



REPORT

THE STAYING POWER OF UKRAINIAN LIGHTS

LESSONS OF WARTIME RESILIENCE OF THE ELECTRICITY SECTOR

| TOMAS JERMALAVIČIUS | HENRY RÕIGAS | OLEKSANDR SUKHODOLIA |
| DMITRI TEPERIK |

MAY 2025

RKK
ICDS

RAHVUSVAHELINE KAITSEUURINGUTE KESKUS
INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
EESTI - ESTONIA

Title: The Staying Power of Ukrainian Lights. Lessons of Wartime Resilience of the Electricity Sector
Authors: Jermalavičius, Tomas (editor); Rõigas, Henry; Sukhodolia, Oleksandr; Teperik, Dmitri
Publication date: May 2025
Category: Report

Cover page photo: Ukrainian soldier seen placing down candles at the LIGHT THE FIRE event, dedicated to the 1 000 days of the Ukrainian people's struggle for freedom and independence (Andreas Stroh/ZUMA Press Wire/Scanpix).

Keywords: air and missile defence, critical infrastructure, cyber defence, cyberattacks, cybersecurity, disinformation, distribution system operator, electricity, energy security, nuclear power, physical protection, power grid, power system, public opinion, renewable energy, repair crews, strategic communication, transmission system operator, war, Ukraine, European Union, NATO, Russia

Disclaimer: This study was supported by a research grant provided by AS Elering. The views and opinions contained in this paper are solely those of its authors and do not necessarily represent the official policy or position of the International Centre for Defence and Security, AS Elering, or any other organisation.

ISSN 2228-0529

ISBN 978-9916-709-46-7 (print)

ISBN 978-9916-709-47-4 (pdf)

© International Centre for Defence and Security
63/4 Narva Rd., 10120 Tallinn, Estonia
info@icds.ee, www.icds.ee

CONTENTS

Acknowledgements	III
About the Authors	III
List of Abbreviations	V
Executive Summary	VI
Introduction	1
1. Physical Resilience of the Power System	3
1.1. Protection and Recovery Measures	3
1.2. Prioritisation in Decision-Making	7
1.3. International Cooperation and Assistance	10
1.4. Balancing Supply and Demand	11
1.5. Cross-Border Electricity Trade	13
1.6. Long-term Transformation	14
1.7. Chapter Conclusion	16
2. Resilience Against Cyber Operations	18
2.1. Data Sources	18
2.2. Cyber Operations	19
2.2.1. The years 2014–21	19
2.2.2. The years 2022–24	20
2.3. The Bigger Picture	22
2.4. Implications	23
2.4.1. The Nature of the Threat	24
2.4.2. Ukraine’s Battle-Hardened Capabilities	25
2.4.3. Lessons Learned and Key Focus Areas	26
2.5. Chapter Conclusion	27
3. Strategic Communication	28
3.1. Public Opinion and Support	28
3.2. Combating Disinformation	30
3.3. Consumer Behaviour and Cooperation	33
3.4. Chapter Conclusion	36
Report Conclusions and Recommendations	37
List of References	43

ACKNOWLEDGEMENTS

We would like to express our gratitude to all the Ukrainian energy, cybersecurity, and strategic communication experts and government officials for their precious time and invaluable insights shared with us in the process of conducting research for this report. We also sincerely thank Olena Ogir from the G.E. Pukhov Institute for Modelling in Energy Engineering (PIMEE) in Kyiv and Susanne Nies for their assistance in identifying and reaching out to many of the individuals and organisations in Ukraine for interviews. Our special thanks to Tetiana Biloborodova from PIMEE, and Inna Skarga-Bandurova from Oxford Brookes University in the UK for their extensive assistance and contributions to the data collection and analysis and to Andrii Davydiuk from NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn for his advice, assistance and feedback for the part on cyber resilience. Finally, we are very grateful to Elering, the Estonian national power and gas transmission system operator, for supporting the project that resulted in this report.

ABOUT THE AUTHORS

TOMAS JERMALAVIČIUS

Tomas Jermalavičius is the head of studies and research fellow at the International Centre for Defence and Security (ICDS) in Tallinn, Estonia. Prior to joining the ICDS, he served at the Baltic Defence College (BALDEFCOL), including as the dean of academics, and worked at the Lithuanian Ministry of National Defence. Since 2017, he has been a visiting professor at the College of Europe in Warsaw. He is also an associated fellow of the Latvian Institute of International Affairs (LIIA). At the ICDS, he deals with various aspects of defence policy and strategy, regional security and defence cooperation in the Baltic area, impact of emerging disruptive technologies on security and defence, energy security and societal resilience. He holds a BA in political science from Vilnius University, an MA in war studies from King's College London, and an MBA from the University of Liverpool.

HENRY RÕIGAS

Henry Rõigas is a non-resident research fellow at the ICDS and the CEO of the cybersecurity research company evisec. He has held various positions at both private and public organisations. He was a principal threat analyst at cybersecurity firm Nortal, chief strategy officer at an AI startup, Sentinel, and head of research and innovation cooperation at the data security company Guardtime. Before joining Guardtime, he was a policy researcher at the NATO Cooperative Cyber Defence Centre of Excellence and the agenda director for CyCon, the world's leading cyber defence conference. During his time at the CCDCOE, he was also a project lead for and contributor to the book *Russian Aggression against Ukraine: Cyber War in Perspective* and co-editor of the book *International Cyber Norms: Legal, Policy and Industry Perspectives*. His research interests focus on the intersection of government policy, international relations, and emerging digital threats, with a focus on cyber conflict and information warfare. He holds an MA in international relations from the University of Tartu.

OLEKSANDR SUKHODOLIA

Dr Oleksandr Sukhodolia is the head of the Critical Infrastructure Protection, Energy, and Ecological Security Department at the National Institute for Strategic Studies in Kyiv, where he has worked since 2012. Having graduated from the National Technical University of Ukraine, he has been working on issues of energy security in different positions at governmental agencies since 1998. He contributed to the development of the Energy Security Strategy of Ukraine (approved by the Ukrainian government in 2021) and the Law of Ukraine "On Critical Infrastructure" (approved by the Ukrainian Parliament in November 2021). He holds doctoral degrees in electrical engineering and public administration.

DMITRI TEPERIK

Dmitri Teperik is an independent senior policy expert and development trainer on societal resilience, FIMI, crisis communication, and civil security. He was a research fellow at the ICDS and then served as the centre's chief executive until 2023. He has over 10 years of experience in contributing as a director or a leading subject matter expert to various international research projects, interdisciplinary studies, development cooperation programmes, professional training and outreach activities on comprehensive resilience and complex measures against hostile foreign influence and disinformation. During 2016-23, he also led the "Resilient Ukraine" development cooperation programme, which focused on assessing and strengthening the resilience of vulnerable communities in Ukraine. He holds an MSc degree from the University of Tartu.

LIST OF ABBREVIATIONS

AFU	Armed Forces of Ukraine
CCDCOE	Cooperative Cyber Defence Centre of Excellence
CEO	chief executive officer
CERT	Computer Emergency Response Team
CESA	Continental Europe Synchronous Area
CHP	combined heat and power
CTI	cyber threat intelligence
DDoS	distributed denial of service
DSO	distribution system operator
ENSECCOE	Energy Security Centre of Excellence
ENTSO-E	European Network of Transmission System Operators – Electricity
ESD	Energy Security Database
ESS	emergency shutdown schedule
EU	European Union
EW	electronic warfare
FOI	Swedish Defence Research Agency (<i>Totalförsvarets forskningsinstitut</i>)
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation (<i>Главное управление Генерального штаба ВС РФ</i>)
HPP	hydro power plant
IT	information technology
ICS	industrial control system
MW	megawatt
NATO	North Atlantic Treaty Organisation
NPP	nuclear power plant
NSDC	National Security and Defence Council
OT	operational technology
PIMEE	G.E. Pukhov Institute for Modelling in Energy Engineering
PV	photovoltaic
RUSI	Royal United Services Institute
SCADA	supervisor control and data acquisition
SME	small and medium enterprises
SSSCIP	State Service for Special Communications and Information Protection
TPP	thermal power plant
TSO	transmission system operator
TTP	tactic, techniques, and procedures
UAV	unmanned aerial vehicle
USAID	United States Agency for International Development
VAT	value added tax

EXECUTIVE SUMMARY

Energy supply disruption brought about by aerial strikes on various parts of the system is clearly an important element of Moscow's strategy to erode Ukraine's will for self-defence and to deepen the economic and humanitarian crisis caused by the full-scale war. It has recently focused on conducting saturation attacks that overwhelm the thinly spread and often depleted Ukrainian air defences. Furthermore, in addition to targeting various parts of the power grid, it has concentrated more persistently on destroying power generation capacity. As a result, Ukraine had lost over half of its pre-invasion power generation capacity by early summer 2024, with some estimates of remaining capacity even lower than that. However, through a complex and dynamic set of whole-of-government and whole-of-society actions, the country managed to avoid the collapse of its power system and emerged as a key source of insights and policy recommendations for wartime resilience of the electricity supply.

This report identifies and analyses some key lessons in physical protection, cybersecurity and strategic communication domains when ensuring the functioning of the power generation, transmission, and distribution system in wartime. It examines how Ukraine responded to the kinetic attacks against its power system that were part of the evolving Russian aerial campaign to destroy it. The report outlines changes in the protection, recovery, and energy market policies and regulations as well as the practical measures implemented by its government, local authorities, and power companies. It then analyses the nature of cyber threats and how Ukraine has countered them during two distinct periods – in 2014-22 and 2022-24. It also shows how Ukraine mounted effective crisis and strategic communication efforts and dealt with the attempts by Russia and its proxies to use disinformation to undermine public self-confidence, trust, and cooperation, while managing the consequences of the attacks against the power system.

The report finds that remarkable resilience of Ukraine's power system is due to multiple factors and draws on certain pre-existing or rapidly introduced conditions: ample redundancies in the power system beforehand; pre-invasion preparedness measures in physical, cyber and information domains; adaptiveness of the system to the nature of the threat; effective provision of foreign aid; connectivity with the European grids; significantly enhanced capacity to restore damaged or destroyed facilities, and effective energy policies as well as regulatory and administrative environment. Just as important was the high priority given by Ukrainian political authorities to protecting the system and to reconstruction needs by setting and reviewing the required protection standards, allocating necessary military (e.g., air and missile defence assets) and civilian resources, and providing a framework for coordination and cooperation between stakeholders.

Moreover, even though the war can trigger an impulse to centralise decision-making and coordination, it also acts as an accelerator of a transition to a more decentralised and distributed power system architecture, where local power generation – especially from renewable sources – and battery storage, as well as smart micro- and nano-grids, emerge as key solutions to ensure uninterrupted power supply for vital services. These solutions have their own limitations and even long-term security risks and will likely be a supplement rather than replacement to large grids. Yet it is obvious that their role in enhancing crisis and wartime resilience will only grow, as will the need to step up investments into multi-layered and well-integrated air and missile defence systems capable of protecting wider urban areas and critical nodes of the power system against diverse aerial threats.

The report concludes that wartime resilience of the power system is a truly comprehensive and multidimensional phenomenon. It requires active and sustained contribution from a broad range of stakeholders – domestic and foreign, civil and military, as well as governmental, corporate, and societal – providing another convincing example of how valuable and important the whole-of-government and whole-of-society approaches are under such severe wartime conditions, including in cyber and cognitive warfare domains.

The report recommends that, in terms of physical protection and broader energy security policy:

- The security of critical energy infrastructure in wartime must become an important element of peacetime inter-agency and multi-stakeholder planning and coordination, including in prioritising allocation of limited air and missile defence assets.
- A regional and pan-European system of mutual assistance to protect and restore critical energy infrastructure should be created, ensuring the supply of equipment and materials necessary for restoration.
- Adequate levels of in-house technical expertise and workforce of energy companies, such as grid operators and power producers, must be preserved, regardless of peacetime pressures to outsource this expertise and wartime pressures to mobilise it for military defence.
- A clear and effective wartime regulatory framework for electricity trading should be established in advance.
- The capacity of market players to build and operate decentralised energy generation and distribution (e.g., micro- and nano-grids) systems should be enhanced.

Meanwhile, with regard to cybersecurity, preparedness for wartime conditions should include:

- Developing and maintaining a clear understanding of the adversary's cyber capabilities, intent, and methods in targeting the power system;
- Consistent investments by the power sector's organisations in both proactive and reactive cybersecurity measures;
- Cybersecurity strategies based on interdisciplinary collaboration within and between energy organisations, government agencies, and other critical infrastructure sectors – through, for example, joint crisis simulations, comprehensive incident response planning, and civil-military coordination.

In strategic and crisis communication efforts aimed at mitigating the effects of the kinetic attacks against the power system on the cognitive domain, it is necessary to:

- Establish a centralised communication hub responsible for synchronising, coordinating, and disseminating information related to energy disruptions, restoration efforts, and energy-saving measures;
- Ensure transparent and proactive public engagement as a high priority in order to manage public expectations, minimise panic, and foster trust and cooperation of the public;
- Establish robust collaborative relationships of crisis communicators with cybersecurity experts, independent media outlets, and fact-checking organisations in order to mitigate the risks associated with cyberattacks and ensuing disinformation.

*You know you're gonna live through the rain
Lord, you gotta keep the faith <...>
Everybody bleeds, everybody, keep the faith*
Bon Jovi, "Keep the Faith" (1992)

INTRODUCTION

Tomas Jermalavičius

Ukraine's energy system has been a target of Russia's cyberattacks since the start of the war in 2014, but protecting it has become a matter of national survival since the start of the full-scale invasion in 2022. Energy supply disruption brought about by aerial strikes on various parts of the system is clearly an important element of Moscow's strategy to erode Ukraine's will for self-defence and to deepen the economic and humanitarian crisis caused by the full-scale war. Russia's campaign in winter 2022–23 put a significant strain on Ukraine's capacity to cope with such disruptions, but effective preparedness and

Energy supply disruption is an element of Moscow's strategy to erode Ukraine's will for self-defence and to deepen the economic and humanitarian crisis

a whole-of-society response, improved air defences, and foreign assistance have helped to mitigate the impact. Some preliminary lessons from this period were captured in the 2023 International Centre for Defence and Security (ICDS) report.¹

Since then, Russia has adjusted its tactics. Since winter 2023–24, having accumulated sufficient reserves of cruise and ballistic missiles as well as drones, it has focused on conducting saturation attacks that overwhelm the thinly spread and often depleted Ukrainian

¹ Tomas Jermalavičius, Veli-Pekka Tynkkynen, Andrian Prokip, Christian Egenhofer, Edoardo Righetti, Arūnas Molis, Priit Mändmaa, Tony Lawrence, and Oleksandr Sukhodolia, *War and Energy Security: Lessons for the Future* (Tallinn: ICDS, 2023).

air defences. Furthermore, in addition to targeting various parts of the power grid, it has concentrated more persistently on destroying power generation capacity, which is more difficult, time-consuming, and expensive to restore. The result of this renewed campaign – partly also due to the insufficient air defence systems and munitions supplied to Ukraine – is that the country had lost over half of its pre-invasion power generation capacity by early summer 2024, with some estimates of remaining capacity being as low as 25%.² This caused lengthy blackouts in various parts of Ukraine – including its capital city of Kyiv – and portended a very difficult period for the public ahead of another winter of the war.

Ukraine had lost over half of its pre-invasion power generation capacity by early summer 2024

Russia's tactical shifts and Ukraine's adjustments – actual and intended – contain further lessons for the latter's partners and allies. The lessons in terms of the air defence requirements, architecture, and prioritisation mechanisms are not addressed in detail in this report due to their sensitive nature. But the learnings also span such areas as the grid's operational management, cross-border electricity supply, stockpiling of equipment and spare parts, surging of repair and reconstruction capacity, strategic communication to the population, strategic planning (redesigning) of the power generation and distribution system, and cybersecurity. Some of these lessons were sufficiently examined in the previous ICDS report, while others were covered in more detail in reports by think-tanks and research institutes such as the Swedish Defence

² Christopher Miller, Isobel Koshiw, and Alice Hancock, "[Russia has taken out over half of Ukraine power generation](#)," *The Financial Times*, 5 June 2024; Volodymyr Omelchenko, "[Енергетика України 2024–2025 років у тумані невизначеності](#) [Ukraine's energy sector in 2024–2025 in a fog of uncertainty]," *Razumkov Centre*, 1 October 2024.

Research Agency (FOI), the Royal United Services Institute for Security and Defence Studies (RUSI), the NATO Energy Security Centre of Excellence (ENSECCOE), and others.³

The purpose of this report is to identify new lessons and revisit older ones regarding ensuring the functioning of the power generation, transmission, and distribution system in wartime. It aims to provide a set of insights and recommendations for defence planners, energy policymakers, electricity producers, transmission and distribution system operators, cybersecurity managers, and strategic communicators that could be applied to enhancing war preparedness.

The first chapter examines how Ukraine responded to the kinetic attacks against its power system that were part of the evolving Russian aerial campaign to destroy it. It outlines the protection and recovery policies and the practical measures implemented by its government, local authorities, and power companies. It also highlights the importance of international cooperation and foreign assistance, as well as less visible but equally important aspects such as the development of electricity market adjustment and cross-border trading mechanisms suited for wartime conditions. Finally, it considers long-term strategic changes to the power system's architecture that are necessary to build greater resilience against wartime challenges.

The second chapter analyses the nature of cyber threats and how Ukraine has attempted to counter them. The chapter begins by providing an overview of the most relevant offensive cyber operations targeting systems related to Ukraine's energy infrastructure over two periods: from Russia's invasion of Crimea

and Donbas in 2014 until 2021, and from the full-scale invasion in February 2022 through the end of 2024. The chapter then places these observations in a broader context and analyses the role and impact of the cyberattacks as part of Russia's overall strategy and offensive operations.

The third chapter focuses on how the impact of the kinetic and cyberattacks is playing out in the cognitive domain of Ukrainian society. It provides an overview of how public opinion and support for the policies and practical measures to preserve the functionality and stability of the power system have evolved. The chapter examines how Ukraine mounted effective crisis and strategic communication efforts, supported by a comprehensive mechanism of coordination, and how it dealt with the attempts by Russia and its proxies to use disinformation to undermine public self-confidence, trust, and cooperation in dealing with the consequences of the attacks against the power system.

The report concludes that wartime resilience of the power system is a truly comprehensive and multidimensional phenomenon. It draws on certain pre-existing or rapidly introduced conditions such as physical and cyber preparedness, robust crisis management architecture, and effective energy policies and regulatory environment. It also requires active and sustained contribution from a broad range of stakeholders – domestic and foreign, civil and military, and governmental, corporate, and societal – providing another convincing example of how valuable and important the whole-of-government and whole-of-society approaches are under such severe conditions.

Moreover, even though the war can trigger an impulse to centralise decision-making and coordination, it also acts as an accelerator of a transition to a more decentralised and distributed power system architecture, where local power generation – especially from renewable sources – and battery storage, as well as smart micro- and nano-grids, emerge as key solutions to ensure uninterrupted power supply for vital services. These solutions have their own limitations and even long-term security risks, but it is obvious that their role in enhancing crisis and wartime resilience will only grow.

³ Anders Odell, Anna Lioufas, Mari Olsén, Karin Mossberg Sonnek, Frej Welander, and Andreas Hörnedal, [Russian Attacks on the Ukrainian Power System](#) (Kista: FOI, 2024); Jack Watling and Darya Dolzikova, ["Fighting for the Light: Protecting Ukraine's Energy System,"](#) RUSI, 12 August 2024; Saulius Rimutis, ["Lessons of War: Ukraine's Energy Infrastructure Damage, Resilience and Future Opportunities,"](#) *Geopolitics and Security Studies Center*, May 2024; Arturs Brekis, [Assessment of the Technologies That Could Increase the Use of Distributed Energy Generation, Thereby Reducing the Impact of Military Strikes on Centralized Power Generation Facilities in Ukraine and Enhancing the Security and Resilience of Energy Supply in Ukraine](#) (Vilnius: NATO Energy Security Centre of Excellence, 2024).

1. PHYSICAL RESILIENCE OF THE POWER SYSTEM

Oleksandr Sukhodolia

The aggression unleashed by Russia led to the destruction of Ukraine's energy infrastructure on a scale that no other country has experienced in modern history. The aggressor's strategy was focused on destroying Ukraine's energy infrastructure using kinetic attacks. To achieve the goal, Russia used repeated strikes on the same targets.⁴

In response to this large-scale destruction, Ukraine implemented many multi-levelled and multifaceted measures. These measures were aimed at strengthening the protection of the energy infrastructure from physical and cyber threats, as well as responding to damage and destruction of energy facilities, speeding up their restoration, and securing electricity supply for consumers. This chapter examines Ukraine's approach to the physical protection of the power system, including the policy and practical measures taken to that end.

Textbox 1: The Scale of Destruction

Before the full-scale invasion, the Ukrainian energy sector was one of the largest in Europe. The capacity of power plants providing energy in the country's integrated power system in February 2022 was approximately 37 GW. The deliberate destruction of Ukraine's energy sector by Russia significantly reduced its potential. The currently available capacity of thermal power plants (TPPs) and cogeneration thermal (so-called combined heat and power, CHP) plants is less than 20% of their pre-war capacity, and the share of available capacity of hydroelectric power plants (HPP) has decreased by 50%. About half of the

⁴ Since the beginning of Russia's full-scale invasion of Ukraine, one of the companies operating thermal power plants (TPPs) reconstituted its power plants 'from scratch' and restored operations after being shelled 41 times. Some plants have been destroyed several times after their restoration. See: DTEK, "[3 лютого 2022 року енергетики ДТЕК Енерго 41 раз «підіймали» ТЕС з нуля після обстрілів](#) [Since February 2022, DTEK Energy's power engineers have "raised" TPPs from scratch 41 times after shelling], 1 August 2024; DTEK, "[DTEK thermal power plant was hit in a new wave of russian attacks. Three workers injured](#)," 20 June 2024.

country's high-voltage power transmission substations have been critically damaged. Almost all the oil refineries and a significant part of the oil and oil products depots have been destroyed. Power outages have become a necessary measure to balance the system. Because of military actions, Ukraine's energy infrastructure had suffered direct losses of more than \$14.6 billion by the end of 2024, even without accounting for the loss of revenue, estimated at \$43.4 billion.⁵

1.1. PROTECTION AND RECOVERY MEASURES

The analysis of the first-year response to Russian attacks demonstrated that a peacetime security system of energy facilities failed to provide the necessary level of protection, as the scale of Russia's armed aggression exceeded the system's restorative capacity.⁶ As

A peacetime security system of energy facilities failed to provide the necessary level of protection

a result, Ukraine started implementing more developed and complex measures that would match the methods and means of attacks used by the aggressor.

It is worth pointing out that the legal framework for strengthening preparedness and protection was put in place shortly before the start of the full-scale invasion. The Law of Ukraine "On Critical Infrastructure," adopted in December 2021, created the basis for streamlining the activities of many stakeholders.⁷ The approaches, standards, and requirements set by the law for those stakeholders included threat-based design that established obligations for various entities to protect critical infrastructure objects from

⁵ Vadim Kolisnichenko, "[Direct damage to Ukraine's infrastructure from the war reached \\$170 billion – KSE](#)," *GMK Center*, 18 February 2025; World Bank, Government of Ukraine, European Union, United Nations, [Ukraine - Fourth Rapid Damage and Needs Assessment \(RDNA4\) : February 2022 - December 2024](#) (Washington, DC: World Bank Publications, 2025)..

⁶ Jermalavičius et al, *War and Energy Security*.

⁷ Verkhovna Rada of Ukraine, [Закон України Про критичну інфраструктуру](#) [Law of Ukraine on the critical infrastructure] (Kyiv: Vidomosti Verkhovnoi Radi, 2023).

the identified threats, continuous analysis of the situation and risk assessment, planning object protection measures, and plans for interaction with entities involved in carrying out protection tasks.

The legal framework for strengthening preparedness and protection was put in place shortly before the start of the full-scale invasion

The proposed tools have been reflected in the legal acts of the Ukrainian government and spurred practical work on the issue since the end of 2022. Among the most important practical measures to protect critical energy infrastructure are:

- strengthening the physical protection of facilities, such as by tightening security on the perimeter and in the surrounding territory;
- introducing protections against unmanned aerial vehicles (UAVs) and missile strikes by employing electronic countermeasures, mobile air defence units, and a three-tier engineering protection system;
- organising missile defence against ballistic and cruise missiles by providing coverage of the facilities with the available air defence systems.

Mobile air defence units were created to cover critical infrastructure facilities in all regions of Ukraine. The process of creating such separate groups and establishing coordination networks between them – so that drones spotted by one team can be targeted by another – began in the spring of 2022. However, staffing, training, and equipping such units with special equipment, such as thermal imaging sights, target detection and tracking systems (e.g., a country-wide network of acoustic sensors), and laser targeting devices, took some time, which led to a high level of successful drone

attacks on energy facilities at the beginning of the full-scale war.⁸

There were also some delays in the deployment of electronic warfare (EW) systems at critical energy infrastructure facilities, as it depended on the supply of the necessary equipment in sufficient quantity, while the number of facilities to be protected significantly increased as the lists of the objects to be protected against drone attacks continued to expand. At the same time, the effectiveness of EW systems against air attacks depended on the tactics, techniques, and procedures (TTPs) employed by the Russian forces, which continued to evolve and improve along with the technologies and means of attack. For instance, more complex flight routes were designed for the Shahed-136/ Geran-2 drones, avoiding clustering in flight. Attackers also took into account intelligence about Ukraine's air defence positions and sought to bypass potential locations of mobile air defence groups, focusing on areas which were less well defended. Russia also began combining different types of drones and missiles, conducting several waves of attacks on the same targets, and improving targeting, all of which required constant adaptation by the defence system of Ukraine.⁹

Ukrainian military and engineering personnel have responded accordingly by adapting the equipment and tactics of the mobile groups.¹⁰ The establishment of interactions between the involved actors – energy and engineering companies, manufacturers of defence systems, law enforcement agencies, and the armed forces – supported the overall efforts to improve the level of protection of critical energy facilities. As a result, for instance, the

⁸ Sania Kozatskiy, "[Україна нарощуватиме кількість мобільних вогневих груп ППО, – ПС ЗСУ](#) [Ukraine will increase the number of mobile air defense fire groups, - Press Service of the Armed Forces of Ukraine]," *Militarnyi*, 7 November 2023.

