

CYBER RESILIENCE UNDER FIRE: OT SYSTEMS AND CRITICAL INFRASTRUCTURE IN THE RUSSIA-UKRAINE WAR

Csaba KRASZNAY

Budapest University of Technology and Economics, Hungary
krasznay.csaba@vik.bme.hu

Abstract

The Russia–Ukraine war has provided an unprecedented opportunity to examine the effectiveness of cyber operations against critical infrastructure and operational technology (OT) systems during an active armed conflict. Prior to the invasion, many experts expected Russia to launch large-scale cyberattacks capable of causing strategic-level disruption to Ukrainian critical infrastructure. However, the practical impact of such operations proved significantly more limited than anticipated. This study examines the extent to which Russian cyber operations against Ukrainian critical infrastructure have produced direct cyber-physical effects at the OT layer and how their operational relevance has varied across different phases of the conflict. The research employs a qualitative design combining structured literature and document analysis, case-study analysis, and selected findings from the Digital Mohács 3.0 research project. The SANS ICS Cyber Kill Chain model is applied to distinguish incidents affecting conventional IT systems from operations progressing towards direct manipulation of industrial processes. The findings indicate that the vast majority of incidents affecting critical infrastructure remained at the conventional IT layer, while operations producing direct cyber-physical effects through specialised OT protocols and control logic were exceptional. The analysis further suggests that the conditions for complex OT-targeting operations are most favourable during hybrid confrontation and the initial phase of armed conflict, whereas their relative utility decreases during protracted conventional warfare. The study is limited by its reliance on publicly documented incidents, as classified, undisclosed, or unsuccessful operations cannot be systematically assessed. The findings underline the importance of protecting IT environments, maintaining effective IT–OT segmentation, and ensuring rapid incident-response capabilities as central components of critical-infrastructure resilience.

Keywords: cyber resilience, critical infrastructure, operational technology (OT), Russia–Ukraine war, cyber operations

1. Introduction

Cyber resilience is a key concept in the European Union’s cybersecurity regulatory framework. This is no coincidence, as European critical infrastructures would, practically without exception, be unable to function without the cyber-physical systems collectively known as operational technology (OT) systems. These systems have been used in manufacturing and industrial operations since the 1970s, primarily to ensure operational safety and reliability. Cybersecurity was not among their original design requirements, as OT environments were generally intended to operate in isolation and the cyber threat landscape was considerably less complex than it is today. The lifecycle of OT systems can span several decades. Consequently, the increasing connectivity and data-driven operation associated with the Fourth Industrial Revolution have exposed legacy systems to threats that were not anticipated when they were designed. At the same time, major powers have increasingly treated cyberspace as an operational domain. As a result, critical infrastructure operators must protect legacy

technologies, industrial processes and operational personnel that were not originally prepared to address contemporary cyber threats.

The operational capability of OT systems is therefore crucial for modern economies, which is why they have become a key target for nation-state cyber operations. One frequently cited early example concerns the alleged manipulation of Soviet industrial control technology in connection with the 1982 Siberian pipeline explosion. According to the account later presented by former U.S. presidential adviser Thomas C. Reed, the CIA facilitated the transfer of deliberately modified control software to the Soviet Union through a technology-transfer operation. However, the causal connection between the alleged manipulation and the pipeline explosion remains disputed, and the available evidence does not allow the incident to be treated as a confirmed historical example of a successful cyber-physical attack (Trachtenberg, 2024). Nevertheless, the case is relevant to the present analysis because it demonstrates that the deliberate manipulation of industrial control technology had already emerged as a conceivable instrument of strategic competition decades before the disclosure of Stuxnet. This is further reinforced by the military simulation organised by Gartner Inc. and the U.S. Naval War College between 24 and 26 July 2002, which was named ‘Digital Pearl Harbour’. (Purchase & Caldwell, 2004) During this exercise, participants analysed cyber-terrorist scenarios in which cyber-attacks targeting industrial systems played a central role.

The vulnerability of OT systems received much greater attention following the disclosure of Stuxnet, which was designed to disrupt Iran’s nuclear programme (Selján, 2020). This recognition came considerably later than the corresponding shift in the traditional IT security domain. In the 2010s, the possibility of a nation-state launching a direct attack against the OT systems of critical infrastructure as part of its cyber operations became increasingly prominent. This conviction was reinforced by the toolkit of Russian hybrid operations against Ukraine, where cyberattacks against industrial systems had become routine by the second half of the 2010s. By the end of the decade, it appeared increasingly likely that cyber operations against critical infrastructure would accompany future conventional conflicts. The remaining question concerned their potential strategic impact. Some experts initially considered cyber warfare to be of decisive importance, whilst others were sceptical about its effectiveness.

The Russia-Ukraine war, which broke out on 24 February 2022, provided a grim opportunity for both sides to analyse the impact of cyber warfare in practice. At the time of writing, with the conflict entering its fifth year, both sides have actively exploited the opportunities offered by cyber operations, a significant proportion of which are well documented. The objective of this study is to assess the extent to which operational technology (OT) systems controlling critical infrastructure can remain resilient against hostile cyber operations during an active armed conflict, using the Russia–Ukraine war as the principal case. Accordingly, the study addresses two research questions:

RQ1: To what extent have Russian cyber operations against Ukrainian critical infrastructure produced direct cyber-physical effects at the OT layer?

