

Industrial Control Systems (ICS) Cyber Targeting in Ukraine

By Brooke Spens

BLUF

The Russian government has engaged in a decade-long cyber campaign to compromise Ukrainian Industrial Control Systems (ICS) enabled through state-backed and pro-Russia hacktivist threat groups as a tool to refine operational capabilities and undermine critical infrastructure resilience of Ukraine and its supporting states.

Key Judgement 1: This report assesses with high confidence a progressive escalation of cyber capabilities targeting the ICS landscape in Ukraine and supporting nations between the invasion of Crimea in 2014 and the full-scale invasion of Ukraine by Russian forces in 2022 by Russian state and non-state actors. Patterns of ICS intrusion demonstrate the accelerating integration of cyberweapons targeting critical infrastructure in Russia's wartime operations as a method of degrading Ukrainian cyber resilience whilst rehearsing operational effectiveness in cyberspace during a time of conflict.

Key Judgment 2: This report assesses with high confidence differential impacts between the malicious industrial control system (ICS) capabilities deployed by Russian state and non-state actors. Nation state actors exhibit sustained attack campaigns of greater technical sophistication, while pro-Russia threat actors ICS attacks can be categorized as opportunistic with limited technical capacity. Varying levels of capability provide insights into the Russian Federation's strategic objectives in attempts to normalize ICS compromise as an enabling mechanism of cyber warfare.

Introduction

On February 24, 2026, the war in Ukraine marked its fourth anniversary since Russia's full-scale invasion. The four years since the invasion have shown rapid kinetic innovation on the battlefield, but more quietly a second battle has been waging in the background. Ukraine serves as a testing ground for Russia to deploy and fine tune cyber capabilities in a time of war while eroding the Ukrainian defensive and ability to retaliate. One category of cyber-attack warranting heightened concern is those targeting industrial processes. Industrial control systems (ICS) ability to control physical systems means ICS attacks pose a significant threat to critical infrastructure.¹

This intelligence report aims to analyze the use of ICS compromise as a form of cyberwarfare in the Russo-Ukrainian war beginning in the initial stages of conflict in 2014. This analysis is structured through two key judgements containing the following assessments. This report

¹ "What Are the Differences Between OT, ICS, & SCADA Security," accessed February 26, 2026, <https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security>.

assesses with high confidence an escalation in ICS as a mechanism of cyberwarfare from 2014 to the present day by both Russian nation state and non-state actors. Anecdotally, this report assesses with medium confidence a low occurrence of coordination between kinetic Russian military attacks and ICS cyberattacks against Ukraine. Moreover, this intelligence product discusses patterns of OT intrusion by pro-Russia hacktivist groups outside of Ukraine against countries providing material support to the Ukrainian war effort. Secondly, this report assesses with high confidence differential impacts between offensive ICS capabilities deployed by Russian nation state and non-state actors. Russian nation state actors utilize greater technical sophistication with nonuniform impacts, while pro-Russia actors ICS attacks are often of limited technical capacity and opportunistic in their implementation.

Analytic Methodology

The analytic technique of Analysis of Competing Hypotheses (ACH) will be utilized in this intelligence estimate. ACH is a method that seeks to identify alternative interpretations of data with the ability to disconfirm existing hypotheses.² ACH is an effective method for controversial topics requiring the evaluation of large amounts of data.³ The ACH framework provides greater awareness and consideration of all plausible alternative hypotheses of available evidence. ICS targeting in the Russo-Ukrainian war situates well within this framework provided the mass amount of data and variation between sources.

ICS Cyber Operations in the Russo-Ukrainian War		
Consistent (C), Inconsistent (I), Neutral (N)		
Evidence	H1: Russian Nation State ICS Targeting	H2: Russian Non-State ICS Targeting
Repeated intrusions into Ukrainian and supporters' ICS	C	C
ICS targeting across sectors of critical infrastructure	C	C
Cyber operations coinciding with Russian kinetic attacks	C	N
High sophistication of ICS targeting methodology	C	I
Opportunistic ICS targeting methodology	I	C

² A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis: (587102011-001), n.d., <https://doi.org/10.1037/e587102011-001>.

³ Ibid.

Objective of undermining Ukrainian cyber resilience	C	N
---	---	---

Furthermore, this product is based on Open-Source Intelligence (OSINT) sources including social media, federal advisories, threat intelligence reports, and vulnerability databases. Information from a wide range of publicly available data has been synthesized to contextualize specific cyberattacks, technical schematics, and threat group profiles relevant to industrial control system (ICS) targeting in the Russo-Ukrainian war. Specific sources employed in this analysis include Telegram channels documenting the behavior of pro-Russia hackers, private threat intelligence firm reports, governmental resources such as reports by the Computer Emergency Response Team of Ukraine (CERT-UA), MITRE and National Institute of Standards and Technology (NIST) vulnerability databases, and advisories by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and its counterparts. The aggregation of third-party data illustrates the landscape of cyberattacks against critical infrastructure by pro-Russia hackers and Russian nation-state actors to provide valuable insights into the unique characteristics of ICS as an attack vector for the purpose of cyberwarfare. The scope of this report is limited to attacks actively targeting or related to industrial control systems. Russian cyber operations deployed against Ukraine extend far beyond those relevant to industrial control processes; however, the intent of this report is to provide a detailed analytical product on ICS attacks perpetrated in alignment with a pro-Russian agenda.

Background

2014-2022:

Ukraine has been at the forefront of European conflict, in both the kinetic and cyber domain, throughout the twenty-first century. The history of Russian aggression towards Ukraine predates the full-scale invasion of Ukraine on February 24th, 2022, by almost a decade.⁴ In 2014, Russia illegally annexed the Crimean Peninsula of Ukraine, an action commonly regarded as a renewal in hostilities continuing to the present day.⁵ Following Russia’s annexation of Crimea, cyberattacks against Ukrainian critical infrastructure occurred alongside the physical infringements on Ukraine’s sovereign boundaries.⁶ Early well-known attacks include the disruption of Ukrainian power grids in the winter of 2015 and 2016 caused by malware known as BlackEnergy3.⁷ The first attack occurring in December 2015, was attributed to Russian nation-state actor and advanced persistent threat (APT) group Sandworm and resulted in power outages leaving around

⁴ Brian E. Humphreys, *Attacks on Ukraine’s Electric Grid: Insights for U.S. Infrastructure Security and Resilience* (Library of Congress, 2024), <https://www.congress.gov/crs-product/R48067>.

⁵ Ibid.

⁶ Ibid.

⁷ CISA, “Ongoing Sophisticated Malware Campaign Compromising ICS (Update E),” July 22, 2021, <https://www.cisa.gov/news-events/ics-alerts/ics-alert-14-281-01e>.

225,000 Ukrainians without power for several hours after disrupting the power distribution of three regional providers.⁸ The 2015 disruption of Ukrainian critical infrastructure is known as the first recorded successful cyberattack against a power grid.⁹ A second significant cyber-attack targeting Ukrainian power occurred in 2016 using malware known as Industroyer (or CrashOverride) perpetrated by the same threat actors leveraging techniques expanded upon since Sandworm's initial targeting of Ukrainian power a year prior.¹⁰ The 2016 attack blacked out sections of Kyiv for an hour.¹¹ The use of BlackEnergy and Industroyer malware against Ukraine are two of the most notable cyber operations given the physical impacts of the malware prior to the intensification of the Russo-Ukrainian war in 2022.

What is an ICS Attack?

The Ukrainian power grid attacks in 2015 and 2016 are both examples of an industrial control system (ICS) attack. An industrial control system (ICS) manages the hardware and software of industrial processes, playing an integral role in power supply, manufacturing, and other critical infrastructure processes.¹² One example of an ICS is Supervisory Control and Data Acquisition (SCADA) systems which provide real-time analysis and management of industrial processes. ICS technology is part of the broader Operational Technology (OT) landscape, the category of tools used to monitor and control the physical environment. ICS technology was once isolated and thus protected from many cyber threats, however, the merging of Information Technology (IT) with OT to provide enhanced automation capabilities in recent decades has introduced greater threats to the systems responsible for managing sensitive industrial processes.¹³ An attack on an ICS can compromise and, in certain cases, permanently damage the integrity of the system's operation. Disruption in ICS function can result in indefinite industrial system downtime, financial loss, and threats to individuals' safety.¹⁴ The 2015 and 2016 attacks against Ukrainian critical infrastructure are not the first occurrence of ICS compromise. The malicious computer worm Stuxnet gained notoriety in 2010 after becoming the first malware designed to attack a specific ICS.¹⁵ The worm targeted Iran's nuclear program by infecting the Natanz nuclear facility to manipulate the centrifuges critical to the uranium enrichment process before rapidly proliferating around the globe.¹⁶ No group claimed responsibility for the attack, but it is

⁸ CISA, "Cyber-Attack Against Ukrainian Critical Infrastructure," July 20, 2021, <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.