⁹ Bogdan Miroshnichenko, "[Тепер не тільки "шахеда". Як Росія наростила виробництво ударних БПЛА і чим відповідають українські інженери](#) [Now it's not just "shaheeds." How Russia increased the production of attack UAVs and with what Ukrainian engineers respond]," *Ukrainska Pravda*, 17 October 2024.

¹⁰ "[Зенітні-дрони "анти-Шахеда": яку головну задачу вирішили українські розробники і це не про швидкість \(відео\)](#) ["Anti-Shahed" anti-aircraft drones: what is the main task solved by Ukrainian developers and it's not about speed (video)]," *Defense Express*, 21 October 2024.

success of attacks using Shahed-136/Geran-2 drones has steadily declined: by November 2024, the percentage of these drones that did

The establishment of interactions between the involved actors supported the overall efforts to improve the level of protection of critical energy facilities

not reach the intended target (i.e., they lost target location or turned back, presumably as a result of the EW measures) increased significantly. According to the Ukrainian Air Force, on 5 September 2024, 15 Shahed-136 out of 78 lost their target location, two returned to Russia, and one returned to Belarus, whereas on 13 October, 36 Shahed-136 out of 68 lost their designated target location.¹¹

The implementation of engineering measures for physical protection started in late 2022. A three-tier system was introduced:¹²

- 1) the construction of gabions and sandbag barriers, protecting facilities from debris from exploded drones and missiles;
- 2) addressing threats from direct hits by drones and indirect (i.e., in close proximity) hits by cruise and ballistic missiles;
- 3) protection against direct hits by cruise and ballistic missiles.

By the end of 2023, the first two levels of protection had been implemented at the main high-voltage substations of the Ukrainian transmission system operator (TSO), Ukrenergo. According to government officials and the management of the TSO, these measures have significantly mitigated the

impact of Russian air strikes on Ukrainian energy infrastructure. In particular, they have considerably reduced the rate of damage to energy infrastructure from indirect hits and debris. According to the chairman of the board of Ukrenergo, it was possible to reduce the impact of attacks on Ukrenergo substations by half due to the creation of two levels of protection.¹³

At the same time, the practice of using passive physical protection has shown that the first- and second-level protection measures are not sufficient against direct missile hits.¹⁴ The third level of passive protection, namely underground placement of equipment or construction of powerful shelters in depressions, can offer potential protection against ballistic missiles or aerial glide bombs. However, the cost of this level of protection is very high, requires a very significant expenditure of resources, and a long time to build.¹⁵ In wartime, such resources may not be available, considering the increased military defence expenditure. The country may also face difficulties in drawing the necessary resources from the market, especially without the special legislative framework prepared in advance that allows increasing prices and tariffs for financing various measures to protect energy facilities while accounting for a drop in market volume due to the destruction of industry and reduction of consumption.

There are also considerations related to the power system's architecture, which currently depends heavily on the three nuclear power plants (NPPs) that remain in operation and are under Ukraine's control. Given the scale of destruction and damage to the TPPs, CHPs, and HPPs, the share of the operational NPPs

¹¹ Air Force of Ukraine, "Збито 60 ударних БПЛА [60 combat UAVs shot down]," Telegram, 5 September 2024; Air Force of Ukraine, "Збито 31 ударний БПЛА [31 combat UAVs shot down]," Telegram, 13 October 2024.

¹² State Agency for Infrastructure Restoration and Development of Ukraine, "Захист енергетичних об'єктів – один з пріоритетів Агентства відновлення [Protection of energy facilities is one of the priorities of the Reconstruction Agency]," Facebook, 20 November 2023; "Енергетична інфраструктура України матиме три рівні захисту від російських атак – голова «Укрєнерго» Кудрицький [Ukraine's energy infrastructure will have three levels of protection against Russian attacks - Ukrenergo head Kudrytskyi]," *Radio Svoboda*, 12 October 2024.

¹³ Ukrenergo, "Мінімум у два рази вдалося знизити наслідки атак на підстанції «Укрєнерго» завдяки створенню двох рівнів захисту [The consequences of attacks on Ukrenergo substations were reduced by at least half thanks to the creation of two levels of protection]," Telegram, 16 April 2024.

¹⁴ Mykhailo Orliuk, "Пасивний захист неефективний: Галущенко поклав відповідальність за збереження енергооб'єктів на ППО [Passive protection is ineffective: Galushchenko placed responsibility for the safety of energy facilities on air defence]," *Biznes-Tsenzor*, 10 September 2024.

¹⁵ Government of Ukraine, "Прес-конференція Прем'єр-міністра України Д. Шмигала [Press conference of the Prime Minister of Ukraine D. Shmyhal]," YouTube, 10 September 2024.

in Ukraine's domestic electricity supply rose to 60%.¹⁶ Russia continuously exploits this dependency by threatening strikes on the NPPs and grid infrastructure connected to them, thus endangering not only a significant proportion of the power supply but also the safety of the plants themselves.¹⁷ Even if the most severe of these threats are yet to be executed, the very possibility of such a concentrated attack on the NPPs and related infrastructure means Ukraine must dedicate military resources (e.g., air and missile defence assets) to ensure their protection, making prioritisation of the use of these resources an even more complex matter under conditions of shortages in western military assistance supplies. As a deterrent, Ukraine also seeks to ensure an international presence in the form of International Atomic Energy Agency (IAEA) observer missions at its NPPs.¹⁸

The resilience of the energy system was bolstered by the pace of post-damage reconstitution exceeding the pace of destruction

Nonetheless, the fact that Ukraine's energy system continues operating even after three years of massive kinetic attacks can be explained. The resilience of the energy system was bolstered not only by the improvement of the protection of the energy facilities against kinetic attacks but also by the pace of post-damage reconstitution exceeding the pace of destruction. Among the most important factors in this regard, and in addition to the dedication and hard work of the repair and reconstruction teams, are:

- The resilient architecture of the power system in Ukraine, which is quite extensive and diversified, combines different voltage classes in the network, allowing it to ensure the supply of the necessary energy to consumers according to reserve schemes, and has a significant reserve capacity

¹⁶ "Amid Russian bombing, Ukraine is planning more nuclear reactors," *The Economist*, 12 December 2024.

¹⁷ International Atomic Energy Agency, "Update 262 – IAEA Director General Statement on Situation in Ukraine," 28 November 2024.

¹⁸ Maria Kholina, "IAEA to send more observers to Ukraine to ensure NPP safety," *RBC-Ukraine*, 13 February 2024.

and redundancy in power generation and transmission.

- The presence of full-time employees (repair units) in energy companies and a fast increase in their number since the beginning of the war. According to Ukrenergo, the availability of thousands of specialists and highly qualified engineers who repair the networks, operate substations and power transmission lines, and balance the power system has become a decisive factor in the quick repair of damage.¹⁹
- The establishment of protocols of interaction and mutual assistance between energy companies. It has become a common practice for distribution system operators (DSOs) to send repair crews and necessary equipment to other regional DSOs for the rapid restoration of damaged infrastructure.
 - Providing the repair crews with the spare parts and necessary equipment stockpiled in advance by energy companies on the eve of the full-scale war, and, later, with the supply of spare parts, equipment, and repair tools from foreign partners of Ukraine.
- The high level of skills and competence of the engineering and technical personnel of the Ukrainian companies, which made it possible to quickly adapt the equipment supplied from other countries to the technical characteristics of the Ukrainian power system.

¹⁹ Liliya Rzhetska, "'Укренерго': Колапсу не буде, але відключення світла можливі [Ukrenergo: There will be no collapse, but power outages are possible]," *DW*, 11 October 2023. Ukraine approved the legislation that permits operators of critical infrastructure to have some exemptions from mobilisation for their staff, even though some personnel of energy companies could still be mobilised under martial law.

- Simplifying the procedures for repairing and connecting new equipment to networks.²⁰
- The high level of motivation of the repair crews and operating personnel to perform the work until it is completed, regardless of legally defined working hours, weekends, or adverse working conditions.
- The safety measures that minimise the presence of the needed personnel onsite, provide suitable shelters, and ensure proper safety instructions and training for the repair and operating crews.

As Ukrenergo's CEO observed, "This war is also a competition of engineers. Some engineers are trying to invent backup power schemes so that millions of people have light, while other engineers, on the other hand, are trying to figure out how to deprive people of it by coordinating strikes by Russian missiles and drones. And I am proud that our Ukrainian engineers won this battle last winter."²¹

The resilience of power supply also became the subject of routine attention of the political-military authorities and high military command

Separately, it should be noted that Ukraine's energy companies learned from the Russian cyberattacks on the energy system in 2015–17. The national cybersecurity system had already been formed before the outbreak of the full-scale war, and legislation, including the Law of Ukraine "On Critical Infrastructure," established the obligations of critical infrastructure operators to protect their facilities

²⁰ Verkhovna Rada of Ukraine and National Commission for State Regulation in the Spheres of Energy and Utilities, [Постанова, 26.03.2022 № 352, про особливості тимчасового приєднання електроустановок до системи розподілу у період дії в Україні воєнного стану](#) [Decree № 352 as of 26.03.2022 on the peculiarities of temporary connection of electrical installations to the distribution system during the period of martial law in Ukraine], Document v0352874-22 (Kyiv: Verkhovna Rada, 2024).

²¹ "Українські енергетики демонструють небачені до війни рекордні темпи ремонтів енергооб'єктів [Ukrainian energy workers demonstrate record pace of energy facility repairs, unprecedented before the war]," *Interfax-Ukraina*, 14 February 2023; Rzheutska, "«Укренаерго»: Колапсу не буде."

from cyberattacks, including by separating their critical information technology (IT) and operational technology (OT) systems from the internet. Therefore, after the start of the full-scale invasion and despite the three- to four-fold increase in cyberattacks, the critical IT systems of the TSO and DSOs were not severely affected (see Chapter 2 for more in-depth analysis).²²

Ukraine's experience demonstrates the importance of placing critical energy infrastructure protection within the system of national security priorities

1.2. PRIORITISATION IN DECISION-MAKING

Ukraine's experience demonstrates the importance of placing critical energy infrastructure protection within the system of national security priorities. The issue of the country's ability to provide consumers with energy has become a priority for the entire country and the subject of attention of the top leadership of the state: the president, the Cabinet of Ministers, and the Parliament of Ukraine. It has also been identified as a critical component of Ukraine's internal resilience plan, as outlined by President Volodymyr Zelenskyy in November 2024. The plan lists measures for the safeguarding of energy infrastructure, initiatives to enhance energy efficiency, and the promotion of sustainable use of resources. In addition, it encompasses endeavours to establish the conditions necessary for Ukraine to evolve into a prominent energy hub in Europe.²³

The security of critical energy infrastructure and the resilience of power supply also became the subject of routine attention of the political-military authorities and high military command, including the Headquarters of the Supreme Commander-in-Chief that performs

²² Rzheutska, "«Укренаерго»: Колапсу не буде."

²³ President of Ukraine, "[Volodymyr Zelenskyy Presented the Plan for Ukraine's Internal Resilience](#)," 19 November 2024.

wartime strategic management of national defence, and the National Security and Defence Council.²⁴ Discussions of the current situation take place regularly in various formats, and relevant decisions are formalised in the documents of all state authorities.

Textbox 2: Decisions of the National Security and Defence Council

The National Security and Defence Council (NSDC) required the implementation of measures regarding:

- proper engineering and physical protection of critical energy infrastructure objects, in particular with regard to anti-drone protection;
- alternative (reserve) energy supply of critical infrastructure objects that ensure the provision of vital services, primarily through the formation of a decentralised power supply based on small distribution systems;
- the creation of protective structures of civil defence, including warning systems and shelters for personnel, as well as the possibility of remote control of the object from an appropriate shelter facility;
- notification of the population that falls into the zone of possible damage about the emergency situation at the object;
- information exchange and interaction in the relevant sectors of critical infrastructure between subjects of the national critical infrastructure protection system.

The following key decisions should be noted:

- By the National Security and Defence Council of Ukraine regarding the organisation of protection and security of the functioning

²⁴ Volodymyr Zelenskiy, “[Ставка. Реалізація плану захисту енергетики та критичної інфраструктури від російських ударів із неба](#) [Council. Implementation of a plan to protect energy and critical infrastructure from Russian air strikes],” Telegram, 9 September 2023; Volodymyr Zelenskiy, “[Енергетична Ставка. Комплексна підготовка до зими](#) [Energy Council. Comprehensive preparation for winter],” Telegram, 15 October 2024.

of Ukraine’s critical infrastructure and energy facilities during military operations (see Textbox 2 for more details).²⁵

- By the Cabinet of Ministers of Ukraine regarding the implementation of engineering and technical measures for the protection of critical energy infrastructure facilities, as well as other critical infrastructure facilities, from air attacks. According to this decision, the Ministry of Energy approves the list of objects of critical energy infrastructure and submits it to the competent body responsible for the construction of protective structures. The decisions on engineering and technical protection of designated objects are taken by energy companies jointly with the Armed Forces of Ukraine (AFU), the State Emergency Service, and local authorities.²⁶
- Approval by the Cabinet of Ministers of the Strategy for the Development of Distributed Generation until 2035 and approval of the operational plan of measures for its implementation in 2024–26 (see Textbox 3 for more details on the latter).²⁷ The main aim of the strategy is to develop distributed generation systems that can guarantee

²⁵ National Security and Defence Council of Ukraine, [Рішення від 17 жовтня 2023 року введено в дію Указом Президента України від 17 жовтня 2023 року № 695/2023 про організацію захисту та забезпечення безпеки функціонування об’єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій](#) [Decision of 17 October 2023 enacted by a Decree of the President of Ukraine on No. 695/2023 about the organization of the protection and safety of the operation of critical infrastructure and energy facilities of Ukraine in the context of military operations] (Kyiv: Verkhovna Rada, 2023).

²⁶ Government of Ukraine, [Постанова від 27 грудня 2022 р. № 1482 Про реалізацію експериментального проекту щодо будівництва, ремонту та інших інженерно-технічних заходів із захисту об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури](#) [Decree of 27 December 2022 No. 1482 On the implementation of an experimental project of construction, repair and other engineering and technical measures for the protection of critical infrastructure in the energy sector] (Kyiv: Verkhovna Rada, 2022).

²⁷ Government of Ukraine, [Розпорядження від 18 липня 2024 р. № 713-р Про схвалення Стратегії розвитку розподіленої генерації на період до 2035 року і затвердження операційного плану заходів з її реалізації у 2024-2026 роках](#) [Order No. 713-r of 18 July 2024 On approval of the Strategy for the Development of Distributed Generation for the period until 2035 and approval of the operational plan of measures for its implementation in 2024-2026] (Kyiv: Verkhovna Rada, 2024).

power supply to critical infrastructure facilities and to the majority of consumers located in particular areas in the event of an accident in the Ukrainian power system.

Textbox 3: Key Measures Envisaged by the Action Plan 2024–26

The near-term (2024–26) Action Plan for implementation of the Strategy for Distributed Power Generation envisages the following measures:

- increasing the total installed capacity of local generation using gas turbine, gas piston, and cogeneration plants;
- increasing installed capacity of renewable energy facilities by producers and active consumers (prosumers);
- increasing the capacity of energy storage facilities to store electricity for periods of supply interruption;
- the modernisation of network infrastructure and, in particular, the creation of micro- and nano-grids based on “smart-grid” technology;
- the popularisation of the need for the development of distributed generation in society and training of qualified personnel.

- By the regulator of the energy markets, regarding the introduction of non-standard network connections for consumers and granting the right to design and develop network connections for different actors (not only for DSOs as was the case before the full-scale war). This includes approval of the procedure for the organisation of a local energy “island” in the power grids of DSOs and the regulation of the activities of small distribution systems to encourage consumers to also become producers to satisfy their own needs.²⁸

Among the most important practical measures to facilitate the interaction of stakeholders involved in carrying out protection tasks were:

- the establishment of requirements and protocols for exchange of information between the sectoral ministries, various governmental agencies (the armed forces, intelligence and security services, law enforcement), local authorities, and energy companies regarding potential threats to energy facilities, including intelligence information, information on types and means of attacks, and planned measures to

²⁸ National Energy and Utilities Regulatory Commission of Ukraine (NEURC), [Постанова 26.03.2022 № 352 Про особливості тимчасового приєднання електроустановок до системи розподілу у період дії в Україні воєнного стану](#) [Resolution of 26 March 2022 No. 352 On the features of temporary connection of electrical installations to the distribution system during the period of martial law in Ukraine] (Kyiv: Verkhovna Rada, 2022); National Energy and Utilities Regulatory Commission of Ukraine (NEURC), [“НКРЕКП відновила з 1 січня 2024 року стандартні та нестандартні приєднання до електричних мереж](#) [The National Energy and Utilities Regulatory Commission (NEURC) has resumed standard and non-standard connections to electricity networks from 1 January 2024], 2 January 2024; National Energy and Utilities Regulatory Commission of Ukraine (NEURC), [Постанова 15.08.2023 № 1494 Про затвердження Змін до Кодексу систем розподілу](#) [Resolution of 15 August 2023 No. 1494 On approval of amendments to the Distribution Systems Code] (Kyiv: Verkhovna Rada, 2023); National Energy and Utilities Regulatory Commission of Ukraine (NEURC), [Постанова 05.12.2023 № 2274 Про затвердження Змін до Кодексу систем розподілу](#) [Resolution of 5 December 2023 No. 2274 On approval of amendments to the Distribution Systems Code] (Kyiv: Verkhovna Rada, 2023); National Energy and Utilities Regulatory Commission of Ukraine (NEURC), [Постанова 12.12.2023 № 2374 Про затвердження Змін до Кодексу систем розподілу](#) [Resolution of 12 December 2023 No. 2374 On approval of amendments to the Distribution Systems Code] (Kyiv: Verkhovna Rada, 2023).

strengthen the air defence of critical energy infrastructure facilities;²⁹

- the establishment of a coordination headquarters for facilitating the interaction of the involved stakeholders (at the level of the energy ministry, TSO, DSOs, and local authorities);³⁰
- an assessment of the needed resources and equipment to prevent damage to energy facilities and ensure their restoration. A working group on the organisation of humanitarian aid to the energy sector was established under the Ministry of Energy, which collects applications from the Ukrainian energy companies regarding their needs, processes these applications, and forwards them to international partners capable of providing appropriate assistance.³¹

1.3. INTERNATIONAL COOPERATION AND ASSISTANCE

The state of affairs in the energy sector became a priority of Ukraine's relations with partner countries and international

organisations.³² The need for the supply of the needed resources and equipment to protect its critical energy infrastructure, as well as for materials and equipment to restore damaged energy facilities, was regularly presented by Ukraine to international partners at various levels, ranging from the highest political level to individual energy companies. The urgency of increasing Ukraine's ability to protect energy infrastructure from air attacks has become an important subject of discussions with the governments of individual partner countries, within the Ukraine Defence Contact Group (so-called Ramstein Group) of nations that coordinates military aid, and in the inter-parliamentary cooperation framework.³³

Upon a request by the European Commission and in agreement with the Ministry of Energy of Ukraine, the Energy Community Secretariat set up the legal framework for the Ukraine Energy Support Fund to counteract the impact of the Russian aggression. The fund became the coordinating body for providing international support to Ukraine's efforts to rebuild its destroyed energy infrastructure. By the end of 2024, Ukraine had received aid in the form of equipment and materials for repairs worth more than €1 billion through the fund.³⁴ More than 6 000 tonnes of equipment – from large transformers to the smallest spare parts – has been procured through this, processing 160 donations from over 100 companies across 24 countries, benefiting 75 companies in 18 regions of Ukraine.³⁵ At the same time, G7 countries and other partners have raised over

²⁹ [“Росія має намір атакувати три українські АЕС - Зеленський в ООН \[Russia intends to attack three Ukrainian nuclear power plants - Zelensky at the UN\],”](#) *Ukrinform*, 24 September 2024; President of Ukraine, [“Війна Росії проти України завершиться тому, що запроцює Статут ООН – виступ Президента під час засідання високого рівня Ради Безпеки ООН \[Russia’s war against Ukraine will end because the UN Charter comes into effect – President’s speech at a high-level meeting of the UN Security Council\],”](#) 24 September 2024; Yuliya Daletska, [“МАГАТЕ розширить свої місії в Україні на об’єкти інфраструктури, що впливають на безпеку АЕС \[IAEA to expand its missions in Ukraine to infrastructure facilities that affect NPP safety\],”](#) *Biznes-Tsenzor*, 13 September 2024; Oleksandr Yan, [“Генерал США розповів про роботу української акустичної системи виявлення дронів \[US general spoke about the work of the Ukrainian acoustic drone detection system\],”](#) *Militarnyi*, 26 March 2024; Joe Barnes, [“How Ukraine is using mobile phones on 6ft poles to stop drones,”](#) *The Telegraph*, 26 March 2024.

³⁰ Denis Shmyhal, [“Провели нараду щодо ключових питань з головами ОВА за участі Віцепрем’єр-міністра Олексія Кулеби та заступника керівника Офісу Президента Віктора Микити \[A meeting was held on key issues with the heads of the OVA with the participation of Deputy Prime Minister Oleksiy Kuleba and Deputy Head of the President’s Office Viktor Mykita\],”](#) Telegram, 12 October 2024.

³¹ [“Міжнародна допомога енергетиці \[International energy assistance\],”](#) Ministry of Energy of Ukraine, last accessed 11 April 2025.

³² European Commission, [“President von der Leyen announces new EU support for Ukraine’s energy security for the winter,”](#) Directorate-General for Neighbourhood and Enlargement Negotiations, 19 September 2024.

³³ Ministry of Defence of Ukraine, [“Україна зміцнює оборонну співпрацю: результати засідання Контактної групи у форматі «Рамштайн» \[Ukraine strengthens defence cooperation: results of the meeting of the Contact Group in the Ramstein format\],”](#) 14 June 2024; [“Стефанчук на саміті G7 закликав партнерів підтримати енергетику України перед початком холодів \[Stefanchuk at the G7 summit called on partners to support Ukraine’s energy sector before the onset of cold weather\],”](#) *Radio Svoboda*, 8 September 2023.

³⁴ [“Ukraine Energy Support Fund,”](#) Energy Community, last updated 2 April 2025.

³⁵ Energy Community, [“Three years of the full-scale war: Energy Community and Ukraine’s Ministry of Energy strengthen resilience with global support,”](#) 24 February 2025.

\$4 billion since the beginning of Russia's full-scale invasion for the restoration of Ukraine's energy infrastructure.³⁶

Ukraine's example indicates the need to have legal procedures to make the deliveries of equipment as fast as possible

Ukraine's example indicates the need to have in place legal procedures to make the deliveries of equipment as fast as possible. According to a senior official of the Ministry of Energy interviewed for this report, there was no predetermined mechanism for collecting the requests for assistance from the energy companies or for emergency financing, procurement, taxation, and transfer of materiel (equipment, spare parts, etc.) to energy companies. Also, significant administrative capacity and technical expertise were needed to vet the assistance requests of the companies to ensure that their modernisation plans and investments were not passed off as emergency requirements to restore power supply. Furthermore, each donor country contributing to the Energy Support Fund often has its own priorities (e.g., supplying only transformers, or only equipment for renewable energy supply, etc.), which sometimes creates mismatches between what is available and what is really needed due to the Russian attacks.

The government and international partners have successfully navigated most of these issues while also engaging in emergency assistance operations.³⁷ However, a more effective solution would be to provide the national legal framework with the necessary mechanisms for organising the protection of critical infrastructure objects in the event of military aggression, including receiving

and distributing international assistance. This would not only save precious time otherwise lost on finding workarounds to inadequate peacetime laws and regulations, but also ensure greater transparency, efficiency, and speed of urgent procurement processes to obtain what is needed for repairs and reconstruction. Given the number of involved national and foreign stakeholders, this is a very important consideration, especially in terms of building and maintaining trust.

1.4. BALANCING SUPPLY AND DEMAND

Ukraine, based on the experience of the war, has revised the procedure for applying and setting the limits on the volume of electricity supply to consumers, in accordance with the changes in load patterns of different locations due to migration of the population and changes in economic activity. The government has initiated a revision of planned hourly outage schedules (HOS) to clarify the real energy needs and ensure fairness of electricity supply for consumers.

Ukraine has revised the procedure for applying and setting the limits on the volume of electricity supply to consumers, in accordance with the changes in load patterns

One of the Ukrainian lessons tells us that the physical protection measures are not sufficient to provide continuity of electricity supply to end users. The Ukrainian TSO was repeatedly forced to introduce HOS, which are determined together with local authorities, and emergency shutdown schedules (ESS) carried out by the dispatcher in order to prevent the collapse of the entire system.