RQ2: How does the effectiveness and operational relevance of cyber operations targeting OT systems differ between periods of hybrid confrontation, the initial phase of armed conflict, and protracted conventional warfare?

The working hypothesis of the study is that cyber operations targeting OT systems pose the greatest risk during hybrid confrontation and the initial stages of armed conflict, while their strategic impact decreases during a protracted conventional war.

The contribution of the study is threefold. First, it examines the extent to which incidents classified as affecting OT environments actually reach specialised OT protocols and control

logic, as opposed to remaining at the conventional IT layer. Second, it applies the SANS ICS Cyber Kill Chain model to distinguish between initial IT compromise and operations capable of producing direct cyber-physical effects. Third, it analyses how the relevance and effectiveness of OT-targeting cyber operations vary across different phases of conflict.

2. Research Design and Methodology

The study employs a qualitative research design combining structured literature and document analysis, case-study analysis, and the secondary analysis of selected findings from the Digital Mohács 3.0 research project. These three components are used to examine the research questions from complementary perspectives: the first establishes the conceptual and empirical context of cyber operations against critical infrastructure; the second examines publicly documented incidents in which cyber operations affected or attempted to affect OT environments; and the third provides expert perceptions of the strategic relevance of cyber threats to critical infrastructure.

The literature and document analysis draws on peer-reviewed academic publications, primary legal and regulatory sources, official reports, and technical threat-intelligence reports. Particular emphasis is placed on sources that document cyber operations conducted in connection with the Russia–Ukraine conflict and on technical analyses that allow a distinction to be made between compromise of conventional IT infrastructure and interference with specialised OT components. The analysis uses the SANS ICS Cyber Kill Chain as its principal analytical framework. Its distinction between Stage 1, involving intrusion, persistence, reconnaissance and access to the target environment, and Stage 2, involving the development and execution of capabilities designed to manipulate industrial processes, provides the basis for assessing whether an incident remained primarily an IT-layer compromise or progressed to a direct cyber-physical effect.

The case-study component focuses on publicly documented incidents associated with the Russia–Ukraine conflict for which sufficient technical information is available to assess the level of OT involvement. Particular attention is given to the 2022 Industroyer2 attack against the Ukrainian electricity grid, the subsequently documented MicroSCADA-based “living-off-the-land” operation against a Ukrainian substation, and the 2024 FrostyGoop attack against district-heating infrastructure in Lviv. These cases are not intended to constitute an exhaustive dataset of all cyber incidents affecting Ukrainian critical infrastructure. Rather, they are selected because publicly available technical reporting makes it possible to determine whether and how the attackers progressed beyond conventional IT compromise towards manipulation of industrial control systems.

The third component draws on selected findings of the Digital Mohács 3.0 research project conducted by Kovács and Krasznay between December 2023 and March 2024. The author of the present study was a co-investigator and co-author of that research. Digital Mohács 3.0 combined an anonymous online questionnaire completed by 101 Hungarian cyber-defence professionals with in-depth interviews involving 13 senior experts and decision-makers working in cyber defence and critical-infrastructure-related roles. The present study does not treat Digital Mohács 3.0 as independent third-party validation. Instead, selected findings are reconsidered here specifically in relation to the perceived strategic importance of cyberattacks against critical infrastructure and are used to complement the technical and conflict-focused analysis developed in the preceding sections.

The research design has several limitations. The analysis is necessarily restricted to incidents for which sufficiently detailed information is publicly available. Cyber operations conducted by state actors are frequently classified, incompletely disclosed, or deliberately concealed, and unsuccessful operations may never become public. Consequently, the absence of documented Stage 2 operations cannot be interpreted as evidence that no such operations

were attempted. Furthermore, the Digital Mohács 3.0 component reflects the perceptions of Hungarian cyber-defence professionals rather than those of Ukrainian practitioners directly involved in the conflict. Its role in the present study is therefore supplementary: it provides expert assessment of the strategic relevance of critical-infrastructure cyber threats rather than direct empirical evidence concerning Russian operations in Ukraine.

3. The conceptual framework of digital resilience and OT systems

To answer the research questions, it is essential to gain a clear understanding of the conceptual framework within which we examine state cyber operations and resilience issues affecting OT systems used by critical infrastructures.

For the purposes of this study, OT systems and cyber-physical systems are understood in accordance with the definition provided in NIST SP 800-82r3: ‘A broad range of programmable systems and devices that interact with the physical environment or manage devices that interact with the physical environment. These systems and devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems.’ (Stouffer et al., 2023) In the context of this study, these systems are used by organisations that are classified as critical under national law in accordance with Annexes I and II of Directive (EU) 2022/2555 of the European Parliament and of the Council, i.e. the NIS2 Directive. (European Union, 2022a)

The definition of digital resilience can be derived, amongst other sources, from European Union legislation. This concept is explicitly set out in the DORA Regulation, which applies to financial institutions, but can generally be applied to any critical infrastructure: ‘the ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by third-party ICT service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions.’ (European Union, 2022b)

For the purposes of this study, the concept of a cyber attack follows Rule 92 of the Tallinn Manual published by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE): ‘A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.’ Rule 14 of the Tallinn Manual further provides that: ‘A State bears international responsibility for a cyber-related act that is attributable to the State and that constitutes a breach of an international legal obligation.’ (Schmitt, 2017) Although state involvement in hybrid cyber operations is often deliberately obscured to preserve plausible deniability, the present study focuses on operations that are publicly attributed to, or widely assessed as associated with, Russian state actors. Accordingly, the analysis concentrates on cyber operations conducted in the context of Russia’s aggression against Ukraine and relevant to the threshold established by the Tallinn Manual definitions above.

