НАПРЯМ 7. ЦИФРОВА БЕЗПЕКА ТА КІБЕРСТІЙКІСТЬ ЯК ЕЛІЕМЕНТ ПРАВОВОЇ СТАБІЛЬНОСТІ

DOI https://doi.org/10.36059/978-966-397-632-7-20

CYBER RESILIENCE IN UKRAINE: A CRISIS-DRIVEN MODEL OF INSTITUTIONAL ADAPTATION AND NORMATIVE STABILITY IN CYBERSPACE

Solomiia Beska
MA in International Relations, Central European University, Vienna, Austria, PhD Researcher in Law, West Ukrainian National University, Ternopil, Ukraine Research Affiliate, Democracy Institute, Central European University, Budapest, Hungary, Administrative Trainee, Federal Ministry for Innovation, Mobility and Infrastructure, Vienna, Austria

The transformation of Ukraine's cybersecurity governance since 2014 provides a unique empirical case for examining how normative stability in legal and institutional frameworks may emerge under conditions of persistent crisis. Contrary to traditional institutional theories that assume stability as a prerequisite for effective governance, the Ukrainian case demonstrates that institutional resilience can be constructed through processes of crisis-driven adaptation and legal transformation.

Since the beginning of Russian hybrid aggression in 2014, Ukraine has experienced a sequence of large-scale cyber operations targeting critical infrastructure and state institutions. Among the most significant incidents were the BlackEnergy cyberattack on Ukraine's electricity grid in 2015, the global NotPetya malware campaign in 2017, and the cyberattack on the Kyivstar telecommunications network in 2023. These incidents revealed significant vulnerabilities within Ukraine's cybersecurity architecture and forced policymakers to reconsider the institutional and legal foundations of cyber governance [1, 2].

Traditional rationalist approaches to cybersecurity governance assume that states develop cyber resilience through anticipatory planning, strategic doctrines, and institutional foresight [3, 4]. Within this framework, resilience is treated as the product of deliberate policy design implemented before major cyber incidents occur. However, Ukraine's experience challenges this assumption. At the beginning of the conflict, Ukraine possessed fragmented

cybersecurity institutions and limited legal coordination mechanisms, which made the country particularly vulnerable to cyber operations.

Instead of emerging from long-term strategic planning, Ukraine's cyber resilience developed through a process of reactive institutional learning. This dynamic can be explained through Peter Hall's theory of third-order policy change, which suggests that major crises may trigger fundamental transformations in policy paradigms and institutional structures [5]. In such situations, policymakers do not merely adjust policy instruments but reconsider the underlying assumptions and goals of governance.

In the Ukrainian case, major cyber incidents functioned as critical junctures that transformed the perception of cybersecurity from a technical IT issue into a core national security concern. The NotPetya cyberattack in particular demonstrated the strategic nature of cyber operations and forced Ukrainian institutions to reconsider the legal and institutional architecture of cybersecurity governance.

The development of cyber resilience in Ukraine can also be explained through Mark Beissinger's theory of institutional learning through emulation. According to this framework, political actors under conditions of uncertainty often adopt institutional models from states perceived as successful examples [6]. Estonia's cybersecurity governance model has frequently been cited as a benchmark for cyber preparedness following the Russian cyberattacks of 2007 [7].

However, Ukraine did not simply replicate the Estonian model. Instead, Ukrainian institutions selectively adapted elements of Estonia's cyber governance architecture within the constraints of wartime governance. This process reflects what scholars describe as bounded learning, where external institutional models are adopted selectively and adapted to domestic political and institutional conditions [8].

These developments resulted in significant legal and institutional reforms in Ukraine's cybersecurity system. The adoption of the Law of Ukraine on Cybersecurity in 2017 established a clearer institutional framework for cyber defense and strengthened coordination among government agencies responsible for cybersecurity governance. Institutions such as the State Service of Special Communications and Information Protection and CERT-UA assumed expanded roles in monitoring cyber threats and coordinating national responses to cyber incidents [9].

From a broader perspective, Ukraine's experience suggests that normative stability in cyberspace does not necessarily arise from institutional continuity alone. Instead, stability may emerge through adaptive governance processes that allow legal frameworks and institutions to respond flexibly to evolving threats. Cyber resilience therefore represents not merely a technical capability but a broader governance strategy that

integrates legal adaptation, institutional coordination, and societal mobilization [10].

Ukraine's trajectory provides an important lesson for international security governance. Resilience should not be understood as a final state achieved through perfect institutional design. Rather, resilience is an ongoing process of adaptation that enables institutions to maintain stability under conditions of uncertainty and continuous disruption.

References

1. CERT-UA. 2023. *Annual Report on Cyber Incidents in Ukraine*. Kyiv.
2. CERT-UA. 2024. *Cyber Threat Landscape in Ukraine 2024*. Kyiv.
3. Libicki, Martin. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica : RAND Corporation.
4. Gartzke, Erik. 2013. "The Myth of Cyberwar." *International Security* 38 (2): 41–73.
5. Hall, Peter A. 1993. "Policy Paradigms, Social Learning, and the State." *Comparative Politics* 25 (3): 275–296
6. Beissinger, Mark R. 2002. *Nationalist Mobilization and the Collapse of the Soviet State*. Cambridge: Cambridge University Press.
7. Herzog, Stephen. 2017. "Revisiting the Estonian Cyberattacks." *Journal of Strategic Studies*.
8. Meseguer, Covadonga. 2005. "Policy Learning, Policy Diffusion, and the Making of a New Order." *Annals of the American Academy of Political and Social Science*.
9. SSSCIP. 2023. *Year in Review: Ukraine's Cyber Defense*. Kyiv.
10. Barnea, Hadar, Amit Weiss, and Eyal Shemer. 2020. "Resilience in the Age of Cyber Threats: Multidimensional State Capacities." *Journal of Cybersecurity Studies* 5 (2): 67–89.