At the same time, there was a need to guarantee electricity provision to some categories of consumers (military units, defence industry, facilities that support the livelihood of communities, etc.). A procedure was introduced to determine the electric power supply needed for the list of identified critical infrastructure objects as well as the

³⁶ US Department of State, "[Secretary Antony J. Blinken with Italian Foreign Minister Antonio Tajani and Ukrainian Foreign Minister Andrii Sybiha at a G7+ Ministerial Meeting on Ukraine Energy Sector Support](#)," 23 September 2024.

³⁷ Government of Ukraine, [Постанова від 22 липня 2022 р. № 824 деякі питання отримання, розподілу, використання та обліку гуманітарної допомоги для задоволення потреб енергетики в умовах воєнного стану](#) [Resolution of 22 July 2022 No. 824 regarding some issues in receiving, distributing, using and accounting for humanitarian aid to meet energy needs under martial law] (Kyiv: Verkhovna Rada, 2022).

obligation to provide a backup power supply in case they need to apply ESS.³⁸

The government also proposed that large industrial consumers meet their electricity needs by importing power through their own arrangements with foreign suppliers. A requirement was established for the TSO and DSOs to consider the volume of imported energy by enterprises when initiating the application of power outage schedules.³⁹ The government reviewed the rules for importing electricity depending on the situation by establishing a percentage of electricity that enterprises must import to avoid the application of power outage schedules to them. This target is periodically revised depending on the situation and the loss of production due to Russian attacks. In October 2023, the percentage of imports required to be exempted from ESS was fixed at 30% to 50% of consumption, depending on the season. Starting from August 2024, this was increased to 80% throughout the year.

The government has initiated the development of autonomous power systems for critical infrastructure facilities

In terms of ensuring the sustainability of communities and the economy at large, the government has initiated the development of autonomous power systems for critical infrastructure facilities in various sectors (supply of electricity, gas, heating, water, transport, communication, etc.), healthcare facilities, administrative buildings, and educational institutions. The approved strategy for the development of distributed electricity generation and storage aims to

³⁸ Government of Ukraine, [Постанова від 24 травня 2024 р. № 600 про затвердження порядку визначення та застосування граничних величин споживання електричної потужності](#) [Resolution of 24 May 2024 No. 600 on approval of the procedure for determining and applying limit values for electric power consumption] (Kyiv: Verkhovna Rada, 2024); National Security and Defence Council of Ukraine, [Рішення від 17 жовтня 2023 року](#).

³⁹ Government of Ukraine, [Постанова від 27 жовтня 2023 р. № 1127 про затвердження положення про особливості імпорту електричної енергії в умовах правового режиму воєнного стану в Україні](#) [Resolution of 27 October 2023 No. 1127 on approval of the regulation on the properties of the import of electricity under the legal regime of martial law in Ukraine] (Kyiv: Verkhovna Rada, 2023).

provide an autonomous power supply for critical infrastructure objects and ensure the resilience of vital services to end users.⁴⁰

These decisions required significant changes in the structure of the local power grids of the DSOs.⁴¹ In order to organise backup power

To organise backup power supply systems, projects were developed to separate the power supply lines of critical infrastructure objects from the general network

supply systems, projects were developed to separate the power supply lines of critical infrastructure objects from the general network. Furthermore, the efforts of local communities were supported and coordinated at the national level. At the Congress of Local and Regional Authorities under the president of Ukraine on 10 August 2024, a memorandum on enhancing the energy resilience of Ukrainian communities was signed. The main goal of the cooperation envisaged by this memorandum was to bring Ukraine closer to energy independence and meet the EU standards in the field of energy efficiency by improving the energy efficiency of buildings, developing alternative power sources, supporting energy service contracts, and attracting investments in the power production sector.⁴²

⁴⁰ Government of Ukraine, [Розпорядження від 18 липня 2024 р. № 713-р про схвалення Стратегії розвитку розподіленої генерації на період до 2035 року і затвердження операційного плану заходів з її реалізації у 2024-2026 роках](#) [Order of 19 July 2024 No. 713-r on approval of the Strategy for the Development of Distributed Generation for the period until 2035 and approval of the operational plan of measures for its implementation in 2024-2026] (Kyiv: Verkhovna Rada, 2024).

⁴¹ Government of Ukraine, [“Інвентаризація критично важливих об’єктів дозволить забезпечити більш справедливий розподіл електроенергії – Руслан Слободян](#) [Inventory of critical facilities will ensure a more equitable distribution of electricity – Ruslan Slobodyan],” 14 June 2024.

⁴² Ministry for Communities, Territories and Infrastructure Development of Ukraine, [“Memorandum on enhancing energy resilience of communities: key ministries and associations of Ukrainian communities will work together to attract investments,”](#) 22 August 2024.

1.5. CROSS-BORDER ELECTRICITY TRADE

Since March 2022, the Integrated Power System of Ukraine has been operating in synchronous mode with the Continental Europe Synchronous Area (CESA) – the synchronous power grid of continental Europe. Before the massive destruction of its energy infrastructure, Ukraine supplied electricity to EU countries to soften price fluctuations in their markets. During electricity shortages, Ukraine had the technical ability to import electricity from EU countries, but the demand for such imports has increased substantially, thus highlighting the importance of expanding cross-border energy transmission lines to ensure the security of supply in wartime.

At the beginning of the full-scale invasion, Ukraine had a rather limited capacity of 1 200 MW of cross-border electricity trade with ENTSO-E countries. However, the technical capacity was expanded as a result of close cooperation with the neighbouring countries in building and reconstructing the interconnectors and optimising power flows through the networks of those countries. By December 2024, Ukraine already had the technical capacity to import up to 2 200 MW of electricity from EU countries.⁴³ There is also a political and economic understanding of the need to further increase the cross-border flow of electricity.

There is a political and economic understanding of the need to further increase the cross-border flow of electricity

However, the expansion of cross-border trade flows depends not only on technical capacity but also on market incentives. Despite the war, the Ukrainian power sector continues to operate in the market model of regulation. Therefore, the interest in importing electricity to Ukraine from neighbouring countries' markets, or exporting it from Ukraine, depends on price offers on the markets, mainly on the day-ahead market at periods of peak consumption. Long-term contracts are

⁴³ Ministry of Energy of Ukraine, "[Ukraine and EU agree to increase winter electricity import capacity to 2.1 GW](#)," 29 October 2024.

not popular in the market in times of military risk. Therefore, if the price parameters on the markets of the EU countries exceed the offers on the Ukrainian market, where prices are kept superficially low by the energy regulator, Ukrainian consumers are not interested in importing electricity.⁴⁴ At the same time, in cases where the demand for electricity in the market of neighbouring countries exceeds the supply, the volume of possible supply of electricity to Ukraine becomes limited and incentives arise for the Ukrainian producers to export electricity – a dynamic that has fed some conspiracy theories in Ukrainian society (see Chapter 3).

Even a wartime emergency does not always override political considerations, which may result in market failures and breakdowns of political solidarity

Furthermore, political processes in individual neighbouring countries also significantly affect the security of supply, as some governments are inclined to make politically motivated decisions regarding the electricity trade flows.⁴⁵ Restrictions on the flow of electricity to Ukraine during certain periods were applied with various justifications, such as the instability of renewable generation, fuel shortages at TPPs, accidents, or scheduled repairs. This could explain, to some degree, a paradoxical situation in July 2024, when Ukrainian consumers experienced power outages of up to 12 hours per day, but market players did not respond to the need, while Ukraine did not fully use the existing cross-border capacities to import additional electricity.⁴⁶ It is evident that even a wartime

⁴⁴ The low prices in the Ukrainian market, in particular, are explained by the establishment of limits on prices in the market (price caps) by the Ukrainian energy regulator. Although such a decision may be politically determined, due to the unwillingness of the country's leadership in wartime conditions to create an additional burden on consumers, consumers are guided by the available price parameters of the domestic market. Such a policy limits the profitability of electricity producers, TSO, and DSOs.

⁴⁵ Ksenya Srybnyanska, "[Угорщина пригрозила Україні «вимкненням світла»](#)" [Hungary threatens Ukraine with "lights out"], *Apostrof*, 22 July 2024.

⁴⁶ Yuriy Doshchatov, "[Володимир Кудрицький: У нас є розуміння, по яким об'єктам енергетики можуть бити росіяни](#)" [Volodymyr Kudrytskyi: We have an understanding of which energy facilities the Russians can attack], *RBC-Ukraine*, 26 September 2023.

emergency does not always override political considerations, which may result in market failures and breakdowns of political solidarity.

1.6. LONG-TERM TRANSFORMATION

Considering the practical impossibility of fully protecting all energy facilities from damage during a war of such intensity, the Ukrainian government chose a strategy to transform the country's energy system, taking it in the direction of decentralisation and the development of distributed generation to guarantee the provision of important services even in the case of protracted hostilities.

One key strand in this effort builds on the earlier policy to increase the share of renewables in the energy mix. Ukraine has been forming the necessary legislative and regulatory framework for expanding the share of local and renewable energy in the energy balance, stimulating the development of distributed energy sources. This effort has gained momentum because of the Russian aggression and its impact on the power generation and distribution system.

In June 2023, changes were made to energy legislation aimed at accelerating the recovery and the green transformation of Ukraine's energy system.⁴⁷ Market stimulation mechanisms for the development of renewable energy were introduced, including support of active consumers (prosumers). The mechanisms were put in place to encourage resource aggregation of various energy sources and consumers, facilitate the development of small distribution systems (micro- and nano-grids independent of the centralised power transmission and distribution system), and promote energy cooperatives designed to ensure the management of the energy supply of individual local groups of consumers and communities.

⁴⁷ Verkhovna Rada of Ukraine, [Закон України про внесення змін до деяких законів України щодо відновлення та "зеленої" трансформації енергетичної системи України](#) [Law of Ukraine on amendments to certain laws of Ukraine on the restoration and "green" transformation of the energy system of Ukraine] (Document No. 3220-IX) (Kyiv: Vidomosti Verkhovnoi Radi, 2023).

Another strand of the transformation is to speed up the process of installing multiple small local power generation sources – supplying municipal districts, local communities, or large industrial consumers – using gas or biomass. Following the approved action plan for the implementation of the distributed generation development strategy, as of the beginning of August 2024, the installation of cogeneration plants, which simultaneously produce electricity and heat energy, had already been completed in 32 cities in Ukraine. As of September 2024, 83 such plants had been connected to the grid, and a further 82 had been delivered for installation.⁴⁸

The overarching objective of the diversification and decentralisation strategy is to establish a more flexible and adaptable energy system

The overarching objective of the diversification and decentralisation strategy is to establish a more flexible and adaptable energy system, capable of functioning in the event that a specific segment of the grid is compromised. Furthermore, the development

The development of smart-grid technologies has been identified as a key objective

of smart-grid technologies has been identified as a key objective, with the potential to enhance the resilience of energy systems to disruptions. These technologies are designed to facilitate enhanced monitoring, forecasting, and control of energy flows, ensuring a more rapid recovery in the event of an attack and

⁴⁸ Government of Ukraine, [Розпорядження від 18 липня 2024 р. № 713-р](#); Government of Ukraine, ["Денис Шмигаль: Потреби житлово-комунальних підприємств у когенераційних установках покриті більш ніж наполовину](#) [Denys Shmyhal: The needs of housing and communal enterprises in cogeneration plants are covered by more than half], Communication Department of the Government Office, 15 October 2024.

thereby mitigating the impact of energy shortages and ensuring a reliable supply.⁴⁹

To speed up the recovery and advance the development of a new energy architecture, economic tools for support have been introduced. Turbines, generators, inverters, photovoltaic (PV) panels, transformers, and other goods imported into Ukraine were exempt from value-added tax (VAT) and import excise duty.⁵⁰ The government programmes of interest-free lending to citizens, as well as the Affordable Loans 5-7-9 and GreenDIM programmes for condominiums and housing complexes for the purchase of renewable power generation equipment and for energy storage, have been launched.⁵¹

⁴⁹ CFC Big Ideas, “[Challenges and Reality of the Energy Infrastructure of Ukraine](#),” 1 March 2023. Gabriel Collins and Kenneth B. Medlock, “[Ukraine Electricity Sector](#),” Working Paper, Baker Institute, August 2024. International Energy Agency, [Empowering Ukraine Through a Decentralised Electricity System: A Roadmap for Ukraine’s Increased Use of Distributed Energy Resources Towards 2030](#) (IAE, 2024); Susanne Nies and Olha Bondarenko (eds.), [Ukraine’s Energy and Climate Challenges](#) (Ukrainian Analytical Digest no. 9) (Zurich: Centre for Security Studies, 2024).

⁵⁰ Verkhovna Rada of Ukraine, [Закон України про внесення змін до підрозділу 2 розділу XX “Перехідні положення” Податкового кодексу України щодо звільнення від оподаткування податком на додану вартість операцій з ввезення товарів для потреб виробництва та/або ремонту машин механізованого розмінювання](#) [Law of Ukraine on amendments to Subsection 2 of Section XX “Transitional Provisions” of the Tax Code of Ukraine on exemption from value added tax on imports of goods for the purposes of production and/or repair of mechanized demining machines] (Document No. 3853-IX) (Kyiv: Vidomosti Verkhovnoi Radi, 2024); Verkhovna Rada of Ukraine, [Закон України про внесення змін до Митного кодексу України щодо звільнення від оподаткування ввізним митом товарів для потреб виробництва та/або ремонту машин механізованого розмінювання, товарів, які сприяють відновленню енергетичної інфраструктури України, та щодо окремих особливостей митного оформлення товарів, призначених для потреб безпеки і оборони](#) [Law of Ukraine on amendments to the customs code of Ukraine regarding exemption from import duty on goods for the production and/or repair of mechanized demining machines, goods contributing to the restoration of Ukraine’s energy infrastructure, and certain features of customs clearance of goods intended for security and defence needs] (Kyiv: Vidomosti Verkhovnoi Radi, 2024).

⁵¹ Ministry of Economy of Ukraine, “[В Україні запрацювали програми пільгового кредитування для громадян, а також для ОСББ та ЖБК для посилення енергетики](#) [In Ukraine, preferential lending programmes have been launched for citizens as well as condominiums and housing associations to strengthen the energy sector],” 22 July 2024; “[Доступні кредити 5-7-9% \[Available loans 5-7-6%\]](#),” Entrepreneurship Development Fund; Government of Ukraine, “[Промова Прем’єр-міністра Дениса Шмигала на засіданні Уряду](#) [Speech by Prime Minister Denys Shmyhal at a Government meeting],” Communication Department of the Government Office, 9 July 2024.

However, there are serious obstacles to the introduction of distributed generation at the level of small and medium-sized companies and in apartment buildings. The problem lies in the lack of knowledge and skills necessary for the operation of distributed generation installations among potential operators. By and large, small and medium enterprises (SMEs), such as renewable energy and smart-grid developers, municipal utilities, energy cooperatives, and sometimes even regional DSOs, do not possess the financial and technical expertise needed to develop projects, attract investments, and properly operate new technologies. In peacetime, this could be resolved through training, recruiting qualified staff, or outsourcing some processes. In a time of war, these options are very limited.

In addition, in Ukraine, the organisational structures of self-management at the level of apartment buildings are not sufficiently developed to support the fast introduction of distributed generation in residential complexes. When the full-scale war started, there were more than 181 000 multi-apartment buildings, but only about 38 000 buildings (about 20%) had a separate management structure – an association of owners. The absence of legal entities able to apply for funding, as well as oversee the implementation of projects and supervise the operation of the installed equipment, is a major obstacle to the ambitions for a distributed power system.

The government of Ukraine, as well as municipalities of various cities and international partners, recognised this problem and have started offering separate specialised programmes to support the implementation of distributed energy generation projects. The government has simplified the procedures for the construction and placement of gas turbine installations, including cogeneration ones. The procedure for connecting these and other generating units to electric, gas, and heat networks has been simplified. To remove the existing restrictions on the connection of new generating capacities to the power system, special auctions were held for the provision of auxiliary services by electricity producers and active consumers.

To increase the availability of financial incentives, the National Bank of Ukraine adopted a strategy for the development of lending, in particular for the rapid reconstruction of the energy infrastructure. According to the memorandum on bank crediting of energy infrastructure restoration projects, funds from 17 banks were involved.⁵² However, the lack of capacity of the SMEs,

Ukrainian engineers and technicians were bringing the damaged energy facilities back online in the shortest possible time

municipal utilities, and housing communities to plan and execute projects can only be addressed by providing project management training and services – something that the national and municipal authorities should consider doing with foreign assistance, at least until specialised consultancies are able to step in.

1.7. CHAPTER CONCLUSION

Russian aggression against Ukraine and the scale of damage inflicted on the energy sector emphasise that countries need to establish an effective system of physical protection of critical energy infrastructure as part of an overarching and well-integrated national security and defence policy. This is a complex task and requires the cooperation of companies, various authorities at the national and local levels, and even civil society. The war underscored

The war underscored the need for joint assessment of dynamic threats, timely exchange of information, and effective interaction in responding

the need for joint assessment of dynamic threats to the power system, timely exchange of information about the evolving situation, and effective interaction in responding to it. During the three years of the full-scale war,

⁵² [“Найбільші банки України підписали меморандум про пільгове кредитування відновлення енергоінфраструктури”](#) [The largest banks in Ukraine signed a memorandum on preferential lending for the restoration of energy infrastructure], *Ukrainska Pravda*, 25 June 2024.

Ukraine established the requirements for protection and the procedures of interaction and coordination, though in some cases these had ad hoc formats. The combined efforts have helped to make the Ukrainian energy system more resilient against attacks, but this hinges on several crucial factors.

First, this requires sustaining and expanding the **pool of technological and engineering expertise** and manpower in the electricity sector, especially in the TSO and DSOs. Ukrainian engineers and technicians were bringing the damaged energy facilities back online in the shortest possible time, often several times faster than required under peacetime regulations. However, this advantage was built contrary to a modern tendency in the energy sector to outsource such services: A few years ago, the Ukrainian TSO, DSOs, and many electricity producers decided to retain technical personnel as part of their staff, which has worked to their advantage during the war, ensuring quick and continuous availability of this crucial workforce.⁵³

The development of a multinational system of mutual assistance should be done in advance

Second, the war in Ukraine has demonstrated how important **mechanisms of regional and European cooperation** are for ensuring the stability of the functioning of critical infrastructure. In the case of targeted destruction of energy facilities throughout the territory, a country by itself will not be able to protect or restore damaged infrastructure. The scale of destruction exceeds peacetime preparedness, and market players are not ready to promptly respond to the surge of requests for spare parts and new equipment. Thus, the development of a multinational system of mutual assistance to protect and restore critical infrastructure, ensuring the supply of equipment and materials necessary for restoration, is of vital importance and should be done in advance.

⁵³ Liliya Rzheutska, “«Укренерго»: Колапсу не буде.”

This involves establishing effective coordination between partner countries by setting up joint working groups on risk analysis and the development of response scenarios that would help anticipate future needs and prepare response plans. Further steps should include developing instruments for monitoring the inventory of available resources among the countries involved, establishing procedures for information exchange and delivery of the required resources and equipment, and adjusting customs clearance procedures and taxation legislation to facilitate rapid assistance. The establishment of a joint reserve of equipment and materiel would not only expedite the recovery of the energy infrastructure in a particular country in a crisis but would also reduce the economic burden for all countries involved to keep such reserves.

The Ukrainian experience demonstrates the shortcomings of **market tools in a time of war**. The usual peacetime logic of market regulation is insufficient to provide a reliable incentive for market actors. The behaviour of actors in energy markets typically demonstrates a preference for short-term earnings or minimising current financial losses over long-term benefits, which, in wartime, can be ensured only through specially designated market instruments introduced by the government. This raises the issue of forming an understandable mechanism and transparent procedures for deviation from peacetime market regulations in wartime, including in cross-border trading, and fair compensation of the resulting losses. This should also include solidarity agreements protecting cross-border trade flows from interference motivated by domestic politics and ensuring wartime security of supply despite the prevailing conditions in the markets of specific countries.

These tools cannot be replaced by civil emergency cooperation mechanisms developed to ease crises created by natural disasters or accidents. They also cannot be substituted by the emergency support tools within the existing framework of cooperation between the TSOs or international civil emergency cooperation mechanisms, as the scale of damage and duration of negative impact are much higher in wartime. They must be worked out in advance and tailored

to the specific conditions expected to arise during war, as demonstrated by the Ukrainian experience.

There were some fundamental challenges that required the national government to make **strategic decisions with long-term implications**. First, it had to decide on the principles of distributing limited military resources between the protection of the civilian infrastructure and the battlefield. As no country can afford a multi-layered integrated air and missile defence that covers its entire territory at all times, the dilemma is acute, and the decisions can have far-reaching consequences, especially when large NPPs are involved. As such, timely decisions must be made about a mix of other defensive measures to match the threat profile. As some of those measures, such as constructing protective structures, are time-consuming and resource-intensive but offer limited protection against some threats, these are not easy decisions to make, plan for, or enact.

No country can afford a multi-layered integrated air and missile defence that covers its entire territory at all times

Finally, long-term choices had to be made concerning **transitioning to a power system that is more decentralised** and thus less vulnerable to single points of failure. This strategic goal was identified by Ukraine through practical efforts to secure energy supply for end users during the non-stop bombardment of energy infrastructure by Russia since February 2022. However, given the range of considerations – including project management capacity, technical expertise, the economic competence of the involved entities, and the appropriate market design – this kind of work must start well before a war breaks out so as to avoid a situation wherein the availability of new equipment for local power production and micro-grids far outstrips the capacity to install and connect it.

There is a need to increase technical education programmes and engineer retraining courses to successfully support the green transition strategy and increase the resilience of the energy system, as well as to raise awareness among potential operators of distributed

generation facilities and local smart grids regarding energy market procedures and regulations. The establishment of sound economic incentives to stimulate the development of decentralised energy sources is an important element of the overall strategy. But it should rest on a coherent and effective institutional framework and instruments to support SMEs in developing and implementing renewable energy, local power generation, and micro- and nano-grid projects, while accounting for the pressure of time and resource shortages inherent in wartime.

Ukraine has had to defend against an adversary widely recognised as a leading cyber power, noted for its sophisticated capabilities

2. RESILIENCE AGAINST CYBER OPERATIONS

Henry Rõigas

Since the events leading to Russia's illegal annexation of Crimea in 2014, Ukraine has been subjected to offensive operations across all domains, with persistent cyberspace activities accompanying kinetic warfare throughout the conflict. Ukraine has thus had to defend against an adversary widely recognised as a leading cyber power, noted for its sophisticated cyber capabilities.⁵⁴

In the early stages of the conflict, particularly with reference to the unprecedented offensive operations against the energy grid in 2015 and 2016, many observers described Russia's actions as treating Ukraine as a testing ground for novel cyber operations. However, as the conflict has progressed – particularly since its escalation in February 2022 into a full-scale war – a continuous stream of offensive cyber operations has become commonplace, targeting a broad array of entities both within Ukraine and among its allies. This chapter examines these operations from a strategic perspective, as part of a broader campaign to weaken Ukrainian society and undermine its trust in the government while advancing Russia's strategic objectives. It also highlights

⁵⁴ For example, see "[Russia Cyber Threat Overview and Advisories](#)," US Cybersecurity and Infrastructure Security Agency.

key lessons to be learned from Ukraine's success in limiting the impact of these operations by building and sustaining the cyber resilience of its critical infrastructure.

2.1. DATA SOURCES

The analysis for this chapter is based on a review of pertinent publicly available materials, data from the Energy Security Database (ESD), and interviews with Ukrainian stakeholders.

The open-source materials reviewed for this report include existing research and analysis papers, news articles, and cyber threat intelligence reports released by the Ukrainian government as well as by private sector companies that possess data derived from their telemetry or incident response activities in Ukraine.

The ESD, an initiative of the National Academy of Sciences of Ukraine's G.E. Pukhov Institute for Modelling in Energy Engineering (PIMEE), offers a comprehensive dataset of all reported attacks – both kinetic and cyberattacks – on Ukrainian energy infrastructure, sourced from publicly available information. Spanning 2022–24, the database details the timing, targets, and classifications of the attacks, as well as any available attributions.⁵⁵

Anonymised semi-structured interviews were carried out with representatives from five organisations in the government or energy sectors, all of whom have either relevant strategic or technical experience with defending against offensive cyber operations targeting energy infrastructure. As the analysis relies on open-source materials and the interviewees were not required nor allowed

⁵⁵ The Energy Security Database (ESD) is a systematically structured dataset documenting Russian physical and cyberattacks on Ukraine's civilian energy infrastructure, electricity grids, public electricity supply entities, and relevant institutions since January 2022. The ESD was developed and is being maintained by researchers Tetiana Biloborodova (PIMEE, Kyiv) and Inna Skarga-Bandurova (Oxford Brookes University, United Kingdom), with contributions from Pavlo Chorniy (Ternopil Ivan Pulu National Technical University, Ternopil, Ukraine, November 2023–January 2024). The ESD was initiated by the PIMEE as part of the project "AI Methods and Tools for Integrating Resilience Analytics and Edge Computing for Energy Systems". Initial development was sponsored by the US Army Engineering Research and Development Center under grant W911NF-22-2-0153 (2022–23).

to reveal sensitive or confidential information, it is important to note that there may be cyber operations that were not captured in this study, as it is likely that not all incidents have been publicly reported.