4. Russian cyber operations during the war

On the eve of the Russian invasion launched in February 2022, many experts feared that the offensive would be accompanied by cyberattacks of unprecedented intensity. Many envisioned a nationwide “cyber-Armageddon”, such as a complete shutdown of the Ukrainian power grid. In contrast, the Russian cyber operations carried out in the first days of the war fell far short of these ominous expectations. Russia did not carry out the anticipated, devastating cyber strike that would have immediately plunged Ukraine into darkness, and thanks to Ukrainian cyber

defence measures, they were largely able to withstand even the most destructive Russian attacks.

The attacks launched by the Russian armed forces were typically limited to the toolkit familiar from previous years. Russian cyber operations against Ukraine since 2014 provided extensive opportunities to develop, test and refine capabilities subsequently relevant to wartime operations. At the same time, research on the pre-2022 conflict indicates that cyber operations had only limited ability to shape battlefield events directly (Kostyuk & Zhukov, 2019; Willett, 2022). Prior to the Russian invasion and during its initial phase, Ukraine was hit by cyberattacks of unprecedented intensity. As early as 13 January 2022, a data-wiping malware identified as WhisperGate appeared on several government networks. This malware disguised itself as ransomware, but in reality, it irretrievably deleted data from the compromised machines. On 23 February, on the eve of the military offensive, Russian military intelligence (GRU) launched another wiper-type attack; for example, HermeticWiper simultaneously paralysed the IT systems of several Ukrainian government, energy and financial organisations with the aim of slowing down the coordination of Ukrainian defences at the start of the invasion. (Przetacznik & Tarpova, 2022)

At the start of the war, Russian cyber operations relied heavily on malware designed to destroy data, particularly so-called wipers. Denial-of-service attacks were also used to render websites inaccessible, while other operations targeted communications infrastructure. Some of these operations nevertheless had serious consequences. In the first hours of the invasion, for example, the AcidRain wiper disrupted approximately 40,000 satellite internet modems connected to Viasat's KA-SAT network, causing communications outages in Ukraine and parts of Europe (Boschetti et al., 2022). The disruption, however, did not paralyse Ukrainian forces in the longer term.

Russian cyber operations also appear to have been insufficiently coordinated with conventional military operations. One contributing factor is the fragmented institutional structure of Russian cyber capabilities. Rather than operating under a single unified cyber command, the FSB, GRU and SVR conduct operations through separate organisational structures, with coordination reportedly limited in some cases. This fragmentation complicates the integration of cyber operations with conventional military planning (Sherman, 2025).

Many also expected Russia to paralyse Ukraine's critical infrastructure through devastating cyberattacks by targeting its OT systems. However, experience shows that these attacks played only a marginal role in the war. Although Russian hacker groups launched numerous coordinated operations in the early days of the war and in the run-up to it, no widespread or strategically significant physical damage to industrial infrastructure was achieved through cyber operations alone. The impact of cyberattacks on critical infrastructure remained limited, particularly in the light of conventional military strikes. (Kostyuk & Gartzke, 2022; Dziwisz & Sajduk, 2023) Cyber operations can be difficult to coordinate with kinetic operations. Moreover, when conventional weapons such as missiles can achieve the intended physical effect more rapidly and reliably, the additional utility of a complex cyber-physical operation may be limited. In practice, we have seen that when Russian forces launched a physical strike against a facility—for example, attacking an electrical substation with missiles—this was sometimes accompanied by a simultaneous cyberattack, yet they failed to achieve any significant, long-term impact. It should be noted, however, that at the start of the war, the destruction of critical infrastructure was not the objective; on the contrary, the Russian leadership was confident of achieving rapid successes and aimed to preserve the infrastructure. Successful cyberattacks could have been of significant assistance in this regard.

5. The methodology of cyberattacks against OT systems

The absence of successful Russian cyber operations targeting OT systems, however, is only seemingly surprising. Although industry reports regularly highlight the vulnerabilities of OT systems, relatively few malware families have been identified that directly target industrial systems through specialised OT protocols such as MODBUS, CODESYS or OPC UA. Over the past few decades, approximately a dozen malware families have been identified as capable of directly targeting industrial systems or their specialised protocols. According to the consensus of analysts, these include Stuxnet, Havex, BlackEnergy3, Industroyer, Triton, Industroyer2, INCONTROLLER/PipeDream, COSMICENERGY, Fuxnet and FrostyGoop/BUSTLEBERM. (Amri, 2024) Malware specifically designed to target OT protocols is therefore far less common than malware targeting conventional IT systems. Such capabilities are also deployed much less frequently and are typically associated with highly targeted, state-sponsored operations. It is true that the last five items on the list appeared after the outbreak of the Russia-Ukraine war (four of them within a year), whilst the first five were detected between 2010 and 2021, but the number of malicious codes is still not increasing massively. Producing deliberate and predictable cyber-physical effects, however, generally requires the attacker to progress beyond conventional IT compromise and interact with industrial control processes, control logic or field devices. Such operations are considerably more demanding than attacks confined to the IT layer.

