

LESSONS FROM POLAND

European Resilience: Cyber, Defense & Cloud as Strategic Infrastructure

Aspen Institute Central Europe | Warsaw Roundtable, 17 June 2026

INTERNATIONAL PARTNERS
aspen institute
aspen institute central europe
Aspen Institute Germany
aspen institute españa

About the Project

The resilience of modern states increasingly rests on the interplay between cyber capabilities, defense, and cloud infrastructure. These domains can no longer be viewed in isolation: secure digital systems underpin military readiness, trusted cloud services enable both government and business, and cyber resilience has become a prerequisite for economic competitiveness.

Against this background, three members of the Aspen International Partners network — Aspen Institute Central Europe, Aspen Institute Germany, and Aspen Institute España — with the support of Microsoft and in collaboration with Aspen Institute Romania, launched a cross-border initiative aimed at examining and strengthening European resilience across the interconnected domains of cyber, defense, and cloud infrastructure.

As part of the project, four European Resilience Roundtables were convened in Warsaw, Berlin, Madrid, and Brussels, bringing together senior representatives from government, defense institutions, industry, and the broader policy community in each country to examine national resilience challenges and identify lessons relevant at the European level. The insights generated across the four roundtables are captured in a series of European Resilience Reports presented to key EU stakeholders.

Drawing on the discussions from the European Resilience Roundtable in Warsaw, held on June 17, 2026, by the Aspen Institute Central Europe, this report examines how Poland is approaching cyber, defense, and cloud infrastructure as integrated elements of strategic infrastructure. The findings included in the report are intended to inform both the Polish national policy debate and the European Resilience report series.

LESSONS FROM POLAND

European Resilience: Cyber, Defense & Cloud as Strategic Infrastructure

Aspen Institute Central Europe | Warsaw Roundtable, 17 June 2026

Executive Summary

Poland occupies a distinct position within the European Union's resilience architecture.

As a North Atlantic Treaty Organization (NATO) and EU frontline state bordering both the Kaliningrad exclave and Belarus, Poland's understanding of resilience is shaped less by the concerns that dominate policy discussions in Western European capitals and more by direct, sustained exposure to state-sponsored hybrid and cyber aggression.

It situates these findings within the broader European Resilience Roundtable series examining cyber, defence and cloud resilience across Germany, Spain and Poland. While the report contributes to a comparative European evidence base, the analysis presented here draws exclusively on insights gathered through the Cyber Resilience Roundtable (Warsaw, 17 June 2026) and therefore reflects a perspective specific to the Polish context. The findings are intended to inform both the national policy debate and the European Resilience report series.

Poland's resilience model cannot be separated from its geography. Direct proximity to Russia and Belarus, and the lessons drawn from the war in Ukraine, mean that resilience in the Polish context is understood first and foremost through a security and defence lens rather than through the broader civil-protection framing that characterises resilience debates in much of Western Europe.

Polish enterprises of strategic importance face persistent and voluminous cyber intrusion attempts, numbering in the thousands per week, attributed to Russian and Belarusian state-sponsored actors. A recurring theme is the evolution of adversary intent: rather than pursuing traditional objectives of espionage, ransomware extraction or data theft, hostile campaigns increasingly aim at logistical paralysis, the erosion of public trust, and the manufacture of social unrest.

On defence modernisation, military effectiveness is now inseparable from the security of digital command systems, data flows and cloud-enabled capabilities, while cautioning that legacy systems, interoperability gaps and transparency-heavy procurement rules constrain the pace of transformation. On cloud infrastructure, the roundtable's central and most contested exchange concerned whether the physical location of data and servers still matters for sovereignty in an era of borderless cyber threats, or whether dispersal and cross-border redundancy now offer the more credible route to resilience.

Four structural weaknesses surface. First, small and medium-sized enterprises embedded in dual-use and defence supply chains lack the financial resources, technical expertise and audit capacity to meet rising cybersecurity obligations, leaving them as the most exploitable entry points into otherwise well-defended systems. Second, public procurement rules for critical digital infrastructure require a degree of transparency that inadvertently exposes sensitive technical specifications and vendor details to hostile intelligence services. Third, cloud governance remains fragmented as Poland has yet to adopt comprehensive national cloud legislation, and existing data-evacuation obligations imposed on strategic entities have not been matched by budgetary support, leaving formally mandated resilience measures largely unimplemented. Fourth, funding mechanisms for cloud-based disaster recovery and data continuity remain underdeveloped relative to the scale of the risk, a gap compounded by Poland's comparatively limited voice in Brussels when competing for EU digital infrastructure funding.

Poland's preparedness is uneven across the three domains examined. Threat awareness is high and well-articulated, state institutions, strategic enterprises and industry share a common, granular understanding of the hybrid and cyber pressure the country faces, and this shared awareness has translated into a level of political will to act that is not always present elsewhere in the Union. Where preparedness falls short is in operational and institutional follow-through. Regulatory ambition has consistently outpaced implementation capacity, evacuation planning exists on paper without funding to operationalise it, procurement rules remain unreformed despite recognised security costs, and national cloud legislation has yet to be enacted. Public-private cooperation, a genuine strength at the level of large strategic enterprises, thins out considerably further down the supply chain. Poland's strategic posture reflects a high degree of awareness of emerging risks and vulnerabilities. At the same time, challenges remain in translating regulatory requirements into the institutional capacities, resources and capabilities needed to support their effective implementation.

Table of Contents

About the Project 2

Executive Summary 4

1. Introduction: Poland's Geopolitical Position 7

2. Resilience of Cyberspace 10

- State of the Threat Landscape 10
- Hybrid Warfare 11
- The Network and Information Systems Directive 2 Implementation Challenge 11
- The Dual-Use SME Bottleneck 12
- Public-Private Cooperation 13

3. Resilience of Defence Policy and Defence Modernisation 14

- Digital Defence Transformation 14
- Data as Strategic Infrastructure 14
- Defence Resilience Challenges 15
- Public Procurement and Security 15
- Strategic Autonomy Concerns 16

4. Resilience of Cloud Technology and Infrastructure 17

- Cloud as Critical Infrastructure 17
- The Geolocation Versus Dispersal Debate 17
- The Data Evacuation Gap 18
- The Funding Contradiction 19
- US Transactional Risk and the Cloud Act 19

5. Lessons Learned for European Coordination & Recommendations 21

Conclusion 25

1 Introduction: Poland's Geopolitical Position

Poland sits at the geographic and strategic hinge of NATO's eastern flank, sharing borders with the Kaliningrad Oblast in Russia and Belarus, both of which are identified as active sources of hybrid pressure. The country lies within the logistical corridor through which Western military and humanitarian support to Ukraine has flowed since 2022. Compared to the danger environment facing states further west, it is safe to state that the level of exposure to hybrid and cyber opera-tions is qualitatively different.