⁹ Andy Greenberg, *This Is the New Leader of Russia's Infamous Sandworm Hacking Unit | WI*, March 15, 2023, <https://www.wired.com/story/russia-gru-sandworm-serebriakov/>.

¹⁰ MITRE, "2016 Ukraine Electric Power Attack," April 16, 2025, <https://attack.mitre.org/campaigns/C0025/>.

¹¹ Dragos, "Electrum Threat Group," 2024, <https://www.dragos.com/threat/electrum>. Ibid.

¹² "What Are the Differences Between OT, ICS, & SCADA Security."

¹³ Ibid.

¹⁴ Ibid.

¹⁵ Paul K. Kerr, John W. Rollins, and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (Congressional Research Service, 2010), <https://www.congress.gov/crs-product/R41524>.

¹⁶ Ibid.

widely considered to be a joint effort between the United States and Israel. Research by the Congressional Research Service described Stuxnet as a “harbinger of an emerging warfare capability”, a fitting forewarning of the cyber weapons that would later emerge in the Russo-Ukrainian conflict.¹⁷

Threat Actors:

Mapping the threat actors relevant to ICS targeting in Ukraine is a complex process given the covert nature of cyber operations, attribution difficulties, overlapping tactics, and inconsistent nomenclature among reporting. (provide context to previous sentence) This report will primarily focus on two categories of threat actors: Russian nation-state actors and non-state actors, specifically pro-Russia hacktivists. For the purpose of this writing, Russian nation-state actors can be defined as cyber actors directly part of the organizational structure of the Kremlin. In the case of Russia, these prevalent actors can be classified as advanced persistent threats (APTs). Pro-Russia hacktivists are hacking groups who do not appear to have direct connections to the Russian government as a part of a formal organizational structure, but demonstrate ideological support. Hacktivists are individuals or groups whose hacking is used to further social or political causes. Throughout the conflict, hacktivist groups reports indicate some pro-Russia groups have demonstrated closeness the Russian government and received financial support directly from the Russian Federation.¹⁸ A Joint Cybersecurity Advisory issued by U.S. federal agencies in December 2025 noted an increase in hacktivist groups supporting the Russian agenda since 2022.¹⁹ Cyber threat intelligence firm Cyble reported in their 2025 annual threat report, that “in 2025, hacktivism evolved into a globally coordinated threat, closely tracking geopolitical flashpoints.”²⁰ Subsequent analysis will document significant Russia-aligned threat actors in the Ukrainian cyber landscape.

Sandworm: Sandworm is a prolific advanced persistent threat (APT) responsible for a substantial amount of high-profile cyberattacks across a variety of attack vectors. Its operations have been cataloged under the names of Unit 74455, APT44, FROZENBARENTS, Voodoo Bear, and Iridium, among others.^{21, 22} Despite being responsible for some of the most debilitating cyberattacks ever, the organization remains veiled in secrecy.²³ Sandworm has facilitated detrimental cyberattacks around the globe and across vectors operating as a highly effective unit

¹⁷ Ibid.

¹⁸ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure* (CISA, 2025), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a>.

¹⁹ Ibid. Ibid.

²⁰ *Annual Threat Landscape Report 2025* (Cyble, 2025), <https://cyble.com/resources/research-reports/annual-threat-landscape-report-2025/>.

²¹ Greenberg, *This Is the New Leader of Russia’s Infamous Sandworm Hacking Unit | WI*.

²² Gabby Roncone et al., *Unearthing APT44: Russia’s Notorious Cyber Sabotage Unit Sandworm*, April 17, 2024, <https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm>.

²³ Greenberg, *This Is the New Leader of Russia’s Infamous Sandworm Hacking Unit | WI*.

in Russia's military intelligence agency, the GRU.²⁴ Sandworm is the group responsible for the 2015 and 2016 cyberattacks against Ukrainian power grids, the release of the notorious worm NotPetya, and disruptions during the Pyeongchang Olympics in 2018, to name a subset of Sandworm's known operations prior to 2022.²⁵ Sandworm's activities have persisted in recent years deploying novel ICS attacks against Ukrainian critical infrastructure that will be detailed in subsequent sections. Sandworm centers its operations on Ukraine, but it conducts campaigns globally and unrestricted to critical infrastructure as evidenced by disruptions like the NotPetya attacks in 2017.²⁶ Reports by Google assert "To date, no other Russian government-backed cyber group has played a more central role in shaping and supporting Russia's military campaign."²⁷ The same reporting finds that Sandworm supports a range of capabilities to further Russian military and political objectives, from espionage to psychological influence.²⁸ Sandworm's structure differs from the standard of threat actors specializing in the narrow execution of capabilities.²⁹ The history and operational scope of Sandworm make it an acute, high-impact threat to Ukraine in the ICS space and beyond.³⁰

APT 28: APT 28 is a capable nation-state threat actor targeting industries across aerospace, defense, and energy.³¹ APT 28, also known by the aliases Fancy Bear, TA422, Strontium, Forest Blizzard, and Pawn Storm, has been in operation since as early as 2008.^{32, 33} The advanced persistent threat group is believed to be a component of the GRU.³⁴ Along with sharing parent leadership organizations, historically prominent individuals within the organization have overlapped with the fellow GRU unit Sandworm.³⁵ The current commander of Sandworm is Evgenii Serebriakov, a former member of APT 28 before serving as the leader of Sandworm.³⁶ APT 28 has targeted entities across Europe and North America since March 2023.³⁷ One instance of APT 28 operations, are observations by researchers noting 10,000 phishing emails attributed

²⁴ Andy Greenberg, *How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter*, July 23, 2024, <https://www.wired.com/story/russia-ukraine-frostygoop-malware-heating-utility/>.

²⁵ Greenberg, *This Is the New Leader of Russia's Infamous Sandworm Hacking Unit* | WI.

²⁶ Ibid.

²⁷ Roncone et al., *Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm*.

²⁸ Ibid.

²⁹ Ibid.

³⁰ Ibid.

³¹ CrowdStrike, "Who Is FANCY BEAR (APT28)?," February 12, 2019, <https://www.crowdstrike.com/en-us/blog/who-is-fancy-bear/>.

³² Ibid.

³³ "APT and Financial Attacks on Industrial Organizations in H2 2023," April 2, 2024, <https://ics-cert.kaspersky.com/publications/reports/2024/04/02/apt-and-financial-attacks-on-industrial-organizations-in-h2-2023/>.

³⁴ Roncone et al., *Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm*.

³⁵ Greenberg, *This Is the New Leader of Russia's Infamous Sandworm Hacking Unit* | WI.

³⁶ Ibid.

³⁷ Greg Lesnewich and Crista Giering, "Espionage TA422's Dedicated Exploitation Loop—the Same Week After Week," December 5, 2023, <https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-week-after-week>.

to APT 28 sent across government, higher education, and manufacturing to gain remote access to systems by leveraging a vulnerability in Microsoft Outlook (CVE-2023-23397).³⁸ Aside from phishing emails designed to steal sensitive information, APT 28 has made a recent foray into attacks designed for OT intrusion.³⁹ APT 28 reportedly used phishing attack to infect energy infrastructure in Ukraine with malware.⁴⁰ A focal point of Sandworm's operational mission is the targeting of critical infrastructure, while APT 28 has recently shifted into partaking in campaigns impacting industrial environments.⁴¹

Cyber Army of Russia: The Cyber Army of Russia Reborn (CARR), or People's Cyber Army of Russia, is a pro-Russia hacktivist group with roots tied to the GRU in the spring of 2022.⁴² The extent of GRU's support of the hacktivists is unclear. Traces of their recruitment and cyber activities are associated on the CyberArmyofRussia_Reborn Telegram channel beginning in 2022.⁴³ The Telegram postings spread pro-Russian disinformation, attack information, and in some cases, leaked information stolen by Sandworm.⁴⁴ According to the U.S. Justice Department, CARR had over 75,000 followers on Telegram, and exceeded 100 members supporting their operations, including some juveniles.⁴⁵ For more than two years, CARR marketed itself as a group working to counter anti-Russian ideology in support of Russia's agenda by conducting cyberattacks such as large-scale distributed denial of service (DDoS) attacks against Ukraine and countries supporting Ukraine.⁴⁶

***Insert image of telegram postings**

A year into operations, CARR began targeting ICS operations in Ukraine and globally against countries offering their support.⁴⁷ CARR has claimed responsibility for the compromise of operational technology involving wastewater facilities in Europe,⁴⁸ drinking water systems, two dairy farms, and a meat processing facility in the U.S..⁴⁹ While CARR's DDoS efforts are well-documented against Ukraine, aside from their existence there are little known details on the cases of CARR targeting OT in Ukraine. In 2024, the U.S. sanctioned Yuliya Vladimirovna Pankratova and Denis Olegovich Degtyarenko due to their involvement in CARR operations

³⁸ Ibid.