Meanwhile, however, a not insignificant proportion of cyber incidents involve industrial targets, which appears to contradict the previous statement. According to 2025 data from the European Union Agency for Cybersecurity (ENISA), 2.9% of the 4,875 high-impact incidents affected the manufacturing sector, whilst 0.8% affected the energy industry; although this may seem small, it still amounts to 170 incidents. OT involvement was identified in 18.2% of all incidents, i.e. 887 cases. A detailed analysis of incidents affecting the manufacturing sector reveals that 39.3% of these were hacktivist attacks, in which pro-Russian groups typically targeting organisations in pro-Ukrainian countries launched distributed denial-of-service (DDoS) attacks against their targets, whilst 59.3% of cases can be linked to cybercriminal groups, generally gangs spreading ransomware. It should also be noted that the Akira and Qilin ransomware groups account for nearly 70 per cent of the reported cybercriminal activity affecting the manufacturing sector in the ENISA dataset. (ENISA, 2025)

There is therefore an apparent contradiction between the low number of malicious codes directly targeting OT's specific protocols and the relatively high number of incidents affecting OT. However, this contradiction can be resolved relatively easily by examining the schematic diagram of OT systems. The NIST SP 800-82r3 standard illustrates the architecture of OT systems as shown in Figure 1. Put very simply, the first layer, designated the Control Centre, typically contains conventional IT systems (e.g. software running on the Windows operating system, Linux-based servers, traditional network solutions), which, however, very often do not follow the basic principles of cybersecurity design. In many legacy environments, basic cybersecurity principles may not have been systematically implemented. Network segmentation may be inadequate, operating systems and applications may remain unpatched, and separation of duties may be limited. Historically, some of these weaknesses were considered less significant when industrial systems operated in isolated or air-gapped environments. In practice, however, complete isolation has become increasingly uncommon. Components of the control-centre environment may now connect directly or indirectly to external networks, either continuously or temporarily. Compromise of these systems may therefore be classified as an OT incident even when the attacker never interacts with specialised OT protocols or field-level devices. This distinction is central to the analysis developed in this study: a substantial proportion of incidents reported as affecting OT environments are, operationally, conventional IT compromises that do not progress to the manipulation of specialised OT protocols, control logic or field devices. Nevertheless, such compromises may

still result in operational disruption if operators shut down production systems as a precaution or lose access to IT services required for continued operations. The IT environment, however, is significantly easier to defend and restore than the rest of the OT system. This distinction may help explain why publicly documented Russian operations affecting critical infrastructure have more frequently involved conventional IT compromise than direct manipulation of specialised OT protocols and control logic. Had Ukraine been successfully defeated, they could have restored the operation of critical infrastructure with relatively few resources; however, Ukrainian cyber defence was adequately prepared for such attacks, so even if they were unable to repel them, they were able to effectively restore business operations even following a successful attack.

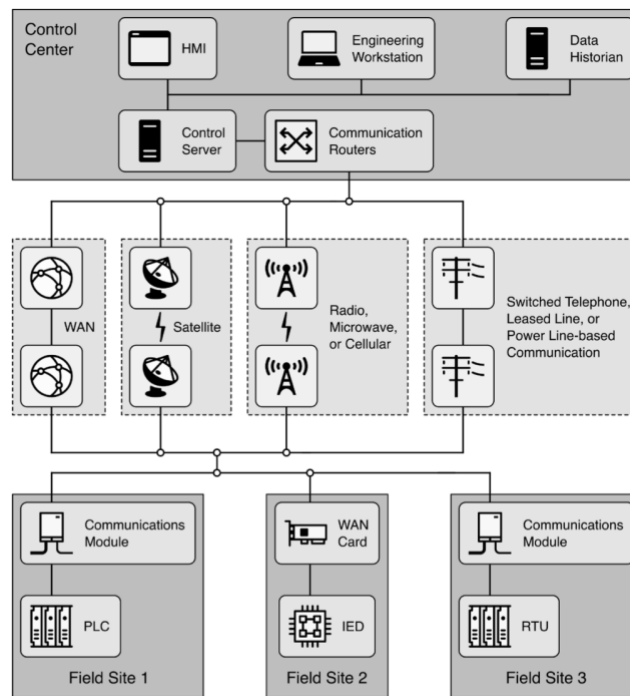


Figure 1: A general SCADA system layout that shows control center devices, communications equipment, and field sites
(Source: Stouffer et al., 2023)

In many cases, moreover, cyberattacks targeting critical infrastructure do not even reach the OT level, but instead target the company's traditional IT management systems. Perhaps the best-known example of this is the 2021 ransomware attack on Colonial Pipeline, where the company was unable to carry out its operations because its billing system was paralysed, whilst the OT system was not affected by the incident at all. (Beerman et al., 2023) A similar distinction can be observed in the September 2025 cyber incident affecting Jaguar Land Rover. Public reporting primarily identified compromise of IT systems rather than direct manipulation of OT components, yet the incident resulted in prolonged production disruption and substantial economic losses. (Jolly & Milmo, 2025).

Since the outbreak of the Russia-Ukraine war, in line with this trend, there have been surprisingly few cyber incidents known to have caused physical effects that are well-documented in public and primary sources and specifically focus on the lower, control layers of OT systems and specialised protocols. Three publicly documented incidents provide particularly useful evidence of operations that progressed towards the lower control layers of OT systems. The first is the Industroyer2/INDUSTROYER.V2 operation against the Ukrainian electricity grid in April 2022, which Ukrainian defenders disrupted before its intended effect

could be achieved. The second is the MicroSCADA-based ‘living-off-the-land’ operation against a Ukrainian substation, in which attackers issued direct SCADA commands without deploying specialised OT malware. The third is the January 2024 disruption of district-heating services in Lviv, where FrostyGoop was used to interact with industrial devices via Modbus (Salazar et al., 2024; Ahlers et al, 2024).

