4. Serhii Lysenko. The Role of Artificial Intelligence in Cybersecurity: Automation of Protection and Detection of Threats. *Economic Affairs.* 2024, № 69. 10.46852/0424-2513.1.2024.6.
5. Chaban Olena. Current Choices of Ukraine to the Avenues to Regulate Artificial Intelligence (AI). 2025. 10.2139/ssrn.5549841.

DOI https://doi.org/10.36059/978-966-397-570-2-97

Chiragova I.,
Postgraduate Student
National Defense University of Azerbaijan
Baku, Azerbaijan

THE INFLUENCE OF STRATEGIC CULTURE ON CYBERSECURITY POLICY FOR CRITICAL INFRASTRUCTURE

Introduction. Critical infrastructure underpins key societal functions and serves as a cornerstone for national security, economic resilience, and state governance. The prevailing understanding of critical infrastructure encompasses any network, virtual or physical asset, or system whose destruction or incapacitation would directly harm national security, public health, economic security, or safety [1]. Everyday the vulnerability is getting more expanded with a broader digitization. The significance of critical infrastructure is now evident in the prioritization of cyberattacks and associated risks by states and collective security organizations. As a result, the imperative to protect critical infrastructure compels states to develop distinct cybersecurity policies, with national approaches to risk management varying considerably. Hence, the necessity to safeguard the critical infrastructure pushes states to formulate their own cybersecurity policies, national approaches to manage the risks of which vary drastically. Futhermore, cybersecurity strategy is not merely technical, but expression of a country's vision, priorities and principles.

Usually defined as a state's ingrained habits of thought, distinct patterns of adaptation to a particular environment, set of beliefs, ideas, values symbols and etc., the concept of strategic culture shapes State's reaction towards the emerging security challenges [2, 3]. Hence, strategic culture can shape state behavior and influence the way cybersecurity policy is constructed. This paper examines whether a nation's pre-existing national strategic culture determines its choice of critical infrastructure defense model. Specifically, it investigates whether nations with historically

offensive strategic cultures adopt different defense models than those with defensive traditions. The central argument is that strategic culture acts as a primary cognitive factor shaping the architecture of critical infrastructure cybersecurity policy and driving the development of divergent defense models.

The cyber domain and strategic culture. Coined by Jack Snyder during the Cold War the concept of strategic culture usually refers to the “unique constellation of a state’s historical experience, institutional memory, military traditions and political values that shape how understands security and use force” [4]. It influences how nations perceive threats, what technologies they prioritize and how they define concepts like deterrence, escalation and victory. Colin Gray offered another prominent perspective, defining strategic culture as "modes of thought and action with respect to force, which derives from perception of the national historical experience, from aspirations for responsible behaviour in national terms" [5]. As Gomez (2022) notes, information asymmetries in cyber operations create profound uncertainty for states. Gomez proposes a strategic culture framework that includes deeply embedded preferences guiding technical operators, policymakers, and military leaders when facing such uncertainty [6]. Building on this, Hare highlights the influence of cultural and societal contexts on cyber behavior [7]. In the context of critical infrastructure defense, strategic culture determines how threats are perceived, who is assigned responsibility for addressing them, and how future governance structures are formed.

The relation between cyber security and critical infrastructure. Prior to examining defense models, it is essential to clarify the interdependence between cybersecurity and critical infrastructure systems. Critical infrastructure cybersecurity can generally be understood through two dimensions: defensive measures and offensive capabilities. The growing dependence of state-vital on sophisticated, internet-based network technologies has made it a primary military target. Consequently, as geopolitical tensions intensify, adversaries may perceive critical infrastructure as a viable military target. This is what forces states to prioritize and invest heavily in defense capacity to safeguard their essential systems against escalating cyber threats. Given that a successful cyberattack could trigger severe economic damage, endanger public safety, and undermine national stability, investing in modernized defense capabilities has become imperative for states. Alternatively, in a mode of attack, a state can pursue a cyber attack capacity to damage an adversary's critical infrastructure partially or completely. The anonymity inherent in cyberspace further complicates both attribution and response. The more critical infrastructure systems become more interconnected and complex, the more the threat landscape continues to evolve, necessitating continuous improvement in both offensive and defensive strategies.

Critical Infrastrcture defense models and deterrence. Contemporary researchers often argue that conventional cybersecurity approaches are becoming insufficient against sophisticated threats. As a result, the concept of cyber resilience has gained prominence. It emphasizes not only resistance to cyberattacks but also the ability to adapt, respond, and swiftly recover, where operational continuity remains with minimal disruption. Since, critical infrastructure sectors form a complex and highly interdependent ecosystem, there appears a strong demand for multilayered defense architectures. These can be categorized into two governance models. Known as centralized architectures rely on a unified network structure managed by core servers. While efficient, such systems can be vulnerable because a single undetected breach may propagate across all connected components. Distributed architectures, by contrast, decentralize control and processing functions across multiple nodes. Albeit this structure enhances adaptability and fault tolerance, simultaneously it requires flexible, coordinated management practices. The choice of defense model frequently corresponds to a state's broader deterrence orientation.

