

Troy Bannister

CYSE 426

Dr. Russell Korb

30 July 2026

CYSE 426: Cyber War Project Paper:

Militarized Cyberspace in the Russia-Ukraine War

Introduction

Going into this research project, I thought of cyberwarfare as a single category that included destructive hacking, social media manipulation, propaganda, and other hostile online actions. The Russia-Ukraine War seemed to support this view, since Russia attacked networks and used digital platforms and disinformation to weaken Ukraine and its allies. However, the course readings and other sources made it clear that these activities are different. Technical cyber operations focus on exploiting or disrupting computer systems, while information warfare aims to influence perceptions, credibility, morale, and decision-making. These are not the same, but cyber operations can support a larger information campaign, and the reverse is also true. Russian strategy places technical and psychological actions within the broader concept of information confrontation, although cyber operations and information warfare remain distinct (Hakala & Melnychuk, 2021; Whyte, 2020).

In this paper, based on the course readings, I define “cyberspace” as militarized when states, defense forces, intelligence groups, or private partners intentionally use, attack, or defend digital systems to achieve military and political goals during war. This definition does not require cyber operations to cause physical destruction or decide the outcome of a war on their own. Instead, it focuses on how much a state integrates digital tools into its regular military efforts (Kello, 2013; Pedersen & Jacobsen, 2024; Zarembo et al., 2025). By this standard, the Russia-Ukraine War is highly militarized. While Ukraine relied on cyber defense, strong infrastructure, foreign technical assistance, and civic digital networks to continue its wartime operations, Russia used destructive malware and disrupted communications to support its invasion (Bateman, 2022; Pedersen & Jacobsen, 2024; Zarembo et al., 2025). Both countries also used digital communication to influence audiences and maintain support at home and abroad (Hogue, 2026;

Whyte, 2020). All of this depended on conventional forces, reliable infrastructure, and credibility and pointed to cyberspace as being a major, contested area of support, not an independent warfare area or one that will decide outcomes on its own.

Measuring ‘ Militarization ’

This paper looks at a few selected cases instead of covering every cyber incident from the conflict. The cases are grouped into three categories that show different ways cyber activity was used: Russia’s offensive hacking, Ukraine’s defense and online resilience, and information warfare through digital means like social media campaigns. The technical cases are analyzed using Pedersen and Jacobsen’s TECI model, which examines an operation’s **Target**, **Effect**, **Complexity**, and **Integration** with conventional forces. This model helps evaluate how cyber operations are used in war and whether they achieve tactical, operational, or strategic utility (Pedersen & Jacobsen, 2024).

Tactical utility means an operation helps a small unit with a specific task or battle. Operational utility means the operation makes a difference across a larger campaign or theater, not just one fight. Strategic utility means the operation affects a country’s resources, power, or its ability and will to keep fighting (Pedersen & Jacobsen, 2024). These distinctions help us see when a cyber incident is militarily relevant, without assuming that every local or temporary technical success is a strategic victory.

Information warfare needs different criteria. Bots, targeted content, compromised platforms, views, and shares can show that a campaign happened and reached people, but not that anyone was persuaded. That requires different evidence (Geissler et al., 2023; Hogue, 2026;

Whyte, 2020). Keeping these measures separate prevents reach or technical access from being mistaken for real influence.

Contrasting Academic Assessments

Kello claims that the usual line between peace and war can make us overlook what cyber operations do. Even without taking the form of more conventional fighting, cyber means can inflict economic, social, political, and even physical destruction. Kello admits that “The cyber revolution—as far as we can tell—has not fundamentally changed warfighting” (Kello, 2013, p. 22). Still, he believes this does not mean cyber operations lack strategic importance. If we only focus on state-on-state violence, we might miss nonmilitary threats or the impact of non-state actors. Kello is not saying cyber operations have replaced conventional war, but that their importance to security goes beyond the battlefield and should be considered both in and out of war.

Gartzke points out a key issue. Cyber operations do have an effect on usual operations like military coordination, communications and can disrupt infrastructure. If conventional forces or other tools cannot take advantage of the disruption, the operation likely will not cause lasting damage or force political concessions. Gartzke says that “cyberwar remains adjunct to terrestrial force unless some way is found for cyberattacks to permanently alter the balance of power” (Gartzke, 2013, p. 60). This means cyber activity can be deeply integrated into warfare, but it does not replace conventional force.

In his portion of a published exchange with Kello, Lindsay makes a similar criticism: advanced technology does not decide political or military outcomes by itself. Things like doctrine, preparations, countermeasures, and the situation that a capability is used can matter just

as much as the tech itself. As Lindsay writes, “there are no technological silver bullets or vouchsafed doctrines for their use” (Lindsay & Kello, 2014, p. 183). While Lindsay wasn’t defending Gartzke directly, the position lines up with Gartzke’s main point because they both reject the idea that just being able to cause digital harm automatically means it produces lasting strategic value.

