Can Cyber Attacks Put An End To The Russo-Ukrainian Conflict?

By: Ahmad Mohee
ORCID: 0000-0003-3440-5199

Cairo in: October 8th, 2023

Abstract

As fighting continues on the ground, cyberspace has remained a secondary theater of the Russo-Ukrainian war.

It is very clear that Russia is adept at employing cyber attacks in conventional conflict through hybrid warfare. It is clear that Ukrainian cyber defense has contributed greatly to undermining the effectiveness of Russian cyber attacks, showing that cyber defense is not a hopeless cause.

Through this analysis, I review some specialists' opinions about the possibility of putting an end to conventional conflicts by employing cyber attacks, and then I try to answer a basic question: Can cyber attacks put an end to the Russo-Ukrainian war?

Keywords: *cyber defense, cyber warfare, conventional war, Russo - Ukrainian war*

Can Cyber Attacks Put an End to a Conventional Conflict?

The effectiveness of cyber attacks cannot be denied. Cyber weapons can be used offensively or defensively and are capable of causing military effects that are sometimes similar to what can be achieved with conventional weapons. By employing cyber attacks on critical infrastructure and facilities, and spreading disinformation and smear campaigns, the population's confidence and their ability to resist conventional invasion can be undermined.

Cyber attacks are a swift and low-cost way to achieve military objectives, such as paralyzing military capabilities, controlling the enemy, and destabilizing the target community. [1]

Although some analysts reduce the possibility of ending a conventional conflict through cyber attacks, especially those targeting infrastructure [2], there is another side of analysts that confirm that cyber attacks on infrastructure can be conventionally devastating. [3]

Andrew Krepinevich noted: “A cyberattack on a developed nation's critical infrastructure achieves results resembling strategic bombing campaigns in World War II.” [4]

In this context, James Acton Co-Director of the Nuclear Policy Program at the Carnegie Endowment for International Peace [5], points out that: “Cyber attacks could target early warning and control systems of nuclear weapons, systems that increasingly rely on digital rather than analog signals, and on operating systems connected to the Internet”.

According to Acton; “the emergence of cyberwar exacerbates the risk of unintended nuclear escalation in a conventional conflict. Cyber attacks can enhance one state’s ability to undermine another state’s nuclear deterrent and fear of cyber attacks can generate escalatory pressures leading one to conclude that "a nuclear-armed state may mistakenly believe its nuclear deterrent is under attack".

https://doi.org/10.33774/apsa-2023-n4h4w **ORCID:** https://orcid.org/0000-0003-3440-5199 Content not peer-reviewed by APSA. **License:** CC BY 4.0

Can Cyber Attacks Put an End to the Russo-Ukrainian Conflict?

Some cyber security experts are skeptical about this, as they believe that this is a hot conflict, where people are dying due to explosions, and it is uncertain whether someone's infiltration of Russian Defense Ministry data will be decisive in determining the outcome of the war.

Charlotte Lindsay, policy director at the Cyber Peace Institute, states: “We were all anticipating that the use of cyber means in the Russo - Ukrainian war would have some major catastrophic humanitarian consequences.” [6]

Empirical evidence shows that although there has been a slight increase in cyber attacks during the conflict, these attacks have not shown an increase in severity, a shift in targets, or a shift in tactics. Trends suggest that cyber operations are not yet having a material impact on the battlefield.

Academics such as Nadia Kostyuk and Eric Gartzke have noted that: “Russian cyber operations neither significantly replaced nor complemented conventional combat activities.”[7]

Jon Bateman explains that: “Russia's main cyber activity in Ukraine may have been focused on intelligence gathering. Russian hackers pursued data collection, kinetic targeting, occupation activities, etc., however, non-cyber intelligence sources - such as images, human agents and signal interception – were more practically useful for Russia.” [8]

It is also clear that Ukrainian cyber defense has greatly contributed to undermining the effectiveness of Russian cyber attacks. In this context, Nick Beecroft explains that: “Ukraine has demonstrated tremendous defensive strength and resilience on the cyber battlefield. Kiev’s ability to harness years of experience from Russian cyber attacks, combined with strong support from Western governments and technology companies, it has allowed Ukraine to deploy cyber defenses at a scale and depth never seen before...The war has shown that cyber defense is not a hopeless cause.”[9]

In fact, no catastrophic use of cyber attacks has yet occurred during the Russo – Ukrainian war; although the Russian ground and air attacks on Ukrainian towns had devastating results on the humanitarian level. No

https://doi.org/10.33774/apsa-2023-n4h4w **ORCID:** https://orcid.org/0000-0003-3440-5199 Content not peer-reviewed by APSA. **License:** CC BY 4.0

cyber attacks with “severe” results, of the kind that many observers and analysts expected, have been reported.