Poland's resilience is rooted in "direct, physical exposure to geopolitical threats" and state-sponsored hybrid/cyber aggression rather than generic business continuity. Poland's National Security Strategy published in 2020 already explicitly identified the Russian Federation's "neo-imperial" policy as the most serious threat, citing Russia's offensive build-up in the Baltic region and Kaliningrad. It described Russian hybrid actions including cyberattacks and disinformation aimed at destabilising Western states and dividing allies.[1]

NATO 2026 estimates show Poland at 4.68% of GDP on defence, well above Germany 2.69%, Spain 2.00%, Finland 2.65%, and NATO Europe/Canada 2.53%; this supports Poland's self-perception as a high-investment front-line actor rather than

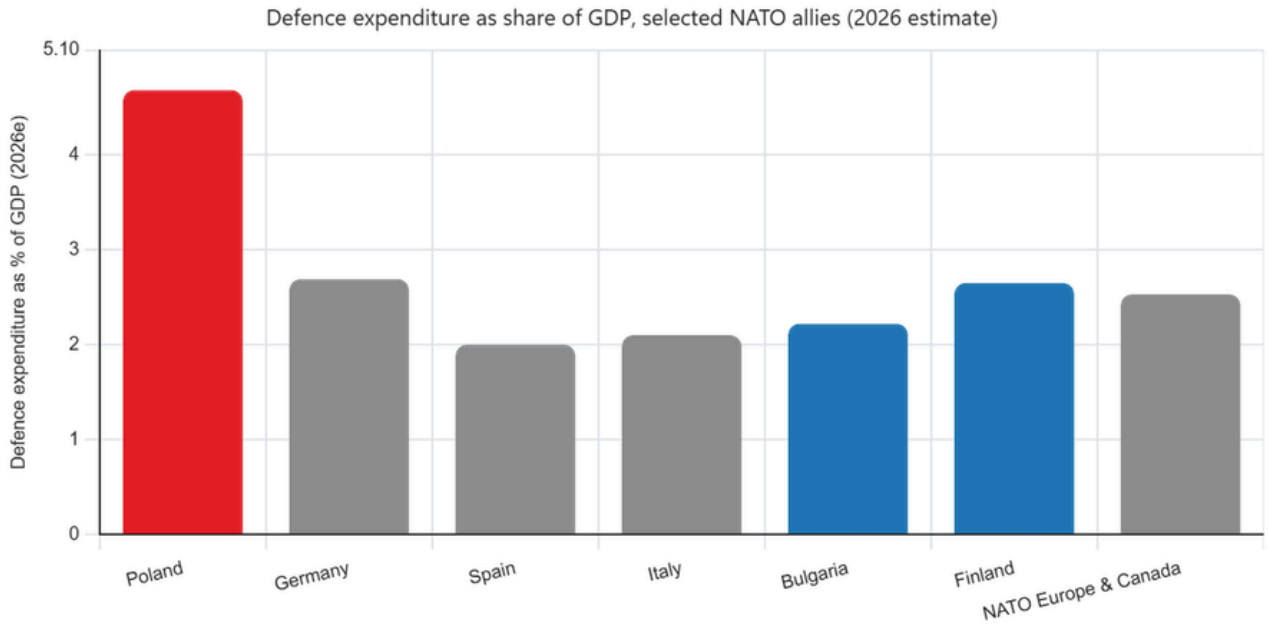


Figure 1: Defence expenditure as a share of GDP in selected NATO allies, using NATO 2026 estimates. Poland and the Baltic/frontline states (detailed on page 8) sit well above Spain and the NATO Europe/Canada average, supporting the Warsaw brief's eastern-flank framing.

1 Bureau of National Security (BBN), National Security Strategy of the Republic of Poland, approved 12 May 2020, https://en.bbn.gov.pl/en/about-bbn/publications/publications/769,National-Security-Strategy-of-the-Republic-of-Poland.html

a normal-risk EU member state.[2] A noteworthy development is that several Eastern frontline countries, while still trailing Poland in 2024 (3.75% of GDP), including Estonia (3.37%), Latvia (3.36%), and Lithuania (3.09%), have now surpassed Poland in 2026, with defence spending reaching 5.10% in Estonia, 4.92% in Latvia, and 5.33% in Lithuania.

Poland's national risk landscape is increasingly characterised by continuous and sustained pressure rather than isolated or episodic incidents. Attacks targeting enterprises of strategic importance were described as occurring at a persistent pace; a single sector may be subject to thousands of intrusion attempts each week. NATO's own cyber exercise reporting similarly states that Russia's war against Ukraine has reinforced the need to understand the battlespace from a cyberspace perspective and that NATO faces cyber threats daily, from low-level attacks to sophisticated incidents.

The war in Ukraine has further heightened this exposure and has provided important insights into the requirements of resilience under conditions of active conflict. There is clear observation on the destruction of physical data infrastructure in conflict-affected areas, including facilities built with extensive underground protection, as evidence that physical hardening alone cannot be assumed to ensure operational continuity during wartime.

A structural theme running through the roundtable was the divergence between how resilience is understood in Western Europe and how it is understood in Poland and the wider Central and Eastern European (CEE) region. In Western capitals (e.g., Madrid), resilience discourse tends to foreground climate adaptation, migration management and the continuity of energy supply during periods of price volatility or infrastructure failure. These are, in the Western European framing, largely civil-protection and economic-continuity concerns. For Poland and the countries of Central and Eastern Europe, resilience is closely associated with the capacity to prevent, withstand and respond to state-sponsored hybrid and cyber threats.

Eurobarometer evidence supports a Europe-wide threat shift but qualifies the "Western vs CEE" asymmetry. In Spring/Autumn 2025, 77% of EU respondents viewed Russia's invasion as a threat to EU security and 73% viewed it as a threat to their own country; Poland was among the countries with high perceived national threat, while Finland, Sweden and Denmark were also very high.[3]

For Poland and its CEE neighbours, by contrast, resilience is discussed first and foremost as a matter of hard national security. Explicitly speaking resilience, in the Polish context, means defence against state-sponsored hybrid and cyber aggression, preparedness for the possibility of kinetic conflict, and the maintenance of strategic continuity should conventional deterrence fail. Climate and migration pressures are not absent from the Polish policy conversation, but they occupy a secondary position relative to the immediate question of

2 Public Diplomacy Division, NATO, Defence Investment of NATO Countries (2014–2026), press release, 7 July 2026, https://www.nato.int/en/news-and-events/articles/news/2026/07/07/defence-investment-update-record-spending-in-europe-and-canada

3 European Commission, Standard Eurobarometer 104 — The EU's Response to the War in Ukraine, Autumn 2025, published 30 December 2025, https://euneighbourseast.eu/wp-content/uploads/2025/12/standard-eurobarometer-104_autumn-2025_eus-response-to-the-war-in-ukraine_report_en.pdf

how the state, its critical infrastructure and its digital systems would function under direct military or hybrid attack.