However, the conflict also saw numerous cyber operations – some of which have been officially attributed – that affected critical infrastructure, though it cannot be proven that they directly targeted OT components (PLC/RTU/SCADA/HMI/DCS). The vast majority of these were carried out using so-called ‘wiper’ malware, i.e. malware designed to delete data. Wipers are practically no different from ransomware in terms of their operating mechanism, but their aim is not financial gain, but rather to render the infected computer or network device inoperable. According to an analysis by the cybersecurity firm Dragos OT, such attacks have been occurring continuously throughout the war, as shown in Figure 2. In addition to these, there were also instances in 2023–24 where Russian hackers targeted the energy sector (electricity, water and district heating systems), but according to the Ukrainian cybersecurity authority, the main aim of these was also to amplify the impact of concurrent missile strikes against critical infrastructure.

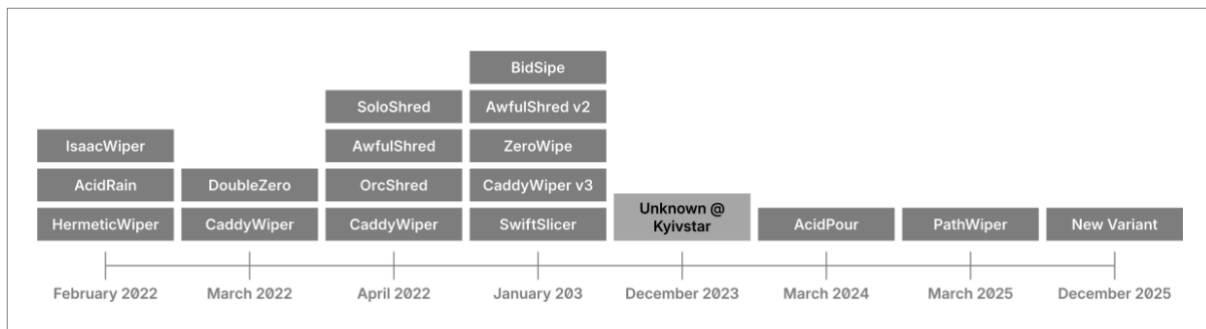


Figure 2: Timeline of ELECTRUM Wiper Capabilities
(Source: Dragos, Inc., 2026)

A further explanation for the low number of direct attacks targeting OT’s specific protocols is provided by the SANS ICS Cyber Kill Chain model, a framework developed to analyse cyberattacks against industrial control systems, which adapts the logic of the classic Cyber Kill Chain to the specific characteristics of cyber-physical systems. One of the model’s key features is that it divides the attack process into two distinct stages. The first stage is cyber intrusion preparation and execution (Stage 1), which essentially involves penetrating the IT infrastructure and reconnaissance of the target system. The second stage is the development and execution of an attack against the industrial control system (ICS attack development and execution – Stage 2), in which the attacker carries out operations specifically aimed at manipulating industrial processes or triggering physical effects. The model therefore distinguishes between gaining access to an organisation’s IT or industrial network and progressing towards an operation capable of manipulating industrial processes and producing cyber-physical effects. (Assante & Lee, 2021)

During the first stage (Stage 1 – preparation and execution of the intrusion), the attacker’s primary objective is to gain access to the target organisation’s IT or industrial network and to conduct reconnaissance of the environment. This process typically begins with the use of classic cyberattack techniques, such as reconnaissance, during which the attacker attempts to map the target system using open-source information, supplier relationships or technical documentation. This is followed by the preparation and customisation of attack tools for the target system, and then the execution of the attack using various intrusion methods, such as phishing campaigns,

via compromised supplier connections, or using infected data storage devices. After gaining initial access, attackers typically establish a persistent presence on the network, set up command and control (C2) channels, and then attempt to reach the OT environment through lateral movement. By the end of Stage 1, the attacker has already gained a detailed picture of the industrial infrastructure, including Supervisory Control and Data Acquisition (SCADA) systems, engineering workstations, Programmable Logic Controllers (PLCs), and other industrial control elements.

The second stage (Stage 2 – development and execution of an attack against an industrial control system) begins when the attacker already possesses sufficient technical and operational information about the industrial process to carry out a targeted attack. In this phase, the focus shifts to developing and testing attack capabilities. Attackers often develop attack tools specifically tailored to the given infrastructure based on previously obtained configuration files, control programs or system parameters. It is not uncommon for attackers to test attack methods in a laboratory environment or on hardware identical to the target system in order to minimise the risk of errors and ensure the desired effect is achieved. Following the development and testing process, the attack components are deployed within the OT environment, for example on SCADA servers, engineering workstations or directly on industrial controllers.

In the final phase of the attack chain, attackers alter the operation of the industrial process, for example by manipulating the logic of Programmable Logic Controllers (PLCs), distorting data on Human–Machine Interfaces (HMIs) or directly modifying control commands. This can result in physical effects, such as power supply disruptions, industrial equipment failures or instability in technological processes. One key finding of the SANS model is that a longer period of time often elapses between the two phases, as attackers require detailed knowledge of technology and process control to successfully carry out attacks against industrial systems.