Although Ukraine has faced intense levels of Russian cyber attacks since the invasion began, these attacks do not appear to have contributed much to Moscow's desired results. Perhaps the most prominent conventional results achieved through cyber attacks were the Russian cyber attack on the Viasat satellite communications network, which significantly hindered the Ukrainian defenses and may have facilitated the crossing of the borders by Russian forces during the start of the invasion. [10]

Some analysts cite other realistic reasons why significant cyber attacks have not yet appeared during the Russian-Ukrainian conflict [11] :

- Defense strategies may be dominant in cyberspace so far. Moscow finds itself facing not only Ukraine, but also a Western cyber alliance, which limits the extent of its ability to exploit cyberspace.
- There may be a tendency to exaggerate threats in cyber reports, making Russian efforts appear more sophisticated and powerful than they actually are.
- It is possible that conventional attacks would be more effective in achieving Russian goals of invasion, allowing Russia to keep its cyber weapons secret for later use, perhaps if the war escalates to include direct combat with the West.

I can also add:

- Russia is well aware of the extent of Western cyber power, the expansion and diversity of their cyber weapons. Moscow does not currently wish to expand the conflict front in order to avoid a comprehensive confrontation, especially with the possibility that large-scale cyber attacks could lead to nuclear escalation, which represents a type of cyber deterrence in Ukraine’s interest.
- Russia may be regrouping in the wake of Ukraine’s success in repelling initial Russian cyber attacks supported by the West, or they may be waiting for the appropriate time to launch larger, more impactful cyber attacks.

- It is likely that Russia’s cyber strategies related to this war focus less on destroying vital infrastructure and more on limiting the ability of the Western coalition that supports Ukraine by waging Narrative Warfare [12], whose operations focus on eroding global trust in Ukraine and changing global public opinion towards the war through propaganda and disinformation campaigns [13]

In order to answer the basic question: whether or not cyber attacks can put an end to the Russo-Ukrainian conflict, it can be said that the possibility of cyber attacks to ultimately end the conflict depends on the extent to which cyber attacks contribute to achieving the goals of the conflict for both sides.

While Russia primarily aims to secure its western borders by deploying forces on the ground and occupying areas west of the Russian-Ukrainian border, cyber attacks are not expected to be a decisive factor in this area, although their influence should not be underestimated as an auxiliary factor to conventional attacks.

Meanwhile, Ukraine is struggling to repel the Russian attack, and the international community is seeking to stop the war and return the two parties to the negotiating table. In this regard, if painful and focused cyber attacks can be directed into the Russian cyber depth, this could represent a decisive factor in deterring the Russian side and forcing them to stop the war and return to the negotiating table.

https://doi.org/10.33774/apsa-2023-n4h4w **ORCID:** https://orcid.org/0000-0003-3440-5199 Content not peer-reviewed by APSA. **License:** CC BY 4.0

References:

[1] Kallberg, J., 2016. Strategic cyberwar theory-A foundation for designing decisive strategic cyber operations, *The Cyber Defense Review*, 1(1), pp.113-128.

[2] Libicki, M.C., 2014. Why cyber war will not and should not have its grand strategist, *Strategic Studies Quarterly*, 8(1), pp.23-39.

[3] Jackson, W., 2012. Fuss over Cyber War Distracts from Real Threats, Security Pioneer Says, *Route Fifty,* online: https://perma.cc/BH29-PDEW

[4] Krepinevich, A., 2012. Cyberwarfare: A "Nuclear Option"? *Centre for Strategic and Bugetary Assessments*, p. 65.

[5] Acton, J., 2020. Cyber Warfare & Inadvertent Escalation, *Carnegie Endowment for International Peace*, online: https://perma.cc/S8YD-GTUF

[6] Foulkes, I., 2023. What does Ukraine tell us about cyber warfare? Swiss Info, online: https://perma.cc/U8LR-HDS9

[7] Kostyuk, N. and Gartzke, E., 2022. Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine (Summer 2022), *Texas National Security Review*.

[8] Bateman, J., Beecroft, N. and Wilde, G., 2022. What the Russian Invasion Reveals about the Future of Cyber Warfare, *Carnegie Endowment for International Peace*, online: https://perma.cc/S8S8-3K9K

[9] Ibid.

[10] Manson, K., 2023. The Satellite Hack Everyone Is Finally Talking About, *Bloomberg*, online: https://perma.cc/MEU8-PLSV

[11] Mueller, G., Jensen, B., Valeriano, B., Maness, R. and Macias, J., 2023. Cyber operations during the Russo–Ukrainian war, *Center for Strategic Int. Studies, Washington, DC, USA,* online: https://perma.cc/29EB-QZH4

[12] Carvin, A., 2023, Narrative Warfare; How the Kremlin and Russian news outlets justified a war of aggression against Ukraine, *Atlantic Council,* online: https://perma.cc/R68V-GCQF

[13] Carvin, A., 2023, Undermining Ukraine; How the Kremlin employs information operations to erode global confidence in Ukraine, *Atlantic Council,* online: https://perma.cc/9NHM-MNVH.

https://doi.org/10.33774/apsa-2023-n4h4w **ORCID:** https://orcid.org/0000-0003-3440-5199 Content not peer-reviewed by APSA. **License:** CC BY 4.0