2.2. CYBER OPERATIONS

Since the onset of the Russo-Ukrainian war in 2014, various types of offensive cyber operations attributed to the Russian state, its allies, or non-state cyber threat actors have persistently targeted both public and private Ukrainian organisations. Broadly, the frequency and severity of these cyber operations mirrored the intensity of military activities and overall geopolitical tensions. The most active periods for such cyber incidents thus generally coincided with the initial warfare in 2014–16 and the escalated political tensions and military build-up leading up to and after the 2022 full-scale invasion.

The frequency and severity of cyber operations mirrored the intensity of military activities and overall geopolitical tensions

Divided into two chronological periods, 2014–21 and 2022–24, this section of the chapter provides an overview of the cyber operations targeting organisations operating Ukraine’s energy infrastructure. The section does not seek to provide an exhaustive overview of all recorded events; rather, it focuses on select cases considered relevant and representative of the different types of activities carried out.

2.2.1. THE YEARS 2014–21

From 2014 to early 2022, Ukraine’s energy sector, like other domains, was subjected to various types of cyber operations that commonly occur during similar conflicts, ranging from distributed denial of service (DDoS) attacks to more advanced ransomware and cyber espionage campaigns. Amid these relatively typical attacks, two cyber operations targeting the Ukrainian electricity grid clearly stood out, not only as pivotal incidents relevant to the energy sector but also as defining moments in the broader spectrum of cyber operations witnessed during the conflict.

Taking place a year apart, in the cold month of December in 2015 and 2016, two cyber operations succeeded in causing disruptions in energy distribution, resulting in outages. Attributed to a unit of Russia’s military intelligence service (GRU), both these events were regarded as distinctive, signifying a shift in the types of cyber activities that nation-states are willing to and capable of executing against critical infrastructure.⁵⁶

- The first operation targeted three regional electric power distribution companies managed by Prykarpattyaoblenergo in western Ukraine, leading to widespread power outages that affected approximately 225 000 customers for several hours on 23 December 2015.⁵⁷ The attackers compromised systems with the BlackEnergy malware, which was delivered through phishing emails to gain access to the utility’s supervisory control and data acquisition (SCADA) systems. The threat actor was able to remotely switch off substations, erase system files, and disrupt both IT and OT networks. Further complicating the incident response, the attack was reportedly coordinated with a “telephonic denial-of-service” to the customer service lines of the utility, hampering outage reports and delaying restoration efforts.⁵⁸

- The second incident took place on 17 December 2016 and impacted the capital city’s energy provider, Kyivoblenergo.⁵⁹ The incident was deemed more sophisticated than the previous year’s attack, as it utilised a novel malware variant named Industroyer or CrashOverride, specifically engineered to manipulate industrial control systems used in electricity distribution. The attackers managed to open every circuit breaker in the transmission station to trigger the power outage, followed again by wiper software that disabled the station’s computers to prevent monitoring of its digital systems. The attack resulted in a

⁵⁶ “Sandworm,” Malpedia, Fraunhofer FKIE.

⁵⁷ US Cybersecurity and Infrastructure Security Agency, “IR Alert (H-16-056-01),” 20 July 2021.

⁵⁸ Kim Zetter, “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid,” *Wired*, 3 March 2016.

⁵⁹ Andy Greenberg, “New Clues Show How Russia’s Grid Hackers Aimed for Physical Destruction,” *Wired*, 12 September 2019.

power outage in parts of Kyiv, reportedly cutting off one-fifth of the city's power supply for about an hour.⁶⁰ In response, Ukrainian grid operators had to manually close breakers at affected substations to restore electricity. Cybersecurity researchers noted that the attack was designed – but failed – to cause prolonged damage that could have lasted for months, exploiting a security flaw in Siemens' protective relays.⁶¹

2.2.2. THE YEARS 2022–24

After the start of the full-scale invasion by Russia in February 2022, Ukraine's public and private organisations continued to face a steady stream of cyber operations, with the energy sector characterised as a priority target by the State Service for Special Communications and Information Protection of Ukraine (SSSCIP).⁶² The SSSCIP documented 29 incidents classified as "critical" that specifically targeted the energy sector in 2022.⁶³ These operations were described as predominantly affecting electricity grids, public electricity supply companies, and institutions involved in the design and construction of gas or oil pipelines.

Among these incidents, there were reports in April 2022 of operations attributed to the Russian military intelligence service, which attempted to deploy an updated version of the malware used in 2016 – dubbed *Industroyer2* – against high-voltage electrical substations in Ukraine.⁶⁴ The apparent aim of the operation was to cause widespread power outages by first gaining access to the IT network of the substations, enabling the threat actor to subsequently access the OT network and tamper with industrial control systems (ICS). Fortunately, disruptive effects were avoided

by CERT-UA in collaboration with western private sector companies.

In addition to cyber intrusions attributed to Russian state actors, energy companies have also faced attacks from non-state actors, primarily (self-proclaimed) hacktivist groups. These operations have included denial of service attacks on public websites as well as assertions regarding access to or publication of confidential data. A notable instance occurred on 1 July 2022, when DTEK, Ukraine's largest private sector energy company, reported being "under a Russian cyberattack to destabilise the technological processes of power generating and distribution companies."⁶⁵ The

In addition to cyber intrusions attributed to Russian state actors, energy companies have also faced attacks from non-state actors, primarily (self-proclaimed) hacktivist groups

incident coincided with a missile attack on the company's Kryvorizka TPP. The pro-Russian hacker group ZakNet, known mainly for orchestrating DDoS attacks against Ukrainian targets, claimed responsibility, posting unverified samples of DTEK's data on its Telegram channel. Despite these claims, DTEK reported no negative operational impacts, leaving it uncertain whether the threat actor had successfully infiltrated the company's networks.

Another representative example of an operation involving DDoS attacks by Russian hacktivist groups occurred on 16 August 2022, when the website of Ukraine's state nuclear power company, Energoatom, was flooded with traffic, rendering it unreachable. The effects of the operation were limited, as it only affected the company's website for three hours and did not influence its internal operations.⁶⁶

In late 2022, a western cybersecurity firm published a report on a cyber operation that led to two unplanned power outages,

⁶⁰ Greenberg, "New Clues."

⁶¹ Greenberg, "New Clues."

⁶² State Service of Special Communications and Information Protection of Ukraine, *Russia's Cyber Tactics: Lessons Learned 2022* (Kyiv: SSSCIP, 2022).

⁶³ State Service of Special Communications, *Russia's Cyber Tactics*.

⁶⁴ Daniel Kapellmann Zafra, Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrandt, Keith Lunden, and Nathan Brubaker, "*Industroyer.V2: Old Malware, New Tricks*," *Google Cloud Blog*, 25 April 2022; Canadian Centre for Cyber Security, *Cyber Threat Activity Related to the Russian Invasion of Ukraine* (Government of Canada, n.d.).

⁶⁵ DTEK, "[Enemy launches hacker attacks on the power system](#)," 1 July 2022.

⁶⁶ Daryna Antoniuk, "[Ukraine's State-Owned Nuclear Power Operator Said Russian Hackers Attacked Website](#)," *The Record*, 17 August 2022.

coinciding with mass missile strikes on Ukraine's critical infrastructure.⁶⁷ Attributed again to the GRU, this operation was noted for utilising novel and expanded capabilities to target OT assets. The initial detection of the threat actor in the victim's environment dates to June 2022, with the final phase – deploying data wipers to erase forensic evidence and enhance disruption – executed in October. Further details on the extent of the impact and other specifics of the incidents remain undisclosed.

Based on official incident reporting and response statistics, the first half of 2023 witnessed a decrease in the frequency of attacks against the energy sector, with eight critical incidents with registered impacts reported, compared to 16 in the second half of 2022, and one case classified as a "disruption operation."⁶⁸ However, the second half of 2023 saw the level of cyber operations targeting the energy sector return to 2022 levels, albeit with a 50% reduction in the number of "critical" incidents. Despite the decrease, the energy sector continued to be a prioritised target for Russian threat actors, with a key objective presumed to be the gathering of intelligence on high-value targets on the physical battlefield, such as the Zaporizhzhia NPP.

A key objective of Russia cyber threat actors was the gathering of intelligence on high-value targets on the physical battlefield, such as the Zaporizhzhia NPP

Available official data from 2024 has not yet provided detailed statistics specifically on attacks targeting the energy sector; however, reports note an overall increase in cyber operations against Ukrainian

organisations, including attacks against energy infrastructure.⁶⁹ One such cyber operation that achieved operational effects targeted an unnamed heating utility in Lviv in January 2024, disabling services to 600 buildings for around 48 hours.⁷⁰ Marking the first known instance of cyber-enabled sabotage on a heating utility, an analysis by a US industrial cybersecurity company revealed that the attackers manipulated temperature readings to deactivate heating and hot water systems.⁷¹ The company's report further highlighted that this attack employed novel technical capabilities, different from those seen in previous incidents.

Many attempts targeted supply chains – either through the exploitation of vulnerabilities in specific software or by compromising service providers

In its report about events in the first half of 2024, the SSSCIP specifically points to continued efforts in March by the GRU to launch destructive attacks on nearly 20 Ukrainian energy infrastructure entities, including power, heat, and water supply facilities.⁷² Referring to the continued development of technical capabilities and a shift in tactics, the report points out that many of these attempts targeted supply chains – either through the exploitation of vulnerabilities in specific software used by energy organisations or by compromising service providers that had access to ICS for maintenance and technical support.⁷³

It is also important to mention that energy infrastructure operations in Ukraine have consistently been the targets of other types of activities that include digital elements but do not strictly qualify as offensive cyber operations involving unauthorised intrusions.

⁶⁷ Ken Proska, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler McLellan, and Chris Sistrunk, "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology," *Google Cloud Blog*, 9 November 2023.

⁶⁸ State Service of Special Communications and Information Protection of Ukraine, *Russia's Cyber Tactics H1'2023. Lessons Learned: Shift in the Patterns, Goals, and Capacity of the Russian Government and Government-Controlled Groups* (Threat Assessment Report) (Kyiv: SSSCIP, 2023).

⁶⁹ State Service of Special Communications and Information Protection of Ukraine, *Russian Cyber Operations* (APT Activity Report H1 2024) (Kyiv: SSSCIP, 2024).

⁷⁰ Andy Greenberg, "How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter," *Wired*, 23 July 2024.

⁷¹ Mark Graham, Carolyn Ahlers, and Kyle O'Meara, "Impact of FrostyGoop ICS Malware on Connected OT Systems," *Intelligence Brief, Dragos Inc.*, July 2024.

⁷² SSSCIP of Ukraine, *Russian Cyber Operations*.

⁷³ SSSCIP of Ukraine, *Russian Cyber Operations*.

For instance, in March 2022, a disinformation campaign – disseminated across various online groups – featured Russian sources spreading false messages urging users to turn off their electrical appliances at a specific time in an attempt to disrupt the power grid by manipulating its frequency balance. Similarly, in October 2022, fake alerts about widespread power outages were circulated through Telegram channels using the Ukrenergol logo, aiming to sow panic and undermine trust.

2.3. THE BIGGER PICTURE

To inform effective defensive measures against such threats, this section examines the role and implications of the observed cyber operations within the context of Russia's overarching strategy and military offensive against Ukraine.

Building on the disruptive operations of 2015 and 2016, which were often characterised as mere tests by Russia, observers initially anticipated that future use of offensive cyber capabilities against critical infrastructure could likely be more significant, particularly if the conflict escalated. Although the first day of the full-scale Russian invasion included an unprecedented destructive attack against satellite infrastructure, aimed at hampering Ukrainian communications, the publicly reported cyber operations following the invasion – including the ones against energy infrastructure – have arguably not achieved noticeable decisive or significant strategic effects that might further Russia's political or military objectives in Ukraine.⁷⁴

Characterising the goals of offensive cyber activities since the large-scale invasion, the SSSCIP described Russian efforts in 2022 as predominantly focused on opportunistically exploiting flaws and vulnerabilities in various Ukrainian targets.⁷⁵ These operations, aimed at dismantling IT infrastructure or exfiltrating sensitive data, were assessed not to have achieved the long-term effects initially intended, as IT systems were quickly

restored.⁷⁶ Reports about Russian cyber offensive activities in 2023 highlighted a shift from destructive goals towards establishing footholds in networks to prioritise extracting information and gathering feedback on kinetic operations.⁷⁷ Building on experiences from the first half of 2024, the SSSCIP further observed a pivot in Russian activities towards operations that directly support military activities in the theatre of war, aiming to maintain a presence in systems and target areas critical to the success of specific military operations.⁷⁸

The absence of successful disruptive cyber operations can be interpreted in various ways. On the one hand, it may reflect the limited strategic capability or effectiveness of cyber operations in terms of causing long-term disruptions to critical infrastructure during full-scale military conflicts. Although public data on cyber operations is scarce, an analysis of open-source reports of incidents in the ESD gives an indication, showing that the occurrence ratio of physical to cyberattacks is approximately one to ten. Thus, in the context of achieving destructive effects against energy infrastructure, particularly considering the large-scale missile and drone campaigns conducted by Russia, cyber operations have neither substituted for nor effectively competed with kinetic operations.

Cyber operations have neither substituted for nor effectively competed with kinetic operations

On the other hand, the absence of destructive effects could also be explained by the capabilities of both Russia and Ukraine, reflecting either the limited offensive capacity of the former or the superior defensive abilities of the latter. Objectively assessing this dynamic is almost impossible, and a statement from Google's chief analyst John Hultquist sheds light on the nature of this power struggle: "There's a misconception that Russian cyber actors are not trying, but in reality, the Russian threat groups are absolutely persistent at

⁷⁴ Viasat, "KA-SAT Network Cyber Attack Overview," 30 March 2022.

⁷⁵ SSSCIP of Ukraine, *Russian Cyber Operations*.

⁷⁶ SSSCIP of Ukraine, *Russian Cyber Operations*.

⁷⁷ SSSCIP of Ukraine, *Russian Cyber Operations*.

⁷⁸ SSSCIP of Ukraine, *Russian Cyber Operations*; Dan Black, "Russia's Cyber Campaign Shifts to Ukraine's Frontlines," *RUSI*, 22 July 2024.

targeting Ukraine and keep coming back again, and again, and again.”⁷⁹

The absence of successful disruptive cyber-enabled operations with long-term effects should not be misinterpreted as evidence that offensive cyber operations against energy infrastructure have lacked strategic value for Russia. Cyber operations, of course, function as a means to an end rather than an end in themselves. The persistent reliance on kinetic methods, such as missile strikes, likely reflects the availability of these capabilities, their potential scale and reach in targeting, as well as the extensive, long-lasting physical damage they can inflict.

Second, when considering the underlying goal of most recorded operations against Ukraine and reflecting on other advanced cyber operations targeting western countries, Russia’s strategy for offensive cyber operations should be viewed within the broader

Offensive cyber capabilities have aimed at either obtaining impactful information for cyber espionage or generating information for propaganda and influence operations

framework of its concept of information warfare.⁸⁰ It can be even argued that all known offensive cyber capabilities targeting energy infrastructure have aimed at either obtaining impactful information for cyber espionage or generating information for propaganda and influence operations. This argument also extends to the few destructive operations observed – while their tangible, real-world impacts were fortunately short-lived, they, nonetheless, served to signal capabilities and exert psychological pressure.

Existing analysis of Russian cyber operations in the Ukraine conflict confirms that most of these activities have focused on intelligence gathering, with the sensitive information

obtained being leveraged in various ways.⁸¹ This is also confirmed by the assessment of the SSSCIP, which states that intelligence gained via cyber intrusions against critical infrastructure has increasingly been utilised to either gauge the success of or support ongoing military operations.⁸² In the context of energy targets – for example, previously mentioned reports regarding Zaporizhzhia NPP – this use may entail gaining access to information that supports planning and tactical decision-making for kinetic military operations.

Other incidents, such as the operation carried out against DTEK, demonstrate that obtained data can also be released to the public with the aim of extorting or otherwise pressuring specific targets or – more commonly – causing societal distress and undermining confidence in Ukraine’s ability to maintain the functionality of its critical infrastructure. The same objective also underlies DDoS attacks, which, while generating news headlines and temporarily denying access to targeted services, are often mitigated quickly, rarely impact operational capabilities, and consequently have a limited overall effect in terms of actual disruption. Even the reported destructive attacks, particularly those in the early stages of the conflict, can

be characterised as influence operations, with Russia seeking to display its capabilities to the world while discrediting Ukraine’s ability to defend its critical infrastructure and inflicting psychological harm on Ukrainians.⁸³

2.4. IMPLICATIONS

Ukraine’s remarkable and sustained resilience in the face of large-scale Russian aggression has rightfully garnered widespread admiration. The capability to withstand and respond to

⁷⁹ Antoniuk, “Ukraine’s State-Owned Nuclear Power Operator Said Russian Hackers Attacked Website.”

⁸⁰ Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016).

⁸¹ Erica D. Lonergan, Margaret W. Smith, and Grace B. Mueller, “Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine,” in *2023 15th International Conference on Cyber Conflict: Meeting Reality*, edited by T. Jančárková, D. Giovannelli, K. Podiņš, and I. Winther, 85–104 (Tallinn: NATO CCDCOE Publications, 2023).

⁸² SSSCIP of Ukraine, *Russian Cyber Operations*.

⁸³ Similar conclusions were reached when analysing the first years of the war since the invasion of Crimea in 2014, see Kenneth Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCDCOE Publications, 2015).

adversity is also apparent in the country's ability to counter offensive cyber operations, including in the energy sector.

2.4.1. THE NATURE OF THE THREAT

The nature, impact, and scope of known cyber operations targeting Ukrainian energy infrastructure highlight critical challenges that must be addressed to guide the development of effective defensive strategies.

First, the observed events confirm that critical infrastructure, including the energy sector, is considered a strategic target for Russia, contested through all available methods deemed effective. Demonstrating the versatility of Russian cyber threat actors, these methods have included DDoS attacks, defacements, sensitive data leaks by self-proclaimed hacktivist groups, and sophisticated cyber intrusions by

Critical infrastructure, including the energy sector, is considered a strategic target for Russia

state actors aimed at espionage or operational disruption. Offensive cyber operations should not be viewed in isolation but as one component in Russia's arsenal, evaluated alongside other methods of influence and coercion for their effectiveness. The logic is straightforward: the adversary identifies the desired strategic or tactical outcome and selects the means most likely to achieve it.

Second, the TTPs employed by threat actors are constantly evolving and remain unpredictable, as offensive operations against energy infrastructure have been carried out by a diverse range of pro-Russian actors, including dedicated military and intelligence units as well as loosely organised hacktivist groups. Operations attributed to Russian state actors

Operations attributed to Russian state actors demonstrate continued investment and innovation in developing offensive capabilities

demonstrate continued investment and innovation in developing offensive capabilities, such as exploiting supply chain vulnerabilities and utilising zero-day exploits. Meanwhile, the

unprecedented activity of hacktivist groups during the war – often organised ad hoc and employing relatively unsophisticated methods – adds a layer of unpredictability, complicating defensive strategies and amplifying Russia's overall cyber capabilities.

Third, Ukraine's experience in defending its energy infrastructure underscores the challenges of managing complex risks inherent to the highly interconnected and interdependent nature of modern infrastructures. In terms of digital systems, for example, cases from Ukraine demonstrate that threat actors seek to exploit vulnerabilities beyond the direct control of energy organisations. These include vulnerabilities in third-party software used in operations or access gained through third-party service providers to energy companies. Beyond cybersecurity, the potential risk posed by malicious insiders, such as foreign agents, must also be considered – although no specific reports on such actors have been disclosed – further complicating risk management efforts. Additionally,

although energy infrastructure underpins nearly all other sectors, interviewees highlighted that operations targeting other critical infrastructure domains can significantly impact the energy sector as well. For instance, the management of energy infrastructure may rely on telecommunication networks, which have also been targeted during the war.

Fourth, the diverse ecosystem of public and private energy organisations in Ukraine leads to varying levels of cyber resilience among individual energy infrastructure providers, shaped by the available resources and overall awareness of cyber risks. Given the extensive kinetic strikes on energy infrastructure and the predominance of cyber operations focused on intelligence gathering without immediate, visible effects, some organisations across Ukraine's energy supply chain likely have a lower sense of urgency regarding addressing these risks. This perception makes it more challenging to encourage organisations to proactively strengthen their cyber resilience, rather than relying predominantly on centrally provided – and often already overstretched – governmental support.

Beyond strategic challenges, Ukraine's experience highlights several specific technical obstacles complicating efforts to defend and build resilience in energy infrastructure. While requiring air-gapping for critical systems emerged as a key lesson from the destructive attacks of 2015–16, isolating OT from IT networks remains a persistent challenge in energy systems.⁸⁴ Related to this issue and as an example, experts have identified a significant number of internet-connected energy infrastructure assets, including OT, visible through public scanning tools such as Shodan.⁸⁵

Efforts to modernise infrastructure naturally expand the attack surface and are bound to introduce new vulnerabilities

Additionally, many energy infrastructure systems in Ukraine rely on legacy technologies or depreciated operating systems. These can range from industrial systems developed during the Soviet era to software components – likely integrated before 2014 – originating from Russian developers. On the other hand, efforts to modernise infrastructure naturally expand the attack surface and are bound to introduce new vulnerabilities. For instance, establishing remote access to energy infrastructure may be essential for efficiency, for safeguarding employees from kinetic attacks during wartime, or for the management of micro-grids, but it requires stable and secure communications and management of the risks associated with home devices.⁸⁶

2.4.2. UKRAINE'S BATTLE-HARDENED CAPABILITIES

First and foremost, Ukraine's success in defending against offensive cyber operations can be explained through the adaptability, resilience, and battle-hardened capabilities

of its people and institutions. Since 2014, Ukraine has been actively developing its national cybersecurity capabilities and governance framework, beginning with the adoption of its first national strategy in 2016, followed by an updated strategy in 2021.⁸⁷ While far from perfect due to the country's limited resources and extreme geopolitical circumstances, the most critical elements for defending its infrastructure are in place.⁸⁸ These include an active national agency tasked with coordinating and supporting energy infrastructure through both proactive measures, such as providing threat detection solutions and promoting best practices, and reactive measures such as coordinating and delivering incident response support. Driven by necessity and under continuous pressure, Ukraine continues to enhance its cybersecurity framework. A recent milestone in this progression was the establishment of a military computer emergency response team (CERT) in October 2024, a dedicated unit tasked with defending the nation's military and communication networks.⁸⁹

In addition, Ukraine has effectively fostered and leveraged support from international partners to bolster its cybersecurity capabilities. The international support and collaboration have been regarded as another key element of success, involving contributions from individual western nations and international organisations, as well as deepened collaborations with and support from private sector companies. This has ranged from intelligence sharing to providing cybersecurity solutions and incident response support. For example, the pre-invasion efforts saw collaborations with the US Cyber Command and private sector companies to fortify the resilience of critical networks.⁹⁰

⁸⁴ Interview with a Ukrainian cybersecurity expert (government); SSSCIP of Ukraine, *Russia's Cyber Tactics*.

⁸⁵ Interview with a Ukrainian cybersecurity expert (government).

⁸⁶ Andrii Davydiuk and Vitalii Zubok, "Analytical Review of the Resilience of Ukraine's Critical Energy Infrastructure to Cyber Threats in Times of War," in *2023 15th International Conference on Cyber Conflict: Meeting Reality*, edited by T. Jančárková, D. Giovannelli, K. Podišš, and I. Winther, 85–104 (Tallinn: CCDCOE Publications, 2023).

⁸⁷ Andrii Davydiuk and Oleksandr Potii, *National Cybersecurity Governance: Ukraine* (National Cybersecurity Governance Series) (Tallinn: CCDCOE Publications, 2024).

⁸⁸ Natalia Spínu, *Ukraine Cybersecurity Governance Assessment* (Geneva: Geneva Centre for Security Sector Governance, 2020).

⁸⁹ Daryna Antoniuk, "Ukraine's Defense Ministry Launches Military CERT to Counter Russian Cyberattacks," *The Record*, 8 October 2024.

⁹⁰ Nick Beecroft, "Evaluating the International Support to Ukrainian Cyber Defense," *Cyber Conflict in the Russia-Ukraine War Series*, *Carnegie Endowment for International Peace*, 3 November 2022.

Since the invasion, the support has intensified, with NATO nations as well as cybersecurity companies sharing cyber threat intelligence on Russian actors and capabilities to increase critical infrastructure protection. This

Continuous, two-way exchange of information and resources has significantly improved the cybersecurity posture of the allies

continuous, two-way exchange of information and resources has not only strengthened Ukraine's defences but is also seen as significantly improving the cybersecurity posture of the allies.

2.4.3. LESSONS LEARNED AND KEY FOCUS AREAS

An examination of Ukraine's experience provides insights and recommendations for strengthening the protection of critical infrastructure both within Ukraine and among its allies, ranging from implementing organisational best practices to adopting specific technological measures.

The observed events underscore the **critical need to prioritise resilience**: the capacity to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises. Attacks on energy infrastructure reveal a broader truth about cyber defence: for today's complex and interconnected digital systems,

For today's complex and interconnected digital systems, absolute security and guaranteed protection are unachievable

absolute security and guaranteed protection are unachievable. Such modern systems inherently carry risks, particularly when targeted by capable nation-state adversaries exploiting vulnerabilities associated with an ever-expanding attack surface and a complex, often poorly managed supply chain.