As a result, diverging perceptions of this issue have significant implications for the development and implementation of European policy. EU-level resilience frameworks, funding instruments and regulatory initiatives are frequently designed around a composite understanding of resilience that reflects the priorities of the Union's larger and more geographically insulated member states. When such frameworks are transposed into the Polish context without adjustment, they risk under-addressing the specific hybrid and military dimensions of resilience that dominate national threat assessments, while over-emphasising dimensions of comparatively lower priority for a frontline state. Bridging this perception gap is a precondition for more effective European coordination, a theme developed further in Section 5.

Resilience in Poland is, in this sense, inseparable from national security policy. Cyber resilience, defence modernisation and cloud infrastructure are not treated as three parallel policy tracks but as a single, integrated continuum: a disruption to cloud services can degrade military command capability; a cyberattack on critical infrastructure can be a precursor to, or component of, a broader hybrid campaign; and defence modernisation is, in practice, increasingly a digital and data infrastructure project as much as a conventional procurement one. The following sections examine each of these three domains in turn before returning, in the concluding section, to their combined implications for European policy.



2 Resilience of Cyberspace

State of the Threat Landscape

Ongoing global events paint a consis-tent picture of a persistent, high-tempo threat environment. Russian and Belarusian state-sponsored groups are identified as the principal source of hybrid and cyber pressure against Polish enterprises of strategic importance, with the scale of activity described as running into thousands of penetration attempts per week against targeted sectors. Iranian cyber activity is a growing feature of the wider European threat picture, operating alongside, though generally at lower intensity than, Russian- and Belarusian-linked campaigns.

Poland's 2017 Defence Concept identified Russia as a primary source of instability on NATO's eastern flank, including in the cyber domain. Since then, cyber activity has increased significantly, rising from 226,914 potential incidents recorded in 2019 to more than 760,000 notifications in 2021, including 26,899 confirmed attacks and 115 coordinated cyber campaigns targeting government institutions and critical infrastructure. The trend accelerated following Russia's invasion of Ukraine. In 2025, cyberattacks increased by 30% year-on-year, with Poland reportedly facing up to 4,000 politically motivated cyber incidents per day, making Poland the world's most targeted country.

High-profile incidents included attempted intrusions against the National Centre for Nuclear Research and a coordinated attack on at least 30 renewable energy facilities in December 2025 that could have affected more than 500,000 people had it not been detected and contained.[4]

Alongside state-linked threats, Poland also faces a substantial volume of cybercrime activity targeting businesses and citizens. Computer Emergency Response Team Poland *(CERT Polska)/Naukowa i Akademicka Sieć Komputerowa* – Research and Academic Computer Network, National Research Institute (NASK), recorded more than 600,000 cyber reports in 2024, representing a 62% increase compared with 2023, while registered incidents rose by 29%. Phishing and online fraud accounted for 94.7% of reported incidents, including 40,120 phishing cases. Similarly, Poland recorded 355,000 suspicious SMS reports in 2024, a 60% increase from the previous year, and blocked nearly 1.5 million malicious text messages.[5] While some cybercrime campaigns may originate from abroad, these figures primarily reflect financially motivated criminal activity and should be distinguished from the state-sponsored cyber operations discussed above; yet, they still underscore the need to improve cybersecurity measures.

---

4 Oksana Trefanenko, The New Battlefield: Poland and Europe's Struggle Against Hybrid Warfare, EPICENTER, Weatherhead Center for International Affairs, Harvard University, 8 June 2026, https://epicenter.wcfia.harvard.edu/articles/new-battlefield-poland-and-europes-struggle-against-hybrid-warfare

5 CERT Polska / NASK, Analiza bezpieczeństwa polskiego internetu w 2024 roku [Analysis of Polish Internet Security in 2024], gov.pl – Serwis Rzeczypospolitej Polskiej, 25 April 2025, https://www.gov.pl/web/baza-wiedzy/analiza-bezpieczenstwa-polskiego-internetu-w-2024-roku

What distinguishes the current threat landscape from earlier phases of state-sponsored cyber activity, according to discussions, is a shift in adversary objectives. Modern operations directed at Polish targets are described as increasingly indifferent to the classic goals of espionage, ransomware extraction or data theft. Instead, the dominant objective is described as societal destabilisation: the deliberate creation of fear, the disruption of logistics and public services, and the erosion of citizens' trust in state institutions. This is, in effect, cyber activity conducted in service of a hybrid warfare logic rather than a purely criminal or intelligence-gathering one, and it demands a correspondingly different resilience posture, one oriented toward the protection of public confidence and continuity of essential services and not solely the protection of data confidentiality.

Hybrid Warfare

Because the objective of hostile cyber activity is increasingly social and psychological rather than purely technical, cyber resilience in Poland is closely linked to the maintenance of public confidence in state institutions. Disruption to transport systems, telecommunications networks, healthcare services or energy supply, even when technically contained and short-lived, carries a reputational and psychological cost that adversaries appear to be deliberately targeting. Resilience planning needs to account explicitly for this dimension: technical recovery of a system is only part of the resilience task; restoring and maintaining public confidence following a disruptive event is an equally important, and often more difficult, objective.

Unfortunately, hostile cyber activity has direct implications for the sectors most vulnerable to hybrid pressure. Transport and logistics networks, telecommunications infrastructure, hospitals and the energy sector are areas where disruption would have an outsized effect on public morale relative to its purely technical or economic cost, making them attractive targets for an adversary whose principal aim is destabilisation rather than material gain. Particular challenges arise for small and medium-sized enterprises operating within dual-use supply chains. Resource constraints limit their capacity to undertake extensive cybersecurity assessments and investments, making them more susceptible to advanced cyber threats.

