

The Case of Ukraine: Continuous Attack on Energy Infrastructure in the Cyber Domain

Examining Hybrid Warfare and Cyber Threats

Oleksiy Tkachenko

National cybersecurity coordination center

National security and defense council
of Ukraine

2025

Introduction

- Ukraine's geopolitical importance
- Role of democracy in post-Soviet Ukraine
- Rise of cyber warfare as a modern battleground
- Critical energy systems increasingly digitalized
- Cybersecurity now integral to national resilience
- Ukraine: a frontline example in hybrid warfare

Background

- Timeline of Russia-Ukraine tensions
- Importance of digital infrastructure in Ukraine
- Cyber as an extension of kinetic warfare



Notable Cyberattacks on Ukraine Critical Infrastructure

- 2015: Black Energy power outage in western Ukraine
- 2016 Industroyer substation control disruption
- 2022 – 2025 hybrid assaults during full-scale war
- Impact: economic disruption, social unrest, political instability



Objectives Behind Cyberattacks

- Disrupt critical infrastructure
- Undermine public trust in government
- Destabilize democratic institutions
- Sow panic among the people
- Influence public opinion

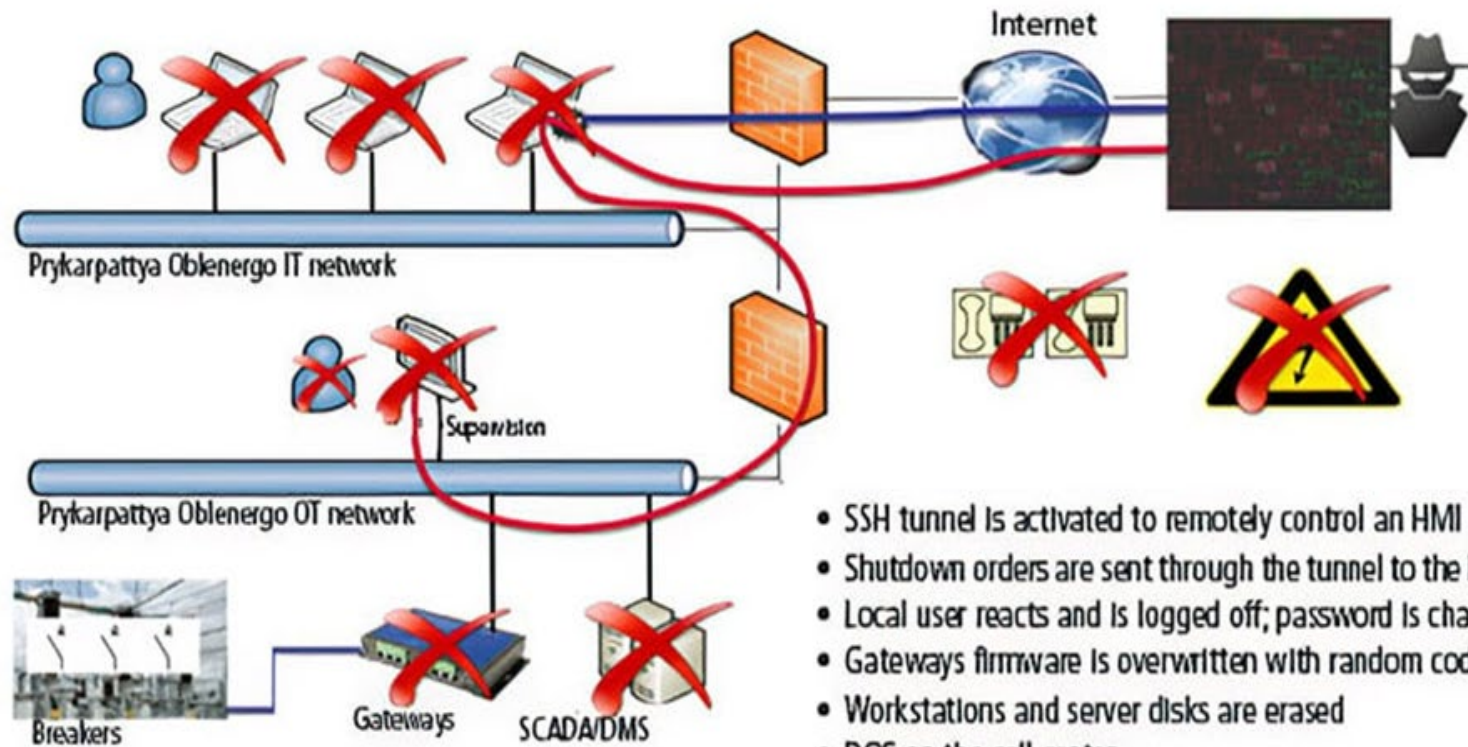


Cyber Tactics Used

- APT attacks
- Malware and ransomware
- Phishing and spear-phishing
- Hybrid Warfare - Disinformation campaigns aligned with cyberattacks



BLACK ENERGY ATTACK DEVELOPMENT



Vulnerabilities in the Sector

- Legacy systems — equipment designed decades ago, without cybersecurity in mind, still controlling critical infrastructure.
- Human and organizational weaknesses — insider threats, fragmented responsibilities, and supply chain gaps that open doors to attackers.
- Geopolitical weaponization — cyberattacks used as tools of coercion and hybrid warfare, where the line between crime and conflict disappears.

Ukraine's Cyber Defense Response

- Establishment of cyber defense units
- Cyber Volunteers
- Public-private partnerships
- International collaboration (NATO, EU)
- Digital Resilience tools (e.g., Diya app)
- Network segmentation, system isolation
- Manual fallback operation drills



International Support and Cyber Solidarity

- Tech aid from global companies (Microsoft, Google)
- Digital diplomacy and policy advocacy
- Support from IT Army of Ukraine and volunteers



Lessons Learned

- Cyber is a central domain of warfare
- Democracies can be targeted without physical invasion
- Cyber hygiene and public awareness are vital
- Proactive and adaptive defense is key
- International cooperation and information sharing



Best Practices & Recommendations

- Zero trust architecture
- Continuous monitoring with AI/ML
- Secure supply chains and updates
- Regular red teaming and training

Implications for Global Democracies

- Ukraine as a case study in cyber resilience
- Early warning signs for other nations
- Need for international frameworks and cooperation



Conclusion

- Cyber threats are ongoing and evolving
- Energy grid security = national security
- Ukraine experience strengthen energy security globally
- Cyber-physical resilience vital
- Shared responsibility: government, industry, society



Q&A

Thank you!

Any questions?

ot@ncscc.gov.ua