Addressing this reality necessitates the development of **robust reactive capabilities within the energy sector**. This involves, for instance, conducting collaborative crisis

simulations and exercises to establish effective incident response plans and fostering coordination at both the sector-wide and national levels. Additionally, strengthening reactive capabilities in the highly interconnected energy sector requires analysing, mapping, and modelling interdependencies in relation to various incident scenarios to understand the potential cascading effects across other domains.

The Ukrainian experience in combating Russian operations targeting multiple domains also highlights that cyber-security strategies should not be developed in isolation. Energy infrastructure operators and national agencies must base their activities on broader strategic risk assessments and develop **interdisciplinary organisational and technical capabilities** that extend beyond the narrow focus of defending networks from intrusions.

An energy company's crisis response plans should not only address technical mitigation measures but also include strategic communication playbooks

For instance, **cyber operations are utilised as part of broader information warfare** in the Russo-Ukrainian war, which suggests that an energy company's crisis response plans should not only address technical mitigation measures but should also include strategic communication playbooks to counter disinformation or maintain public confidence. Furthermore, particularly in the case of Ukraine, effective cybersecurity responses also depend heavily on civil-military collaboration to enhance coordination, share risk assessments, and enable resource-sharing.

Although international and national support is crucial in effective cyber defence, **enhancing the individual capabilities of organisations** operating within the energy infrastructure is unavoidable. While governments can establish regulatory frameworks, offer basic support capabilities, and assist in incident response, the primary defence responsibility rests with the energy organisations themselves. These entities must continuously maintain a high level

of security to prevent opportunistic adversaries from exploiting easily avoidable vulnerabilities and dependencies, which often arise from neglecting basic security best practices. For instance, lapses might include failing to fully isolate critical operational technologies from office networks, neglecting software updates and vulnerability management, or leaving assets publicly exposed.

The primary defence responsibility rests with the energy organisations themselves

Compliance with and adherence to security best practices or requirements are not only difficult for government agencies to monitor comprehensively but also a challenge for organisations to implement, particularly in sectors with diverse stakeholders, some of whom have limited resources. In such circumstances, cybersecurity policymakers should consider developing tailored frameworks and providing financial support to ensure organisations can meet these standards. Additionally, organisational uptake depends heavily on the **awareness of decision-makers** regarding these challenges, making targeted training, education, and promotional efforts essential across the complex supply chain of energy infrastructure providers.

Beyond getting the basics right, energy organisations – especially given how frequently they are targeted by capable nation-state actors – should use cyber threat intelligence (CTI) to inform the adoption of targeted security measures that reflect the evolving TTPs of these adversaries. Where security budgets are limited, the most effective approach is **active threat information sharing** among sector stakeholders, ideally coordinated by state agencies or industry associations with access to classified intelligence and supported by feeds from leading commercial CTI providers.

2.5. CHAPTER CONCLUSION

Since the events leading to Russia's armed invasion in 2014, Ukraine's energy infrastructure has been a persistent target of offensive cyber operations orchestrated by Russian state and non-state actors, reflecting the broader intensity of the Russo-Ukrainian

conflict. These cyber operations have ranged from low-impact DDoS attacks to sophisticated intrusions aimed at accessing sensitive information or disrupting operational systems. Notable incidents in 2015 and 2016 caused power outages, demonstrating the disruptive potential of cyberattacks on critical infrastructure. Since the 2022 large-scale invasion, Russian cyber threat actors have continued targeting energy systems with varying degrees of success in causing disruptions.

The limited ability of Russian cyber campaigns to achieve lasting, large-scale destructive effects highlights the inherent challenges of using cyber operations for enduring disruption, especially when compared to the effectiveness of kinetic operations, which remain Russia's primary method to cause significant physical destruction against energy infrastructure. At the same time, Ukraine's defensive efforts and battle-hardened capabilities have played a crucial role in mitigating large-scale destructive effects of cyber threats. These defences have been bolstered by substantial international support from allied nations and western cybersecurity companies, which have provided resources, intelligence, and expertise to strengthen Ukraine's cyber resilience.

While certain cyber operations have demonstrated the potential for significant damage, most align with the core objectives of Russia's broader information warfare strategy, which primarily focuses on intelligence gathering or influence operations. This is exemplified by the bulk of cyber operations that have sought to collect sensitive data or support hostile propaganda efforts by leaking information to undermine trust, apply pressure on victims, or reinforce disinformation narratives. Cyber operations targeting the energy grid have also revealed constantly evolving TTPs by Russian threat actors, such as exploiting vulnerabilities within supply chains, including weaknesses in software and third-party organisations, to penetrate critical systems.

Countering such an advanced threat actor requires energy sector organisations to adapt constantly and establish sustained investments in both proactive and reactive cybersecurity

measures. The Russo-Ukrainian war also shows that it is important to avoid developing cybersecurity strategies in isolation. Building

Countering such an advanced threat actor requires energy sector organisations to adapt and invest in both proactive and reactive cybersecurity measures

resilience necessitates understanding the adversary's broader strategy, building interdisciplinary collaboration within energy companies, and coordination with other organisations both within and across domains. This includes conducting multi-stakeholder simulations and exercises, integrating strategic communication strategies into incident response plans, and establishing working civil-military partnerships. Ukraine's ability to withstand sophisticated cyberattacks also underscores the importance of mapping interdependencies across critical infrastructure, implementing cyber awareness initiatives, and making targeted investments in technological upgrades and organisational preparedness – not only by government agencies but, more importantly, by energy companies themselves.

3. STRATEGIC COMMUNICATION

Dmitri Teperik

Since Russia's full-scale invasion of Ukraine in February 2022, the energy sector infrastructure in Ukraine has faced unprecedented challenges. Consequently, the issue of power system resilience has become a significant topic in both domestic crisis communication, led primarily by emergency services and energy companies, and strategic communication conducted by Ukraine's state authorities and political establishment at the national and international levels.⁹¹ The repeated disruption to the electricity supply

⁹¹ This chapter is based on open-source data and analysis of in-depth interviews conducted with six Ukrainian experts in different fields – energy security, strategic communication, crisis management, emergency response, political sociology, and media – conducted in December 2024.

has had a significant impact on millions of Ukrainians, shaping public perceptions regarding energy-related decision-making and the image of various stakeholders involved in this complex system.

Since power supply is crucial for the well-being of citizens and the cohesion of society, and it also directly impacts governance effectiveness, efforts to protect and ensure the long-term

resilience of Ukraine's power system are not only essential for national security but also for maintaining public morale during the ongoing war. In October 2024, Ukrenergo issued a warning that the upcoming winter was likely to be the most challenging in the past three years in terms of power supply.⁹² Eventually, the challenge was successfully managed, but at a high cost and with major multi-directional efforts, which included efforts to inform society and limit the spread and impact of disinformation. This chapter examines some of the key lessons from Ukraine's crisis and strategic communication and counter-

Efforts to protect and ensure the long-term resilience of Ukraine's power system are essential for national security and maintaining public morale during the ongoing war

disinformation measures that were aimed at maintaining public support and cooperation when dealing with the consequences of the destruction and disruption of its power system by Russian attacks.

3.1. PUBLIC OPINION AND SUPPORT

There is a wealth of public opinion data to draw upon to assess how the resilience of Ukrainian society evolved and where it came under significant pressure during Russia's campaign to destroy the country's power system. A survey conducted in May 2024 revealed that Ukrainians demonstrated a high level of awareness regarding the situation

⁹² "В «Укренерго» спрогнозували найважчу за останні три роки зиму [Ukrenergo predicted the most severe winter in the last three years]," *Slovovidlo*, 30 October 2024.

in the energy sector.⁹³ Specifically, 81% of respondents reported being informed about Russia's attacks against energy facilities, while 57% had come across photos or videos, primarily on social media and other online platforms, that depicted the extent of the damage. Furthermore, 74% of respondents expressed the opinion that such attacks are part of a long-term strategy on the part of Russia to destroy the Ukrainian energy sector and force the country to surrender. Nevertheless, 35% of respondents expressed the conviction that Ukraine's energy infrastructure possesses the capacity to withstand the challenges posed by missile strikes, while 56% believe that it can do so only partially.

Regarding shortages, 66% of respondents indicated that a stable electricity supply is important to them, but that short-term interruptions can be tolerated. In the event of a deterioration in the energy supply situation, 54% of respondents indicated their intention to utilise power banks at home, while 43% indicated their intention to employ alternative energy sources. In the event of an emergency, 41% of respondents indicated their intention to seek refuge in emergency shelters or other municipal facilities equipped with autonomous generators. Urban residents, younger people, and those with higher incomes were more likely than other groups to report plans to use individual energy storage devices at home. Conversely, rural respondents exhibited a greater inclination towards using alternative energy sources. Those with lower incomes were more likely to mention the use of emergency points or public places.

According to 41% of the respondents, the entire energy infrastructure needs to be restored immediately, while 52% believed that only the most important facilities should be restored immediately, with the remainder to be addressed after the war. Furthermore, 55% of respondents expressed support for the implementation of increased tariffs, a measure intended to facilitate the restoration of damaged power infrastructure, but 40% expressed opposition to this, despite the

⁹³ Sociological Group Rating, "[Діяльність енергетичного комплексу України в умовах російського вторгнення](#) [Activities of the Ukrainian energy complex in the context of the Russian invasion]," 6-8 May 2024.

acknowledgement of a potential deterioration in electricity supply. Furthermore, 76% of respondents reported that, in response to appeals from Ukraine's energy sector, they reduced electricity consumption during peak hours.

As of September 2024, 74% of respondents reported consistent efforts to utilise electricity in a cost-effective manner, with 22% admitting to doing so only occasionally.⁹⁴ Furthermore, 31% of surveyed Ukrainians reported experiencing power outages, nevertheless, 89% of respondents indicated their intention to remain at their permanent residences in the autumn and winter of 2024–25 in spite of challenges with power supply. Moreover, 66% of respondents expressed satisfaction with the government's efforts to improve the energy sector, while 30% expressed dissatisfaction. According to respondents, the most notable measures undertaken by Ukraine's authorities in the energy sector are restoring destroyed energy facilities (50%), augmenting funds and energy equipment from international partners (38%), and strengthening the protection of energy facilities (36%). It is noteworthy that younger demographic groups demonstrate a higher level of awareness regarding measures aimed at improving the energy situation. The data indicates a high degree of public support for Ukraine's plans and efforts to repair and reinforce substations, transmission lines, and power plants as well as for the deployment of advanced air defence systems to protect key facilities.⁹⁵

By the end of 2024, only 12% of Ukrainian businesses were saying they would benefit from greater protection and restoration of Ukraine's energy system, compared to 34.5% in August of the same year, even though 68% of companies had temporarily suspended operations due to power outages in November 2024. This could be interpreted as a measure

⁹⁴ Sociological Group Rating, "[Діяльність енергетичного комплексу України: оцінки та практики споживачів](#) [Activities of the energy complex of Ukraine: consumer assessments and practices]," 20-23 October 2024.

⁹⁵ "Енергетична інфраструктура України матиме три рівні захисту," *Radio Svoboda*; President of Ukraine, "[Життя України має зберегтися, і це стосується, зокрема, енергетичного забезпечення – звернення Президента](#) [The life of Ukraine must be preserved, and this applies, in particular, to energy supply - the President's address]," 20 June 2024.

of trust in the ability of the government and power system operators to maintain power supply as well as of confidence in their own decentralised solutions to replace it, if necessary, over the winter of 2024-25; meanwhile, other challenges such as tax burden eclipsed concerns about availability of electricity. However, it must be noted that small businesses suffered more losses, with metallurgy and metalworking experiencing the greatest time losses among industries.⁹⁶

The survey revealed that 64% of respondents were aware of the NPPs accounting for the largest share of electricity generation in Ukraine. Furthermore, 78% of respondents expressed support for the further development of nuclear energy as deemed necessary. Concurrently, a resounding 95% of respondents expressed support for increasing the share of electricity generated from alternative sources such as solar and wind in Ukraine's overall energy structure. This attitude is consistent with Ukraine's energy diversification strategy, which emphasises the importance of a diverse power generation portfolio to reduce reliance on any single type of electricity source (see Chapter 1).

Public attitude is consistent with Ukraine's energy diversification strategy

Nevertheless, a number of energy experts have published a series of critical remarks regarding the preservation of stability and the restoration of power generation in Ukraine. In particular, the inequitable distribution of electricity across Ukraine's regions during the summer and winter of 2024 has been the subject of criticism, as many customers found the fundamental principles of the HOS to be opaque or even confusing.⁹⁷

⁹⁶ Oksana Kuziakiv, Yevhen Angel, Anastasya Hulik, and Daria Shapovalova. [Національне опитування щодо відновлюваних джерел енергії в Україні, січень 2025](#) [National survey on renewable energy sources in Ukraine, January 2025] (Kyiv: Institute for Economic Research and Policy Consulting, 2025).

⁹⁷ Mariya Babenko, "[Міфи щодо відключень світла: графіки, експорт, тарифи та борги](#) [Myths about power outages: schedules, exports, tariffs and debts]," *Ukraina Kriminalna*, 1 July 2024; "[«Укренерго» обіцяє встановити справедливі графіки відключення світла в усіх областях](#) [Ukrainian promises to establish fair power outage schedules in all regions]," *Radio Svoboda*, 12 December 2024.

In early February 2025, 81% of Ukrainians rated energy supply as stable, with some regional differences in the eastern (65%), southern (71%), and western (88%) parts of Ukraine. 62% said that the energy situation was better than they had expected, while 32% said that it met their expectations. Some 69% of Ukrainians said the situation in the energy sector had improved as a result of the authorities' actions, including restoring destroyed energy facilities, strengthening protection of other energy facilities, raising funds and energy equipment from international partners, increasing electricity imports, and developing distributed generation.⁹⁸

The Ukrainian public demonstrated a significant level of trust in the government's efforts

Notwithstanding the pressing challenges confronting the nation, the Ukrainian public demonstrated a significant level of trust in the government's efforts to ensure the security of its energy infrastructure. This confidence is particularly noteworthy considering the ongoing Russian aggression. As the interviewed experts noted, the swift and effective response to the attacks, resulting in the rapid restoration of power, is widely regarded as a hallmark of competence. This, in turn, has helped sustain public confidence in Ukraine's political and corporate leadership.

3.2. COMBATING DISINFORMATION

Over the past three years, the issue of energy has become important to many Ukrainians because of power outages, and it has also attracted widespread attention and discussion in the online media, where 37% of energy-related publications were found to have a balanced and neutral tone, 30% had negative

⁹⁸ Sociological Group Rating, "[Енергетична ситуація в Україні: очікування, виклики та перспективи](#) [Energy situation in Ukraine: expectations, challenges and prospects], February 2025.

sentiments, and 33% had more positive and constructive content.⁹⁹

Given how sensitive and vital the energy supply is, the power disruptions have given rise to a plethora of conspiracy theories among the Ukrainian population concerning an irreversible energy crisis. The principal false narratives include the following: the suspicion

The power disruptions have given rise to a plethora of conspiracy theories

that Ukrainian oligarchs are exporting electricity for self-enrichment; the suspicion that authorities are storing and concealing electricity for themselves; the suspicion that someone is deliberately withholding electricity to further increase social tensions in the context of mobilisation; the suspicion that funds for protection and reparation have been stolen; and the suspicion that missile attacks were successful because of such theft and embezzlement.¹⁰⁰

Even though 58% of surveyed Ukrainians indicated in September 2024 that the primary cause of the blackouts was damage to Ukraine's energy infrastructure resulting from Russian attacks, 39% still believed in manipulative versions or conspiracy theories, including that substantial amounts of electricity had been exported in pursuit of profit (15%), shortages had been created to raise energy prices (19%), or they were deliberate actions by the state to remind people of the ongoing war (5%). It was imperative for the Ukrainian government to recognise the significance of affordable energy prices as a primary concern within the energy sector. In order to circumvent potential speculation and manipulation of information within the energy sector, it remains crucial for the government to strike a balance in power market regulation

⁹⁹ Dmytro Bakrar, "Тиск на психіку та битва за здоровий глузд: що медіа України пишуть про відключення електрики [Pressure on the psyche and the battle for common sense: what the Ukrainian media write about power outages]," *Institute of Mass Information*, 19 July 2024.

¹⁰⁰ Volodymyr Omelchenko, "Що відбувається в енергетиці!? Факти і конспірологія [What's going on in the energy sector? Facts and conspiracy theories]," *Razumkov Centre*, 10 June 2024.

mechanisms and their communication between greater transparency in damage reporting to explain the need for changes in pricing on the one hand, and the security imperative to limit intelligence about such damage that becomes available to the enemy on the other.¹⁰¹

Given the tendency of Russian disinformation to exploit internal disagreements, societal problems, and misbeliefs, it is unsurprising that energy-related topics have emerged as a prominent vehicle for disseminating anti-Ukrainian narratives. A recurring tactic in the disinformation campaign is the exaggeration or fabrication of narratives surrounding critical energy shortages. Pro-Russian social media channels have been known to disseminate false reports of widespread blackouts and claims that the Ukrainian government was unable to restore power in a timely manner.

A recurring tactic in the disinformation campaign is the exaggeration or fabrication of narratives surrounding critical energy shortages

These claims were frequently accompanied by images or videos of purportedly damaged energy infrastructure that did not always accurately reflect the actual situation.¹⁰²

A further facet of Russia's disinformation campaign involves the portrayal of the Ukrainian government as inept in its management of

These messages are designed to provoke panic and division and to subvert Ukraine's international support

the energy infrastructure, particularly during power outages caused by Russian missile attacks. By portraying the Ukrainian

¹⁰¹ Dixi Group, "Європейське майбутнє України: довкілля, енергетика та повоєнна відбудова очима громадян [Ukraine's European future: environment, energy and post-war reconstruction through the eyes of citizens]," Analytical note, December 2024.

¹⁰² Centre for Countering Disinformation, "Навіщо ru-пропаганда поширює маніпуляції навколо відключень електроенергії [Why is ru-propaganda spreading manipulations around power outages?]," 10 June 2024.

government as ineffective in protecting its citizens from such disruptions, Russian disinformation aims to erode the population's confidence in state institutions. Furthermore, the dissemination of disinformation is intended to engender feelings of fear and anxiety in Ukrainian society. Propagandists have utilised social media platforms and online forums to disseminate messages suggesting the collapse of the electricity grid or a deliberate deprivation of power in specific regions. These messages are designed to provoke panic and division, thereby hindering the government's ability to effectively manage the energy crisis.¹⁰³

Russia's actions also indicate an intent to subvert Ukraine's international support, particularly from the European nations. Disinformation efforts frequently portray Ukraine as ungrateful for foreign aid or imply that energy supply issues can be attributed to reliance on external assistance. These efforts are designed to erode Ukraine's relationships with its international allies, particularly in the context of energy cooperation and the integration of Ukraine's energy grid with the CESA.¹⁰⁴

Over the course of a decade, Ukrainian society has been counteracting Russia's disinformation campaigns, developing a range of countermeasures to mitigate the risks, effects, and consequences of malign narratives, including regarding the energy sector. In an effort to provide the population with a comprehensive understanding of the situation, the Ukrainian authorities have outlined Russia's strategic objectives in the destruction of the energy infrastructure.¹⁰⁵

A fundamental strategy employed by Ukraine is to ensure transparency and provide timely, regular updates to the public about the general status and current situation of the energy sector. The Ministry of Energy, in conjunction with Ukrenergo, has been providing a consistent and transparent account of the real-time status of the grid, the ongoing repair efforts, and the anticipated disruptions resulting from Russian missile attacks.¹⁰⁶ This communication is disseminated through official government channels, including social media platforms, websites, and public announcements. Furthermore, private media outlets and numerous news groups on social media (predominantly Facebook and Telegram) have been producing and distributing easy-to-understand infographics and other relevant text and visual materials – forms that have been adopted because they make for better understanding and more rapid sharing.¹⁰⁷

Authorities have adopted a policy of transparent and honest communication with citizens

According to the experts interviewed, Ukrainian authorities have managed to establish a centralised communication coordination framework with the objective of aligning the messaging of various stakeholders involved in the energy sector. The function of this framework is to ensure that there is no overlap or contradiction in the information being communicated to the public. By centralising the coordination process, the government has fostered a unified approach among the TSO, DSOs, and electricity producers, thereby increasing trust and credibility. Considering some of the lessons learned from missteps in 2022, the authorities have adopted a policy of transparent and honest communication with citizens, addressing the challenges faced in the energy sector and other critical domains.¹⁰⁸

¹⁰³ Dixi Group, "[Війна рф проти України: енергетичний вимір](#) [The war of the Russian Federation against Ukraine: the energy dimension]," Weekly overview, 12 August 12, 2024; Centre for Countering Disinformation, "[Фейк про планові відключення світла в листопаді](#) [Fake about planned power outages in November]," 1 November 2023.

¹⁰⁴ Sergiy Barbu, "[Поки пів країни у темряві: чи продає уряд світло за кордон](#) [While half the country is in the dark: is the government selling electricity abroad?]," *LB.ua*, 13 June 2024.

¹⁰⁵ Centre for Countering Disinformation, "[Навіщо росія обстрілює об'єкти енергетики України](#) [Why is Russia shelling Ukrainian energy facilities?]," 22 March 2024.

¹⁰⁶ Olena Bogdaniok, "[Який зараз стан енергосистеми — дані Укренерго](#) [What is the current state of the power system — data from Ukrenergo]," *Suspilne*, 19 December 2024.

¹⁰⁷ "[Скільки електроенергії імпортує та експортує Україна під час великої війни](#) [How much electricity did Ukraine import and export during the big war?]," *Slovo i Dilo*, 2 October 2024.

¹⁰⁸ Mykola Tesla, "[Блекаут. Владі потрібні план та чесна розмова з громадянами](#) [Blackout. The authorities need a plan and an honest conversation with citizens]," *Dzerkalo Tizhnia*, 17 November 2024.

In Ukraine, information campaigns are also focused on debunking and pre-bunking false claims. In instances where disinformation

By offering concrete data, Ukrainian government agencies aim to counter false narratives and build public confidence

regarding widespread blackouts or the inability to restore power in certain regions is disseminated, the government provides factual, up-to-date information that includes specific timelines for repairs and the status of critical infrastructure. By offering concrete data, such as the number of substations repaired or the kilowatts of energy supply being restored, Ukrainian government agencies aim to counter false narratives and build public confidence in the country's resilience.¹⁰⁹ Furthermore, independent fact-checking organisations and other civil society actors contribute to the efforts to combat Russia's disinformation.¹¹⁰

Another critical element of Ukraine's strategy to counter disinformation is non-formal public education endorsed by the government, supported by international donors, and conducted by civil society organisations through various campaigns aimed at educating the public about the importance of energy conservation and the technicalities of power grid operations. These educational initiatives often focus on the realities of energy infrastructure and provide clear, accessible information about the repair and restoration processes following missile strikes. The government of Ukraine seeks to impart a more profound comprehension of the electricity sector to the general public, with a view to immunising it against the dissemination of false information – a goal that also highlights the media community's responsibility to communicate about the functioning of the energy sector to diverse social groups within Ukraine, including those residing in rural areas and those particularly vulnerable to the effects

¹⁰⁹ Centre for Countering Disinformation, "[Що очікує енергосистему України взимку?](#)" [What awaits Ukraine's energy system in winter?], 4 September 2024.

¹¹⁰ Centre for Countering Disinformation, "[Чим загрожують Україні нові атаки на енергосистему](#)" [What new attacks on the energy system threaten Ukraine with?], 28 March 2024.

of disinformation.¹¹¹ Ukrainian Energy, a website operated by DiXi Group, and until recently supported by the US Agency for International Development (USAID), is a good example of a competent web resource dedicated to energy issues, providing in-depth material on various topics in various formats (news articles, interviews, analytics, investigations, reports, announcements, energy maps, dashboards, etc.).¹¹²

3.3. CONSUMER BEHAVIOUR AND COOPERATION

In light of the government of Ukraine's declaration of energy shortages, particularly during the summer and winter months, there has been an imperative for the public to adapt their behaviours to these new circumstances.¹¹³ Citizens were encouraged to conserve energy through government campaigns promoting energy-saving measures, such as reducing heating or cooling, and limiting electricity consumption during peak hours.¹¹⁴ These measures were met with a largely positive response, as many citizens recognised their importance in maintaining the functionality of the national energy system during challenging periods.

Notwithstanding the challenges posed by power shortages, the Ukrainian government

¹¹¹ Valeryia Buniak, "[Як журналістам розповідати про енергетику простими словами](#)" [How to tell journalists about energy in simple words], *Detector Media*, 27 December 2022; "[Як пережити блекаут: корисні поради та рішення](#)" [How to survive a blackout: useful tips and solutions], *ТТТ*, 20 August 2024; Commission on Journalistic Ethics, "[Про енергетичну журналістику простими словами: поради Комісії з журналістської етики](#)" [About energy journalism in simple words: advice from the Commission on Journalistic Ethics], 28 December 2022; Olena Bogdaniok, "[Чи готові мобільні оператори до блекаутів та як це вплине на зв'язок та ціни](#)" [Are mobile operators ready for blackouts and how will this affect connectivity and prices?], *Suspilne*, 15 December 2024.

¹¹² *UA Energy* (accessed December 16, 2024).

¹¹³ Inna Yeshchenko, "[Економно — не значить погано. Нові рішення для нових реалій, або як заощаджувати електроенергію з комфортом для себе](#)" [Economical does not mean bad. New solutions for new realities, or how to save electricity with comfort for yourself], *Rubryka*, 17 February 2023.