This characteristic distinguishes OT attacks from cyber operations against traditional IT systems and also highlights that attacks against critical infrastructure are often the result of a lengthy preparation process. This helps explain why many attacks stop at Stage 1. At this point, attackers may already be able to deploy ransomware or wipers and cause significant disruption without developing capabilities tailored to the victim's industrial processes. Progressing to Stage 2 requires substantially greater knowledge of the target environment, additional preparation and, in many cases, purpose-built capabilities. The trade-off is that such operations are generally better suited to disruption than to producing deliberate and sustained cyber-physical effects.

Dragos, in its 2025 report summarising the year and focusing on OT threats, mentions that of the 26 attacker groups it had recorded, only 11 were active in that year, and of these, the groups KAMACITE and ELECTRUM – which work closely together and are otherwise active in Ukraine – most comprehensively covered the steps described in Stages 1 and 2. KAMACITE's activities are primarily aimed at reconnaissance and compromise of critical infrastructure, particularly in the energy sector. Based on public analyses, the group's operations are highly likely to be linked to Russian state interests and show overlaps in several respects with the activities of certain cyber operations units of the Russian military intelligence service, the GRU. KAMACITE's campaigns typically focus on reconnaissance of IT and industrial networks within critical infrastructure, mapping access points, and establishing a persistent presence. The group's activities can therefore often be interpreted as preparation for potential future operations against critical infrastructure, with the aim of securing long-term access to OT systems.

ELECTRUM is one of the best-known industrial cyber threat groups in Dragos's threat taxonomy, widely identified in the literature as being linked to the Sandworm/APT44 operations associated with Russian military intelligence. The group has become particularly well-known for its operations against energy infrastructure, during which it employed malicious

code and specialised attack techniques targeting industrial control systems, typically executed on infrastructure previously compromised by KAMACITE. ELECTRUM has been linked, among other things, to attacks against the Ukrainian electricity grid, during which the manipulation of industrial control systems resulted in direct cyber-physical effects and disruption of electricity supply. Apart from these two groups, other active attackers primarily seek to gather as much information as possible about the critical infrastructure they have breached and to prepare for future attacks using this information; destruction is not the objective anywhere else at present, only in Ukraine. (Dragos, Inc., 2026)

6. Lessons regarding digital resilience

There are therefore numerous reasons why cyberattacks targeting the OT systems of critical infrastructure are rarely successful. These systems are extremely heterogeneous and complex – every facility uses different hardware, software and protocols. There is no universal procedure; every attack requires unique reconnaissance and customised code. Attackers must be familiar with the specific equipment, manufacturers, engineering networks and operational processes of the targeted company. Successfully progressing from initial compromise to deliberate manipulation of an industrial process generally requires detailed knowledge of the target technology and operational environment. Ukraine's energy infrastructure inherited substantial technological legacy from the Soviet period. Since 2014, however, Ukraine has progressively reduced its dependence on Russian infrastructure and technology, while strengthening integration with European energy systems. These changes, together with improved network segmentation, modernisation and decentralisation, have altered the technical and operational environment facing Russian attackers.

A further difficulty is that such attacks generally require lengthy preparation. The so-called ICS kill chain involves months of reconnaissance, code development and testing before the attacker is ready for a live sabotage operation. This lengthy process can be carried out during hybrid operations, i.e. in a period of 'neither peace nor war' but carries serious risks in the dynamic environment of war. If the target's configuration changes in the meantime, if the attack is detected prematurely, or if the evolving military situation simply renders it pointless, changes in the target environment may therefore render previously developed capabilities ineffective. This provides a further explanation for why state-linked groups may prioritise Stage 1 activities, including reconnaissance, persistence and pre-positioning, without immediately progressing to destructive Stage 2 operations. In hybrid operations, these covert access points can facilitate successful operations.

Russia has presumably been preparing for a large-scale confrontation since the hybrid operations period began in 2014, but has primarily focused on Stage 1, whilst also 'testing' the implementation of Stage 2 in certain instances. At the very outset of the war, it deployed its pre-prepared cyber weapons in the hope of achieving a swift victory. However, the protracted nature of the conflict made it difficult to carry out further, similarly complex operations. Meanwhile, Ukraine has also significantly strengthened the cyber defences of its critical infrastructure with international assistance, making it increasingly difficult for attackers to infiltrate undetected. It is common for industrial control networks to be physically and, from a network security perspective, isolated (or at least segmented) from the public internet, meaning that attackers must first fight their way through the traditional IT network.

It is also worth noting that the deliberate destruction of critical infrastructure serving the civilian population contravenes international law. Just as a physical attack on a hospital or power station may constitute a war crime, sabotage carried out in cyberspace may also have legal consequences. In recent years, the international community's stance on this issue has become increasingly firm. Depending on the target, effects and circumstances, such operations may violate international humanitarian law and, where the relevant legal elements are met, may

potentially constitute war crimes. (Gisel, Rodenhäuser & Dörmann, 2020) The legal and reputational risks are therefore significant. A country that takes even the slightest account of the rules-based international order would find it difficult to justify, if it openly admitted to it, deliberately depriving millions of civilians of, for example, electricity during the winter. During the war, however, compliance with international law is becoming an increasingly minor constraint, including in the case of cyberattacks.