The Network and Information Systems Directive 2 (NIS2) Implementation Challenge

The transposition of the EU's NIS2 Directive into Polish law and administrative practice was identified as a significant governance challenge, as only 21 of the 27 Member States have transposed the NIS2 directive despite the October 2024 deadline.[6] The directive expands the scope of entities subject to cybersecurity obligations and raises compliance requirements considerably relative to its predecessor. Therefore, the implementation across the Union as a whole has been uneven, with a substantial minority of member states, including Poland at various points in the process, lagging behind the transposition deadline, although its implementation

6 European Cyber Security Organization (ECSO), NIS2 Directive Transposition Tracker, https://ecs-org.eu/activities/nis2-directive-transposition-tracker/.

is now completed.[7] For entities newly brought within the directive's scope, the compliance burden, spanning incident reporting, risk management measures and governance accountability, was described as considerable relative to available administrative and technical capacity, particularly outside the largest state-owned enterprises.

The core governance challenge identified was not the ambition of the NIS2 framework itself, which was broadly endorsed, but the mismatch between EU-level regulatory ambition and the national administrative capacity and funding needed to operationalise it. Without matching implementation support, the framework risks producing formal com-pliance on paper while leaving underlying vulnerabilities largely unaddressed.

Poland's amended National Cybersecurity System Act (*ustawa o krajowym systemie cyberbezpieczeństwa*, *KSC Act*) entered into force on 3 April 2026, implementing NIS2 through new categories of key and important entities, expanded sectors, risk-management obligations, management responsibility, sectoral Computer Security Incident Response Teams (CSIRTs), stronger supervisory powers and new penalties. [8] Entities meeting the criteria on entry into force must register by 3 October 2026, connect to S46 and implement obligations by 3 April 2027, and key entities must conduct their first audit by 3 April 2028. Compliance requirements may pose particular challenges for small and medium-sized enterprises, especially for those operating within dual-use supply chains. At the same time, the legislative framework provides for obligations that are proportionate to risk, rather than applying uniform requirements across all enterprises.

The Dual-Use SME Bottleneck

Among the structural vulnerabilities identified by various stakeholders, none was developed as extensively as the position of small and medium-sized enterprises within defence and dual-use supply chains. Such firms frequently hold contracts that place them, often unknowingly, within the security perimeter of larger defence contractors and state institutions. Yet these firms typically lack dedicated cybersecurity personnel, lack the budget to commission regular audits, and lack the technical infrastructure to meet the security standards expected of prime contractors.

The European Union Agency for Cybersecurity (ENISA) found in its 2024 report on NIS2 investment that information security accounted for 9% of EU IT investments, median information-security spending increased from €0.7 million to €1.4 million, 59% of SMEs struggled to fill cybersecurity roles, and 34% of SMEs were unable to secure the additional budget needed for NIS2 compliance.[9]

---

7 NIS 2 Directive | Transposition in Poland, nis-2-directive.com, updated 12 March 2026, https://www.nis-2-directive.com/Transposition/Poland.html

8 Ministerstwo Cyfryzacji (Ministry of Digital Affairs, Poland), Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (KSC) — obowiązki podmiotów kluczowych i ważnych [Amendment to the National Cybersecurity System Act (KSC) — obligations of key and important entities], 05.06.2026, https://www.gov.pl/web/cyfryzacja/nowelizacja-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ksc---obowiazki-podmiotow-kluczowych-i-waznych

9 European Union Agency for Network and Information Security (ENISA), Navigating Cybersecurity Investments in the Time of NIS 2, distributed via EIN Presswire, 21 November 2024, https://www.einpresswire.com/article/762664634/navigating-cybersecurity-investments-in-the-time-of-nis-2

What is repeatedly described is a weakest-link dynamic: national and military-sector resilience is only as strong as the least-defended supplier within a given supply chain. Hostile actors seeking access to well-defended state or military systems are understood to increasingly route their efforts through smaller, less well-protected suppliers, using them as a gateway rather than attacking hardened targets directly. EU-level regulation compounds rather than resolves this problem in its current form: obligations such as the requirement to migrate data to secure cloud environments are imposed on SMEs without corresponding guidance on financing, tooling or implementation pathways, leaving smaller providers to interpret and fund compliance largely on their own. The result is a policy gap in which the sector most responsible for aggregate supply-chain risk is also the sector least equipped, and least supported, to reduce it.

Public-Private Cooperation

Public-private cooperation was recognised as a genuine strength of Poland's current cyber resilience posture, but one operating below its potential. Cooperation between public authorities, private-sector organisations and research institutions is increasingly recognised as an important component of cybersecurity governance. Existing mechanisms for threat information sharing and incident coordination appear to support cooperation among larger and better-resourced organisations.

The principal barriers identified concerned scale and consistency rather than the absence of goodwill. Information-sharing arrangements were described as more developed among large strategic enterprises than among the broader base of smaller suppliers, creating a two-tier system of resilience in which well-connected large firms benefit from timely threat intelligence while smaller entities, including the SMEs discussed above, often learn of relevant threats only after the fact, if at all. Strengthening and broadening these cooperation mechanisms, extending their reach further down supply chains, was identified as a priority for closing the gap between the country's overall threat awareness and its actual, distributed resilience capacity.

Poland's cyber threat landscape is defined by high-tempo, socially destabilising attacks from Russian- and Belarusian-linked actors; NIS2 implementation is constrained more by capacity and funding than by regulatory ambition; SMEs within dual-use supply chains constitute the most significant structural vulnerability; and public-private cooperation, while a relative strength, remains unevenly distributed across the size and tier of the enterprises involved.



3 Resilience of Defence Policy and Defence Modernization

Digital Defence Transformation

Military effectiveness today is inseparable from digital infrastructure for several reasons. Command and control systems, secure military networks, sensor and intelligence platforms, and the logistics systems that sustain deployed forces are all understood to depend on digital connectivity and, increasingly, cloud-enabled capability. Digital transformation is not a discrete modernisation workstream running alongside conventional procurement, but as the substrate on which most other modernisation efforts now depend.

Interoperability, both across branches of the Polish armed forces and with allied NATO militaries, was identified as a central objective and a persistent challenge of this transformation. Achieving genuine interoperability requires not only compatible hardware but shared data standards, common security architectures and coordinated procurement choices, none of which can be assumed to emerge automatically from parallel national investment programmes.

Data as Strategic Infrastructure

A recurring formulation during the roundtable held that data itself has become a form of strategic infrastructure, on a par with more traditional categories such as energy or transport networks. Modern military effectiveness depends on the ability to move information securely and rapidly between sensors, command structures and deployed units, and increasingly relies on cloud-enabled capabilities to do so at the speed and scale that contemporary operations require. This effectiveness has significant implications for how defence planners think about resilience: protecting a military capability today means protecting the data flows and cloud infrastructure that enable it, not merely the physical platforms themselves.