¹¹⁴ "[Основні правила економного використання електроенергії](#)" [Basic rules for economical use of electricity], State Inspectorate for Energy Supervision of Ukraine, last accessed 12 April 2025.

maintained consistent public support, largely due to its transparent communication and concerted efforts to mitigate the impact

A significant factor contributing to this support was the perception of fairness in government policies

of energy disruptions. As highlighted by the interviewed experts, a significant factor contributing to this support was the perception of fairness in government policies. For instance, the Ukrainian authorities demonstrated a commitment to power restoration in areas with hospitals, schools, communication companies, and emergency services, fostering a sense of equity and solidarity within communities.¹¹⁵ Moreover, the alignment of energy security policies with Ukraine's European integration was viewed positively, with many citizens perceiving it as a step toward achieving greater energy independence from Russia.

In circumstances where there is a significant disruption to the energy supply, the issuing of emergency alerts is initiated through a variety of channels, including mobile phone notifications, TV and radio broadcasts, and social media. These alerts provide guidance on energy conservation, safety during blackouts, and the expected time of power restoration.

Representatives of Ukraine's government, in conjunction with energy sector executives, frequently convene to deliver press briefings and provide updates on the energy situation. These events are of crucial importance in ensuring transparency and in the process of building public confidence. They serve as a conduit through which government and energy sector representatives articulate complex technical issues in lay terms, thereby

¹¹⁵National Security and Defence Council of Ukraine, [Рішення від 26 листопада 2022 року введено в дію Указом Президента України № 802/2022 про забезпечення електронними комунікаційними послугами в умовах воєнного стану](#) [The decision of 26 November 2022 put into effect by Decree of the President of Ukraine No. 802/2022 on providing electronic communication services under martial law] (Kyiv: Verkhovna Rada, 2022); Ministry of Health of Ukraine, ["План на випадок блекаутів: як українські лікарні можуть працювати в умовах відключень світла?"](#) [Blackout plan: how can Ukrainian hospitals operate during power outages?], 30 January 2024.

ensuring the public is informed about the challenges being faced and the actions being taken to restore power.¹¹⁶

TSOs such as Ukrenergo and DSOs are integral partners in the communication process, providing vital updates on the technical status of the power grid.¹¹⁷ These organisations often communicate directly with the public through their own websites or social media accounts, and via local media. They deliver updates on specific regions, informing residents about localised outages, expected restoration times, and emergency energy-saving measures.¹¹⁸ Moreover, local communities are involved in implementing energy security solutions.¹¹⁹

Ukraine's energy sector has also engaged in cross-sector collaboration with cybersecurity experts, media organisations, and civil society groups.¹²⁰ In particular, the cyber

Ukraine's energy sector has also engaged in cross-sector collaboration with cybersecurity experts, media organisations, and civil society groups

community and media outlets have been identified as playing a key role in amplifying government messaging and fact-checking any disinformation that may arise in the wake of

¹¹⁶Ukrainian Institute for the Future, ["Дебати про майбутнє: Енергетика майбутнього](#) [Debate about the future: Energy of the future], 22 November 2024; Oksana Bedratenko, ["Не все так погано". Експерти міркують, чи готова Україна до опалювального сезону](#) ["It's not all that bad." Experts wonder if Ukraine is ready for the heating season], *Voice of America*, 21 October 2024.

¹¹⁷Ukrenergo, ["Стан енергосистеми України](#) [State of the energy system of Ukraine], Telegram, 14 April 2025.

¹¹⁸"[В «Укренерго» розповіли, за яких умов зима зможе пройти без відключень світла](#) [Ukrenergo explained under what conditions winter might pass without power outages], *Slovo i Dilo*, 30 September 2024.

¹¹⁹Oksana Stelmakh, ["Розпочато цикл навчально-консультативних заходів з енергетичної безпеки у громадах](#) [A cycle of educational and advisory activities on energy security in communities has begun], *U-LEAD*, 28 February 2023.

¹²⁰Olga Chayka, ["Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему](#) [Russian hackers coordinate with the military and intensify attacks ahead of winter. How Ukraine is countering cyberattacks on the energy system], *Forbes*, 15 November 2023.

energy disruptions.¹²¹ By collaborating with media and civil society, Ukraine is able to ensure that critical information reaches the widest possible audience. Effective cooperation and aligned crisis communication between the Ukrainian government (mainly the Ministry of Energy and State Emergency Service), electricity producers, and grid managers help to manage the public's expectations, guide behaviour during energy disruptions, and ensure transparent information flows regarding the status of energy restoration efforts.¹²² Moreover, journalists and newsrooms can also showcase best practices in coping with power outages and preparing for winter to ensure uninterrupted operations without central power supplies.¹²³

In addition, cooperation with industry associations and consumers' unions is a key element in the strategy to ensure that the public understands the role of alternative and renewable energy sources in maintaining power supply during crises. Public communication campaigns often highlight Ukraine's efforts to diversify its energy sources, including by increasing the share of solar and wind energy in the grid.¹²⁴ By highlighting cooperation with the EU on energy matters, particularly Ukraine's integration into the European power grid, the government not only ensures

a reliable power supply but also strengthens public confidence in the country's energy future.¹²⁵

As the results of the recent survey of Ukrainian companies in the energy sector show, the need to develop generation capacity in Ukraine, including nuclear power and the transition to environmentally friendly energy sources, is strongly supported in the business community. However, there are some doubts about its economic feasibility and efficiency in wartime, as the main concerns of Ukrainian energy companies are corruption, bureaucratic red tape, and the lack of adequate protection against missile attacks.¹²⁶

Despite efforts to maintain coordination and cooperation in the face of Russian attacks, several political issues undermine the effectiveness of unified communication in Ukraine's electricity sector. These challenges include the politicisation of energy issues and limitations in energy infrastructure. For example, opposition parties have accused the government of mismanaging the energy crisis or failing to protect the population from Russian attacks, using power outages as a tool for political gain. In some cases,

The challenges include the politicisation of energy issues and limitations in energy infrastructure

local authorities may exaggerate restoration efforts or present a more optimistic timeline than national grid operators, which can lead to disillusionment when expectations are not met. Conversely, some local leaders may understate the severity of the situation to

¹²¹“[Проти енергетичних компаній України готується нова кібератака – експерти](#) [A new cyberattack is being prepared against Ukrainian energy companies – experts],” *UNIАН*, 14 December 2017.

¹²²“[Оперативно про ситуацію в енергетиці](#) [Operational situation in the energy sector],” Ministry of Energy of Ukraine, last accessed 12 April 2025; State Emergency Service of Ukraine, “[Відключення електроенергії: убезпечте себе, близьких і житло від пожежі](#) [Power outage: protect yourself, your loved ones and your home from fire],” 26 November 2022; Olga Katsan, “[Російські удари руйнують українську енергетику. Який масштаб втрат і що робити?](#) [Russian strikes are destroying Ukraine's energy sector. What is the scale of the losses and what should be done?],” *Radio Svoboda*, 12 December 2024.

¹²³Olga Chorna, “[Як українські журналісти долають відімкнення електрики та готуються до зими](#) [How Ukrainian journalists are coping with power outages and preparing for winter],” *Detector Media*, 4 July 2024.

¹²⁴Dixi Group, [Енергетична дипломатія України: аналіз статус-кво та практичні рекомендації](#) [Energy diplomacy of Ukraine: status-quo analysis and practical recommendations] (Kyiv: Dixi Group, 2021).

¹²⁵“[Україна домовилася з ЄС щодо збільшення імпорту електроенергії взимку](#) [Ukraine has agreed with the EU to increase electricity imports in winter],” *Slovo i Dilo*, 29 October 2024; “[Шлях до Європи: як українська енергосистема інтегрувалася до європейської енергомережі ENTSO-E](#) [The path to Europe: how the Ukrainian power system integrated into the European power grid ENTSO-E],” *Ukrenergo*, last accessed 12 April 2025.

¹²⁶Energy Club, “[Аналіз результатів опитування: Майбутнє української енергетики – думка бізнесу](#) [Analysis of survey results: The future of Ukrainian energy – business opinion],” 16 January 2025.

avoid public criticism, further complicating the government's overall messaging strategy.¹²⁷ Also, due to various technical limitations, energy operators are sometimes unable to provide accurate or realistic timelines for power supply restoration, which may breed frustration and misperception among the affected customers.

3.4. CHAPTER CONCLUSION

The ongoing war of aggression by Russia has had a significant impact on Ukraine's energy sector, particularly in the context of sustained aerial attacks on critical infrastructure, including power plants, substations, and transmission lines, but also on the morale and psychological state of the Ukrainian people. In response to these attacks, the Ukrainian government, electricity producers, and grid operators have implemented a multifaceted strategic communication approach to ensure the public is informed, resilient, and able to adapt. Providing real-time updates, leveraging social media, coordinating messages across sectors, and embracing new digital tools, these stakeholders have collaborated to mitigate the impact of disinformation, guide public behaviour, and maintain confidence in the energy system. The coordination of these communication efforts is critical for maintaining energy security and resilience,

The Ukrainian government, electricity producers, and grid operators have implemented a multifaceted strategic communication approach to ensure the public is informed, resilient, and adaptable

ensuring that the Ukrainian population can withstand and adapt to the challenges posed by external aggression.

The Ukrainian government, energy producers, and grid operators collaborate to provide

real-time, transparent information via digital platforms (including the state app Diia), traditional media, and localised messaging through groups on Facebook and Telegram. Nevertheless, significant challenges are presented by the existence of political tensions, the politicisation of energy issues, disinformation campaigns, and infrastructure limitations, which impede the coordination and consistency of messaging. Addressing these political and operational challenges is essential for maintaining the integrity of Ukraine's energy communication efforts and ensuring continued public resilience during the crisis.

The whole-of-society adoption of energy-saving measures and active participation in voluntary repair and mutual support initiatives underscore the efficacy of broad-based strategic communication

The decisions regarding energy security and the power system's resilience also contributed to the consolidation of national unity. The attacks against Ukraine's power grid were perceived by Russia not only as a military stratagem but also as an assault on the Ukrainian people's modus vivendi. In response, there was a significant rise in the sentiment of shared responsibility and the need for collective effort to overcome the ensuing challenges. The whole-of-society adoption of energy-saving measures and active participation in voluntary repair and mutual support initiatives by the public served to underscore the efficacy of broad-based strategic communication in managing the cognitive effects of the Russian aggression.

¹²⁷“[NYT: Політичні чвари в Україні ускладнюють зусилля відвернути енергетичну кризу цієї зими](#) [NYT: Political strife in Ukraine complicates efforts to avert energy crisis this winter],” *Voice of America*, 15 October 2024.

REPORT CONCLUSIONS AND RECOMMENDATIONS

Tomas Jermalavičius

*with contributions by Oleksandr Sukhodolia,
Henry Rõigas, and Dmitri Teperik*

Ukraine's power system continues its struggle to maintain the supply of electricity to customers across the country, as Russia has ramped up its aerial campaign against it and shifted its focus towards the destruction of power generation facilities. The remarkable resilience of the system is due to multiple factors: ample redundancies in the power system beforehand, pre-invasion preparedness measures; adaptiveness of the system to the nature of the threat; effective provision of foreign aid; connectivity with the European grids; and significantly higher capacity to restore damaged or destroyed facilities. Just as important was the high priority given by Ukrainian political authorities to protecting the system and to reconstruction needs by setting and reviewing the required protection standards, allocating necessary military and civilian resources, and providing a framework for coordination and cooperation between stakeholders.

On the other hand, insights harnessed in the process of researching for this report suggest that, while the system described above and governance properties can go a long way in ensuring the resilience of power supply, there have been some sharp dilemmas and difficult choices that have to be made in the face of the Russian aggression. Chief among them, of course, is the allocation of air defence resources. As no country can afford multilayered coverage of its entire territory – and even less so the largest country in Europe, while being engaged in a massive war against an even larger opponent – it cannot ensure that it will be able to provide comprehensive coverage of all energy facilities at all times.

Despite successfully multiplying the number of well-equipped, mobile counter-drone teams, Ukraine's air defences are less effective in dealing with ballistic and cruise missile threats – especially as Russia has been adapting its tactics and finding ways to get

through to power generation facilities while also increasing pressure on the frontlines. Thus, dependence on large and economically efficient but highly exposed power generation facilities, including NPPs, becomes a key vulnerability of the system. These facilities can be protected with additional measures only to a limited extent and by shifting the onus of resilience to connectivity with the foreign suppliers (and their solidarity in emergencies) and to the availability of repair teams,

Dependence on large and economically efficient but highly exposed power generation facilities becomes a key vulnerability

construction equipment, and stocks of spare parts, adequate levels of which are determined by the scale and pace of destruction and, therefore, difficult to anticipate in advance.

Other frontline states such as Estonia and NATO planners will also face such dilemmas should a war break out in the Baltic region, which means military planning and energy planning should become closely interlinked. The military must have clarity about which

Military planning and energy planning should become closely interlinked

priority facilities must be comprehensively defended and which ones are dispensable from the perspective of power system management. Conversely, energy planners must understand military limitations and plan wartime preparedness accordingly, including reserve rapid repair and reconstruction capabilities. Intelligence assessments must be shared by the military authorities about Russian capabilities, concepts, and practices to anticipate, at least to some extent, the scale and rate of attrition that would be inflicted on the energy system and develop adequate stockpiles of critical equipment, such as transformers and spare parts.

Ukraine's experience also demonstrates how war becomes a major driver in many strategic decisions, such as electricity market design and integration with foreign markets, the desired system architecture, and the evolution of a regulatory framework. This

entails that energy policymakers today must make strategic long-term decisions about such aspects with the possibility of a major war in mind if they wish to minimise risks and mitigate the impact of military action against the power system. Legislation and regulations – from those governing electricity markets to those regulating connection of new sources to the grid and establishing physical protection requirements for various facilities – must be reviewed through the wartime lens, to ensure that the entire legal framework remains fit for purpose under the pressures of war that manifested themselves in Ukraine and have been discussed in this report.

Energy policymakers today must make strategic long-term decisions with the possibility of a major war in mind

Ukraine's lessons indicate that a shift towards a more decentralised and distributed system might reduce nationwide vulnerability and might better protect the society and government against attempts to coerce them into surrender through the destruction of power supply systems. This is not to conclude that such a shift would be free from various challenges and risks. For example, a military mobilisation system that exempts only critical personnel of the TSO/DSOs, including repair crews, would have to consider excluding from mobilisation requirement a larger and more diverse pool of technical personnel distributed among a larger number of entities providing critical management and repair services to micro-grids and nano-grids, small producers, and prosumers.

At the same time, national policy should not lose sight of long-term challenges beyond the ongoing war. The development of decentralised grids and the transition to renewable sources currently relies heavily on hardware and software supplied by China, which currently not only supports Russia's war against Ukraine but has also emerged as a major strategic adversary to the west. The head of the Estonian Foreign Intelligence Service has recently warned that some parts of the China-linked supply chain – for instance, the inverters connecting PV panels to the grid that can be switched off remotely – will pose security risks in the future, should Beijing step up its efforts

to assist Russia or enter a period of more severe confrontation with the west.¹²⁸ Today's solutions can easily become tomorrow's problems if such risks are not anticipated and managed – including in the cyber domain.

Cyber resilience would remain a major consideration but might be more challenging to manage than in the centralised system, as the attack surface would increase manifold, and the number of entities involved in providing cybersecurity to a multitude of customers would grow significantly. This would make coordination and cooperation in defending the cyber domain more challenging, even without taking into account the various cyber vulnerabilities associated with China-made equipment currently dominating the market for renewable energy equipment. Ukraine's success in mounting a cyber defence of its power system has many ingredients, but it is all too easy to become overly focused on the kinetic impact and neglect the cyber domain and its extensive use by Russia to collect intelligence, impair coordination of the defenders, or amplify the psychological effects of its aggression.

The management of the psychological effects is partially undertaken through strategic communication – an area that has received less attention in researching lessons from the war than kinetic or cyberattacks themselves. As this report shows, in shaping the behaviour of consumers – individuals, households, businesses, and public sector entities – the Ukrainian authorities faced a two-fold challenge: maintaining the stability of the power system under Russian attacks while also preventing or limiting the corroding impact of the enemy's malignant information operations that exploit the real and purported effects of the kinetic attacks on the energy sector.

Ukraine adopted a broad-based but centrally coordinated approach to informing and educating society, countering false narratives, and sustaining resilience in the face of Russia's persistent attacks against its power system. It is designed not only to respond to real-time

¹²⁸ ["Eesti luurejuht: NATO-l tuleb Venemaad ohjeldada järgmised 20 aastat](#) [Estonian intelligence chief: NATO must contain Russia for the next 20 years], *ERR*, 20 December 2024.

issues but also to maintain trust and enhance the capacity of society to manage future energy supply challenges. It involves not only governmental authorities at various levels but also the public and corporate sectors, as well as civil society organisations and social media influencers, harnessing the technological tools that are widely used in a rapidly digitalising nation. They do face some headwinds chiefly related to the properties and dynamics of relations between the state, society, and businesses that pre-date the full-scale war, but the unifying impact of the external aggression and effective frameworks and mechanisms of vertical and horizontal cooperation more than compensate for those negative aspects, as public opinion polls and surveys of the Ukrainian businesses amply demonstrate.

It is obvious that Russia's hybrid campaign of strategic coercion against the targeted society and its governance does not stop once high-intensity warfighting begins. It only seeks to build upon and amplify the effects caused by kinetic and cyber operations, including against the fundamental infrastructure such as the power system. The enemy's expectation is that this will translate into physical and psychological exhaustion that will put pressure on the decision-makers to capitulate. As the report shows, however, such expectations are dashed when facing a society and organisations as adaptive and resilient as Ukraine's, where a variety of stakeholders act in unison, embracing energy resilience as a shared responsibility, and with steady support from foreign partners.

As Richard Pape pointed out, "dozens of conflicts over the past century have demonstrated, using airpower against civilian targets is almost always doomed to failure."¹²⁹ This is not, however, a predetermined outcome and, based on Ukraine's experience, there are a host of measures to be enacted prior to and during a full-scale high-intensity war to ensure such a failure by an enemy. To the stakeholders who are responsible for national security and defence, for the maintenance of the vital functions of society, and for the protection of its critical infrastructure – including its power

system – in wartime, the following recommendations should apply:

Critical infrastructure protection and energy policy:

- **The security of critical energy infrastructure in wartime must become an important element of peacetime inter-agency and multi-stakeholder planning and coordination.** Physical protection of energy facilities from a range of threats through multiple domains is a complex task that requires close cooperation between the energy companies, governmental authorities (at the national and local levels), and security and defence agencies. The necessary protective measures must be developed jointly by all these actors because this task requires multidimensional risk assessments and adequate identification of threats (including evolving dynamic wartime threats). This also calls for some strategic political decisions by the governments to establish principles for distributing available military resources – especially air and missile defence assets – between the protection of civil infrastructure and defence needs, identifying the most important requirements to protect critical infrastructure from physical damage, and outlining key elements of deterrence strategy (e.g., retaliation strikes).
- **A regional system of mutual assistance to protect and restore critical energy infrastructure should be created, ensuring the supply of equipment and materials necessary for restoration.** The scale of destruction will inevitably exceed the capacity of peacetime preparedness measures, but market players are not ready to promptly respond to the surge in requests for spare parts and new equipment. There is a need for some tools of coordination between partner countries. As a first step, partner countries could institutionalise joint working groups on risk analysis and the development of response scenarios. It will help to anticipate future needs and prepare response plans. The next steps could include the development of instruments for the inventorisation of available resources in partner countries, the procedure for information exchange and delivery of the

¹²⁹ Robert A. Pape, "[Bombing to Lose: Why Airpower Cannot Salvage Russia's Doomed War in Ukraine](#)," *Foreign Affairs*, 20 October 2022.

needed resources and equipment, the customs clearance and taxation legislation, and so on. The establishment of a joint reserve of equipment and materials will not only speed up the recovery of energy infrastructure in a particular country in a crisis but will also reduce the economic burden on all to maintain such reserves.

- **Adequate levels of in-house technical expertise and workforce of energy companies, such as grid operators and power producers, must be preserved.** The resilience of the energy system depends heavily on the work of the technical personnel of energy companies. In fact, power system engineering could be treated as a critical aspect of modern warfare – the side that has superiority in it is more likely to prevail in prolonged, large-scale attrition campaigns. This resource cannot be built, sustained, and surged based on the widespread peacetime practice of outsourcing maintenance and repair works to third parties. Decisions to keep technical and engineering personnel required for such work in-house might not appear cost-efficient in peacetime, but they can make all the difference in wartime, when speedy repair of damaged infrastructure and restoration electricity supply is essential.
- **A clear and effective wartime regulatory framework for electricity trading should be established in advance.** The Ukrainian experience demonstrates the flaws of market tools in wartime. The usual peacetime logic of market regulation could be insufficient to provide reliable incentives for market actors. The behaviour of these actors typically demonstrates the preference for short-term earnings (or minimisation of current financial losses) over long-term benefits, which, in wartime, may be ensured only by special regulation, through specially designated market instruments or tools introduced by the state that are understandable and transparent on how deviations from the peacetime market framework will occur. This should include the regulation of both the internal market and cross-border trading to guarantee the supply of the necessary volumes at agreed prices and should establish principles of

compensation of losses if the price of imports exceeds the prices fixed in contracts with the consumers. These tools cannot be replaced by civil emergency cooperation mechanisms or tools of emergency support within the existing framework of cross-border cooperation of TSOs, as the scale of damage and duration of negative impact are much higher in wartime.

- **The capacity of market players to build and operate decentralised energy generation and distribution systems should be built up.** The success of the decentralisation of the energy system depends on the readiness of consumers, especially small and medium-sized companies and communities, to participate in this process. Forming a sufficient level of technical and economic expertise among them is an important task in the process of energy system transformation. There is a need to increase technical education programmes and training courses to successfully support the strategy of transition to a decentralised power system architecture and to increase the awareness of potential operators of distributed generation facilities and local smart grids of electricity market procedures and regulations, as well as the wartime dynamics and long-term risks related to the supply chain (e.g., cybersecurity). At the same time, a framework for developing such projects in wartime is needed in order to be able to respond to damage to energy infrastructure expeditiously, under time pressure and amid shortages of qualified personnel.

Cybersecurity:

- **Defensive strategies must begin with a clear understanding of the adversary's capabilities, intent, and methods.** In Ukraine, Russia and its state and non-state allies have persistently targeted energy infrastructure using both kinetic and cyber operations. While missile strikes, drone attacks, and sabotage remain the primary instruments of physical destruction, cyber operations – supporting espionage, causing disruption, or enabling influence or propaganda campaigns – are actively carried out to support Russia's broader strategy of information warfare. The cyber operations

witnessed during the war demonstrate that the energy sector is targeted by a diverse, adaptive, opportunistic, and well-resourced group of capable threat actors.

- **Organisations in the energy sector must invest consistently in both proactive and reactive cybersecurity measures.** Resilience – not just prevention – should guide capability development, as adversaries will inevitably find weaknesses to exploit through constantly evolving TTPs. Ukraine’s experience demonstrates that effective cyber resilience hinges on shared responsibility. This includes mapping cross-sector interdependencies, maintaining continuous cyber awareness efforts, and investing in both technical upgrades and organisational capability development. While public institutions play a key role, lasting security ultimately depends on leadership and sustained commitment from the energy companies themselves.
- **Cybersecurity strategies should not be developed in isolation, as offensive cyber operations are embedded within wider efforts by the adversary.** Resilience, therefore, depends on interdisciplinary collaboration within and between energy organisations, government agencies, and other critical infrastructure sectors – through, for example, joint crisis simulations, comprehensive incident response planning, and civil-military coordination.

Strategic communication:

- **A centralised communication hub responsible for synchronising, coordinating, and disseminating information related to energy disruptions, restoration efforts, and energy-saving measures should be established** by the national government, in collaboration with rescue services, grid operators, and electricity producers. This approach ensures that the public receives consistent, accurate, and real-time updates, avoiding confusion and misinformation. The establishment of such a hub should be accompanied by the implementation of a multifaceted communication strategy, encompassing dedicated social media channels, regular press briefings by experts, officials and opinion leaders, and updates
- via government websites and mobile applications. Furthermore, the strategy should ensure the integration of classical communication channels, thereby reaching all socio-demographic groups, including minorities, remote communities, and those with limited internet access. The effectiveness of this unified messaging is of paramount importance in maintaining public trust, managing expectations, and ensuring the seamless recovery of energy services during crises.
- **Transparent and proactive public engagement should be a high priority.** In order to manage public expectations and minimise panic, it is essential to communicate public safety information regarding the status of energy supply disruptions and expected recovery times, in addition to energy conservation and emergency measures. Such information should be communicated proactively, in cooperation with recognised subject-matter experts, local municipalities, the media, and civil society organisations. A comprehensive public engagement strategy has been shown to foster trust and cooperation among non-government organisations, voluntary associations, and citizens, thereby minimising confusion, mitigating disruptions to daily life, and preventing the erosion of support for government actions.
 - To mitigate the risks associated with cyberattacks and ensuing disinformation, it is essential to **establish robust collaborative relationships with cybersecurity experts, independent media outlets, and fact-checking organisations.** This approach enables the identification of cyber threats and refutation of false narratives that are likely to erode public confidence and engender mistrust in government responses. The establishment of a specialised task force, comprising individuals with in-depth knowledge of energy-related subjects, could be a valuable approach. This task force would be responsible for the monitoring and countering of disinformation related to the energy sector, thereby ensuring the accuracy of information disseminated during crises. The use of verified information and the initiation of pre-bunking initiatives have been identified as effective

measures in fostering a collective sense of responsibility among members of the public who are accustomed to clear and easily comprehensible guidelines. Furthermore, regional cooperation with neighbouring allies (e.g., Finland and Latvia for Estonia)

in conducting strategic communication is recommended, with the aim of facilitating the exchange of information on cyberattacks and related propagation of hostile narratives across the information space.