³⁹ "APT and Financial Attacks on Industrial Organizations in H2 2023."

⁴⁰ Ibid.

⁴¹ Roncone et al., *Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm*.

⁴² *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure*.

⁴³ SOCRadar, "Dark Web Profile: Cyber Army of Russia Reborn," August 13, 2024,

<https://socradar.io/blog/dark-web-profile-cyber-army-of-russia-reborn/>.

⁴⁴ Ibid.

⁴⁵ Tom Uren, *Dumb and Dumber: Russia's State-Backed "Hacktivists,"* December 19, 2025,

<https://www.lawfaremedia.org/article/dumb-and-dumber--russia's-state-backed-'hacktivists'>.

⁴⁶ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure*.

⁴⁷ Ibid.

⁴⁸ Ibid.

⁴⁹ Uren, *Dumb and Dumber: Russia's State-Backed "Hacktivists."*

targeting the U.S..⁵⁰ In late 2024, CARR disassociated from the GRU following frustration with GRU support and funding to join with pro-Russia hackers in creating a new pro-Russia hacker group.⁵¹

NoName057(16): NoName057(16), abbreviated as NoName, is a pro-Russia hacker group stemming from the Center for the Study and Network Monitoring of the Youth Environment (CISM) created by Russian President Vladimir Putin.⁵² CISM contributed heavily to NoName by having “CISM employees [pay] for NoName's infrastructure, [develop] and [customize] its proprietary DDoS tool, [administer] its Telegram channels, and [select] DDoS targets.”⁵³ Similar to CARR, NoName communications heavily occur on Telegram channels.⁵⁴ NoName is primarily concentrated on DDoS attacks using its proprietary tool DDoSia, but the group collaborated with CARR to conduct intrusions into OT systems in the U.S..⁵⁵ Cyberattacks have been coordinated across hacker groups, among them NoName, to support a pro-Russian agenda.⁵⁶

Z-Pentest: Z-Pentest is one recent addition to pro-Russia hackers targeting Ukraine and those supporting Ukraine. Comprised of CARR and NoName, Z-Pentest was created in September 2024 as an offshoot organization of pro-Russia hackers with less direct GRU involvement.⁵⁷ While CARR and NoName share direct links tracing back to the Russian government, the formation Z-Pentest is the result of dissatisfaction by CARR and NoName administrators with the GRU.⁵⁸ The group's existence is a sign of a fracture in the relationship between the Russian government and pro-Russian actors traditionally closely involved with the government. Given the newness of Z-Pentest as a group, documented attacks are more limited than their counterparts, however, they have been linked to attacks in Europe and against NATO members.⁵⁹ Patterns of Z-Pentest operations include the tendency to target OT systems through “hack and leak” techniques for the purpose of gaining media attention to further Z-Pentest's ideological messaging.⁶⁰ Despite publicly aligning with NoName and CARR, Z-Pentest's main focus on OT attacks differs from other prominent pro-Russia hackers relying on DDoS tactics.⁶¹

⁵⁰ “Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn,” July 19, 2024, <https://home.treasury.gov/news/press-releases/jy2473>.

⁵¹ *Pro-Russia Hackers Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

⁵² Uren, *Dumb and Dumber: Russia's State-Backed “Hackers.”*

⁵³ Ibid.

⁵⁴ Ibid.

⁵⁵ *Pro-Russia Hackers Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

⁵⁶ SOCRadar, “Dark Web Profile: Cyber Army of Russia Reborn.”

⁵⁷ *Pro-Russia Hackers Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

⁵⁸ Ibid.

⁵⁹ *Annual Threat Landscape Report 2025.* Ibid. Click or tap here to enter text.

⁶⁰ *Pro-Russia Hackers Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

⁶¹ Ibid.

Sector 16: In addition to the emergence of Z-Pentest is that of Sector 16. Sector 16 is a pro-Russia hacktivist group sharing many characteristics with preceding hacktivist groups.⁶² Sector 16 broadcasts their operations on Telegram channels, collaborates with other pro-Russia hacktivist groups such as Z-Pentest, and propagates a pro-Russian agenda online.⁶³ Similar to Z-Pentest, Sector 16 differentiates itself as primarily targeting ICS; Sector 16 centers on attacking and exposing Human Machine Interfaces (HMI), a type of ICS interface used to monitor and control industrial processes.⁶⁴

Dark Engine (Infrastructure Destruction Squad): True to its name, the Russian-linked group Dark Engine, or Infrastructure Destruction Squad, focuses on attacking critical infrastructure. Dark Engine's tactics are comparable to Sector 16 as they aim to compromise ICS's, particularly HMI and SCADA systems.⁶⁵ Threat intelligence firm Cyble tracked Dark Engine to 26 ICS attacks in the second quarter of 2025 in Asia, Latin America, and Europe.⁶⁶ The Dark Engine group has operated in alignment with Russian cyber strategic objectives.⁶⁷

Key Judgement 1: This report assesses with high confidence progressive escalation of cyber operations targeting the ICS landscape in Ukraine between the invasion of Crimea in 2014 and the full-scale invasion of Ukraine by Russian forces in 2022 by Russian state and non-state actors. Patterns of ICS intrusion demonstrate the accelerating integration of cyberweapons targeting critical infrastructure in Russia's wartime operations as a method of degrading Ukrainian cyber resilience whilst rehearsing operational effectiveness in cyberspace during a time of conflict.

The first Key Judgement asserts with high confidence an escalation of targeting against industrial control systems (ICS) proliferated by Russian-linked actors. An analysis of the proliferation of critical infrastructure attacks can be classified into two categories: those perpetrated by Russian nation state actors and those conducted by non-state actors, otherwise referred to as pro-Russia hacktivist groups. This report assesses with high confidence the amplification of ICS attacks against Ukraine in both categories since the rise in hostilities between Russia and Ukraine. Patterns of escalation discussed demonstrate an increase in ICS targeting being deployed as a tool to damage critical infrastructure and weaken Ukrainian resilience in the Russo-Ukrainian war.

⁶² Ibid.

⁶³ Ibid.

⁶⁴ *Annual Threat Landscape Report 2025*.

⁶⁵ Ibid.

⁶⁶ Cyble, *Hacktivist Attacks On Critical Infrastructure Surge In 2025*, July 11, 2025, <https://cyble.com/blog/hacktivist-attacks-on-critical-infrastructure/>.

⁶⁷ Ibid.

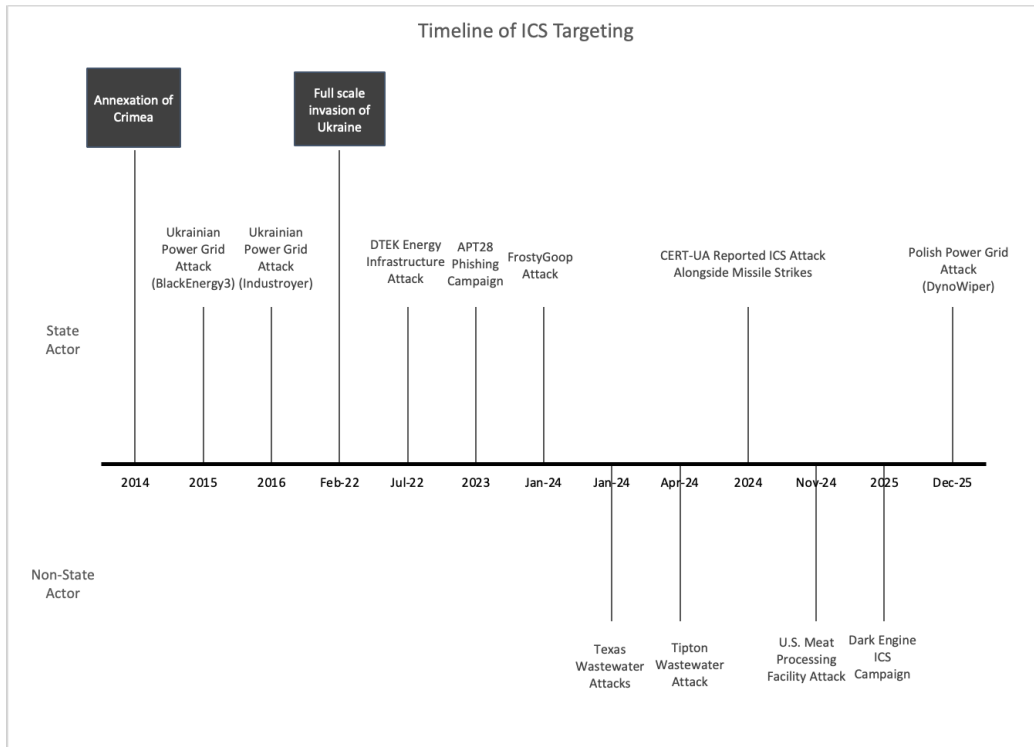


Figure 1: Timeline of ICS targeting by state and non-state actors assessed in this report