Poland's National Security Strategy calls for a national integrated situational-awareness system based on reconnaissance, communications and command systems, including satellite observation and unmanned systems, and for full-spectrum military cyberspace capabilities and cyber forces. NATO's Cyber Coalition 2024 tested cyberspace situational-awareness dashboards by correlating mission, threat and network information; NATO says such capability provides "cognitive advantage" and supports operational cyber-risk assessment.

- According to NATO's 2026 estimates, Poland's defence effort, measured as a share of GDP, is substantially above that of Germany, Spain and the NATO Europe/Canada average.[10]

10 Public Diplomacy Division, NATO, Defence Investment of NATO Countries (2014–2026), press release, 7 July 2026, https://www.nato.int/en/news-and-events/articles/news/2026/07/07/defence-investment-update-record-spending-in-europe-and-canada

- NATO Cyber Coalition 2025 was held onsite at the Estonian Cyber Range and brought together more than 1,300 cyber defenders from 29 NATO Allies and seven partner nations.[11]

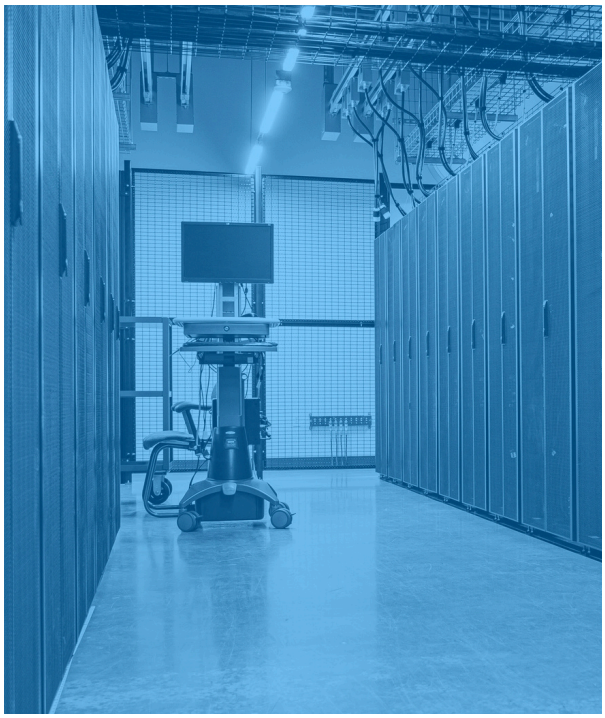
Defence Resilience Challenges

Several organisational and technical barriers to defence digital resilience currently exist. Legacy systems, procured and designed before current interoperability and cybersecurity standards existed, continue to constrain the pace at which newer, more secure architectures can be adopted. Interoperability challenges extend beyond the technical layer into organisational and doctrinal differences in how digital systems are integrated into operational planning. Evidently, barriers are not unique to Poland but are compounded, in the Polish case, by the scale and urgency of the modernisation task relative to available resources and timeframes, given the country's frontline position.

Public Procurement and Security

One of the more important findings concerns an unintended consequence of Poland's public procurement framework which has increasingly come to be perceived as an "X-ray effect", whereby procurement requirements expose sensitive information regarding critical infrastructure, systems and capabilities. Current rules require a high degree of transparency in IT system tenders for critical infrastructure, including the publication of detailed technical specifications alongside information on winning bidders and contract values. While designed to ensure fairness and accountability in public spending, this transparency requirement was described as functioning, in the security domain, as an inadvertent intelligence gift to hostile actors: a complete technical blueprint of critical infrastructure security arrangements, openly published and easily accessible.

Excessive transparency in this specific category of procurement represents a governance gap requiring urgent correction that is pointed toward the model used for Urgent Operational Requirements within the military procurement system, which allows for classified handling of sensitive purchases, as a potential template for reform of the broader public procurement regime governing critical digital infrastructure.

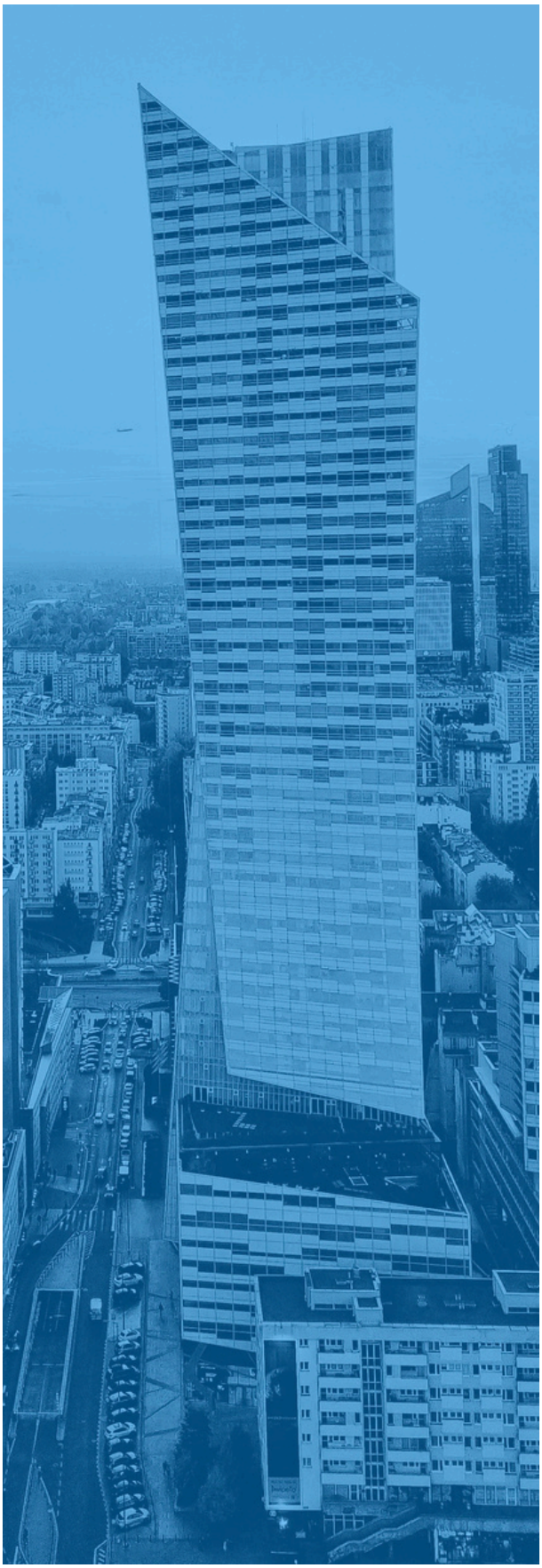


11 NATO Allied Command Transformation, NATO Cyber Coalition 2025: Advancing Cyber Defence and Strengthening Alliance Resilience, 5 December 2025, https://www.act.nato.int/article/cyber-coalition-2025/

Strategic Autonomy Concerns

Discussions also addressed the question of technological dependence on foreign providers, particularly in light of a less predictable transatlantic relationship. Concerns centre on the reliability of foreign technology partners under conditions of geopolitical stress, and on the extent to which dependence on external providers for critical defence-relevant digital capability could constrain Poland's freedom of action in a crisis.

