

Policy Brief

Ukraine's Cyber Defence Evolution: The Role of Non-State Actors and Public-Private Partnerships



Executive Summary

Ukraine's cyber defence ecosystem has undergone a major transformation since the February 2022 full-scale Russian invasion, creating an important case for understanding modern cyber defence during a long-term active conflict. Together with our partners, NATO CCDCOE has conducted interviews and surveys with 39 respondents from 21 Ukrainian organisations across government, military, private sector, and civil society organisations. This brief examines how Ukraine has adapted its cyber defence architecture and identifies some critical lessons for NATO and allied countries going forward.

Ukraine's cyber resilience rests on four interconnected pillars: the government's innovative approach, expanded roles for private sector actors, intensive international partnerships, and integration with multinational technology companies. While vital for survival, these arrangements have created strategic dependencies that may impact sovereign decision-making and raise questions about their long-term sustainability. Over 85% of the surveyed Ukrainian organisations rely heavily on US-based technology providers, creating a vulnerability where operational continuity could depend on the political and financial alignment of foreign entities. Moreover, informal personal networks have frequently proven more effective than formal coordination channels during a crisis, providing the agility that rigid structures lack. Ukraine's own 2021 Cybersecurity Strategy acknowledged the absence of an effective public-private partnership (PPP) model, a gap that the conflict has forced rapid and largely ad hoc improvisations to address, resulting in a resilient but fragmented ecosystem.¹

As a result, three key recommendations may be derived: (i) developing pre-crisis partnership frameworks, (ii) formalising the role of non-state actors in cyber defence, and (iii) collectively addressing the digital sovereignty implications of deep dependencies on foreign technology companies.

1 Ukraine. (2021). Decree of the President of Ukraine on the Decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine." <https://zakon.rada.gov.ua/laws/show/447/2021#Text>

Authors

Erik Kursetgjerde (STRAT, CCDCOE)
Erdi Dönmez (STRAT, CCDCOE)
Dr. Aleksı Kajander (LAW, CCDCOE)
Dr. Andrii Davydiuk (P&C, CCDCOE)

Contributors

Mykola Khudyntsev — Institute of Telecommunications and Global Information Space of National Academy of Sciences of Ukraine
Natalia Mishyna — former Visiting Scholar (CCDCOE)

Introduction

Russia's full-scale invasion of Ukraine on 24 February 2022 created an unprecedented test for modern cyber defences. Unlike previous conflicts where cyber operations remained largely outside the public view, Ukraine has been compelled to simultaneously defend against sophisticated state-sponsored attacks while maintaining service continuity under kinetic bombardment and responding to the physical seizure of digital infrastructure. This dynamic was starkly illustrated in Kherson, where Russian occupying forces seized local data centres and network equipment,² turning physical control of territory directly into leverage over digital infrastructure.

The kinetic destruction and seizing of data centres accelerated an urgent migration of government data and critical services to cloud platforms. For NATO and allied nations, Ukraine's experience raises fundamental questions about crisis preparedness: how quickly can international cyber partnerships mobilise? What are the consequences of deep reliance on foreign technology companies for sovereign functions? How can volunteers and private sector actors be effectively integrated without compromising operational security? What legal and institutional frameworks enable coherent cyber defence under wartime conditions?

This brief synthesises findings from a comprehensive literature review, an analysis of Ukrainian domestic legislation and academic sources, and a NATO CCDCOE survey and interviews.³ The survey and interviews span 39 respondents from 21 different Ukrainian organisations, representing a diverse cross-section of the ecosystem, including government, military, private sector, and civil society organisations.

Public-Private Partnerships in Ukrainian Law and Practice

Ukraine's 2021 Cybersecurity Strategy explicitly acknowledged the absence of an 'effective model of public-private partnership,' describing the existing situation as one at the level of political declarations, partnership is supported, but institutionally it is not formed.⁴ Ukraine entered the full-scale conflict in 2022 with formal institutional frameworks lagging, and the strong vertical and horizontal trust within the cyber community became the substitute for the missing regulations. When the full-scale invasion necessitated an immediate response, the informal foundation allowed for the rapid integration of private expertise.