LIST OF REFERENCES

- “Amid Russian bombing, Ukraine is planning more nuclear reactors.” *The Economist*, 12 December 2024. <https://www.economist.com/europe/2024/12/12/amid-russian-bombing-ukraine-is-planning-more-nuclear-reactors>.
- Antoniuk, Daryna. “Ukraine’s State-Owned Nuclear Power Operator Said Russian Hackers Attacked Website.” *The Record*, 17 August 2022. <https://therecord.media/ukraines-state-owned-nuclear-power-operator-said-russian-hackers-attacked-website>.
- Antoniuk, Daryna. “Ukraine’s Defense Ministry Launches Military CERT to Counter Russian Cyberattacks.” *The Record*, 8 October 2024. <https://therecord.media/ukraine-creates-military-cert>.
- Babenko, Mariya. “Міфи щодо відключень світла: графіки, експорт, тарифи та борги [Myths about power outages: schedules, exports, tariffs and debts].” *Ukraina Kriminalna*, 1 July 2024. <https://cripo.com.ua/likbez/mify-shhodo-vidklyuchen-svitla-grafiky-eksport-taryfy-ta-borgy>.
- Bakrar, Dmytro. “Тиск на психіку та битва за здоровий глузд: що медіа України пишуть про відключення електрики [Pressure on the psyche and the battle for common sense: what the Ukrainian media write about power outages].” *Institute of Mass Information*, 19 July 2024. <https://imi.org.ua/monitorings/tysk-na-psyhiku-ta-bytva-za-zdorovyj-gluzd-shho-media-ukrayiny-pyshut-pro-vidklyuchennya-elektryky-i62566>.
- Barbu, Sergiy. “Поки пів країни у темряві: чи продає уряд світло за кордон [While half the country is in the dark: is the government selling electricity abroad?].” *LB.ua*, 13 June 2024. https://lb.ua/economics/2024/06/13/618454_poki_piv_kraini_temryavi_chi_prodaie.html.
- Barnes, Joe. “How Ukraine is using mobile phones on 6ft poles to stop drones.” *The Telegraph*, 26 March 2024. <https://www.telegraph.co.uk/world-news/2024/03/26/ukraine-mobile-phones-poles-sensors-russian-drones-simple/>.
- Bedratenko, Oksana. “«Не все так погано». Експерти міркують, чи готова Україна до опалювального сезону [“It’s not all that bad.” Experts wonder if Ukraine is ready for the heating season].” *Voice of America*, 21 October 2024. www.holosameryky.com/a/energy-ukraine-winter/7830079.html.
- Beecroft, Nick. “Evaluating the International Support to Ukrainian Cyber Defense.” *Cyber Conflict in the Russia-Ukraine War Series*, *Carnegie Endowment for International Peace*, 3 November 2022. <https://carnegieendowment.org/research/2022/11/evaluating-the-international-support-to-ukrainian-cyber-defense?lang=en>.
- Black, Dan. “Russia’s Cyber Campaign Shifts to Ukraine’s Frontlines.” *RUSI*, 22 July 2024. <https://rusi.org/explore-our-research/publications/commentary/russias-cyber-campaign-shifts-ukraines-frontlines>.
- Bogdaniok, Olena. “Чи готові мобільні оператори до блекаутів та як це вплине на зв’язок та ціни [Are mobile operators ready for blackouts and how will this affect connectivity and prices?].” *Suspilne*, 15 December 2024. <https://suspilne.media/902989-ci-gotovi-mobilni-operatori-do-blekautiv-ta-ak-ce-vpline-na-zvazok-ta-cini-suspilne-videonovini/>.
- . “Який зараз стан енергосистеми — дані Укренерго [What is the current state of the power system — data from Ukrenerg].” *Suspilne*, 19 December 2024. <https://suspilne.media/906123-akij-zaraz-stan-energositemi-dani-ukrenerg>.
- Brekis, Arturs. *Assessment of the Technologies That Could Increase the Use of Distributed Energy Generation, Thereby Reducing the Impact of Military Strikes on Centralized Power Generation Facilities in Ukraine and Enhancing the Security and Resilience of Energy Supply in Ukraine*. Vilnius: NATO Energy Security Centre of Excellence, 2024. https://www.enseccoe.org/wp-content/uploads/2024/09/2024_09_03_Research_Report_Energy_Ukraine.pdf.
- Buniak, Valeryia. “Як журналістам розповідати про енергетику простими словами [How to tell journalists about energy in simple words].” *Detector Media*, 27 December 2022. <https://detector.media/production/article/206388/2022-12-27-yak-zhurnalistam-rozpovidaty-pro-energetyku-prostymy-slovamy>.
- Canadian Centre for Cyber Security. *Cyber Threat Activity Related to the Russian Invasion of Ukraine*. Government of Canada, n.d. <https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf>.
- Centre for Countering Disinformation. “Навіщо ru-пропаганда поширює маніпуляції навколо відключень електроенергії [Why is ru-propaganda spreading manipulations around power outages?].” 10 June 2024. <https://cpd.gov.ua/result/navishho-ru-propaganda-poshyryuye-manipulyacziyi-navkolo-vidklyuchen-elektroenergiji>.
- . “Навіщо росія обстрілює об’єкти енергетики України [Why is Russia shelling Ukrainian energy facilities?].” 22 March 2024. <https://cpd.gov.ua/articles/navishho-rosiya-obstrilyuye-ob%ca%bcyekty-energetyky-ukrayiny>.
- . “Фейк про планові відключення світла в листопаді [Fake about planned power outages in November].” 1 November 2023. <https://cpd.gov.ua/warnin/fejk-pro-planovi-vidklyuchennya-svitla-v-lystopadi>.

- “Чим загрожують Україні нові атаки на енергосистему [What new attacks on the energy system threaten Ukraine with].” 28 March 2024. <https://cpd.gov.ua/articles/chym-zagrozhuyut-ukrayini-novi-ataky-na-energosystemu>.
- “Що очікує енергосистему України взимку? [What awaits Ukraine’s energy system in winter?].” 4 September 2024. <https://cpd.gov.ua/articles/shho-ochikuye-energosystemu-ukrayiny-vzymku>.
- CFC Big Ideas. “Challenges and Reality of the Energy Infrastructure of Ukraine.” 1 March 2023. <https://cfcbigideas.com/challenges-and-reality-of-the-energy-infrastructure-of-ukraine>.
- Chayka, Olga. “Російські хакери координують дії з військовими та посилюють атаки напередодні зими. Як Україна протистоїть кібератакам на енергосистему [Russian hackers coordinate with the military and intensify attacks ahead of winter. How Ukraine is countering cyberattacks on the energy system].” *Forbes*, 15 November 2023. <https://forbes.ua/company/rosiyski-khakeri-koordinuyut-dii-z-viyskovimi-ta-posilyuyut-ataki-naperedodni-zimi-yak-ukraina-protistoit-kiberatakam-na-energosystemu-08112023-17242>.
- Chorna, Olga. “Як українські журналісти долають відімкнення електрики та готуються до зими [How Ukrainian journalists are coping with power outages and preparing for winter].” *Detector Media*, 4 July 2024. <https://detector.media/community/article/229132/2024-07-04-yak-ukrainski-zhurnalisty-dolayut-vidimknennya-elektryky-ta-gotuyutsya-do-zymy>.
- Collins, Gabriel, and Kenneth B. Medlock. “Ukraine Electricity Sector.” Working Paper, *Baker Institute*, August 2024. www.bakerinstitute.org/sites/default/files/2024-08/20240814-Ukraine%20Electricity%20Sector-WP.pdf.
- Commission on Journalistic Ethics. “Про енергетичну журналістику простими словами: поради Комісії з журналістської етики [About energy journalism in simple words: advice from the Commission on Journalistic Ethics].” 28 December 2022. <https://cje.org.ua/news/strong-pro-enerhetychnu-zhurnalistyku-prostymy-slovamy-porady-komisii-z-zhurnalistskoi-etyky-strong>.
- Daletska, Yuliya. “МАГАТЕ розширить свої місії в Україні на об’єкти інфраструктури, що впливають на безпеку АЕС [IAEA to expand its missions in Ukraine to infrastructure facilities that affect NPP safety].” *Biznes-Tsenzor*, 13 September 2024. https://biz.censor.net/news/3509672/magate_rozshyryt_svoyi_misiyi_v_ukrayini_na_obyekty_infrastruktury_scho_vplyvayut_na_bezpeku_aes.
- Davydiuk, Andrii, and Oleksandr Potii. *National Cybersecurity Governance: Ukraine*. National Cybersecurity Governance Series. Tallinn: CCDCOE Publications, 2024. https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf.
- Davydiuk, Andrii, and Vitalii Zubok. “Analytical Review of the Resilience of Ukraine’s Critical Energy Infrastructure to Cyber Threats in Times of War.” In *2023 15th International Conference on Cyber Conflict: Meeting Reality*, edited by T. Jančárková, D. Giovannelli, K. Podiňš, and I. Winther. Tallinn: CCDCOE Publications, 2023. https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.
- Dixi Group. “Війна рф проти України: енергетичний вимір [The war of the Russian Federation against Ukraine: the energy dimension].” Weekly overview, 12 August 12, 2024. https://dixigroup.org/wp-content/uploads/2024/08/vijna-rf-proty-ukrayiny_2024_08_12_ua.pdf.
- “Європейське майбутнє України: довкілля, енергетика та повоєнна відбудова очима громадян [Ukraine’s European future: environment, energy and post-war reconstruction through the eyes of citizens].” Analytical note, December 2024. https://dixigroup.org/wp-content/uploads/2024/12/analitychna_zapyska_jevropejske_majbutnye_ukrayiny_-1.pdf.
- *Енергетична дипломатія України: аналіз статус-кво та практичні рекомендації* [Energy diplomacy of Ukraine: status-quo analysis and practical recommendations]. Kyiv: Dixi Group, 2021. <https://dixigroup.org/wp-content/uploads/2021/12/enerhetychna-dyplomatiya-ukrayiny.-doslidzhennya-1.pdf>.
- Doshchatov, Yuriy. “Володимир Кудрицький: У нас є розуміння, по яким об’єктам енергетики можуть бити росіяни [Volodymyr Kudrytskyi: We have an understanding of which energy facilities the Russians can attack].” *RBC-Ukraine*, 26 September 2023. <https://www.rbc.ua/rus/news/volodimir-kudritskiy-nas-e-rozumynnya-kim-1695680406.html>.
- DTEK. “DTEK thermal power plant was hit in a new wave of russian attacks. Three workers injured.” 20 June 2024. <https://dtek.com/en/media-center/news/dtek-thermal-power-plant-was-hit-in-a-new-wave-of-russian-attacks-three-workersinjure/>.
- “Enemy launches hacker attacks on the power system.” 1 July 2022. <https://dtek.com/en/media-center/news/vslid-za-raketnimi-udarami-po-tes-vorog-zavdae-khakerskikh-udariv-po-energosistemi/>.
- “З лютого 2022 року енергетики ДТЕК Енерго 41 раз «підіймали» ТЕС з нуля після обстрілів [Since February 2022, DTEK Energy’s power engineers have “raised” TPPs from scratch 41 times after shelling].” 1 August 2024. <https://energo.dtek.com/media-center/press/z-lyutogo-2022-roku-energetiki-dtek-energo-41-raz-pidymali-tes-z-nulya-pislya-obstril/>.

- “Eesti luurejuht: NATO-l tuleb Venemaad ohjeldada järgmised 20 aastat [Estonian intelligence chief: NATO must contain Russia for the next 20 years].” *ERR*, 20 December 2024. <https://www.err.ee/1609557013/eesti-luurejuht-nato-l-tuleb-venemaad-ohjeldada-jargmised-20-aastat>.
- Energy Club. “Аналіз результатів опитування: Майбутнє української енергетики – думка бізнесу [Analysis of survey results: The future of Ukrainian energy – business opinion].” 16 January 2025. www.iclub.energy/news/analiz-rezultativ-opytuvannia-maybutnie-ukrainskoi-enerhetyky-dumka-biznesu.
- Energy Community. “Three years of the full-scale war: Energy Community and Ukraine’s Ministry of Energy strengthen resilience with global support.” 24 February 2025. <https://www.energy-community.org/news/Energy-Community-News/2025/02/24.html>.
- . “Ukraine Energy Support Fund.” Last updated 2 April 2025. <https://www.energy-community.org/Ukraine/Fund.html>.
- Entrepreneurship Development Fund. “Доступні кредити 5-7-9% [Available loans 5-7-6%].” <https://bdf.gov.ua/programs/dostupni-kredyty-5-7-9/>.
- European Commission. “President von der Leyen announces new EU support for Ukraine’s energy security for the winter.” Directorate-General for Neighbourhood and Enlargement Negotiations, 19 September 2024. https://neighbourhood-enlargement.ec.europa.eu/news/president-von-der-leyen-announces-new-eu-support-ukraines-energy-security-winter-2024-09-19_en.
- Fraunhofer FKIE. “Sandworm.” Malpedia. <https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm>.
- Geers, Kenneth, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCDCOE Publications, 2015. https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf.
- Giles, Keir. *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/resources/docs/NDC%20fm_9.pdf.
- Government of Ukraine. “Денис Шмигаль: Потреби житлово-комунальних підприємств у когенераційних установках покриті більш ніж наполовину [Denys Shmyhal: The needs of housing and communal enterprises in cogeneration plants are covered by more than half].” Communication Department of the Government Office, 15 October 2024. <https://www.kmu.gov.ua/news/denys-shmyhal-potreby-zhytlovo-komunalnykh-pidpryemstv-u-koheneratsiinykh-ustanovkakh-pokryti-bilsh-nizh-napolovynu>.
- . “Інвентаризація критично важливих об’єктів дозволить забезпечити більш справедливий розподіл електроенергії – Руслан Слободян [Inventory of critical facilities will ensure a more equitable distribution of electricity – Ruslan Slobodyan].” 14 June 2024. <https://sies.gov.ua/news/inventaryzatsiia-krytychno-vazhlyvykh-obiektiv-dozvolyt-zabezpechyty-bilsh-spravedlyvyi-rozpodil-elektroenerhii-ruslan-slobodian>.
- . “Прес-конференція Прем’єр-міністра України Д. Шмигала [Press conference of the Prime Minister of Ukraine D. Shmyhal].” YouTube, 10 September 2024. <https://www.youtube.com/live/dvk4ekf6lRo>.
- . “Промова Прем’єр-міністра Дениса Шмигала на засіданні Уряду [Speech by Prime Minister Denys Shmyhal at a Government meeting].” Communication Department of the Government Office, 9 July 2024. <https://www.kmu.gov.ua/news/promova-premier-ministra-denysa-shmyhalia-na-zasidanni-uriadu-09072024>.
- . *Постанова від 22 липня 2022 р. № 824 деякі питання отримання, розподілу, використання та обліку гуманітарної допомоги для задоволення потреб енергетики в умовах воєнного стану* [Resolution of 22 July 2022 No. 824 regarding some issues in receiving, distributing, using and accounting for humanitarian aid to meet energy needs under martial law]. Kyiv: Verkhovna Rada, 2022. <https://zakon.rada.gov.ua/laws/show/824-2022-%D0%BF#Text>.
- . *Постанова від 24 травня 2024 р. № 600 про затвердження порядку визначення та застосування граничних величин споживання електричної потужності* [Resolution of 24 May 2024 No. 600 on approval of the procedure for determining and applying limit values for electric power consumption]. Kyiv: Verkhovna Rada, 2024. <https://zakon.rada.gov.ua/laws/show/600-2024-%D0%BF#Text>;
- . *Постанова від 27 грудня 2022 р. № 1482 про реалізацію експериментального проекту щодо будівництва, ремонту та інших інженерно-технічних заходів із захисту об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури* [Decree of 27 December 2022 No. 1482 on the implementation of an experimental project of construction, repair and other engineering and technical measures for the protection of critical infrastructure in the energy sector]. Kyiv: Verkhovna Rada, 2022. <https://zakon.rada.gov.ua/laws/show/1482-2022-%D0%BF#n24>.
- . *Постанова від 27 жовтня 2023 р. № 1127 про затвердження положення про особливості імпорту електричної енергії в умовах правового режиму воєнного стану в Україні* [Resolution of 27 October 2023 No. 1127 on approval of the regulation on the properties of the import of electricity under the legal regime of martial law in Ukraine]. Kyiv: Verkhovna Rada, 2023. <https://zakon.rada.gov.ua/laws/show/1127-2023-%D0%BF#Text>.

- *Розпорядження від 18 липня 2024 р. № 713-р про схвалення Стратегії розвитку розподіленої генерації на період до 2035 року і затвердження операційного плану заходів з її реалізації у 2024-2026 роках* [Order No. 713-r of 18 July 2024 On approval of the Strategy for the Development of Distributed Generation for the period until 2035 and approval of the operational plan of measures for its implementation in 2024-2026]. Kyiv: Verkhovna Rada, 2024. <https://zakon.rada.gov.ua/laws/show/713-2024-%D1%80#Text>.
- *Розпорядження від 18 липня 2024 р. № 713-р про схвалення Стратегії розвитку розподіленої генерації на період до 2035 року і затвердження операційного плану заходів з її реалізації у 2024-2026 роках* [Order of 19 July 2024 No. 713-r on approval of the Strategy for the Development of Distributed Generation for the period until 2035 and approval of the operational plan of measures for its implementation in 2024-2026]. Kyiv: Verkhovna Rada, 2024. <https://www.kmu.gov.ua/npas/pro-skhvalennia-stratehii-rozvytku-rozpodilenoii-heneratsii-na-period-do-2035-roku-i-zatverdzhennia-s713180724>.
- Graham, Mark, Carolyn Ahlers, and Kyle O'Meara. "Impact of FrostyGoop ICS Malware on Connected OT Systems." *Intelligence Brief, Dragos Inc.*, July 2024. https://hub.dragos.com/hubfs/Reports/Dragos-FrostyGoop-ICS-Malware-Intel-Brief-0724_r2.pdf.
- Greenberg, Andy. "How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter." *Wired*, 23 July 2024. <https://www.wired.com/story/russia-ukraine-frostygoop-malware-heating-utility/>.
- "New Clues Show How Russia's Grid Hackers Aimed for Physical Destruction." *Wired*, 12 September 2019. <https://www.wired.com/story/russia-ukraine-cyberattack-power-grid-blackout-destruction/>.
- International Atomic Energy Agency. "Update 262 – IAEA Director General Statement on Situation in Ukraine," 28 November 2024. <https://www.iaea.org/newscenter/pressreleases/update-262-iaea-director-general-statement-on-situation-in-ukraine>.
- International Energy Agency. *Empowering Ukraine Through a Decentralised Electricity System: A Roadmap for Ukraine's Increased Use of Distributed Energy Resources Towards 2030*. IAE, 2024. <https://iea.blob.core.windows.net/assets/b9124406-5b8b-444f-8b20-c4fc22a9221e/EmpoweringUkraineThroughaDecentralisedElectricitySystem.pdf>.
- Jermalavičius, Tomas, Veli-Pekka Tynkkynen, Andrian Prokip, Christian Egenhofer, Edoardo Righetti, Arūnas Molis, Priit Mändmaa, Tony Lawrence, and Oleksandr Sukhodolia. *War and Energy Security: Lessons for The Future*. Tallinn: ICDS, 2023. <https://icds.ee/en/war-and-energy-security-lessons-for-the-future/>.
- Kapellmann Zafra, Daniel, Raymond Leong, Chris Sistrunk, Ken Proska, Corey Hildebrandt, Keith Lunden, and Nathan Brubaker. "Industroyer.V2: Old Malware, New Tricks." *Google Cloud Blog*, 25 April 2022. <https://cloud.google.com/blog/topics/threat-intelligence/industroyer-v2-old-malware-new-tricks>.
- Katsan, Olga. "Російські удари руйнують українську енергетику. Який масштаб втрат і що робити? [Russian strikes are destroying Ukraine's energy sector. What is the scale of the losses and what should be done?]" *Radio Svoboda*, 12 December 2024. www.radiosvoboda.org/a/ruynuvannya-ukrayinskoyi-enerhetyky-pid-chas-viyny/33237255.html<https://www.radiosvoboda.org/a/ruynuvannya-ukrayinskoyi-enerhetyky-pid-chas-viyny/33237255.html>.
- Kholina, Maria. "IAEA to send more observers to Ukraine to ensure NPP safety." *RBC-Ukraine*, 13 February 2024. <https://newsukraine.rbc.ua/news/iaea-to-send-more-observers-to-ukraine-to-1726226842.html>.
- Kolisnichenko, Vadim. "Direct damage to Ukraine's infrastructure from the war reached \$170 billion – KSE." *GMK Center*, 18 February 2025. <https://gmk.center/en/news/direct-damage-to-ukraines-infrastructure-from-the-war-reached-170-billion-kse/>.
- Kozatskiy, Sania. "Україна нарощуватиме кількість мобільних вогневих груп ППО, – ПС ЗСУ [Ukraine will increase the number of mobile air defense fire groups, - Press Service of the Armed Forces of Ukraine]." *Militarnyi*, 7 November 2023. <https://mil.in.ua/uk/news/ukrayina-naroshhuvatyme-kilkist-mobilnyh-vognevyyh-grup-ppo-ps-zsu/>.
- Kuziakiv, Oksana, Yevhen Angel, Anastasya Hulik, and Daria Sharovalova. *Національне опитування щодо відновлюваних джерел енергії в Україні, січень 2025* [National survey on renewable energy sources in Ukraine, January 2025]. Kyiv: Institute for Economic Research and Policy Consulting, 2025. www.ier.com.ua/files/Projects/2025/NRES/2025_NRES_January_FINAL_UKR.pdf.
- Loneran, Erica D., Margaret W. Smith, and Grace B. Mueller. "Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine." In *2023 15th International Conference on Cyber Conflict: Meeting Reality*, edited by T. Jančárková, D. Giovannelli, K. Podišš, and I. Winther. Tallinn: NATO CCDCOE Publications, 2023. https://www.ccdcoe.org/uploads/doc/CyCon_2023_book_print.pdf.
- Miller, Christopher, Isobel Koshiw, and Alice Hancock. "Russia has taken out over half of Ukraine power generation." *The Financial Times*, 5 June 2024. <https://www.ft.com/content/4d583259-7565-4c9c-972e-ea77f4a76175>.