Maschmeyer explains part of this problem with what he calls the subversive trilemma. Cyber operations depend on breaking into systems controlled by an adversary and that creates tradeoffs between speed, intensity, and control. If you move faster, you lose time for observation and testing. If you expand or get more aggressive, you are more likely to get caught or cause unintended consequences. Getting greater control takes more preparation, which can make the operation too slow to be useful, especially if it is needed urgently. In his words, “a gain in one variable tends to produce losses across the other two variables” (Maschmeyer, 2021, p. 55). Looking at Russian operations against Ukraine from 2014 to 2017, he found these limitations kept getting in the way of any real strategic payoff (Maschmeyer, 2021).

Pedersen and Jacobsen describe Russia’s 2022 cyber operations as having limited military impact because they caused little physical damage, relied on expensive and complicated actions, and were rarely coordinated with conventional forces. They point out two main opportunities: repeated attacks on governments and infrastructure can add up to significant costs, and operations prepared before the war may give early tactical advantages (Pedersen & Jacobsen, 2024). This shows that while cyberspace can be used for military purposes, cyber operations do not usually decide the outcome of a war.

Russian Offensive Cyber Operations

WhisperGate shows both cyber operations being militarized, and their limits. Microsoft found the malware on Ukrainian systems on January 13, 2022. Affected systems belonged to government, nonprofit, and IT organizations. WhisperGate showed a ransom note, but Microsoft found no mechanism to pay the ransom or recover the data and assessed that its purpose was to destroy data and make devices inoperable instead of making money (Microsoft Digital Security Unit et al., 2022). A later advisory from several countries connected WhisperGate to Russia's GRU Unit 29155 (Cybersecurity and Infrastructure Security Agency [CISA], 2024).

WhisperGate appeared to be a planned attack with evidence of preparation, access, intent to destroy, and a link to Russian military intelligence. Public reporting does not establish that WhisperGate caused lasting disruption to Ukrainian military or government operations. Bateman notes Russia's cyber attacks typically do less damage than physical hits but still redirect Ukraine's resources (Bateman, 2022). WhisperGate was militarized in its purpose and sponsorship, but the available evidence does not show that it produced lasting operational or strategic effects.

The KA-SAT attack on Viasat gives stronger evidence that cyber operations were coordinated with the physical invasion. It started on February 24, 2022, and knocked out consumer satellite internet for several thousand customers in Ukraine and tens of thousands more across Europe. Viasat said the attackers got in by exploiting a misconfigured VPN device, made their way into a trusted management network, and used legitimate admin commands to overwrite data on residential modems, which knocked them offline. Viasat also said its own directly managed government and mobility customers weren't affected (Viasat, 2022).

The EU said Russia was behind the operation, which took place about an hour before the invasion and disrupted communications for public authorities, businesses, and users in Ukraine

and some EU countries (Council of the European Union, 2022). Pedersen and Jacobsen use this opening-stage attack to show how advance planning can sometimes overcome the difficulty of coordinating cyber and conventional forces. (Pedersen & Jacobsen, 2024). With its timing, target, and invasion match, Viasat is the clearest case of a cyber operation tied to conventional fighting.

The real battlefield impact is unclear. Ukrainian commanders noted major communications issues near Kyiv, citing Russian jamming, not just the Viasat incident. Bateman suggests the outage contributed to broader disruption, but its effect blends with electronic warfare (Bateman, 2022). While Viasat caused disruption, public evidence does not establish a lasting command impact or major strategic shift.

Ukrainian Cyber Defense and Digital Resilience

The Industroyer2 attack illustrates the importance of defense. In April 2022, Sandworm attempted to deploy malware on Ukrainian high-voltage substations, using Industroyer2 and wiper programs for Windows, Linux, and Solaris. The attack, scheduled for April 8, was thwarted when ESET and CERT-UA detected and removed the malware before it caused power disruption (ESET Research, 2022).

The attackers did get into a sensitive infrastructure environment and had malware in place that could interact with industrial equipment. Still, the physical effect they were aiming for did not happen. Maschmeyer's argument is that getting discovered lets defenders shut down access and take advantage of how hard it is for attackers to hold onto control once they're spotted, and Pedersen and Jacobsen find that operations aiming for complicated physical effects tend to have a high chance of failing (Maschmeyer, 2021; Pedersen & Jacobsen, 2024). This shows that cyber defense itself is part of militarization: stopping a wartime cyber effect protected

infrastructure that mattered for both civilian life and the overall war effort. Ukraine's resilience wasn't because of one tool or one organization. Bateman points to a mix of factors: decentralized ownership and design of the telecom system, engineers who could adapt on the fly, cybersecurity investment made beforehand, help from the private sector, foreign threat intelligence, cloud services, and backup satellite communication. He also notes it's hard to measure exactly how much each individual piece of help mattered (Bateman, 2022). Put together, these measures shortened the window in which Russian access or disruption was militarily useful, since they let systems get restored, communications get rerouted, threat info get shared, and alternative services get adopted quickly.