Legislative Gaps

The legislative architecture is fragmented. The Law of Ukraine 'On the Basic Principles of Ensuring Cybersecurity in Ukraine' and the National Cybersecurity Strategy are framework documents that lack implementing regulations.⁵ Critically, until the 2025 amendment, the Law 'On Public-Private Partnership' from 2010 did not list cybersecurity as an eligible domain for PPP agreements, effectively blocking formal partnership contracts at national and regional levels.⁶ Draft Law No. 14150 'On Public-Private Cooperation in the Field of Cybersecurity', registered in parliament in October 2025, represented an attempt to address this gap, but its very necessity confirms that the current framework remains inadequate.⁷ While the 2025 amendments to Law 'On Public-Private Partnership' have recognised cybersecurity as an eligible domain, the classic PPP-model remains inapt.⁸ The frameworks are designed for infrastructure-heavy, long-horizon investments, while wartime cyber defence requires agile instruments for rapid mobilisation and resource sharing.

- 2 Freedom House. (2022). Freedom on the Net 2022: Ukraine. <https://freedomhouse.org/country/ukraine/freedom-net/2022>
- 3 Interviews and survey conducted between August and October 2025. The sample size is limited and may not reflect the full diversity of Ukraine's cybersecurity ecosystem.
- 4 Ukraine. (2021). Decree of the President of Ukraine On the Decision of the National Security and Defence Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine". <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
- 5 Ukraine. (2017). Law of Ukraine On the Basic Principles of Ensuring Cybersecurity of Ukraine. <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
- 6 Ukraine. (2010). Law of Ukraine On Public-Private Partnership. <https://zakon.rada.gov.ua/laws/show/2404-17#Text>
- 7 Ukraine. (2025). Draft Law No. 14150 "On Public-Private Partnership in the Field of Cybersecurity". Verkhovna Rada of Ukraine. <https://itd.rada.gov.ua/billInfo/Bills/Card/45219>
- 8 Ukraine. (2025). Law of Ukraine "On Public-Private Partnership" No. 4510-IX. Verkhovna Rada of Ukraine. <https://zakon.rada.gov.ua/laws/show/4510-20>

Institutional Fragmentation

The 2020 Information and Cybersecurity Council (ICSC, in Ukrainian: RIKB) was designed as a multi-stakeholder platform, with no more than 40% membership from the public sector.⁹ However, limited institutionalisation has constrained its financial and communicative capacity, with the price of RIKB's independence being a limited resource base, which in the long-term risks reducing the sustainability of the instrument. This further constrains RIKB's capability to serve as a reliable anchor for broader coordination across the cybersecurity ecosystem. Without stable coordination platforms, private sector and civil society actors have engaged in cyber defence primarily on a volunteer or temporary basis, dependent on individual initiative rather than systemic procedures.

The IT Army and Volunteer Integration

The creation of the IT Army of Ukraine, initiated by the Ministry of Digital Transformation following the February 2022 invasion, demonstrated the spontaneous self-organising capacity of the Ukrainian IT community. These formations provided critical functions in countering disinformation, sharing attack data, and conducting defensive operations. However, their legal status

remained ambiguous.¹⁰ The lack of formal mechanisms for integrating such volunteer communities into the defence framework creates risks for both law and order and the state's cybersecurity as a whole. There is a clear need to move from spontaneous mobilisation toward structured, legally grounded models of private and volunteer participation. Ukraine's experience therefore highlights a broader challenge faced by allied nations: how to utilise the speed and technical capacity of non-state actors without leaving them, and the state, exposed by the absence of a clear legal framework. It is precisely this gap that more institutionalised international mechanisms are beginning to address.