Escalation of ICS Targeting by Russian Nation State Actors

First, APTs linked to nation state actors demonstrate the shifting approach to ICS targeting by the Russian military. Russian APTs, or nation state actors, have served as versatile mechanism of influence able to facilitate intelligence collection and disruption campaigns against Ukraine and countries supporting Ukraine.⁶⁸ APTs acting on behalf of the Russian Federation have engaged in deliberate targeting aimed at disrupting industrial control systems (ICS) in Ukraine and beyond to purposefully inhibit actions that oppose the Russian agenda.⁶⁹ This is supported by an analysis of two Russian-linked APTs, Sandworm and APT28, threat intelligence reports, and recent real-world cases of ICS damage in Ukraine. The Russian Federation has continually prioritized the development of offensive cyber capabilities in the OT environment beginning around the 2015 and 2016 Ukrainian electric grids attacks and continuing to present day.⁷⁰ Techniques displayed in a recent 2022 cyberattack involving SCADA ICS environments in Ukrainian critical infrastructure executed by Sandworm led Google to write “techniques leveraged during the incident suggest a growing maturity of Russia’s offensive OT arsenal, including an ability to recognize novel OT threat vectors, develop new capabilities, and leverage

⁶⁸ Roncone et al., *Unearthing APT44: Russia’s Notorious Cyber Sabotage Unit Sandworm*.

⁶⁹ Ibid.

⁷⁰ Ken Proska et al., *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*, November 9, 2023, <https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/>.

different types of OT infrastructure to execute attacks.”⁷¹ According to Google, the presence of Living-off-the-Land (LotL) tactics recorded during OT operations were “more lightweight and generic than those observed in prior OT incidents,” an indication of pressure during wartime cyber operations to scale the amount of ICS operations being carried out.⁷² The escalation of cyberattacks in the Russo-Ukrainian conflict has provided Russia with a playing field the finetune their operational capabilities against ICS targets. The refinement process beginning a decade ago has resulted in ICS cyberweapons that are streamlined to communicate and attempt controlling OT systems.⁷³ The changes in the sustained targeting of ICS indicate the testing of operational capabilities to sabotage the Ukrainian offensive through critical infrastructure disruption. This reporting on early operations of the Russian APT Sandworm supports the assessment by this intelligence product pointing to the intensification of ICS targeting by the Russian government to undermine Ukrainian cyber resilience. Incidents of prominent ICS compromise in Ukraine further exemplify patterns of ICS targeting by Russian threat actors.

Case Study - FrostyGoop

On January 22, 2024, Russian-linked hackers disrupted heating for over 48 hours in the western city of Lviv, Ukraine in the dead of winter as part of their continuing attack on Ukraine. The attack is a first-of-its-kind ICS attack against heating infrastructure allowing the direct manipulation of energy infrastructure that disrupted heating services powering over 600 apartment buildings. The malware used in the attack has been named FrostyGoop by cybersecurity firm Dragos, specifically designed to gain access to and control industrial processes.⁷⁴ The attack was a show of technical prowess. Hackers gained access to months prior to the attack in April 2023 by exploiting an internet-facing router known as a MikroTik router, allowing attackers to set up a remote VPN connection into the network that was calling home to the Kremlin.⁷⁵ Following initial access, attackers carried out commands sent through Modbus. Modbus serves as a client/server message protocol designed for Programmable Logic Controllers (PLCs) that outlines the process used by a controller to request and gain access to another device.⁷⁶ The widespread use of Modbus in industrial settings makes FrostyGoop a concerning development in ICS-specific malware with potential impacts globally. Dragos assesses with medium confidence that FrostyGoop malware sent Modbus commands to ENCO controllers, controllers used to monitor temperature, pressure and insulation sensors that are commonly used in heating substations and water systems.⁷⁷ In the January attack, the Russian-linked perpetrators

⁷¹ Ibid.

⁷² Ibid.

⁷³ Ibid.

⁷⁴ Mark (Magpie) Graham, Carolyn Ahlers, and Kyle O’Meara, *Impact of FrostyGoop ICS Malware on Connected OT Systems* (2024), <https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology>.

⁷⁵ Greenberg, *How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter*.

⁷⁶ Graham, Ahlers, and O’Meara, *Impact of FrostyGoop ICS Malware on Connected OT Systems*.

⁷⁷ Ibid.

conducted a downgrade attack against the network to reduce system monitoring capabilities and further facilitate disruption of the heating utilities. Improper network segmentation allowed commands to be sent directly to the heating system controllers causing the targeted system to malfunction.⁷⁸ The malware caused the system to produce inaccurate measurements resulting in control systems erroneously running cool water through the buildings pipes in place of the hot water integral to the central heating service. The effect was 600 municipal buildings left without proper heating for two days.⁷⁹ The impact was felt by the Ukrainians left without heating in the winter and amplified by harsh sub-zero conditions. While the attack is a technical demonstration targeting the Ukrainian heating utilities, the ripple effect extends beyond the buildings without heat to the impact the Ukrainian psyche.⁸⁰ The case of FrostyGoop represents serious risks to the safety of civilians due to Russian-linked targeting of ICS attacks against Ukrainian energy infrastructure. Dragos did not attribute the attack to a specific Russian-linked actor, but the Computer Emergency Response Team of Ukraine (CERT-UA) assessed the attack as part of a broader campaign by Sandworm against 20 critical infrastructure facilities.⁸¹ FrostyGoop provides two inflection points for the cyber conflict being waged in Ukraine: the real-world damage critical infrastructure cyberattacks can inflict, and the evolving Russian arsenal of ICS cyberweapons capable of being a key player in the war on Ukraine.

Escalation of ICS Targeting by Pro-Russia Hacktivists

The second category within the initial Key Judgement relates to cyber targeting behaviors by pro-Russia hacktivists against Ukraine. This report assesses with high confidence an increase in the presence of pro-Russia hacktivists in recent years, and the emphasis of ICS intrusion attempts used as attack vectors deployed by pro-Russian hacktivists in Ukraine and beyond. Additionally, patterns of pro-Russia hacktivism beyond Ukraine's borders will be discussed.

2025 saw record sightings of hacktivism worldwide. On a global scale, threat reporting by Cyble indicated a 51% increase in hacktivism sightings from 0.7 million in 2024 to 1.06 million in 2025.⁸² Cyble's Annual Threat Report stated, "Hacktivism has evolved into a persistent, conflict-driven threat, capable of rapid mobilization, cross-regional coordination, and the material disruption of critical infrastructure."⁸³ Researchers have observed a distinct shift in hacktivism

⁷⁸ Ibid.

⁷⁹ Greenberg, *How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter*.

⁸⁰ Ibid.

⁸¹ Pawel Knapczyk and Nikita Kazymirskyi, "The Russia-Ukraine Cyber War Part 3: Attacks on Telecom and Critical Infrastructure," March 5, 2026, <https://www.levelblue.com/blogs/spiderlabs-blog/the-russia-ukraine-cyber-war-part-3-attacks-on-telecom-and-critical-infrastructure#:~:text=Additionally%2C%20the%20Ukrainian%20Government%20Computer,inaccurate%20measurements%20and%20system%20failures.>

⁸² *Annual Threat Landscape Report 2025*.