Zarembo et al. push resilience beyond just government and military networks. Their study combined an online survey of 1,060 people with twelve interviews. People described their smartphones as important for things like air raid warnings, donations, volunteering, sharing information, navigation, government services, documentation, and supporting the defense effort from behind the front lines. The authors do point out that their survey skews toward younger, urban, educated, well-connected, tech-savvy users, so it can't be generalized to all Ukrainians (Zarembo et al., 2025).

Those same phones could also expose locations, identities, and personal networks. Ukrainians near the front or under occupation mentioned deleting data, shutting their phones down, or having separate phones/devices to lower their risk (Zarembo et al., 2025). Smartphones helped support resistance, but they also caused issues with surveillance and security.

Cyber Operations and Information Warfare

My original assumption lines up close enough with Russian strategic thinking (enough that I didn't start on a new topic) on one key point: Russia doesn't treat technical and psychological activity as two totally separate national-security problems. The NATO Strategic Communications Centre of Excellence report explains that Russia sees cyber operations as just one tool inside a bigger concept it calls information confrontation, alongside psychological operations, electronic warfare, disinformation, and physical military action. The report also stresses that cyber or information-technological warfare is only one piece of that larger framework, not the whole thing (Hakala & Melnychuk, 2021).

Whyte draws an academic line between cyber operations and information warfare. Cyber operations can strengthen an information campaign in several ways: stealing private information, pulling attention away from more urgent matters, draining the resources of security organizations, compromising institutions people trust, and eroding confidence in whether information is credible or genuine (Whyte, 2020, pp. 2–3). But after looking at how these mechanisms work inside bigger influence campaigns, Whyte concludes that "though the role of cyber operations in ensuring the success of democracy hacking may be minimal, the incentive to use cyber assets is strong" (Whyte, 2020, p. 14). Cyber operations and information warfare should be treated as two separate tools that reinforce each other. The technical operation might supply information, access, disruption, or credibility to an influence campaign, without being the main reason that campaign persuades anyone.

The March 2022 Ukraine 24 incident shows this relationship in action. An information operation spread an AI-generated video showing President Volodymyr Zelenskyy supposedly telling Ukraine to surrender. That same false message showed up after Ukraine 24's website and TV news ticker were apparently hacked and defaced. Mandiant could not establish that the same

actors conducted every related destructive and informational action observed that day (Wahlstrom et al., 2022). The incident still shows how technical access can support an influence campaign without making cyber operations and information warfare the same activity (Whyte, 2020).

The suspected compromise of the trusted media platform was the technical cyber component, while the false surrender message was the information-warfare component. Their combination shows how unauthorized access can lend visibility and apparent credibility to an influence message, even though the available evidence does not prove that the same actors conducted every related destructive and informational action observed that day (Whyte, 2020).

Russian information activity also spread widely across social media. Geissler and colleagues studied 349,455 pro-Russian Twitter posts from February through July 2022. Those posts generated roughly 251,000 retweets and had a potential reach of about 14.4 million users. About 20.28% of the accounts they identified were bots, and bots played an outsized role in the early wave of amplification. However, pro-Russian content typically went less viral than pro-Ukrainian content, humans hardly ever directly reshared bot accounts, and the majority of the original content was created by actual people (Geissler et al., 2023). The campaign reached a large potential audience, but reach is not the same as influence. Geissler et al. note that the content may not have penetrated communities deeply enough to shift public opinion, and its actual impact remains difficult to measure (2023).

Ukraine also built digital communication into its war effort. Hogue analyzed more than 2,500 United24 Media videos posted to Instagram and YouTube between February 2023 and September 2024. His argument is that United24 "translates its narratives into the popular languages of social media platforms" (Hogue, 2026, p. 3). On Instagram, the focus was Russian

aggression, civilian destruction, Ukrainian resilience, identity, and international support. On YouTube, 35% of coded content was combat footage and another 23% covered military technology, while civilian destruction and resilience were almost completely left out (Hogue, 2026).