The emerging EU Cyber Reserve, foreseen by the EU Cyber Solidarity Act and operationally managed by ENISA, illustrates how wartime lessons from Ukraine are being translated into institutionalised crisis mechanisms — offering pre-contracted services from trusted private providers deployable when national resources prove insufficient. Ukraine has begun the process of joining the Cyber Reserve, providing a structured pathway to mobilise private sector incident response expertise during crises affecting critical infrastructure.

Key Findings from Survey and Interviews

Together with our Ukrainian partners, NATO CCDCOE conducted a survey and interviews with Ukrainian cybersecurity stakeholders between August and October 2025. In total, 39 responses were received from representatives from 21 different military organisations, government agencies, private sector companies, and civil society institutions. Respondents spanned technical experts, consultants, policymakers, and senior decision-makers. Due to security considerations, individual responses and institutional identities are not disclosed. The research revealed deep intertwining with multinational technology companies, limited formal coordination between public and private sector, gaps in legislation and the decisive role of the international partnerships.

Dependencies on Multinational Technology Companies

Ukraine's cyber defence infrastructure has become deeply intertwined with multinational technology companies, particularly US-based providers. Over 85% of the surveyed organisations indicated heavy reliance on entities such as Microsoft, Amazon Web Services, Cloudflare, Cisco, and Palo Alto Networks across cloud infrastructure, endpoint protection, network security, and threat intelligence.

85%



of surveyed organisations rely on U.S. technology providers

(Microsoft, AWS, Cloudflare, Cisco, Palo Alto Networks)



62%



share of the global cloud market controlled by three U.S. providers



29%

20%

13%

⁹ State Service of Special Communications and Information Protection of Ukraine. (2020). The expert council on information and cybersecurity at the State Service for Special Communications will bring together specialists from government agencies, the commercial sector, and scientists, which will strengthen Ukraine's national cybersecurity system. <https://cip.gov.ua/ua/news/ekspertna-rada-z-informacii-noy-ta-kiberbezpeki-pri-derzhspeczv-yazku-ob-yednaye-fakhivciv-z-derzhavnikh-organiv-komer-ciinogo-sektoru-ta-naukovciv-sho-posilit-nacionalnu-sistemu-kiberbezpeki-ukrayini>

¹⁰ DOU. (2022). The Ministry of Digital Transformation is creating an IT Army. There are tasks for everyone. <https://dou.ua/forums/topic/36716/>

The scale of international support has been extraordinary, though it represents an intersection of security assistance and strategic market expansion where Ukraine has become a proving ground for technologies deployed at a scale and intensity unmatched in any previous conflict environment. Several companies made substantial contributions to Ukraine: Amazon AWS migrated critical government data to European data centres.¹¹ Microsoft established an encrypted round-the-clock channel with the Ukrainian government and provided technical support exceeding half a billion US dollars.¹² Google expanded cybersecurity services enabling continued operations despite heavy cyberattacks.¹³

However, this dependence has generated significant strategic vulnerabilities. The most frequently cited concern involves vendor lock-in, where architectural decisions made under emergency

conditions have created path dependencies that are prohibitively difficult to reverse. As of Q3 2025, AWS, Microsoft Azure, and Google Cloud collectively controlled 62% of the global cloud market (29%, 20%, and 13% respectively).¹⁴ Several technical experts explained that switching vendors would require rebuilding entire technology stacks, effectively trapping organisations in existing arrangements regardless of future geopolitical considerations. In response, Ukraine’s Cabinet of Ministers approved new rules in 2024 specifically designed to prevent vendor lock-in in state IT systems.¹⁵

Financial sustainability was a further concern. In the survey several organisations acknowledged that initial international support came through humanitarian or subsidised channels whose continuation beyond the active conflict phase remains uncertain. This creates a