Within cyber strategy, deterrence is commonly conceptualized along two complementary lines [8]. First of all, it is deterrence by punishment, aiming to discourage aggression by signaling that any cyberattack will provoke a retaliatory response severe enough to outweigh expected gains. Secondly, deterrence by denial seeking to prevent attacks by making them technically infeasible or strategically unrewarding through robust defense, resilience, and coalition-based security cooperation. Denial strategies are often regarded as the more sustainable approach, as they reduce incentives for aggression while strengthening overall system resilience.

Methodology. This paper employs a qualitative comparative case study approach to identify how differences in national strategic culture – specifically offensive versus defensive postures – influence the critical infrastructure (CI) defense model of a state. To execute this research, the study focuses on Russia and Estonia, selected owing to their highly contrasting strategic cultures and geopolitical realities which offer a clear basis for comparison. The research methodology combines thematic analysis with data drawn from a wide range of sources, including government publications from both nations, whitepapers on cybersecurity, academic journals, industry reports, and current news coverage.

Case Studies

A. **Estonia**

Estonia's strategic culture began to crystallize during the country's re-emergence as an independent state in the late 1980s and early 1990s. As Piirimäe (2020) notes, this formative period involved reconstructing a unified national historical perspective that would guide the state's strategic outlook and policy priorities [9]. Rooted in victimhood, foreign occupation and a long-standing perception of Russian coercive potential, Estonia's

security identity rests on a resilience-oriented defense posture. Central to this approach is a twofold defense doctrine. On one hand, Estonia anchors its security in transatlantic cooperation through NATO. On the other, it promotes national self-reliance via a comprehensive whole-of-society framework known as Total Defence, ensuring that civil and military structures are integrated to maintain readiness and resilience in times of crisis [10].

B. **Russia**

Based on the strategic culture, Estonia, a state with a highly digitized society, can be characterized by a defensive orientation and an emphasis on societal resilience which have been heavily influenced by a post-Soviet history and especially by triggering experience of the 2007 cyberattacks. By contrast to Estonia, Russia perceiving a historically offensive strategic culture, is featured by great power aspirations, expansionist tendencies and utilization of aggressive cyber operations. Moreover, Russia, taking into consideration historical experiences, specifically Barbarossa syndrome, opted for the narrative of Russia as a besieged fortress. In other words, Russian leadership argued that Russia was always under existential threat of foreign attacks, therefore this is how the leadership justified use of force and military. After investigating the divergence in critical infrastructure's governance structures, general technological philosophies and policies of those two in the field of international cooperation, the analysis indicates a strong correlation between strategic culture of the one state and its consequent critical infrastructure defense model.

Conclusions. This paper examined the extent to which a nation's pre-existing national strategic culture can somehow determine its choice of critical infrastructure defense model. In order to implement this study, a comparative two case study approach with focus on Russia and Estonia, has been employed. The comparative analysis of CI defense models in Russia and Estonia reveal that Strategic Culture is the decisive variable shaping cybersecurity policy. Russia's historically offensive strategic culture yields a highly centralized, isolationist model prioritizing state control and technological autarky, fundamentally relying on the threat of aggressive, offensive operations for national security or in other words detterence by punishment. Estonia's defensive strategic culture, catalyzed by the 2007 attacks and traumatic historical experience during the Soviet Union, results in a distributed, cooperative model centered on societal resilience, strategic entanglement, and deterrence by denial.

Bibliography:

1. J. Moteff, and P. Paufomak, "Critical infrastructure and key assets: definitions and indentifiction," The Library of Congress. USA: Washington, DC, October 2004.

2. J. Snyder, “The Soviet Strategic Culture: Implications for limited nuclear operations,” The RAND Corporation. USA, 1977.

3. C.Gray, “Comparative strategic culture,” Parameters, vol. 14, no. 4, 1984, pp. 27.

4. J. Snyder, “The Soviet Strategic Culture: Implications for limited nuclear operations,” The RAND Corporation. USA, 1977.

5. C.Gray, “Nuclear Strategy and National Style,” Lanham, Md. : Hamilton Press, 1986, pp. 36–37.

6. M. Gomez and C. Whyte, “Unpacking strategic behavior in cyber-space: a schema-driven approach,” *Journal of Cybersecurity*, vol. 8, issue 1, 2022.

7. F. Hare, “The cyber threat to national security: why can’t we agree?,” Cooperative Cyber Defence Centre of Excellence, Tallinn, 211-25, 2010. [In proceedings of the 2010 Conference on Cyber Conflict, 2010].

8. A.Bendiek and T.Metzger, “Deterrence theory in the cyber-century,” Working Paper RD Germany : Berlin, May 2015.

9. K.Piirimäe, “From an “Army historians” to an “Army professionals”: History and the strategic culture in Estonia,” *Scandinavian Journal of Military Studies,* 3(1), 2020, pp. 100–113.

10. V. Veebel, “Estonia: The comeback of the total defence in the light of Russia’s aggression in Ukraine,” In European Total Defence, Routledge, 2025, pp. 135–152.