Hogue found that United24's YouTube videos almost always showed Ukrainian battlefield wins, drone strikes, artillery, and frontline footage, even though the bigger picture on the battlefield was less favorable at the time (Hogue, 2026). This selective visibility helps explain how repeatedly viewing footage of successful Ukrainian strikes could give the impression that overall battlefield performance was better than the aggregate reporting supported. This does not make the footage false; it shows how real tactical victories can be selected and incorporated into a broader strategic narrative. Hogue does not show that specific videos persuaded audiences or influenced aid decisions, but the study does show that Ukraine tailored its wartime messaging to different platforms.

Conclusion

The Russia–Ukraine War shows how deeply cyberspace has become part of modern conflict. Russia used destructive malware and digital influence campaigns, while Ukraine relied more heavily on cyber defense, digital resilience, and strategic communication. Even with all this activity, the evidence suggests that cyber operations rarely decide the outcome by themselves.

WhisperGate and the Viasat attack both showed intent and caused some disruption, but public evidence does not show that either operation broke Ukraine's ability to organize or keep fighting. Industroyer2 was caught before it could do real damage, which points to the importance

of defense and quick response. Social media campaigns reached a lot of people, but the effect on actual opinions or policy is much harder to measure.

In retrospect, I can see that some of my assumptions were not just blurring the lines between two areas of warfare, but also missing some key differences, treating all digital and information operations as the same. Information warfare, cyberattacks, and digital resilience are all important, but they don't work in isolation. The conflict implies that cyberspace is contested and militarized, but its primary function is as a force multiplier rather than as the primary determinant of the result. At the end of the day, the outcome is dependent on how digital tools, traditional power, and human flexibility are integrated.

References

- Bateman, J. (2022, December). *Russia's wartime cyber operations in Ukraine: Military impacts, influences, and implications* [Working paper]. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_Cyber-FINAL21.pdf
- Council of the European Union. (2022, May 10). *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union*. <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/>
- Cybersecurity and Infrastructure Security Agency. (2024, September 5). *Russian military cyber actors target U.S. and global critical infrastructure* (AA24-249A). <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-249a>
- ESET Research. (2022, April 12). *Industroyer2: Industroyer reloaded*. <https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/>
- Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, 38(2), 41–73. <http://www.jstor.org.proxy.lib.odu.edu/stable/24480930>
- Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of Ukraine. *EPJ Data Science*, 12(1), 35. <https://doi.org/10.1140/epjds/s13688-023-00414-5>

- Hakala, J., & Melnychuk, J. (2021, June). *Russia's strategy in cyberspace*. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf
- Hogue, S. (2026). Uniting the world behind Ukraine: The platformization of United24 Media's narratives on Instagram and YouTube and the in/visibilization of war. *Media, War & Conflict*. Advance online publication. <https://doi.org/10.1177/17506352261448727>
- Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, 38(2), 7–40.
<http://www.jstor.org.proxy.lib.odu.edu/stable/24480929>
- Lindsay, J. R., & Kello, L. (2014). A cyber disagreement. *International Security*, 39(2), 181–192. <http://www.jstor.org.proxy.lib.odu.edu/stable/24480587>
- Maschmeyer, L. (2021). The subversive trilemma: Why Cyber Operations Fall Short of Expectations. *International Security*, 46(2), 51–90. https://doi-org.proxy.lib.odu.edu/10.1162/isec_a_00418
- Microsoft Digital Security Unit, Microsoft Incident Response, & Microsoft Threat Intelligence. (2022, January 15). *Destructive malware targeting Ukrainian organizations*. Microsoft Security Blog. <https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/>
- Pedersen, F. A. H., & Jacobsen, J. T. (2024). Narrow windows of opportunity: the limited utility of cyber operations in war. *Journal of Cybersecurity*, 10(1)
<https://doi.org/10.1093/cybsec/tyae014>

Viasat, Inc. (2022, March 30). *KA-SAT network cyber attack overview*.

<https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/>

Wahlstrom, A., Revelli, A., Riddell, S., Mainor, D., & Serabian, R. (2022, May 19). The IO

Offensive: Information Operations Surrounding the Russian Invasion of Ukraine |

Mandiant. *Google Cloud Blog*. [https://cloud.google.com/blog/topics/threat-](https://cloud.google.com/blog/topics/threat-intelligence/information-operations-surrounding-ukraine)

[intelligence/information-operations-surrounding-ukraine](https://cloud.google.com/blog/topics/threat-intelligence/information-operations-surrounding-ukraine)

Whyte, C. (2020). Cyber conflict or democracy “hacked”? How cyber operations enhance

information warfare. *Journal of Cybersecurity*, 6(1)

<https://doi.org/10.1093/cybsec/tyaa013>

Zarembo, K., Knodt, M., & Kachel, J. (2025). Smartphone resilience: ICT in Ukrainian civic

response to the Russian full-scale invasion. *Media, War & Conflict*, 18(3), 305–324.

<https://doi.org/10.1177/17506352241236449>