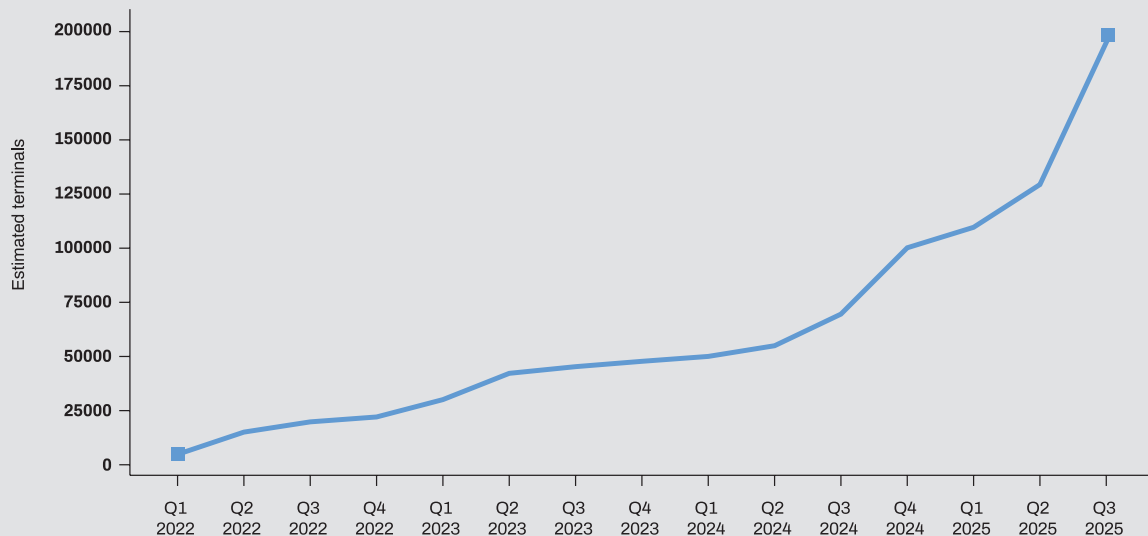
Case: The Starlink Dependency

Ukraine's former Minister of Digital Transformation Mykhailo Fedorov described Starlink as 'the blood of our entire communication infrastructure.' Yet the service is controlled by a single individual whose commercial and political decisions directly affect Ukrainian military and civilian capabilities.

In October 2022, Elon Musk announced SpaceX would no longer provide the service for free, and subsequently

declined to activate Starlink coverage for a Ukrainian military operation against the Russian Black Sea fleet.¹⁶ This case illustrates the fundamental challenge: Big Tech support is voluntary and can change rapidly for political, economic, or personal reasons, with no guarantee of continuity. For Ukraine, this has necessitated a shift toward diversifying satellite providers to ensure that no single individual can exercise a veto over national defence operations.

Estimated Starlink Terminals Deployed to Ukraine (2022-2025)



Estimates compiled by the author based on R. Guarantz, *Satellites in the Russia-Ukraine War* (Carlisle, PA: U.S. Army War College Press, 2024); and G. Tskhakaia, "Space and the Data Domain: Lessons from Ukraine" (Washington, D.C.: Center for Strategic and International Studies, 2025).