⁸³ Ibid.

from its ideological roots to a key factor in contested cyberspace.⁸⁴ Scholars theorize that the reemergence of global conflict in 2022, “legitimized their actions and the narratives they projected publicly, recasting them from protestors to combatants in national or ideological conflicts.”⁸⁵ The escalation in hacktivism is not restricted to pro-Russia hacktivists, in fact pro-Ukrainian hacktivist groups targeted Russian power plants in 2024, among other widespread hacktivism activities spanning global conflict.⁸⁶ One significant observation is patterns of straying from traditional methods of hacktivism such as DDoS and website defacements as attack vectors to the escalation of ICS targeting.⁸⁷ The intensification of hacktivism has been accompanied by a shift to the targeting of the services civilians rely on for daily needs, many of which are operated used ICS.⁸⁸ ICS targeting has historically been reserved to heavily resourced groups akin to nation state actors, but recent hacktivist groups display a higher level of involvement with governments and a higher willingness to target OT than traditionally reported.⁸⁹ The rise of pro-Russia hacktivism is one piece an expansive surge in hacktivism as a tool in global conflict.⁹⁰

Of reported hacktivism sightings in 2025, the majority of hacktivism occurred in Europe with 38% of recorded sightings taking place in Europe with pro-Russia hacktivists named as main drivers.⁹¹ While the actual effectiveness of ICS targeting methods by pro-Russia hacktivist groups will be dissected in the subsequent key judgement, this discussion emphasizes with high confidence in an overall increase in the existence of pro-Russia hacktivist groups and the related intensification of ICS intrusion attempts by these groups against Ukrainian and Ukrainian’s supporters critical infrastructure. A U.S. Joint Cybersecurity Advisory observed an increase in pro-Russia hacktivist groups since Russia’s full-scale invasion of Ukraine tied to those outside of the government highly supportive of Russian national interests.⁹² Mandiant noted high rates of hacktivism mobilization targeting OT due the Russo-Ukrainian war by both pro-Ukraine hacktivists and pro-Russia hacktivist.⁹³

Alongside the shift from pro-Russia hacktivists deploying cyberattacks to include the targeting of OT/ICS, a second distinct characteristic of pro-Russia hacktivist behavior is patterns of targeting

⁸⁴ Richard Derbyshire et al., “From Protest to Power Plant: Interpreting the Role of Escalatory Hacktivism in Cyber Conflict,” *arXiv*, ahead of print, September 5, 2025, <https://doi.org/10.48550/arxiv.2509.05104>.

⁸⁵ Ibid.

⁸⁶ Ibid.

⁸⁷ Ibid.

⁸⁸ Ibid.

⁸⁹ Ibid.

⁹⁰ Daniel Kapellmann Zafra, Keith Lunden, and Nathan Brubaker, “We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems,” March 22, 2023, <https://cloud.google.com/blog/topics/threat-intelligence/hacktivists-targeting-ot-systems>.

⁹¹ *Annual Threat Landscape Report 2025*.

⁹² *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure*.

⁹³ Zafra, Lunden, and Brubaker, “We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems.”

countries outside of Ukraine supporting the Ukrainian war effort. The U.S. CISA and partnering U.S. agencies have documented extensive cyberattacks against U.S. critical infrastructure in recent years.⁹⁴ Annual cybersecurity threat reports indicate pro-Russia hacktivists targeting ICS in EU and NATO members states, significant supporters of Ukraine following Russia's invasion.⁹⁵ A target comparison between Russian APTs to pro-Russian hacktivist targeting the provides an indication of the differing strategic objectives guiding the operations. As discussed previously, pro-Russia hacktivist threat actors have been linked to or claim responsibility for ICS disruptions outside of Ukraine including: the Cyber Army of Russia Reborn (CARR), NoName, Z-Pentest, Sector 16, and Dark Engine. Pro-Russia hacktivists groups have been connected to ICS activity in North America, Europe, Asia, and Latin America.⁹⁶

Case Study – Targeting Beyond Ukraine's Borders

One example of pro-Russian hacktivist targeting ICS outside of Ukraine is the campaign by the Cyber Army of Russia Reborn (CARR) against U.S. assets. In January 2024, CARR claimed responsibility on their Telegram channel for causing the malfunction of wastewater management systems in the U.S..⁹⁷ CARR breached systems in Abernathy and Muleshoe, Texas allowing them to alter the human-machine interfaces (HMIs) and cause an overflow of water storage tanks resulting in the loss of tens of thousands of gallons of water.⁹⁸ CARR has been linked to the malfunction of control systems causing the overflow of water in multiple states.⁹⁹ Beyond the January 2024 attack in Texas, CARR has targeted drinking water, wastewater, food, and energy sectors across the U.S..¹⁰⁰ CARR tampered with the HMIs of two U.S. dairy farms,¹⁰¹ the SCADA system of a U.S. energy company,¹⁰² and even a car wash in Florida.¹⁰³ An incident of significance due to the impact of the ICS compromise is the attack of a Los Angeles meat processing facility. The November 2024 breach spoiled thousands of pounds of meat and caused an ammonia leak in the facility that led to an evacuation of the premises.¹⁰⁴ Two Russian cybercriminals, Yuliya Vladimirovna Pankratova and Denis Olegovich Degtyarenko were sanctioned for their efforts as part of CARR to target U.S. critical infrastructure.¹⁰⁵ Victoria Eduardovna Dubranova joined the two at the end of last year as an individual charged by the

⁹⁴ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

⁹⁵ *Annual Threat Landscape Report 2025.*

⁹⁶ Cyble, *Hacktivists Attacks On Critical Infrastructure Surge In 2025.*

⁹⁷ SOCRadar, "Dark Web Profile: Cyber Army of Russia Reborn."

⁹⁸ Uren, *Dumb and Dumber: Russia's State-Backed "Hacktivists."*

⁹⁹ Greg Otto, "US Charges Hacker Tied to Russian Groups That Targeted Water Systems and Meat Plants," December 10, 2025, <https://cyberscoop.com/us-charges-russian-backed-hacker-critical-infrastructure-attacks-carr-noname05716/>.

¹⁰⁰ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

¹⁰¹ *Ibid.*

¹⁰² "Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn."

¹⁰³ Uren, *Dumb and Dumber: Russia's State-Backed "Hacktivists."*

¹⁰⁴ Otto, "US Charges Hacker Tied to Russian Groups That Targeted Water Systems and Meat Plants."

¹⁰⁵ "Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn."

U.S. government for involvement with CARR resulting in damage to U.S. system.¹⁰⁶ While the nature of targets may seem trivial, the documented ICS cyberattacks aimed at U.S. critical infrastructure serve as a case study in the overall escalation of ICS targeting by pro-Russia hackers against Ukraine and its supporters.

Kinetic and Cyber Attack Overlap

Since the escalation between Russia and Ukraine into the full-scale invasion of Ukraine in 2022, there have been differing hypotheses on level of coordination between cyberattacks and kinetic attacks occurring in Ukraine. Analysis of ICS targeting is an area of particular interest when compared to kinetic attacks as the goal of ICS attacks is primarily to create a disruption in the physical world through the compromise of industrial processes. This analysis finds with medium confidence that the coordination between kinetic and cyberattacks is becoming an increasingly common strategy used by the Russian Federation. The case of kinetic and cyber operations overlap can be understood as a subset of the broader escalation of ICS targeting in the conflict, with the caveat that it captures one aspect of a wider trend. Analysts familiar with the relationship between kinetic and cyberwarfare assert that developments in Ukraine's ability to intercept missiles has driven Russia to offensive cyber tools.¹⁰⁷ Several cases display coordination between kinetic and cyberattacks. Reports note Sandworm cyber operations have disrupted OT coinciding with missile strikes in the same region as the originating cyberattack.¹⁰⁸ Mandiant reporting similarly claimed the coordination of cyberattacks against critical infrastructure with conventional military strikes.¹⁰⁹ One specific case of coinciding attacks includes the July 2022 attack against the energy provider DTEK Group where a Russian cyberattack coincided with missiles targeting its power stations.¹¹⁰ Finally, CERT-UA claimed that ICS targeting of Ukrainian critical infrastructure was used to "enhance the effect of missile strikes on Ukrainian infrastructure facilities in the spring of 2024."¹¹¹ The synthesis of reported cases demonstrates that ICS cyber-attacks occurring in coordination with kinetic tactics is becoming an increasingly common strategy deployed by the Russian military through the duration of the war.

A progressive escalation of ICS targeting since the full-scale invasion of Ukraine is represented through the maturation of Russian state actors and rise of pro-Russia hacking aimed at damaging Ukrainian critical infrastructure. The extensive attacks by APTs and hackers have given Russian-aligned actors a playing field to finetune their operational capabilities. Moreover, the deliberate ICS targeting of countries providing material support to Ukraine by pro-Russia

¹⁰⁶ Otto, "US Charges Hacker Tied to Russian Groups That Targeted Water Systems and Meat Plants."

¹⁰⁷ Greenberg, *How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter*.

¹⁰⁸ Proskia et al., *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*.

¹⁰⁹ Roncone et al., *Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm*.

¹¹⁰ Humphreys, *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*.