- Ministry for Communities, Territories and Infrastructure Development of Ukraine. “Memorandum on enhancing energy resilience of communities: key ministries and associations of Ukrainian communities will work together to attract investments.” 22 August 2024. <https://www.kmu.gov.ua/en/news/memorandum-pidvyschennia-enerhetychnoi-stiykosti-hromad-kliuchovi-ministerstva-ta-asotsiatsii-ukrainskykh-hromad-razom-zaluchatyut-investytsii>.
- Ministry of Defence of Ukraine. “Україна зміцнює оборонну співпрацю: результати засідання Контактної групи у форматі «Рамштайн» [Ukraine strengthens defence cooperation: results of the meeting of the Contact Group in the Ramstein format].” 14 June 2024. <https://www.mil.gov.ua/news/2024/06/14/ukraina-zmicznyue-oboronnu-spivpracyu-rezultati-zasidannya-kontaktnoi-grupi-u-formati-ramshtajn/>.
- Ministry of Economy of Ukraine. “В Україні запрацювали програми пільгового кредитування для громадян, а також для ОСББ та ЖБК для посилення енергетики [In Ukraine, preferential lending programmes have been launched for citizens as well as condominiums and housing associations to strengthen the energy sector].” 22 July 2024. <https://www.kmu.gov.ua/news/v-ukraini-zapratsiuvaly-prohramy-pilhovoho-kredytuvannia-dlia-hromadian-a-takozh-dlia-osbb-ta-zhbk-dlia-posylennia-enerhetyky>.
- Ministry of Energy of Ukraine. “Ukraine and EU agree to increase winter electricity import capacity to 2.1 GW.” 29 October 2024. <https://www.kmu.gov.ua/en/news/ukraina-ta-ies-domovylysia-pro-zbilshennia-mozhlyvosti-importu-elektroenerhii-vzymku-do-21-hvt>.
- . “Міжнародна допомога енергетиці [International energy assistance].” Last accessed 11 April 2025. <https://mev.gov.ua/reforma/mizhnarodna-dopomoha-enerhetytsi>.
- . “Оперативно про ситуацію в енергетиці [Operational situation in the energy sector].” Last accessed 12 April 2025. <https://mev.gov.ua/storinka/operatyvno-pro-sytuatsiyu-v-enerhetytsi>.
- Ministry of Health of Ukraine. “План на випадок блекаутів: як українські лікарні можуть працювати в умовах відключень світла? [Blackout plan: how can Ukrainian hospitals operate during power outages?].” 30 January 2024. <https://moz.gov.ua/uk/plan-na-vipadok-blekautiv-jak-ukrainski-likarni-mozhut-pracjuvati-v-umovah-vidkljuchen-svitla>.
- Miroshnichenko, Bogdan. “Тепер не тільки «шахеда». Як Росія наростила виробництво ударних БПЛА і чим відповідають українські інженери [Now it’s not just “shaheeds.” How Russia increased the production of attack UAVs and with what Ukrainian engineers respond].” *Ukrainska Pravda*, 17 October 2024. <https://www.epravda.com.ua/publications/2024/10/17/720684/>.
- National Energy and Utilities Regulatory Commission of Ukraine (NEURC). *Постанова 26.03.2022 № 352 про особливості тимчасового приєднання електроустановок до системи розподілу у період дії в Україні воєнного стану* [Resolution of 26 March 2022 No. 352 on the features of temporary connection of electrical installations to the distribution system during the period of martial law in Ukraine]. Kyiv: Verkhovna Rada, 2022. <https://zakon.rada.gov.ua/rada/show/v0352874-22#Text>.
- . “НКРЕКП відновила з 1 січня 2024 року стандартні та нестандартні приєднання до електричних мереж [The National Energy and Utilities Regulatory Commission (NEURC) has resumed standard and non-standard connections to electricity networks from 1 January 2024].” 2 January 2024. <https://www.nerc.gov.ua/news/nkrekp-vidnovila-z-1-sichnya-2024-roku-standartni-ta-nestandardni-priyednannya-do-elektrichnih-merezh>.
- . *Постанова 15.08.2023 № 1494 про затвердження Змін до Кодексу систем розподілу* [Resolution of 15 August 2023 No. 1494 on approval of amendments to the Distribution Systems Code]. Kyiv: Verkhovna Rada, 2023. <https://zakon.rada.gov.ua/rada/show/v1494874-23#n2>.
- . *Постанова 05.12.2023 № 2274 про затвердження Змін до Кодексу систем розподілу* [Resolution of 5 December 2023 No. 2274 on approval of amendments to the Distribution Systems Code]. Kyiv: Verkhovna Rada, 2023. <https://zakon.rada.gov.ua/rada/show/v2274874-23#n2>.
- . *Постанова 12.12.2023 № 2374 про затвердження Змін до Кодексу систем розподілу* [Resolution of 12 December 2023 No. 2374 on approval of amendments to the Distribution Systems Code]. Kyiv: Verkhovna Rada, 2023. <https://zakon.rada.gov.ua/rada/show/v2374874-23#n5>.
- National Security and Defence Council of Ukraine. *Рішення від 17 жовтня 2023 року введено в дію Указом Президента України від 17 жовтня 2023 року № 695/2023 про організацію захисту та забезпечення безпеки функціонування об’єктів критичної інфраструктури та енергетики України в умовах ведення воєнних дій* [Decision of 17 October 2023 enacted by a Decree of the President of Ukraine on No. 695/2023 about the organization of the protection and safety of the operation of critical infrastructure and energy facilities of Ukraine in the context of military operations]. Kyiv: Verkhovna Rada, 2023. <https://zakon.rada.gov.ua/laws/show/n0040525-23#Text>.
- . *Рішення від 26 листопада 2022 року введено в дію Указом Президента України № 802/2022 про забезпечення електронними комунікаційними послугами в умовах воєнного стану* [The decision of 26 November 2022 put into effect by Decree of the President of Ukraine No. 802/2022 on providing electronic communication services under martial law]. Kyiv: Verkhovna Rada, 2022. <https://zakon.rada.gov.ua/laws/show/n0020525-22#Text>.

- Nies, Susanne, and Olha Bondarenko, eds. *Ukraine's Energy and Climate Challenges*. Ukrainian Analytical Digest no. 9. Zurich: Centre for Security Studies, 2024. <https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/ukrainiananalyticaldigest009.pdf>.
- “NYT: Політичні чвари в Україні ускладнюють зусилля відвернути енергетичну кризу цієї зими [NYT: Political strife in Ukraine complicates efforts to avert energy crisis this winter].” *Voice of America*, 15 October 2024. www.holosameryky.com/a/ukrainina-enerhetyka-polityka/7822796.html.
- Odell, Anders, Anna Lioufas, Mari Olsén, Karin Mossberg Sonnek, Frej Welander, and Andreas Hörnedal. *Russian Attacks on the Ukrainian Power System*. Kista: FOI, 2024. <https://www.foi.se/rest-api/report/FOI-R--5596--SE>.
- Omelchenko, Volodymyr. “Енергетика України 2024–2025 років у тумані невизначеності [Ukraine's energy sector in 2024–2025 in a fog of uncertainty].” *Razumkov Centre*, 1 October 2024. <https://razumkov.org.ua/statti/enerhetyka-ukrainy-20242025-rokiv-u-tumani-nevyznachenosti>.
- . “Що відбувається в енергетиці? Факти і конспірологія [What's going on in the energy sector? Facts and conspiracy theories].” *Razumkov Centre*, 10 June 2024. <https://razumkov.org.ua/komentari/shcho-vidbuvaetsia-v-enerhetytsi-fakty-i-konspirologiia>.
- Orliuk, Mykhailo. “Пасивний захист неефективний: Галущенко поклав відповідальність за збереження енергооб'єктів на ППО [Passive protection is ineffective: Galushchenko placed responsibility for the safety of energy facilities on air defence].” *Biznes-Tsenzor*, 10 September 2024. https://biz.censor.net/news/3514095/galuschenko_poklav_vidpovidalnist_za_zahyst_energoobyektiv_na_ppo.
- Pape, Robert A. “Bombing to Lose: Why Airpower Cannot Salvage Russia's Doomed War in Ukraine.” *Foreign Affairs*, 20 October 2022. <https://www.foreignaffairs.com/ukraine/bombing-to-lose-airpower-cannot-salvage-russia-doomed-war-in-ukraine>.
- President of Ukraine. “Volodymyr Zelenskyy Presented the Plan for Ukraine's Internal Resilience.” 19 November 2024. <https://www.president.gov.ua/en/news/volodimir-zelenskij-predstaviv-plan-vnutrishnoyi-stijkosti-u-94505>.
- . “Війна Росії проти України завершиться тому, що запрацює Статут ООН – виступ Президента під час засідання високого рівня Ради Безпеки ООН [Russia's war against Ukraine will end because the UN Charter comes into effect – President's speech at a high-level meeting of the UN Security Council].” 24 September 2024. <https://www.president.gov.ua/videos/vijna-rosiyyi-proti-ukrayini-zavershitsya-tomu-sho-zapracyuye-6969>.
- . “Життя України має зберегтися, і це стосується, зокрема, енергетичного забезпечення – звернення Президента [The life of Ukraine must be preserved, and this applies, in particular, to energy supply - the President's address].” 20 June 2024. www.president.gov.ua/news/zhittya-ukrayini-maye-zberegtysya-i-ce-stosuyetsya-zokrema-e-91685.
- Proska, Ken, John Wolfram, Jared Wilson, Dan Black, Keith Lunden, Daniel Kapellmann Zafra, Nathan Brubaker, Tyler McLellan, and Chris Sistrunk. “Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology.” *Google Cloud Blog*, 9 November 2023. <https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/>.
- Rimutis, Saulius. “Lessons of War: Ukraine's Energy Infrastructure Damage, Resilience and Future Opportunities.” *Geopolitics and Security Studies Center*, May 2024. https://www.gssc.lt/wp-content/uploads/2024/05/v04_Rimutis_Ukrainos-energetikos-sektoriaus-zala_EN_A4.pdf.
- Rzheutska, Liliya. “«Укренерго»: Колапсу не буде, але відключення світла можливі [Ukrenergo: There will be no collapse, but power outages are possible].” *DW*, 11 October 2023. <https://www.dw.com/uk/kerivnik-ukrenergo-kolapsu-ne-bude-ale-vidklucenna-svitla-mozlivi/a-67058497>.
- Sociological Group Rating. “Діяльність енергетичного комплексу України в умовах російського вторгнення [Activities of the Ukrainian energy complex in the context of the Russian invasion].” 6-8 May 2024. https://ratinggroup.ua/files/ratinggroup/reg_files/rg_energy_052024_press.pdf.
- . “Діяльність енергетичного комплексу України: оцінки та практики споживачів [Activities of the energy complex of Ukraine: consumer assessments and practices].” 20-23 October 2024. https://ratinggroup.ua/files/ratinggroup/reg_files/rg_energy_092024.pdf.
- . “Енергетична ситуація в Україні: очікування, виклики та перспективи [Energy situation in Ukraine: expectations, challenges and prospects]. February 2025. https://ratinggroup.ua/files/ratinggroup/reg_files/rg_energy_012025_press.pdf.
- Spînu, Natalia. *Ukraine Cybersecurity Governance Assessment*. Geneva: Geneva Centre for Security Sector Governance, 2020. <https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf>.
- Srybnyanska, Ksenya. “Угорщина пригрозила Україні «вимкненням світла» [Hungary threatens Ukraine with “lights out”].” *Apostrof*, 22 July 2024. <https://apostrophe.ua/ua/news/economy/2024-07-22/vengriya-prigrozila-ukrainie-vyiklyucheniem-sveta/327058>.

- State Emergency Service of Ukraine. “Відключення електроенергії: убезпечте себе, близьких і житло від пожежі [Power outage: protect yourself, your loved ones and your home from fire].” 26 November 2022. <https://dsns.gov.ua/uk/news/ostanni-novini/vidklyucennya-elektroenergiyi-ubezpecte-sebe-blizkix-i-zitlo-vid-pozezi>.
- State Inspectorate for Energy Supervision of Ukraine. “Основні правила ощадливого використання електроенергії [Basic rules for economical use of electricity].” Last accessed 12 April 2025. <https://sies.gov.ua/zvernennya-gromadyan/najbilsh-zapituvana-informaciya/osnovni-pravila-oshchadlivogo-vikoristannya-elektroenergiyi>.
- State Service of Special Communications and Information Protection of Ukraine. *Russia’s Cyber Tactics: Lessons Learned 2022* Kyiv: SSSCIP, 2022. <https://cip.gov.ua/services/cm/api/attachment/download?id=53466>.
- . *Russia’s Cyber Tactics H1’2023. Lessons Learned: Shift in the Patterns, Goals, and Capacity of the Russian Government and Government-Controlled Groups*. Threat Assessment Report. Kyiv: SSSCIP, 2023. <https://cip.gov.ua/services/cm/api/attachment/download?id=60068>.
- . *Russian Cyber Operations*. APT Activity Report H1 2024. Kyiv: SSSCIP, 2024. <https://cip.gov.ua/services/cm/api/attachment/download?id=65898>.
- Stelmakh, Oksana. “Розпочато цикл навчально-консультативних заходів з енергетичної безпеки у громадах [A cycle of educational and advisory activities on energy security in communities has begun].” *U-LEAD*, 28 February 2023. <https://u-lead.org.ua/news/142>.
- Teslia, Mykola. “Блекаут. Владі потрібні план та чесна розмова з громадянами [Blackout. The authorities need a plan and an honest conversation with citizens].” *Dzerkalo Tizhnia*, 17 November 2024. <https://zn.ua/ukr/economic-security/blekaut-vladi-potribni-plan-ta-chesna-rozmova-z-hromadjanami.html>.
- Ukrainian Institute for the Future. “Дебати про майбутнє: Енергетика майбутнього [Debate about the future: Energy of the future].” 22 November 2024. <https://uifuture.org/publications/energetyka-majbutnogo>.
- Ukrenergо. “Шлях до Європи: як українська енергосистема інтегрувалася до європейської енергомережі ENTSO-E [The path to Europe: how the Ukrainian power system integrated into the European power grid ENTSO-E].” Last accessed 12 April 2025. https://ua.energy/entso_e.html.
- US Cybersecurity and Infrastructure Security Agency. “IR Alert (H-16-056-01).” 20 July 2021. <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.
- . “Russia Cyber Threat Overview and Advisories.” <https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia>.
- US Department of State. “Secretary Antony J. Blinken with Italian Foreign Minister Antonio Tajani and Ukrainian Foreign Minister Andrii Sybiha at a G7+ Ministerial Meeting on Ukraine Energy Sector Support.” 23 September 2024. <https://2021-2025.state.gov/secretary-antony-j-blinken-with-italian-foreign-minister-antonio-tajani-and-ukrainian-foreign-minister-andrii-sybiha-at-a-g7-ministerial-meeting-on-ukraine-energy-sector-support/>.
- Verkhovna Rada of Ukraine and National Commission for State Regulation in the Spheres of Energy and Utilities. *Постанова, 26.03.2022 № 352, про особливості тимчасового приєднання електроустановок до системи розподілу у період дії в Україні воєнного стану* [Decree № 352 as of 26.03.2022 on the peculiarities of temporary connection of electrical installations to the distribution system during the period of martial law in Ukraine]. Document v0352874-22. Kyiv: Verkhovna Rada, 2024. <https://zakon.rada.gov.ua/rada/show/v0352874-22#Text>.
- . *Закон України про внесення змін до деяких законів України щодо відновлення та «зеленої» трансформації енергетичної системи України* [Law of Ukraine on amendments to certain laws of Ukraine on the restoration and “green” transformation of the energy system of Ukraine]. Document No. 3220-IX. Kyiv: Vidomosti Verkhovnoi Radi, 2023. <https://zakon.rada.gov.ua/laws/show/3220-20#Text>.
- . *Закон України про внесення змін до підрозділу 2 розділу XX «Перехідні положення» Податкового кодексу України щодо звільнення від оподаткування податком на додану вартість операцій з ввезення товарів для потреб виробництва та/або ремонту машин механізованого розмінування* [Law of Ukraine on amendments to Subsection 2 of Section XX “Transitional Provisions” of the Tax Code of Ukraine on exemption from value added tax on imports of goods for the purposes of production and/or repair of mechanized demining machines]. Document No. 3853-IX. Kyiv: Vidomosti Verkhovnoi Radi, 2024. <https://zakon.rada.gov.ua/laws/show/3853-IX#Text>.

- Закон України про внесення змін до Митного кодексу України щодо звільнення від оподаткування ввізним митом товарів для потреб виробництва та/або ремонту машин механізованого розмінування, товарів, які сприяють відновленню енергетичної інфраструктури України, та щодо окремих особливостей митного оформлення товарів, призначених для потреб безпеки і оборони [Law of Ukraine on amendments to the customs code of Ukraine regarding exemption from import duty on goods for the production and/or repair of mechanized demining machines, goods contributing to the restoration of Ukraine's energy infrastructure, and certain features of customs clearance of goods intended for security and defence needs]. Kyiv: Vidomosti Verkhovnoi Radi, 2024. <https://zakon.rada.gov.ua/laws/show/3854-IX#Text>.
- Закон України про критичну інфраструктуру [Law of Ukraine on the critical infrastructure]. Kyiv: Vidomosti Verkhovnoi Radi, 2023. <https://zakon.rada.gov.ua/laws/show/1882-20#Text>.
- Viasat. “KA-SAT Network Cyber Attack Overview.” 30 March 2022. <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>.
- Watling, Jack, and Darya Dolzikova. “Fighting for the Light: Protecting Ukraine’s Energy System.” *RUSI*, 12 August 2024. <https://rusi.org/explore-our-research/publications/commentary/fighting-light-protecting-ukraines-energy-system>.
- World Bank, Government of Ukraine, European Union, and United Nations. *Ukraine - Fourth Rapid Damage and Needs Assessment (RDNA4): February 2022 - December 2024*. Washington, DC: World Bank Publications, 2025. https://www.undp.org/sites/g/files/zskgke326/files/2025-02/ukraine_fourth_rapid_damage_and_needs_assessment_rdna4_february_2022_december_2024.pdf.
- Yan, Oleksandr. “Генерал США розповів про роботу української акустичної системи виявлення дронів [US general spoke about the work of the Ukrainian acoustic drone detection system].” *Militarnyi*, 26 March 2024. <https://mil.in.ua/uk/news/general-ssha-rozpoviv-pro-robotu-ukrayinskoyi-akustychnoyi-systemy-vyavlennya-droniv/>.
- Yeshchenko, Inna. “Економно — не значить погано. Нові рішення для нових реалій, або як заощаджувати електроенергію з комфортом для себе [Economical does not mean bad. New solutions for new realities, or how to save electricity with comfort for yourself].” *Rubryka*, 17 February 2023. <https://rubryka.com/article/yak-zaoshhadzhuvaty-elektroenergiyu>.
- Zetter, Kim. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” *Wired*, 3 March 2016. <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>.
- “В «Укренерго» розповіли, за яких умов зима зможе пройти без відключень світла [Ukrenenergo explained under what conditions winter might pass without power outages].” *Slovo i Dilo*, 30 September 2024. www.slovoidilo.ua/2024/09/30/novyna/suspilstvo/ukrenerho-rozpovily-yakyx-umov-zyma-zmozhe-projty-vidklyuchen-svitla.
- “В «Укренерго» спрогнозували найважчу за останні три роки зиму [Ukrenenergo predicted the most severe winter in the last three years].” *Slovoidilo*, 30 October 2024. www.slovoidilo.ua/2024/10/30/novyna/suspilstvo/ukrenerho-sprohnozuvaly-najvazhchu-ostanni-try-roky-zyumu.
- “Енергетична інфраструктура України матиме три рівні захисту від російських атак – голова «Укренерго» Кудрицький [Ukraine’s energy infrastructure will have three levels of protection against Russian attacks - Ukrenenergo head Kudrytskyi].” *Radio Svoboda*, 12 October 2024. <https://www.radiosvoboda.org/a/news-enerhetyka-zakhyst-ataky-rf/32634122.html>.
- “Зенітні-дрони “анти-Шахеда”: яку головну задачу вирішили українські розробники і це не про швидкість (відео) [“Anti-Shahed” anti-aircraft drones: what is the main task solved by Ukrainian developers and it’s not about speed (video)].” *Defense Express*, 21 October 2024. https://defence-ua.com/weapon_and_tech/zenitni_droni_anti_shahedi_jaku_golovnu_zadachu_virishili_ukrajinski_rozrobniki_i_tse_ne_pro_shvidkist_video-16947.html.
- “Найбільші банки України підписали меморандум про пільгове кредитування відновлення енергоінфраструктури [The largest banks in Ukraine signed a memorandum on preferential lending for the restoration of energy infrastructure].” *Ukrainska Pravda*, 25 June 2024. <https://www.epravda.com.ua/news/2024/06/25/715756/>.
- “Проти енергетичних компаній України готується нова кібератака – експерти [A new cyberattack is being prepared against Ukrainian energy companies – experts].” *UNIAN*, 14 December 2017. <https://www.unian.ua/economics/energetics/2297199-proti-energetichnih-kompaniy-ukrajini-gotuetsya-nova-kiberataka-eksperti.html>.
- “Росія має намір атакувати три українські АЕС - Зеленський в ООН [Russia intends to attack three Ukrainian nuclear power plants - Zelensky at the UN].” *Ukrinform*, 24 September 2024. <https://www.ukrinform.ua/rubric-ato/3909283-rosia-mae-namir-atakuvati-tri-ukrajinski-aes-zelenskij-v-oon.html>.

- “Скільки електроенергії імпортує та експортує Україна під час великої війни [How much electricity did Ukraine import and export during the big war?].” *Slovo i Dilo*, 2 October 2024. www.slovoidilo.ua/2024/10/02/infografika/ekonomika/skilky-elektroenerhiyi-importuye-ta-eksportuye-ukrayina-velykoyi-vijny.
- “Стефанчук на саміті G7 закликав партнерів підтримати енергетику України перед початком холодів [Stefanchuk at the G7 summit called on partners to support Ukraine’s energy sector before the onset of cold weather].” *Radio Svoboda*, 8 September 2023. <https://www.radiosvoboda.org/a/news-stefanchuk-g7-partnery-enerhetyka-ukrainy/32584162.html>.
- “Україна домовилася з ЄС щодо збільшення імпорту електроенергії взимку [Ukraine has agreed with the EU to increase electricity imports in winter].” *Slovo i Dilo*, 29 October 2024. www.slovoidilo.ua/2024/10/29/novyna/suspilstvo/ukrayina-domovylasya-yes-shhodo-zbilshennya-importu-elektroenerhiyi-vzymku.
- “Українські енергетики демонструють небачені до війни рекордні темпи ремонтів енергооб’єктів [Ukrainian energy workers demonstrate record pace of energy facility repairs, unprecedented before the war].” *Interfax-Ukraina*, 14 February 2023. <https://interfax.com.ua/news/general/891319.html>.
- “«Укренерго» обіцяє встановити справедливі графіки відключення світла в усіх областях [Ukrenergo promises to establish fair power outage schedules in all regions].” *Radio Svoboda*, 12 December 2024. www.radiosvoboda.org/a/news-ukrenerho-spravedlyvi-hrafiky-vidklyuchennya-svitlo/33237392.html.
- “Як пережити блекаут: корисні поради та рішення [How to survive a blackout: useful tips and solutions].” *TTT*, 20 August 2024. <https://www.ttt.ua/ua/articles-reviews/kak-perezhit-blekaut-poleznye-sovety-i-resheniia>.

RECENT ICDS PUBLICATIONS

REPORTS

- Arjakas, Merili, Kai Kaarelson, Solveig Niitra, Hille Hanso, Ivan U.K. Lyszcz. *Eesti roll muutuvast rahvusvahelise arengukoostöö arhitektuuris* [Estonia's Role In the Changing Architecture of International Development Cooperation]. March 2025.
- Klyszcz, Ivan U.K., Tony Lawrence, Eric Chan, Jun-yi Lee. *Deterrence and Hybrid Warfare: Lessons from Russia's War in Ukraine for Taiwan and the Nordic-Baltic Region*. February 2025.
- Hosaka, Sanshiro. *A Mountain to Climb: Russia's Influence in the South Caucasus and EU Policy Options*. January 2025.
- Gretskiy, Igor. *New Russian Immigration to the EU: The Case of the Baltic States, Finland, Germany & Poland*. October 2024.
- Atanassova-Cornelis, Elena, Takuya Matsuda, Bart Gaens, and Nele Loorents. *Japan, NATO, and the Diversification of Security Partnerships*. September 2024.
- Klyszcz, Ivan U.K. (editor), Che-chuan Lee, and James Sherr. *China's and Russia's Aggressive Foreign Policies: Historical Legacy or Geopolitical Ambitions?* June 2024.

POLICY PAPERS

- Klyszcz, Ivan U.K. "Distance is Not a Shield. Russia's Transnational Repression in Wartime," May 2025.
- Praks, Henrik. "Russia's Hybrid Attacks in Europe: From Deterrence to Attribution to Response." April 2025.
- Loorents, Nele, and Jun Nagashima. "Bridging Two Oceans: The Evolving NATO-Japan Relationship." July 2024.

ANALYSES

- Hanso, Toomas. "Central Asia's New Railways: Russia's Pain, China's Gain." March 2025.
- Alatalu, Siim. "The EU's NIS2 Directive A Business Opportunity for the Defence Sector." March 2025.
- Peterson, Annabel. "The Enemy Within: Russians in Ukrainian Army Ranks and the Fracturing of Post-Soviet Identity." February 2025.
- Idarand, Tõnis. "For as Long as It Works: Russia's Nuclear Signalling During Its War in Ukraine." January 2025
- Hanso, Toomas. "China's New Information Support Force: Military Lessons from Ukraine." December 2024.
- Sõukand, Kaspar. "The Iron Leviathan: Russia's Rail Network in its War against Ukraine." December 2024.
- Sundquist, Sara Matea. "High Noon for the High North? Norway, Russia, and the Svalbard Stronghold." November 2024.
- Leveque, Justin. "Russian Malign Activities in France Since 2022: Stoking Tensions, Sowing Disorder, Disrupting Assistance to Ukraine." September 2024.
- Vitiello, Alessandro. "Shared Goals, Different Paths, and a Complex Outcome: A Deep Dive into Ukraine's 2024 Bilateral Security Agreements." September 2024.

BRIEFS

- Cordet, Maxime, and Marianne Paire. *EU Defence Series*. April 2025.
- Tõhk, Tauno. "More Than a Systemic Rival: China as a Security Challenge for the EU." March 2025.
- Cordet, Maxime, and Marianne Paire. *EU Defence Series*. March 2025.
- Hosaka, Sanshiro. "Why the 'Reverse Nixon' Strategy Will Fail: The Illusion of Decoupling." March 2025.
- Claessen, Koen. "The EU's Dilemmas in the Black Sea Region: Security and Enlargement." March 2025.
- Klyszcz, Ivan U.K. "Russia's Self-Serving Aid Policy: Influence, Opacity, and Propaganda." March 2025.
- Blockmans, Steven. "A New but Ambiguous Momentum in EU Enlargement." February 2025.
- Nazarov, Mykola, Andriy Stavyt'skyi, Leonid Polyakov, Stanislav Zhelikhovskiy, Maryna Vorotyntseva, Vitaliy Goncharuk, and Mykhailo Samus. "Russia's War in Ukraine Series, Volume 2." March 2024 / January 2025.
- Riley, Alan. "The End of the Affair? The Transit of Russian Gas Across Ukraine." December 2024.

All ICDS publications are available from <https://icds.ee/category/publications/>.



ICDS.TALLINN



@ICDS-TALLINN.BSKY.SOCIAL



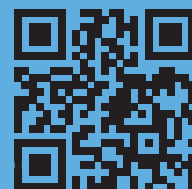
@ICDS _ TALLINN



ICDS-TALLINN



WWW.ICDS.EE



INTERNATIONAL CENTRE FOR DEFENCE AND SECURITY
63/4 NARVA RD., 10120 TALLINN, ESTONIA
INFO@ICDS.EE

ISSN 2228-0529
ISBN 978-9916-709-46-7 (PRINT)
ISBN 978-9916-709-47-4 (PDF)