- Lilly, B. et al. (2023). *Business@War: The IT Companies Helping to Defend Ukraine*. Proceedings of: 15th International Conference on Cyber Conflict: Meeting Reality. Tallinn, Estonia, 2023. https://www.researchgate.net/publication/372516532_BusinessWar_The_IT_Companies_Helping_to_Defend_Ukraine
- Mearian, L. (2022). "How Microsoft Is Helping Ukraine's Cyberwar Against Russia," *Computerworld*, <https://www.computerworld.com/article/1617301/how-microsoft-is-helping-ukraine-s-cyberwar-against-russia.html>.
- Google Cloud. (2022). "How Google Cloud Is Helping Those Affected by War in Ukraine," *Google Cloud Blog*, <https://cloud.google.com/blog/products/identity-security/how-google-cloud-is-helping-those-affected-by-war-in-ukraine>
- Synergy Research Group. (2025, November 19). *Cloud market share trends — Big Three together hold 63% while Oracle and the Neoclouds inch higher*. <https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher>
- Cabinet of Ministers of Ukraine. (2024). "Government adopted new rules for the establishment and administration of state IT systems," Available at: <https://www.kmu.gov.ua/news/uriad-ukhvalyv-novi-pravyla-dlia-stvorennia-ta-administruvannia-derzhavnykh-it-system>
- Browne, R. (2023). How Elon Musk's control of Starlink complicates U.S. support for Ukraine. *The New York Times*. <https://www.nytimes.com/interactive/2023/07/28/business/starlink.html>

sustainability gap, where the transition from emergency assistance to long-term commercial contracts may become a fiscal burden that the state cannot yet fully absorb, potentially leading to a degradation of cyber capabilities. Most respondents weighed data sovereignty concerns against the reality that domestic infrastructure faces greater risk from Russian kinetic and cyber attacks than from foreign legal jurisdiction. As one government decision-maker noted, ‘the risk of data loss due to hostilities far outweighs the risk of storing data abroad, making foreign cloud services a pragmatic necessity despite sovereignty concerns.’ The European Union faces parallel exposure: three out of four European listed companies depend on American cloud services, with some countries exceeding 90% dependency.¹⁷ Ukraine’s experience demonstrates both the critical importance of Big Tech capabilities and the strategic vulnerability created when national security relies heavily on a small number of private companies.

vulnerability. When personnel change or informal relationships deteriorate, coordination mechanisms can collapse. The absence of institutionalised channels means that effective information sharing depends on personal relationships.

Legal and Regulatory Frameworks

Ukrainian cybersecurity legislation was generally rated as ‘somewhat effective to effective’ by respondents, with acknowledgement that regulatory documents and technical standards reflect international best practices. However, respondents consistently distinguished between legislative quality and practical implementation: even well-designed regulations fail when institutions lack resources, personnel, or political will to enforce them.

Frameworks for non-state actors received particularly critical assessments. With the exception of critical infrastructure regulations,

Formal structures meet reality:

78%

use official channels



64%

report coordination problems



What actually works:

42%

depend on informal contacts



61%

use Signal and other secure messaging services



34%

participate in external projects outside the hierarchy



Challenges in Coordination: From Informal Networks to Institutional Frameworks

Prior to February 2022, formal coordination between government agencies and private sector cybersecurity organisations remained limited. The intensity of Russian cyber operations forced rapid improvisation, with private companies, volunteer groups, and international organisations stepping in to fill critical capability gaps.

Respondents described a coordination landscape operating simultaneously through official channels: formal correspondence, working groups, memorandums of understanding — and informal trust networks, with personal contacts frequently proving more effective for rapid response. As one technical expert noted, ‘personal contacts play the biggest role in effective coordination.’

Communication primarily relied upon Signal, WhatsApp, and direct personal contact rather than secure institutional channels. This informality acted as both a strength for enabling speed impossible through official processes but also as a structural

the state does not meaningfully regulate volunteer cyber defence activities or private sector incident response operations, which creates a legal grey zone that complicates long-term integration and compliance with international law. While Law No. 4336-IX strengthens accountability for officials and operators of critical information systems, the implementing instruments remain incomplete as the broader challenge of public-private coordination remains unresolved.¹⁸

Multiple respondents called for frameworks enabling expedited decision-making and temporary suspension of certain requirements during active cyber attacks, balanced against tougher sanctions for serious violations. Formal rapid-exchange mechanisms that would institutionalise the proven informal communication channels were specifically identified as a priority. These legal uncertainties, notably absent from international academic literature, reinforce the case for comparative research into national legislative frameworks and their adequacy under crisis conditions.