¹¹¹ CERT-UA, *UAC-0133 (Sandworm) Plans for Cyber Sabotage on Almost 20 Critical Infrastructure Facilities in Ukraine* (2024), <https://cert.gov.ua/article/6278706>.

hacktivists points to attempts by Russian-linked threat actors to sabotage the ability of Ukraine to retaliate against Russian aggression. Taken together, reported ICS cyberattacks facilitated by both state and non-state threat actors illustrate a comprehensive image of Russia's campaign to weaken the Ukrainian offensive by attacking the systems required for the daily lives of Ukrainians and the citizens of those supporting Ukraine.

Key Judgment 2: This report assesses with high confidence differential impacts between the malicious industrial control system (ICS) capabilities deployed by Russian state and non-state actors. Nation state actors exhibit sustained attack campaigns of greater technical sophistication, while pro-Russia actors ICS attacks can be categorized as opportunistic with limited technical capacity. Varying levels of capability provide insights into the Russian Federation's strategic objectives in attempts to normalize ICS compromise as an enabling mechanism of cyber warfare.

The renewal of Russo-Ukrainian conflict has marked an unprecedented mobilization of malicious cyber actors across the board.¹¹² The previous Key Judgement discussed a progressive escalation of cyber conflict targeting the ICS landscape in Ukraine concurrently by state and non-state actors. The next component to this discussion is the effectiveness of those cyberattacks. This Key Judgement addresses the question: assuming the escalation of Russian-linked groups utilizing ICS attack mechanisms, how effective are Russian state and non-state actors in achieving their desired outcome? In this intelligence product, a "successful" ICS intrusion can be defined as a threat actors presumed intent matching the result; for the case of Russian state and non-state actors, a successful ICS intrusion means a threat group was able to breach a critical infrastructure system and leverage a capability where the result mirrored the intended level of impact and severity. Additionally, this discussion outlines the implications of differential impacts by threat actor group presented by the normalization of ICS compromise as a tool wielded by the Russian Federation in a time of conflict.

Russian Nation State Actors Outcomes

This report assesses differential impacts between the malicious industrial control system (ICS) capabilities deployed by Russian state and non-state actors with Russian state actors deploying more technically complex cyberweapons aimed at serving as an instrument of Russian control over Ukraine and its supporters. In a comprehensive analysis of the Russia and Ukrainian conflict, there is the worthwhile distinction between cyberattacks conducted and the level of impact or effective ability to achieve the assumed objective.¹¹³ This assessment finds greater technical sophistication of attacks conducted by the Russian Federation, but inconsistent outcomes between cyberattacks.

¹¹² Zafra, Lunden, and Brubaker, "We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems."

¹¹³ Derbyshire et al., "From Protest to Power Plant: Interpreting the Role of Escalatory Hacktivism in Cyber Conflict."

Several technical reports detail the increasingly complex publicly available tactics, techniques, and procedures (TTPs) guiding Russian nation state actors. 2016 attacks against the Ukrainian electric grid displayed advanced methods including the automation of ICS manipulations within the malware itself, a step up from the 2015 attacks allowing greater scalability for attackers.¹¹⁴ As noted previously, Russian APTs have continued to expand their offensive ICS arsenal since the escalation in hostilities through lightweight and scalable pieces of malware embedded with Living-off-the-Land (LotL) tactics.¹¹⁵ These tactics enable prolonged presence in targeted systems but display a lower number of disruptive components per attack such as the removal wiper activities alongside ICS manipulation.¹¹⁶ These modern capabilities are technically complex and streamlined to for simple proliferation by Russian nation-state actors. Although recent attacks lack certain disruptive traits, Russian APTs remain formidable threats to ICS security in Ukraine with Russian APT Sandworm being “responsible for nearly all of the disruptive and destructive operations against Ukraine over the past decade.”¹¹⁷ However, the evolution in Russia’s approach since 2022 and the shift to speed of operations may compromise the effectiveness by straining the resources and time needed to execute individual cyberattacks. Despite a consensus among government and industry on the growing technical complexity of ICS targeting, the effectiveness of ICS compromise implementation conducted by Russian nation state threat actors remains nonuniform across targets. Much of the inconsistent implementation can be attributed to barriers associated with ICS targeting to successfully gain access to an ICS system and manipulate it in alignment with the intruder's intent.¹¹⁸ These challenges persist even against a capable threat actor. Research outlines “inherent limitations” to the use of ICS targeting in a time of war due to the “extensive reconnaissance and industry-specific knowledge to successfully execute.”¹¹⁹ Non-ICS targets are typically more standardized adding an additional layer of difficulty to successfully carrying out an attack against ICS.¹²⁰ The strategic decision to streamline targeting during wartime may have resulted in lower effectiveness of Russian ICS attacks by APTs.

Case Study – DynoWiper Attack on Polish Power Grids

One example of an ICS attack with high technical sophistication but lacking results is late December 2025 cyber intrusions attributed to Sandworm due to overlap of past methodology.¹²¹ On December 29th and 30th 2025, Poland’s power grid was subject to wiper malware known as

¹¹⁴ Humphreys, *Attacks on Ukraine’s Electric Grid: Insights for U.S. Infrastructure Security and Resilience*.

¹¹⁵ Proska et al., *Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology*.

¹¹⁶ Ibid.

¹¹⁷ Roncone et al., *Unearthing APT44: Russia’s Notorious Cyber Sabotage Unit Sandworm*.

¹¹⁸ Humphreys, *Attacks on Ukraine’s Electric Grid: Insights for U.S. Infrastructure Security and Resilience*.

¹¹⁹ Ibid.

¹²⁰ Ibid.

¹²¹ Mathew J. Schwartz, “Wiper Malware Targeting Poland’s Power Grid Tied to Moscow,” January 26, 2026, <https://www.govinfosecurity.com/wiper-malware-targeting-polands-power-grid-tied-to-moscow-a-30596>.

DynoWiper aimed at causing a power outage for half a million Polish citizens.¹²² While two Polish power plants and an energy management system were breached in the attack, no disruptions took place.¹²³ Provided the recency and sensitivity of the breach, limited details have been released on the technical schematics of the attack, but the wiper malware used in the attack is said to have been designed to erase computers resulting in a service outage and overwritten files in IT systems essential to the outage recovery, effectively taking critical systems off the grid and hindering efforts to restore service.¹²⁴ The attempted attack against Polish energy infrastructure is a first of its kind attack against a NATO alliance country, a significant escalation in targeting by Sandworm.¹²⁵ The attack notably coincided with the tenth anniversary of the 2015 attacks attributed to the same threat group against the Ukrainian electric grid that left a quarter of a million Ukrainians without power.¹²⁶ The case of DynoWiper in Poland illustrates an audacious and technically sophisticated attempt to retaliate in the cyber domain against countries supporting Ukraine. Moreover, it demonstrates that sustained ICS disruption campaigns facilitated by the Russian Federation to undermine the critical infrastructure necessary to the Ukrainian offensive have varying, unpredictable impacts with documented cases of threat actors falling short of their presumed objective. Actions undertaken by Russian state actors provide an overview of the Kremlin's strategic push to use ICS targeting as an influential force in cyberwarfare.

Pro-Russia Hacktivism Outcomes

This report assesses with high confidence a lower overall level of successful ICS intrusion by pro-Russia hacktivism groups due to a simpler technical sophistication and the redundancy of tactics, techniques, and procedures (TTPs) by hacktivism groups. Two factors support this Key Judgement assessing the lower ability of pro-Russia hacktivism to achieve their intended outcome by leveraging their available technical capabilities: the baseline technical ability of pro-Russia hacktivism groups and the commonplace alliances between pro-Russia hacktivism groups. First, the technical sophistication of pro-Russia hacktivism is lacking when compared to heavily resourced groups like APTs.¹²⁷ Pro-Russia hacktivism transition from common hacktivism tactics like DDoS and website defacement to ICS targeting does mark an upgrade in the technical complexity of attempted attacks.¹²⁸ However, the ability of pro-Russia hacktivism groups to effectively render these ICS attacks is questionable. The December advisory by CISA and other U.S. agencies termed pro-Russia hacktivism is “opportunistic,” meaning groups “leverage

¹²² Kim Zetter, “Cyberattack Targeting Poland’s Energy Grid Used a Wiper,” January 23, 2026, <https://www.zetter-zeroday.com/cyberattack-targeting-polands-energy-grid-used-a-wiper/>.

¹²³ Schwartz, “Wiper Malware Targeting Poland’s Power Grid Tied to Moscow.”

¹²⁴ Zetter, “Cyberattack Targeting Poland’s Energy Grid Used a Wiper.”

