Arina Bieliaieva
Dmytro Motornyi Tavria State
Agrotechnological University
Language adviser: PhD, Associate Professor
Viktoriia Lemeshchenko-Lagoda

# CYBERSECURITY RESILIENCE IN HYBRID WARFARE: UKRAINE'S DIGITAL INFRASTRUCTURE AS A MODEL OF NATIONAL SECURITY

At present, national security encompasses several factors and seeks to balance technological sovereignty, independence, and economic stability. The key objective of such a system is to maintain security, as a threat in one area should not affect others. Critical infrastructure is among the most vulnerable, and it is most frequently targeted during hybrid wars. This is especially true for the banking system and government services.

One of the most useful examples is Ukraine's public service platform "Diia". "Diia" has a ready-made, versatile structure and, since 2022, has been continuously implementing new, flexible technologies that set a real benchmark for other countries. Continuous transformation has become a key tool for ensuring global community security and preventing external threats. Particular attention should be paid to the main features of "Diia":

• **The absence of a single database** prevents data from being "open." They do not use a server to store information. During each session, the application makes an instant query to the relevant registries, rendering hacking useless. This eliminates a "single point of failure," which prevents attacks from causing national-scale disasters. The specialized "Trembita" system acts as an intermediary between them, protecting every message with a digital signature and logging it.

• **Channel encryption (TLS)**.

• **The biometric key (Diia. Signature)** is a hybrid of advanced mathematics and AI. Liveness detection is triggered every time, reading fixed facial landmarks in real

time and comparing them with those already stored in government registries. After confirmation based on physical characteristics (pupillary distance, facial shape, etc.), a unique digital code is generated and later used in other contexts.

• **Cloud resilience** is ensured by storing backups outside of Ukraine, which protects against physical attacks.

• **Bug Bounty**.

In 2025, there were approximately 275 attacks on government agencies, resulting in data breaches and operational paralysis. This has driven the development of both cybersecurity measures and new attack methods. AI began to be used even in attacks, leading to an epidemic of biometric data bypass techniques. "Phishing" has become much more sophisticated through the analysis of digital footprints and the reading of all publicly available information. Increased autonomy has become devastating – about 14% of major corporate breaches were carried out without human assistance. Code mutation and payload rewriting after being blacklisted bypass the defenses of traditional antivirus software, rendering it useless. The creation of synthetic identities has also become a serious threat, and AI Vulnerability Discovery (Zero-Day) outpaces humans in code analysis, exploiting discovered flaws for its own purposes. This has led to a situation where, in 2026, approximately 41% of all new vulnerabilities were discovered using AI tools.

These widespread challenges have led to a shift from a "react to a breach" model to a "predict and prevent" approach, accelerating advancements in security technologies. New algorithms that are more resistant to quantum computing are currently being implemented. Defensive AI also plays a well-deserved role in the chain, as human operators cannot keep up with the speed of attacks. Autonomous Incident Response independently detects an attack, isolates the infected object, and replaces it. This has reduced threat detection time by an average of 12 days and damage by $1.9 million.

Cyber Digital Twins are also gaining ground in the market, driving its growth to $50 billion. Creating a complete replica enables the simulation of thousands of scenarios and the identification of vulnerabilities before they are detected in real time.

This makes the system more predictable, while crypto-adaptability and the transition to a modular software architecture allow for a rapid switch to a backup system.

These efforts have yielded measurable results. As of 2026, Ukraine ranks 13th in the National Cybersecurity Index, having moved up from 25th place in just a few years. It is recognized as a Tier 1 nation for cybersecurity excellence, serving as a global benchmark for resilience in hybrid warfare.

Nevertheless, a significant paradox remains. While AI attacks have become widespread, only 37% of companies have a formal AI policy, which is hindering the adoption of new technologies. That said, there are innovators, and governments around the world (the U.S., Canada, and the EU) have set deadlines. By April 2026, all federal departments are required to submit plans for transitioning to quantum-resistant encryption.

Thus, the contemporary cybersecurity landscape demonstrates that the future of national resilience depends on integrating adaptive architectures, AI-powered defense systems, and proactive security governance capable of responding to the rapidly evolving nature of hybrid threats.

**REFERENCES**

1. Cloudflare. (2025). Cloudflare's 2025 Q3 DDoS threat report. https://blog.cloudflare.com/ddos-threat-report-2025-q3/
2. Quantum Security 2026. (2026). 2026: Year of quantum security. https://quantumsecurity2026.org/
3. Державне підприємство «ДІЯ». (n.d.). Послуги електронної взаємодії та ідентифікації. https://se.diia.gov.ua
4. Дніпропетровська обласна державна адміністрація. (n.d.). Система «Трембіта». https://egov.dp.gov.ua/services/sistema-trembita