¹⁷ Proton AG. (n.d.). Europe’s tech sovereignty watch. Proton for Business. <https://proton.me/business/europe-tech-watch>

¹⁸ Ukraine. (2025). Law of Ukraine No. 4336-IX “On Amendments to Certain Laws of Ukraine Regarding Information Protection and Cybersecurity of State Information Resources, Critical Information Infrastructure Objects”. Verkhovna Rada of Ukraine. <https://zakon.rada.gov.ua/laws/show/4336-20#Text>

International Partnerships: Critical Enablers with Sustainability Challenges

An overwhelming majority of respondents confirmed that international partnerships have significantly improved cyber defence capabilities. The United States emerged as the dominant partner. European partners, particularly Estonia, Germany, Poland, the United Kingdom, and Denmark, received frequent mention as important technology suppliers and sources of technical assistance. The primary advantages centre on access to technology and knowledge, trained workforce development, and gaining visibility into adversary tactics through international threat intelligence sharing networks.

However, much of the support provided since February 2022 came through emergency assistance channels or corporate humanitarian programmes that were explicitly temporary. Grant dependency emerged as a recurring concern where organisations have built critical capabilities around equipment, software, and services provided through donor programmes that, when they end, may leave organisations facing capability gaps they cannot fund independently.

Recommendations

Recommendation 1: Develop Pre-Crisis Partnership Frameworks

Ukraine's experience demonstrates that waiting until the crisis starts to establish technology partnerships results in critical delays and suboptimal arrangements made under emergency conditions. Allied nations should:

- Negotiate standing agreements with major technology providers for crisis support, pre-positioning equipment, licences, and data migration capabilities;
- Establish secure communication channels and coordination protocols before they are needed, and test them through regular joint exercises;
- Address the underlying tensions between private and public sector interests within these frameworks, building trust before it is tested under fire;
- Develop crisis procurement procedures, allowing rapid acquisition of technology, licences, and services during active incidents, with pre-agreed pricing and delivery terms that do not require full peacetime procurement cycles;
- Explicitly integrate civilian capabilities into NATO COPD planning processes, conduct CIMIC exercises and ensure civilian actors are included from the outset rather than consulted after crisis begins.

Recommendation 2: Formalise the Role of Non-State Actors in Cyber Defence

Modern cyber defence cannot rely solely on government and military capabilities. Private sector companies, volunteer organisations, and individual experts provide critical capabilities that government institutions cannot match at the required speed and scale. NATO should develop model frameworks that member states can adapt, establishing:

Ukraine's wartime experience underscores that PPP is not only about emergency donations or informal coordination, but also about enhancing supply chain security by reducing single points of failure, limiting vendor lock-in, and ensuring that critical services remain defensible even when the front line extends into software, cloud infrastructure, and outsourced digital services.

Ukraine's experience demonstrates that effective cyber defence requires continuous civilian involvement — not just consultation once a crisis has arrived. While NATO's Comprehensive Operations Planning Directive (COPD) already partly addresses civil-military coordination in crisis planning, its application to cyber defence remains underdeveloped.¹⁹ NATO should explicitly integrate non-state cyber capabilities into COPD planning processes, ensuring that private sector and volunteer actors are incorporated into operational planning from the outset.

- Clear legal authorities that authorise the participation of the private sector in cyber defence activities, as well as outlining their tasks or responsibilities;
- Liability protections that encourage engagement without exposing participants to undue legal risk;
- Establish frameworks that ensure sensitive proprietary data shared by the private sector is protected from unauthorised government disclosure or competitive misuse;
- Security clearance procedures enabling appropriate information sharing;
- Coordination mechanisms that function under crisis conditions.

Volunteer organisations should not exist in a legal limbo where their responsibilities, status, and tasks remain undefined. NATO member states should conduct national legal audits to assess whether their existing frameworks would provide sufficient certainty for private sector and volunteer actors during an active armed conflict. This includes evaluating whether current labour laws and mobilisation frameworks allow private experts to contribute to national cyber defence without losing their primary employment or facing conflict-of-interest charges.