¹²⁵ Schwartz, “Wiper Malware Targeting Poland’s Power Grid Tied to Moscow.”

¹²⁶ Zetter, “Cyberattack Targeting Poland’s Energy Grid Used a Wiper.”

¹²⁷ Derbyshire et al., “From Protest to Power Plant: Interpreting the Role of Escalatory Hacktivism in Cyber Conflict.”

¹²⁸ SOCRadar, “Dark Web Profile: Cyber Army of Russia Reborn.”

superficial criteria, such as victim availability and existing vulnerabilities, rather than focusing on strategically significant entities.”¹²⁹ A claim supported by the broad targeting of assets as seemingly insignificant as a car wash and water fountain.¹³⁰ As for the attack methodology, pro-Russia hacktivist groups primarily target external facing human machine interface (HMI) devices known as virtual network computing (VNC)-connected HMI devices.¹³¹ VNC connections are typically used to facilitate remote system access in critical infrastructure settings, but are vulnerable to attack due to their outward connection. An example of an attack flow a hacker gaining initial access to in these scenarios can be depicted as follows: scan for vulnerable devices containing open VNC ports, execute password brute force attack software, utilize the VNC software to gain access to hosts, confirm connection and brute force password if necessary, gain initial access to the HMI device where the attack will be executed further.¹³² The tactics, techniques, and procedures (TTPs) were described by organizations in the U.S. government as unsophisticated, “inexpensive to execute, and easy to replicate.”^{133, 134} The detailed methodology has raised comparisons to attackers simply flipping switches without the know-how to understand the impact on the environment they aim to disrupt.¹³⁵ Pro-Russia hacktivists are observed haphazardly applying this attack methodology to inflict physical harm to a broad array of systems without having the technical expertise to estimate the impact.¹³⁶ In reference to the impact of disruption attempts, researchers note a “gap between hacktivist intent and achieved results.”¹³⁷ This assessment is further underpinned by patterns of pro-Russian hacktivism encompassing a variety of sectors and targets as outlined above. The motivation of Pro-Russia hacktivism lies more so in the desire for notoriety to propagate their pro-Russia messaging than the ability to effectively exploit high-value systems. This is emphasized through pro-Russian hackers active presence on platforms such as Telegram where hackers routinely claim responsibility for ICS attacks while exaggerating or misrepresenting the impact of their operations.¹³⁸ While pro-Russia hacktivists have yet to cause physical injury, the haphazard implementation of their operational tactics warrants apprehension. The second factor relevant to the lower overall effectiveness of pro-Russia hacktivism is the high level of association between threat groups. As detailed in depth previously, CARR and NoName are both the result of Kremlin initiatives and routinely collaborate in operations.¹³⁹ The creation of Z-Pentest mirrors

¹²⁹ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

¹³⁰ Uren, *Dumb and Dumber: Russia’s State-Backed “Hacktivists.”*

¹³¹ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

¹³² *Ibid.*

¹³³ “Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn.”

¹³⁴ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

¹³⁵ Uren, *Dumb and Dumber: Russia’s State-Backed “Hacktivists.”*

¹³⁶ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

¹³⁷ Derbyshire et al., “From Protest to Power Plant: Interpreting the Role of Escalatory Hacktivism in Cyber Conflict.”

¹³⁸ SOCRadar, “Dark Web Profile: Cyber Army of Russia Reborn.”

¹³⁹ Uren, *Dumb and Dumber: Russia’s State-Backed “Hacktivists.”*

this as it was created by individuals from both CARR and NoName.¹⁴⁰ Alongside similar origins, pro-Russia hackers jointly claim responsibility for ICS intrusions, deliberately misconstruing the severity and prevalence of cyberattacks.¹⁴¹ Substantial overlap between non-state actors is further exemplified through collaboration between groups such as Sector 16, Z-Pentest, CARR and NoName. Much of the collaboration between groups is visible through public Telegram channels. Actors such as CARR use Telegram to coordinate with other pro-Russia hackers, share TTPs, and amplify pro-Russia messaging to propagate their ideals.¹⁴² Cyble reported that these groups share “aligned messaging, coordinated timing, and shared targeting priorities, suggesting deliberate collaboration supporting Russian strategic cyber objectives.”¹⁴³ The interconnectedness of threat groups has been intentionally leveraged by pro-Russia hackers to enable the modular and rapid deployment of ICS attacks at an unprecedented scale. Traditionally, ICS attacks have been limited to high resourced groups akin to nation-states, but the widespread availability of ICS tactics on open-source platforms and among groups has lowered the barrier of entry for hackers with low technical knowledge.¹⁴⁴ While semantic similarities within technical methodology can accelerate proliferation, the quality of the attacks proliferated remain unsophisticated and opportunistic in application. Despite differential impacts, widespread targeting of ICS by non-state actors indicates the broader intentions to normalize ICS compromise as a tool of interstate warfare critical to undermining the resilience of critical infrastructure and aid the Russian war effort.

Case Study – Tipton Wastewater Treatment Center

One example of pro-Russia hackers conducting an attack against industrial control systems utilizing opportunistic methodology paired with limited technical capacity is the targeting of the Tipton Wastewater Treatment Plant in Indiana. The pro-Russia hacker group CARR posted on Telegram in April 2024 claiming responsibility for cyberattacks against U.S. wastewater systems.¹⁴⁵ The post showed the alleged intrusion of into the critical infrastructure providing electric power, water, and wastewater treatment to the 5,000 person town of Tipton.¹⁴⁶ Officials conceded to the targeting of ICS facilities, but reported that they remained operational through the duration of the attacks.¹⁴⁷ There is inconsistent reporting on the realized impacts of the cyberattack. Town officials stated that the facility had not been compromised, but other

¹⁴⁰ *Pro-Russia Hackers Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

¹⁴¹ *Ibid.*

¹⁴² SOCRadar, “Dark Web Profile: Cyber Army of Russia Reborn.”

¹⁴³ Cyble, *Hackers Attacks On Critical Infrastructure Surge In 2025.*

¹⁴⁴ *Pro-Russia Hackers Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

¹⁴⁵ Anna Riberio, “Hackers Target Tipton Municipal Utilities Wastewater Treatment Plant, Prompting Federal Investigation Prompting Federal Investigation - Industrial Cyber,” April 23, 2024, https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-tipton-municipal-utilities-wastewater-treatment-plant-prompting-federal-investigation/?utm_source=chatgpt.com.

¹⁴⁶ *Ibid.*

¹⁴⁷ Daryna Antoniuk, “Russian Hackers Claim Cyberattack on Indiana Water Plant,” April 23, 2024, https://therecord.media/russia-hackers-cyberattack-tipton-indiana?utm_source=chatgpt.com.

estimations of the Tipton ICS impact publicly reported the overflow of a singular tank at the Tipton Municipal Utilities.¹⁴⁸ The Telegram posts claiming responsibility for the Tipton Municipal Utilities attack followed their January 2024 posts taking credit for the malfunction of water facilities in Texas.¹⁴⁹ The ICS targeting of facilities in Abernathy and Muleshoe successfully resulted in the overflow of water equivalent to an Olympic-size pool; however, considering the range of possible consequences, the incident portrays a relatively low severity outcome.¹⁵⁰ Telegram posts crediting CARR with the cyberattack match techniques outlined by the U.S. Government as patterns of pro-Russia hacktivists frequently exaggerating or misrepresenting their capabilities and ability to undermine critical infrastructure.¹⁵¹ The ICS targeting of the Tipton Wastewater Treatment Plant in a small Indiana town reflects limited impacts against low-level targets chosen arbitrarily by a pro-Russia threat group. Although not directly attributed to the Russian state, the actions of pro-Russia hacktivists provide insight into the objectives of the pro-Russia agenda through their well-known collaboration to push nationalistic ideals and normalize ICS targeting as a tool of modern warfare. Tipton Municipal Utilities is a recent case study in the opportunistic and comparatively limited technical sophistication of cyberattacks conducted by non-state actors that erode critical infrastructure and situate ICS targeting as a key player in modern cyber conflict.

Conclusion

The targeting of ICSs has been a significant factor in the Russo-Ukrainian war beginning more than a decade ago and escalating to the present day. The broader OT landscape is inherently complex with exceedingly damaging impacts for those threat actors who do succeed in compromising the technology that underlays essential critical infrastructure services. This assessment depicts a cyber landscape increasingly saturated with cyberattacks targeting ICS components like HMIs and SCADA systems critical to the daily operation of industrial processes relied on by billions of people worldwide. These trends have extended onto the battlefield with ICS cyber operations playing an influential role in the Russo-Ukrainian conflict in recent years with key players including both state and non-state actors.

