively improve resilience against hybrid threats, a whole-of-society approach is needed as well as transformational change in how to build hybrid attack defense at the international level.

Dominik Rehbaum
Research Assistant, German Institute for International and Security Affairs (SWP)

Driss Köhler
Program Assistant in the Digital Program, Aspen Germany

Dr. Stormy-Annika Mildner
Executive Director, Aspen Germany

Elisabeth Nöfer
Program Officer in the Digital Program, Aspen Germany

This text represents the personal views of the authors. The authors do not speak on behalf of the institution which they are associated with.

About this series

This publication is part of the event series Democracy 2.0, hosted by the Aspen Institute Germany in partnership with Microsoft Berlin. The two-part workshop series brings together international experts on wartime digital operations from politics, business, academia and civil society. More information can be found here.

Aspen Institute Germany expresses its gratitude to the former intern Coalter Palmer for his contribution to this publication and diligent commitment during his three months internship.

Publisher: Aspen Institute Germany e.V.
Editors: Dr. Stormy-Annika Mildner
Design & Layout: Jahongir Zaynobiddinov