Finally, it is worth noting that we have not seen similar attacks on the Ukrainian side either. Hacker groups linked to the Ukrainian government or pro-Western groups have so far mostly targeted traditional IT systems in Russia, but there have been no reports of them carrying out cyberattacks causing physical destruction against Russian critical infrastructure. Only in the case of the Fuxnet malware can it be suspected that the Ukrainian secret service used it against a Russian target.(INCIBE, 2024) One reason for this is clearly that they would face the same difficulties that are holding the Russians back. Without in-depth knowledge of a Russian power station or utility network, it is not easy to attack them remotely. Furthermore, Ukraine is striving to maintain international support and the moral high ground, which would be difficult to achieve if it were to strike at civilian targets, even in cyberspace. Under the current circumstances, therefore, cyberattacks against critical infrastructure are feasible and effective only to a limited extent; thus, although the threat remains in principle, it has not yet influenced the decisive course of the war.

7. Findings from “Digital Mohács 3.0” relevant to OT resilience

As described in the methodology, Digital Mohács 3.0 examined the perceptions of Hungarian cyber-defence professionals regarding strategic cyber threats and Hungary’s exposure in cyberspace. For the purposes of the present study, the most relevant findings are those concerning critical infrastructure and industrial systems. These findings provide a complementary expert perspective on whether threats to critical infrastructure are perceived as strategically significant, while the preceding analysis examines the technical and operational conditions under which such threats can produce direct cyber-physical effects.

The questionnaire assessed a total of 33 strategic cyber threats, four of which were directly related to critical infrastructure. According to the original dataset of the Digital Mohács 3.0 survey, 88 of the 101 respondents identified cyberattacks affecting critical infrastructure as a strategic threat requiring government attention. A further 80 respondents identified unsecured infrastructure in critical services and the exploitation of vulnerabilities in industrial IT systems as a strategic threat, while 79 identified distributed denial-of-service (DDoS) attacks against critical services. Overall, cyberattacks against critical infrastructure ranked as the fourth most important strategic cyber threat. The in-depth interviews reinforced this assessment: five of the 13 interviewees included cyberattacks targeting critical infrastructure, or hybrid operations associated with the Russia–Ukraine war more broadly, among the three most significant cyber threats. These detailed frequencies are derived from the original research dataset; the published study presents the findings in aggregated form. (Kovács & Krasznay, 2024)

These findings do not provide direct evidence concerning the technical effectiveness of Russian cyber operations against Ukrainian OT systems. Rather, they demonstrate that cyberattacks against critical infrastructure are perceived as a strategic-level threat by a substantial majority of the surveyed cyber-defence professionals. When considered alongside the technical and case-study analysis presented in the preceding sections, the findings highlight an important distinction between the perceived strategic significance of threats to critical infrastructure and the practical difficulty of achieving sustained cyber-physical effects against OT systems.

8. Conclusions

The findings provide clear answers to the two research questions formulated in the Introduction. With regard to RQ1, the analysis indicates that Russian cyber operations against Ukrainian critical infrastructure have only rarely progressed beyond the conventional IT layer to produce direct cyber-physical effects through specialised OT protocols and control logic. Publicly documented cases demonstrate that such operations are technically feasible, but they remain exceptional compared with the much larger number of incidents affecting conventional IT systems associated with critical infrastructure.

Regarding RQ2, the findings suggest that the operational relevance of cyber operations targeting OT systems varies across different phases of conflict. The conditions for complex Stage 2 operations are most favourable during periods of hybrid confrontation, when attackers can conduct prolonged reconnaissance, establish persistent access and develop capabilities tailored to the target environment. Pre-positioned capabilities may also be employed during the initial phase of armed conflict. During protracted conventional warfare, however, the time, intelligence and technical preparation required for such operations reduce their relative utility, particularly when kinetic means can achieve comparable or greater destructive effects more rapidly.

The working hypothesis is therefore supported by the available evidence: cyber operations targeting OT systems pose their greatest strategic risk during hybrid confrontation and the initial stages of armed conflict, while their relative strategic impact decreases during protracted conventional warfare. This conclusion should be understood within the limitations of publicly available reporting identified in the methodology, particularly because undocumented or classified operations cannot be included in the analysis.

Experiences of the Russia-Ukraine war highlight that the role of cyberspace in modern armed conflicts differs from the picture that frequently appeared in the literature in the early 2010s. Contrary to earlier expectations, cyber operations have not become a strategic weapon capable of replacing traditional military operations. Rather, they appear as supplementary tools, primarily suited to information gathering, disruption, and the temporary hindrance of the adversary's operations. Carrying out cyberattacks against the OT systems of critical infrastructure that cause direct physical impact remains an extremely complex, time-consuming and costly task, which only a few states are capable of carrying out regularly and reliably.

This does not mean, however, that the cyber defence of critical infrastructure can be sidelined. On the contrary: one of the most important lessons of the conflict is that digital resilience depends to a significant extent on the protection of the IT infrastructure and the proper separation of IT-OT systems. Appropriate network segmentation, rapid incident response capabilities, and cyber defence support based on international cooperation can significantly reduce the strategic impact of cyberattacks, even in a wartime environment. Based on the experiences of the conflict under review, therefore, the digital resilience of critical infrastructure is determined not primarily by the specific vulnerabilities of OT systems, but by the security of the IT environment serving them. It is therefore a key issue for future cyber defence strategies that the protection of critical infrastructure should not be treated solely as a problem of industrial systems, but as an integrated IT-OT security challenge, encompassing not only technological issues but also the protection of processes and human resources, thereby facilitating the cyber security convergence of these systems.