In conclusion, this report assesses with high confidence progressive escalation of ICS targeting spanning a decade from the invasion of Crimea in 2014 to the full-scale invasion of Ukraine in 2022. This report finds the intensification of cyber operations being leveraged against critical infrastructure is conducted by both Russian state and non-state threat actors. ICS targeting has been a key player in contested cyberspace between Russia and Ukraine as the means to degrade Ukrainian cyber resilience while finetuning wartime operational capabilities. This assessment utilizes cases of Ukrainian power grid compromise, ICS targeting beyond Ukraine's borders, and

¹⁴⁸ Ibid.

¹⁴⁹ Ibid.

¹⁵⁰ Uren, *Dumb and Dumber: Russia's State-Backed "Hacktivists."*

¹⁵¹ *Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure.*

coordination between kinetic and cyberattacks to outline Russia's strategic approach to ICS compromise in the war with Ukraine and gain an understanding of Russia as a threat actor in cyberspace. Secondly, this report assesses with high confidence differential impacts between comparable offensive cyber capabilities deployed by Russian nation state and non-state threat actors. State actors deploy technically sophisticated attacks with inconsistent results exemplified through specific cases of streamlined ICS targeting methodology resulting in nonuniform impacts against ICS facilities. Non-state actors leverage ICS attacks in a haphazard, opportunistic manner. This report assesses a lower overall level of successful ICS intrusion by pro-Russia hacktivists groups due to a simpler technical sophistication and the redundancy of tactics, techniques, and procedures (TTPs) by hacktivist groups. This report constructs threat actor profiles and cases of documented attacks to facilitate an analysis of the presumed intent, reported outcomes of cyberattacks, and effectiveness of threat groups. The differing capabilities provide insights into the Russian Federation's push to normalize ICS compromise as a instrument of cyber dominance to further support the Russian war effort. Collectively, the findings of this report highlight the growing use of ICS targeting as a component of modern warfare and an indication of how state and non-state actors employ cyber capabilities in today's conflicts and beyond.

A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis: (587102011-001). n.d. <https://doi.org/10.1037/e587102011-001>.

Annual Threat Landscape Report 2025. Cyble, 2025.
<https://cyble.com/resources/research-reports/annual-threat-landscape-report-2025/>.

Antoniuk, Daryna. "Russian Hackers Claim Cyberattack on Indiana Water Plant." April 23, 2024. https://therecord.media/russia-hackers-cyberattack-tipton-indiana?utm_source=chatgpt.com.

"APT and Financial Attacks on Industrial Organizations in H2 2023." April 2, 2024.
<https://ics-cert.kaspersky.com/publications/reports/2024/04/02/apt-and-financial-attacks-on-industrial-organizations-in-h2-2023/>.

- CERT-UA. *UAC-0133 (Sandworm) Plans for Cyber Sabotage on Almost 20 Critical Infrastructure Facilities in Ukraine*. 2024. <https://cert.gov.ua/article/6278706>.
- CISA. "Cyber-Attack Against Ukrainian Critical Infrastructure." July 20, 2021. <https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01>.
- . "Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)." July 22, 2021. <https://www.cisa.gov/news-events/ics-alerts/ics-alert-14-281-01e>.
- CrowdStrike. "Who Is FANCY BEAR (APT28)?" February 12, 2019. <https://www.crowdstrike.com/en-us/blog/who-is-fancy-bear/>.
- Cyble. *Hacktivists Attacks On Critical Infrastructure Surge In 2025*. July 11, 2025. <https://cyble.com/blog/hacktivists-attacks-on-critical-infrastructure/>.
- Derbyshire, Richard, Diana Selck-Paulsson, Charl van der Walt, and Joe Burton. "From Protest to Power Plant: Interpreting the Role of Escalatory Hactivism in Cyber Conflict." *arXiv*, ahead of print, September 5, 2025. <https://doi.org/10.48550/arxiv.2509.05104>.
- Dragos. "Electrum Threat Group." 2024. <https://www.dragos.com/threat/electrum>.
- Graham, Mark (Magpie), Carolyn Ahlers, and Kyle O'Meara. *Impact of FrostyGoop ICS Malware on Connected OT Systems*. 2024. <https://hub.dragos.com/report/frostygoop-ics-malware-impacting-operational-technology>.
- Greenberg, Andy. *How Russia-Linked Malware Cut Heat to 600 Ukrainian Buildings in Deep Winter*. July 23, 2024. <https://www.wired.com/story/russia-ukraine-frostygoop-malware-heating-utility/>.
- . *This Is the New Leader of Russia's Infamous Sandworm Hacking Unit | WI*. March 15, 2023. <https://www.wired.com/story/russia-gru-sandworm-serebriakov/>.
- Humphreys, Brian E. *Attacks on Ukraine's Electric Grid: Insights for U.S. Infrastructure Security and Resilience*. Library of Congress, 2024. <https://www.congress.gov/crs-product/R48067>.
- Kerr, Paul K., John W. Rollins, and Catherine A. Theohary. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*. Congressional Research Service, 2010. <https://www.congress.gov/crs-product/R41524>.

Knapczyk, Pawel, and Nikita Kazymirskyi. "The Russia-Ukraine Cyber War Part 3: Attacks on Telecom and Critical Infrastructure." March 5, 2026.
<https://www.levelblue.com/blogs/spiderlabs-blog/the-russia-ukraine-cyber-war-part-3-attacks-on-telecom-and-critical-infrastructure#:~:text=Additionally%2C%20the%20Ukrainian%20Government%20Computer,inaccurate%20measurements%20and%20system%20failures.>

Lesnewich, Greg, and Crista Giering. "Espionage TA422's Dedicated Exploitation Loop—the Same Week After Week." December 5, 2023.
<https://www.proofpoint.com/us/blog/threat-insight/ta422s-dedicated-exploitation-loop-same-week-after-week.>

MITRE. "2016 Ukraine Electric Power Attack." April 16, 2025.
[https://attack.mitre.org/campaigns/C0025/.](https://attack.mitre.org/campaigns/C0025/)

Otto, Greg. "US Charges Hacker Tied to Russian Groups That Targeted Water Systems and Meat Plants." December 10, 2025. [https://cyberscoop.com/us-charges-russian-backed-hacker-critical-infrastructure-attacks-carr-noname05716/.](https://cyberscoop.com/us-charges-russian-backed-hacker-critical-infrastructure-attacks-carr-noname05716/)

Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure. CISA, 2025. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a.>

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.* November 9, 2023.
[https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/.](https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/)

Riberio, Anna. "Hackers Target Tipton Municipal Utilities Wastewater Treatment Plant, Prompting Federal Investigation Prompting Federal Investigation - Industrial Cyber." April 23, 2024. https://industrialcyber.co/utilities-energy-power-water-waste/hackers-target-tipton-municipal-utilities-wastewater-treatment-plant-prompting-federal-investigation/?utm_source=chatgpt.com.

Roncione, Gabby, Dan Black, John Wolfram, Tyler McLellan, Nick Simonian, Ryan Hall, Anton Prokopenkov, et al. *Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm.* April 17, 2024. <https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm.>

Schwartz, Mathew J. “Wiper Malware Targeting Poland’s Power Grid Tied to Moscow.” January 26, 2026. <https://www.govinfosecurity.com/wiper-malware-targeting-polands-power-grid-tied-to-moscow-a-30596>.

SOCRadar. “Dark Web Profile: Cyber Army of Russia Reborn.” August 13, 2024. <https://socradar.io/blog/dark-web-profile-cyber-army-of-russia-reborn/>.

“Treasury Sanctions Leader and Primary Member of the Cyber Army of Russia Reborn.” July 19, 2024. <https://home.treasury.gov/news/press-releases/jy2473>.

Uren, Tom. *Dumb and Dumber: Russia’s State-Backed “Hacktivists.”* December 19, 2025. <https://www.lawfaremedia.org/article/dumb-and-dumber--russia’s-state-backed-’hacktivists’>.

“What Are the Differences Between OT, ICS, & SCADA Security.” Accessed February 26, 2026. <https://www.paloaltonetworks.com/cyberpedia/ot-vs-ics-vs-scada-security>.

Zafra, Daniel Kapellmann, Keith Lunden, and Nathan Brubaker. “We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems.” March 22, 2023. <https://cloud.google.com/blog/topics/threat-intelligence/hacktivists-targeting-ot-systems>.

Zetter, Kim. “Cyberattack Targeting Poland’s Energy Grid Used a Wiper.” January 23, 2026. <https://www.zetter-zeroday.com/cyberattack-targeting-polands-energy-grid-used-a-wiper/>.