Recommendation 3: Collectively Address Digital Sovereignty Implications

Ukraine's necessary reliance on US-based cloud services during wartime highlights challenges all allied nations face regarding data jurisdiction, service continuity, and strategic autonomy. Rather than pursuing purely national solutions, allies should develop collective approaches:

- Negotiated agreements with major technology providers regarding data handling, continuity obligations, and legal jurisdiction over sensitive government data;
- Investment in European and allied technology capabilities providing alternatives to dominant platforms, reducing the

19 NATO Allied Command Operations. (2010). Comprehensive Operations Planning Directive (COPD), Interim Version 1.0. Supreme Headquarters Allied Powers Europe (SHAPE)

concentration risk illustrated by Ukraine's experience;

- Regulatory frameworks ensuring critical services maintain operations even during periods of geopolitical tension.

As the Royal United Services Institute's analysis of European cloud adoption for national security concludes, 'the strategic question is therefore not whether governments should adopt cloud technologies, but how they should navigate trade-offs to maximise benefits for national security and defence.'²⁰

The Path Forward

Cyber defence transformation under sustained conflict provides invaluable lessons. Ukraine's experience reveals both remarkable capabilities that can be mobilised through international partnerships and structural vulnerabilities that emerge when national defence becomes deeply dependent on foreign technology companies and donor funding. The value of preparation is evident across all four pillars: public-private partnerships, legislative frameworks, coordination channels, and international support arrangements.

Both the international academic literature and Ukrainian domestic sources confirm the three structural themes underlying PPP in cyber defence: the inherent tension between private and public sector interests; the challenges of trust and information sharing; and the strengthening, if still incomplete, role of the state. Ukraine has been forced to navigate all three simultaneously, amidst an active armed conflict, and largely without the benefit of pre-crisis preparation.

For NATO and allied nations, the most fundamental insight is that effective modern cyber defence requires integration across the government, military, private sector, and civil society in ways that defy traditional organisational boundaries. Effective cyber support to an ally under attack requires not just government-to-government assistance, but the facilitation of private sector engagement, volunteer mobilisation, and rapid technology transfer. The frameworks to enable this must be built before they are needed.

The question of digital sovereignty emerges as perhaps the most strategically significant long-term challenge. Dependence on American technology platforms has been essential for Ukraine's survival, but creates vulnerabilities regarding data control, service continuity, and strategic autonomy that extend well beyond the current conflict. Ukraine's ongoing adaptation will undoubtedly continue to inform alliance thinking for years to come.

20 Jarnecki, J. (2025). European Cloud Adoption for National Security. Available at: <https://static.rusi.org/european-cloud-adoption-for-national-security.pdf>

Acknowledgments

This brief is based on NATO CCDCOE research conducted in partnership with Ukrainian stakeholders, whose cooperation and openness under extraordinarily difficult conditions made this work possible. We are also grateful to all the Ukrainian respondents and organisations who participated in our survey and interviews.

We acknowledge the valuable contributions of our Ukrainian research partners, Mykola Khudyntsev of the Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, and Natalia Mishyna, former Visiting Scholar at CCDCOE, whose expertise and networks were instrumental in shaping both the research and its findings.

About NATO CCDCOE

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia is the leading dedicated hub for NATO allies and like-minded nations to jointly raise their cyber defence capabilities. The NATO-accredited Centre provides valuable expertise on cyber defence across strategic, legal, operational, and technical realms. Today, 39 Allied and Partner countries are contributing to the work of the Centre.

Disclaimer. This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). The expressions reflected are those of the author(s) alone; publication by the Centre should not be interpreted as endorsement thereof by the Centre, its Sponsoring Nations or NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication. Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation. Please contact industry@ccdcoe.org with any further queries.