This paper was supported by the Bolyai János Research Scholarship of the Hungarian Academy of Sciences.

REFERENCES

Ahlers, C., Graham, M., & O'Meara, K. (2024). Impact of FrostyGoop ICS Malware on Connected OT Systems. *Dragos – Intelligence Brief*. <https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology>

Amri, F. R.-V. L., Daniel dos Santos, Sai Molige, Amine. (2024, October 22). ICS Threats: Malware Targeting OT? It's More Common Than You Think. *Fore Scout*. <https://www.forescout.com/blog/targeting-ot-security-ics-threats-malware/>

Assante, M. J., & Lee, R. M. (2021). *The Industrial Control System Cyber Kill Chain*. SANS Institute. <https://sansorg.egnyte.com/dl/k7gJ2gVBj5>

Beerman, J., Berent, D., Falter, Z., & Bhunia, S. (2023). A Review of Colonial Pipeline Ransomware Attack. *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, 8–15. <https://doi.org/10.1109/CCGridW59191.2023.00017>

Boschetti, N., Gordon, N. G., & Falco, G. (2022, October 24). Space Cybersecurity Lessons Learned from the ViaSat Cyberattack. *ASCEND 2022*. ASCEND 2022. <https://doi.org/10.2514/6.2022-4380>

Dragos, Inc. (2026). *9TH ANNUAL YEAR IN REVIEW | OT/ICS CYBERSECURITY REPORT*. Dragos, Inc. <https://www.dragos.com/blog/dragos-2026-ot-cybersecurity-year-in-review>

Dziwisz, D., & Sajduk, B. (2023). The Russia-Ukraine Conflict from 2014 to 2023 and the Significance of a Strategic Victory in Cyberspace. *Applied Cybersecurity & Internet Governance*, 2(1). <https://doi.org/10.60097/ACIG/162842>

ENISA. (2025). *ENISA Threat Landscape 2025*. ENISA. https://www.enisa.europa.eu/sites/default/files/2025-11/ENISA%20Threat%20Landscape%202025_0.pdf

European Union. (2022a). *DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555>

European Union. (2022b). *Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011*. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>

Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, 102(913), 287–334. <https://doi.org/10.1017/S1816383120000387>

INCIBE. (2024, September 26). *Fuxnet: The malware that paralyzed ICS systems | INCIBE-CERT | INCIBE*. <https://www.incibe.es/en/incibe-cert/blog/fuxnet-malware-paralyzed-ics-systems>

Jolly, J., & Milmo, D. (2025, September 20). Inside the Jaguar Land Rover hack: Stalled smart factories, outsourced cybersecurity and supply chain woes. *The Guardian*. <https://www.theguardian.com/business/2025/sep/20/jaguar-land-rover-hack-factories-cybersecurity-jlr>

Kostyuk, N., & Gartzke, E. (2022). Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review*, 5(3), 113–126. <https://doi.org/10.26153/tsw/42073>

Kostyuk, N., & Zhukov, Y. M. (2019). Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution*, 63(2), 317–347. <https://doi.org/10.1177/0022002717737138>

Kovács, L., & Krasznay, C. (2024). Digitális Mohács 3.0. *Hadtudomány*, 34(3), 40–55. <https://doi.org/10.17047/HADTUD.2024.34.3.40>

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks*. European Parliament. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI\(2022\)733549_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf)

Purchase, E., & Caldwell, F. (2004). Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In S. Ghosh, M. Malek, & E. A. Stohr (Eds), *Guarding Your Business* (pp. 47–64). Kluwer Academic Publishers. https://doi.org/10.1007/0-306-48638-5_4

Salazar, L., Castro, S. R., Lozano, J., Koneru, K., Zambon, E., Huang, B., Baldick, R., Krotofil, M., Rojas, A., & Cardenas, A. A. (2024). A Tale of Two Industroyers: It was the Season of Darkness. *2024 IEEE Symposium on Security and Privacy (SP)*, 312–330. <https://doi.org/10.1109/SP54263.2024.00162>

Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn). Cambridge University Press. <https://doi.org/10.1017/9781316822524>

Selján, G. (2020). The Remarkable 10th Anniversary of Stuxnet: Analytical Summary of the SolarStorm Cyber Espionage Campaign. *Academic and Applied Research in Military and Public Management Science*, 19(3), 85–98. <https://doi.org/10.32565/aarms.2020.3.6>

Sherman, J. (2025). *Confronting Russia's Cyber Power: Reassessing assumptions, sizing up the threat, and building a proactive response*. Atlantic Council. <https://www.atlanticcouncil.org/wp-content/uploads/2025/05/Confronting-Russias-Cyber-Power.pdf>

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to Operational Technology (OT) security* (NIST SP 800-82r3; p. NIST SP 800-82r3). National Institute of Standards and Technology (U.S.). <https://doi.org/10.6028/NIST.SP.800-82r3>

Trachtenberg, M. (2024). *Operation Farewell and the Siberian Pipeline Explosion: A Research Note*. H-Diplo | Robert Jervis International Security Studies Forum, Commentary III-2, 7–20.

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, 64(5), 7–26. <https://doi.org/10.1080/00396338.2022.2126193>