Digital and cloud-enabled capability now underpins conventional military effectiveness; data flows themselves constitute strategic infrastructure requiring dedicated protection; procurement transparency rules designed for civilian accountability create unintended security exposure in the defence and critical-infrastructure context; and concerns about technological dependence on foreign providers are increasingly central to how defence modernisation is planned and assessed.



4 Resilience of Cloud Technology and Infrastructure

Cloud as Critical Infrastructure

Roundtable discussions were unambiguous in treating cloud infrastructure as strategic, critical infrastructure in its own right, on the same footing as energy grids or transport networks. Government services, defence-related data processing, healthcare systems and the operational technology underpinning critical infrastructure sectors are all increasingly dependent on cloud platforms for continuity, scalability and rapid response. Because of heavy dependence on cloud platforms, disruption carries systemic risk across multiple sectors simultaneously, rather than being confined to a single point of failure.

The Geolocation Versus Dispersal Debate

The most extensively debated question and the one this report treats as the central analytical thread connecting cyber, defence and cloud resilience, concerned whether the physical location of data centres and servers within Polish territory still matters for sovereignty and security, or whether geographic dispersal now offers the more credible resilience strategy. There are two clearly articulated positions:

1. Digital Security and Data Dispersion
In the digital domain, geography is of diminishing relevance because cyberspace itself has no meaningful borders. On this view, meaningful security guarantees are increasingly digital in nature, resting on cryptography, rigorous access procedures and resilient system architecture, rather than on the physical location of hardware. Discussions drew directly on lessons from Ukraine and the Iran War of 2026, where physical data centres, including facilities constructed with substantial underground protection (12 metres underground), have been destroyed by missile strikes. No degree of physical hardening within national territory can be assumed to survive sustained kinetic conflict, and that genuine resilience therefore requires embracing distributed architectures: cross-border redundancy, data dispersion across multiple jurisdictions, the concept of "data embassies" that extend legal protection to data hosted abroad, and pre-planned strategic evacuation of critical datasets beyond national borders in the event of escalating conflict.

For example, Estonia's official e-Estonia material describes its Data Embassy as an extension of the Estonian government cloud, with server resources outside territorial boundaries, under Estonian control, protected with KSI Blockchain, and capable of backing up and operating critical services from Luxembourg. Estonia's parliament ratified the Luxembourg hosting agreement in 2018, citing continuity of the Estonian state if domestic data centres stop functioning or are disturbed.

2. Sovereignty Through Territorial Control
Geolocation retains fundamental military and economic importance that digital security measures alone cannot replace. In a state of war or acute crisis, proponents argued, only infrastructure physically located within national territory can be def-

ended, secured or, if necessary, seized and controlled by domestic military units; data held abroad, in jurisdictions (e.g., in Ireland) that host substantial European cloud capacity, falls outside the reach of Polish defensive and legal jurisdiction at precisely the moment when control might matter most. Moreover, from the economic perspective, domestically located data centres generate local technical know-how, employment and tax revenue, benefits that are lost when critical data processing is hosted offshore. On this view, sovereignty, jurisdiction, military protection and strategic autonomy are best served by building and maintaining domestic hosting capacity, even where this entails higher physical vulnerability to direct attack.

Neither position commanded full consensus, and the report does not resolve the debate. What the discussions did establish clearly is that the two positions rest on different underlying assumptions about the nature of future conflict: Position A assumes that kinetic attacks on physical infrastructure are a near-certain feature of any serious escalation and plans accordingly for survivability through dispersal; Position B assumes that the ability to physically control and defend infrastructure will remain operationally decisive and that dependence on foreign-hosted infrastructure introduces its own, different, category of strategic risk. A credible national data policy will likely need to draw selectively on both positions rather than treating them as mutually exclusive: maintaining meaningful domestic hosting capacity for reasons of jurisdiction, economic development and immediate operational control, while simultaneously building the cross-border redundancy and evacuation capability that Position A identifies as essential to surviving sustained conflict.

The Data Evacuation Gap

A specific and urgent governance failure was identified in the implementation of data evacuation planning. Poland's Government Centre for Security, through its 2023 National Programme for Critical Infrastructure Protection, formally required strategic entities to prepare data evacuation plans for use in the event of kinetic conflict. However, strategic state-owned enterprises received zero budgetary support to implement these measures. Consequently, compliance remains a dead letter due to fears of permanent state audits regarding unauthorized spending.

On the other hand, Taiwan stands out internationally as the only jurisdiction to have systematically implemented lessons of this kind at scale, offering a potential model for Polish planners. Taiwan's Executive Yuan identified 18 critical public systems and an NT$1.34 billion investment for 2024–2027 to promote cryptographic splitting and backup mechanisms, plus transfer of critical public-information data to cloud storage.[12] Ukraine's emergency model is more wartime-evacuation than pre-negotiated data embassy: Ukrainian law was changed one week before the invasion to allow cloud movement, and AWS reports more than 10 petabytes migrated from gov-

12 Department of Information Services, Executive Yuan (Taiwan), Government Plan to Enhance Digital Resilience of Critical Public Information Systems, 16 November 2023, https://english.ey.gov.tw/Page/61BF20C3E89B856/b6376ceb-8367-4fd8-b287-02c5dedad875

ernment authorities, universities and private-sector entities.[13]

In Poland, by contrast, the formal obligation has not translated into operational capability: public admini-stration bodies, hospitals and banks were described as still lacking established, workable procedures for evacuating or securing critical data in the event of an escalating conflict, despite the existence of a formal regulatory mandate to do so.

The Funding Contradiction

The reason for this implementation gap was traced directly to a disconnect between regulatory obligation and budgetary support. Although the 2023 programme imposed the evacuation-planning requirement on State Treasury companies and other strategic entities, no corresponding budgetary allocation was made available to fund the necessary technical work. Affected entities have been reluctant to pursue implementation even where some capacity exists, out of concern that doing so would expose them to burdensome and repeated audit processes or to allegations of financial mismanagement should implementation choices later be questioned. The result is that the regulation has become a dead letter, a legally binding obligation that exists on paper but produces little operational resilience in practice.

US Transactional Risk and the Cloud Act

Cloud Act-related concerns can be understood across three distinct layers:

Established legal risk: Major US cloud providers remain subject to US jurisdiction, and concerns regarding the extraterritorial application of US law have been recognised in European policy and research literature.

Perceived risk: Concerns persist among some users regarding the potential loss of control over data, even in cases where mitigation measures, such as encryption or operation within European jurisdictions, may reduce exposure.

Political and geopolitical risk: Concerns regarding the possibility of service restrictions, political retaliation or access disruption remain largely speculative. While such scenarios continue to inform stakeholder debates, they should be distinguished from established legal and operational risks.

The reliability of dependence on United States-based technology providers, amid a less predictable transatlantic political environment, was also discussed. Participants raised concerns about the extraterritorial reach of US legal frameworks, under which American cloud providers may be compelled to hand over data held on behalf of foreign customers, including European government and enterprise clients, in response to requests from US authorities. Concern was also expressed about the possibility that shifts in the transatlantic trade and technology relationship, including the prospect of European measures such as a digital services tax on large US technology firms, could prompt retaliatory restrictions on the technological support extended to European partners.

13 Amazon News (AWS), Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future, 9 June 2022, updated 14 April 2023, https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future

Growing concerns regarding the unconditional reliability of technology providers operating under a single foreign jurisdiction are shaping procurement behaviour and cloud diversification strategies which have contributed to increased interest in European-developed cloud alternatives, contractual safeguards against extraterritorial data access, and diversified provider arrangements for critical workloads.

Cloud infrastructure is now critical infrastructure in its own right; the geolocation-versus-dispersal debate remains genuinely unresolved and likely requires a hybrid national approach rather than a binary choice; a formally mandated data evacuation obligation exists without the funding needed to implement it; and geopolitical uncertainty surrounding US technology providers is reshaping Polish and European cloud diversification strategy.



5 Lessons Learned for European Coordination & Recommendations

Lessons for Europe

Poland's experience carries broader implications for how the European Union approaches resilience governance, cross-border cooperation, digital sovereignty and interoperability. The Polish case illustrates, in particularly acute form, a pattern likely present to varying degrees across the Union: a gap between the ambition of EU-level regulatory frameworks and the national administrative and financial capacity needed to implement them; a structural vulnerability concentrated in SMEs embedded within critical and dual-use supply chains; and an unresolved tension between the openness required for economic integration and the sovereignty concerns raised by dependence on non-European technology providers.

EPRS reports that three US-based companies account for 65% of the EU cloud services market and that the US has twice Europe's share of global data-centre capabilities despite comparable GDP.[14] Bertelsmann Stiftung argues that more than 80% of Europe's digital technologies and infrastructures are imported and 70% of foundational AI models used globally originate in the United States.[15]

European Coordination Challenges

Several specific coordination challenges emerge. Funding fragmentation across national and EU instruments was identified as limiting the ability of individual member states, and particularly smaller or less well-resourced ones, to compete effectively for major EU digital and resilience funding streams. Limited coordination among Central and Eastern European states compounds this problem as larger Western European member states have been more successful in mounting joint, cross-border applications for flagship EU projects, including AI infrastructure initiatives, while CEE states have more often competed individually and with less success, producing a pattern of unequal access to strategic EU projects that CEE participants argued does not reflect the underlying technical capability of the region's firms and institutions.

Cloud sovereignty at the European level is a further coordination challenge, addressed in more detail below, alongside the broader difficulty of achieving genuine interoperability, technical, procedural and legal, across member states with differing threat perceptions, administrative traditions and levels of digital maturity.

---

14 Tristan Marcelin, Cloud and AI Development Act, European Parliamentary Research Service, PE 779.251, December 2025, https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/779251/EPRS_BRI%282025%29779251_EN.pdf

15 Bertelsmann Stiftung, EuroStack – A European Alternative for Digital Sovereignty, 13 February 2025, https://www.bertelsmann-stiftung.de/en/our-projects/reframetech-algorithmen-fuers-gemeinwohl/project-news/eurostack-a-european-alternative-for-digital-sovereignty

Western Institutional Protectionism

Another sensitive theme concerns the design of EU-level cloud sovereignty initiatives and their effect on the participation of CEE technology firms. There exists a belief among Polish stakeholders that the structure of the EU tenders for sovereign cloud capacity has evolved in a manner that favours French and German firms while placing well-established Polish technology companies at a competitive disadvantage.

EUISS reports Member State divisions over EUCS sovereignty requirements, with Poland among countries that earlier opposed strict sovereignty clauses, while France, Germany, Italy and Spain supported stricter approaches.[16] The European Commission's sovereign cloud tender awarded four contracts and explicitly justified diversification and objective sovereignty scoring, so the discrimination claim should be presented as a stakeholder concern requiring procurement-record analysis, not as verified fact. The European Commission's sovereign cloud framework assessed providers against eight sovereignty objectives and SEAL levels; its 2026 tender was worth up to €180m over six years.[17]

What the discussion does establish is that regulatory protectionism toward the region's larger Western economies is itself a factor shaping how CEE governments and firms approach future European sovereignty and procurement initiatives. Changes to the design of the European sovereign cloud procurement process reduced the participation of mature Polish technology companies with international operations. As a result, the initiative became increasingly concentrated among a small number of consortia of French and German companies. Building regional coalitions, for instance among Poland, the Czech Republic and Slovakia, offers a more effective route to securing equitable participation than pursuing national-level advocacy alone.

Recommendations

National Level:

- **Establish a classified procurement pathway** for critical digital infrastructure, modelled on the Urgent Operational Requirement mechanism used in military procurement, to remove the current requirement for full public disclosure of technical specifications and vendor details in sensitive IT tenders.

- **Create a national data management policy** that establishes a comprehensive framework for data protection, emergency continuity measures and the development of domestic cloud capabilities, while enabling the secure and responsible utilisation of data assets.

16 European Union Institute for Security Studies (EUISS), Technical is Political: When a Cloud Certification Scheme Divides Europe, 3 November 2025, https://www.iss.europa.eu/publications/briefs/technical-political-when-cloud-certification-scheme-divides-europe

17 European Commission, Commission Advances Cloud Sovereignty Through Strategic Procurement, 17 April 2026, https://commission.europa.eu/news-and-media/news/commission-advances-cloud-sovereignty-through-strategic-procurement-2026-04-17_en

- **Accelerate adoption of national cloud legislation** within the current parliamentary term; discussions noted that failure to pass such legislation within this window would see the current legislative effort lapse, delaying Poland's cloud resilience transformation by a further legislative cycle.

- **Create dedicated, ring-fenced funding mechanisms** to operationalise the existing data evacuation obligations imposed on strategic entities, resolving the current gap between regulatory mandate and budgetary support.

- **Develop a targeted SME cybersecurity capability support programme**, providing dual-use and defence-supply-chain SMEs with financing, tooling guidance and technical assistance to meet rising compliance obligations, rather than leaving smaller firms to interpret and fund these requirements unassisted.

- **Adopt a national resilience governance framework** that formally integrates cyber, defence-digital and cloud resilience planning, reflecting the functionally fused nature of these domains in the Polish threat environment.

Regional Level:

- **Establish a Central and Eastern European resilience coalition** capable of coordinating policy positions, funding applications and procurement standards across the region.

- **Conduct joint cyber exercises** among CEE states to build shared technical capability and interoperable incident-response procedures.

- **Pursue shared procurement and funding initiatives**, including joint applications for EU digital infrastructure funding, to overcome the coordination disadvantage CEE states currently face relative to larger Western European member states.

- **Build a CEE resilience consortium** around cloud disaster recovery, NIS2 implementation tooling, public-sector cyber workforce, and critical-entity exercises, using EU CER and NIS2 mechanisms for cross-border preparedness.

- **Coordinate public procurement demand** so Polish, Czech and Slovak providers can scale into EU sovereign-cloud and AI infrastructure tenders, rather than bidding as fragmented national suppliers.

European Level:

- **Strengthen implementation support** for the NIS2 Directive, recognising that uneven transposition across the Union reflects capacity constraints as much as differences in political will, and that EU-level technical and financial assistance could materially improve compliance outcomes.

- **Strengthen coordination and representation** within European Union structures to support participation in major EU-funded initiatives and strategic projects. Enhanced cooperation among Central and Eastern European countries may facilitate the development of joint cross-border proposals and improve access to funding opportunities (e.g., AI Factories / IPCEI).

- **Strengthen regional cooperation** in European cloud and digital infrastructure initiatives to support broader participation in strategic technology programmes and procurement opportunities. Enhanced coordination with other Central and Eastern European countries could help increase the visibility of regional capabilities and facilitate greater involvement of technology companies from the region in European digital and cloud-related projects.

- **Deepen EU-NATO coordination** on digital defence and resilience standards, building on the interoperability lessons emerging from national defence modernisation efforts.

- **Develop European crisis data-continuity mechanisms** capable of supporting member states' data evacuation and dispersal needs in the event of escalating conflict, drawing on the concepts of data embassies and cross-border redundancy discussed in Section 4.

Conclusion

Poland's approach to resilience reflects the reality of its position as a frontline state: threat awareness is high, the political will to act is evident, and the roundtable discussions summarised in this report demonstrate a policy community that understands, in granular detail, the nature of the risks it faces. Yet resilience in Poland remains a whole-of-society challenge whose components are deeply interconnected rather than separable: a cyberattack on critical infrastructure is rarely a purely technical event but increasingly a tool of hybrid warfare aimed at eroding public trust; defence modernisation is, in practice, a data and cloud infrastructure project as much as a conventional capability programme; and the debate over cloud geolocation versus dispersal sits at the intersection of all three domains, touching sovereignty, military protection, economic development and digital security simultaneously. Addressing any one domain effectively requires attention to the other two.

The structural gaps identified in this report, SME vulnerability within dual-use supply chains, procurement transparency rules that inadvertently expose sensitive infrastructure, fragmented cloud governance, and resilience mandates issued without matching funding, are not unique to Poland, but they are experienced with particular intensity given the country's exposure. Left unaddressed, they risk leaving substantial parts of Poland's critical infrastructure less resilient in practice than national regulation suggests on paper.

Meeting these challenges will require sustained action at the national level, closer coordination among Central and Eastern European states facing similar structural pressures, and a European Union policy architecture that more fully accounts for the frontline perspective in the design of resilience funding, sovereignty initiatives and regulatory implementation support. Poland's experience offers the European Union a concentrated view of resilience challenges that other member states may encounter in less acute form as the continent's threat environment continues to evolve. Treated as a source of lessons rather than an exceptional case, it can usefully inform a more coherent and better-resourced European approach to resilience across cyber, defence and cloud infrastructure.

About the European Resilience Project

In a joint effort, three members of the Aspen International Partners network — Aspen Institute Central Europe, Aspen Institute Germany, and Aspen Institute España — with the support of Microsoft and in collaboration with Aspen Institute Romania, launched a cross-border initiative aimed at examining and strengthening European resilience across the interconnected domains of cyber, defense, and cloud infrastructure. As part of the project, four European Resilience Roundtables were convened in Warsaw, Berlin, Madrid, and Brussels, bringing together senior representatives from government, defense institutions, industry, and the broader policy community in each country to examine national resilience challenges and identify lessons relevant at the European level. The insights generated across the four roundtables are captured in a series of European Resilience Reports presented to key EU stakeholders.

About the Aspen Institute Central Europe

Aspen Institute Central Europe is an independent platform that mediates interdisciplinary and regional cooperation and supports young Central European leaders. It serves as a politically and ideologically neutral platform for democratic discussions about global, political, economic and social issues to promote the functioning and development of democratic values. Aspen Institute Central Europe fosters values-based leadership with the belief that it is essential for a free, just and equitable society.

More information about the Aspen Institute Central Europe:
https://www.aspeninstitutece.org

More information about the Aspen Institute International Partners:
https://www.aspeninstitute.org/programs/international-partners

Imprint

Publishers:
Aspen Institute Central Europe
Palackého 740/1
110 00 Prague 1
Czech Republic

The Aspen Institute
2300 N St NW, Suite 700
Washington, DC 20037
USA

Authors:
Aspen Institute Central Europe

International Project Lead: Florentina Dumitru
Domestic Project Lead: Bartlomiej Kot

Design and Layout: Logan Richman | The Aspen Institute

Publication: October 2026

The Aspen Institute International Partners and Aspen Institute Central Europe wish to thank Microsoft for its support and partnership in this project.

The findings included in this report are drawn from the roundtable and expert discussions and do not necessarily reflect the official views of the Institute. All content was reviewed and verified by the project team. Photography was sourced via Unsplash and Pexels.

INTERNATIONAL PARTNERS
aspen institute

aspen institute central europe

Microsoft