National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

# Offensive Cyber Operations in War: From Russia with Lessons

**Lieutenant-Colonel D'Arcy Lemay**

## JCSP 49 DL

## Exercise Solo Flight

**Disclaimer**



## PCEMI n° 49 AD

## Exercice Solo Flight

**Avertissement**



Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 49 DL - PCEMI n° 49 AD
2022 - 2024

Exercise Solo Flight – Exercice Solo Flight

# Offensive Cyber Operations in War: From Russia with Lessons

**Lieutenant-Colonel D'Arcy Lemay**

## OFFENSIVE CYBER OPERATIONS IN WAR: FROM RUSSIA WITH LESSONS

Since 24 February 2022 and the launch of a full-scale invasion of Ukraine by Russia, the conflict has been considered by some as the first cyber war by a major cyber power.[1] Throughout the immediate pre-war and initial invasion period there was a marked increase in cyber events experienced by Ukraine compared to the prior, already high, frequency of attacks.[2] This greater volume has been focused on the information and cognitive domains rather than supporting combined arms. With few exceptions, Russia's offensive cyber has not been a major force enabler for the conventional military campaign as had been expected.[3] This leads to the question of why Russia's vaunted cyber capabilities did not turn into battlefield operational success during the invasion and ensuing war. Canada and its allies have valuable lessons to learn from Russia's cyber operations in Ukraine despite the difference in goals and the limited success observed in areas of common interest. This paper will derive several considerations through a series of arguments beginning with the organizational philosophy on cyber operations for Russia. Several disclosed examples of Russian cyber tactical successes and failures in Ukraine to date will be examined as they relate to the conventional campaign. This will be followed by potential explanations for the outcomes observed. The paper will conclude by providing considerations for Canada in development of its military offensive cyber efforts based on the observations in war related to initiative, targeting, effects and organization.

## RUSSIAN CYBER ORGANIZATION AND DOCTRINE

Since the "special military operation" in Ukraine began there has been additional research into the organization of state level cyber in Russia to understand the origins of the various activities and their potential goals. Russia has distributed actors in cyberspace amongst both the intelligence services and the armed forces. Within the military their cyber actors belong to the military intelligence agency *Glavnoye Razvedyvatelnoye Upravlenie* (GRU).[4] The GRU's cyber efforts are closely linked to direction from the Presidential Administration and Security Council instead of the military leadership, or a bespoke national Cyber Command, that could coordinate the efforts of the various Russian actors.[5] The GRU has been tasked through that political structure to take the lead on cyber operations in Ukraine though both it, and the *Federalnaya*

---

[1] Erica D. Lonergan, Margaret W. Smith, and Grace B. Mueller, "Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine*," in *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 2023, 86, https://doi.org/10.23919/CyCon58705.2023.10182101.

[2] Grace B. Mueller et al., "Cyber Operations during the Russo-Ukrainian War: From Strange Patters to Alternative Futures," On Future War, July 13, 2023, 7, https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

[3] Gavin Wilde, "Cyber Operations in Ukraine: Russia's Unmet Expectations" (Washington, DC: Carnegie Endowment for International Peace, December 12, 2022), 11, https://carnegieendowment.org/research/2022/12/cyber-operations-in-ukraine-russias-unmet-expectations?lang=en.

[4] Andrei Soldatov and Irina Borogan, "Russian Cyberwarfare: Unpacking the Kremlin's Capabilities," CEPA, September 8, 2022, https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

[5] Soldatov and Borogan; Wilde, "Russia's Unmet Expectations," 10.

*sluzhba bezopasnosti Roddiyskoy Federatsii* (FSB), have operated there historically for cyber operations.[6]

Many states link their intelligence and military cyber resources together for technical reasons related to the domain. Russia follows this pattern as their cyber campaigns are primarily directed to execute intelligence collection.[7] Furthermore, Russia continues in this vein due to how they view combat in the information space and cyberspace. For them, the technical and the psychological are linked together and part of an ongoing information warfare that starts long before armed conflict and continues throughout.[8] While linked, Russia doctrinally has an emphasis on the cognitive/psychological over the technical effects.[9] The former is the main strategic effort, when they are in competition with other states with whom direct action is anticipated/planned, to attempt to destabilize them before and during conventional actions. The latter is applied in competition below the level of inciting retaliation, and largely reserved for conflict with a significant adversary.[10] Maintaining the significant cyber-technical attacks in reserve is tied to the concept of *udar* – "the crushing, mortal blow that is delivered with speed, surprise, and force".[11] The evidence would indicate that Russia did not see Ukraine as an adversary for which the concept of cyber *udar* was worth applying.

## TACTICAL OFFENSIVE CYBER SUCCESSES

In the hours prior to the initial drive to Kyiv, a well-planned, and executed cyber-attack supported the invasion. This hack disrupted service from a commercial satellite communications provider to the Ukrainian government, military, and police. In addition to the functional targeting of command and control means at a critical moment, this event is notable for both the technical target – a US based company operating the satellite constellation, and an Italian based company for the ground stations – and the multi-layered methodology used to execute the supply chain attack.[12] Due to the payload being indiscriminate in its target selection there was significant collateral damage of the attack outside of Ukraine, impacting other European customers of the space segment.[13] This attack indicates that the planners involved were well prepared and integrated unlike many of the other military operations to open the war. The offensive cyber action was also a tactical success, achieving the objective of disrupting one communications link, and allowing other assets to focus through electronic warfare or kinetic strikes on other C2

---

[6] Taylor Grossman et al., "The Cyber Dimensions of the Russia-Ukraine War" (European Cyber Conflict Research Initiative, April 19, 2023), 6, https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf.
[7] Jon Bateman, "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endowment for International Peace, 22, accessed May 5, 2024, https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.
[8] Keir Giles, "Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine" (Royal Institute of International Affairs, December 14, 2023), 3-4,50, https://doi.org/10.55317/9781784135898.
[9] Wilde, "Russia's Unmet Expectations," 8.
[10] Rod Thornton and Marina Miron, "Winning Future Wars: Russian Offensive Cyber and Its Vital Importance: In Moscow's Strategic Thinking," *The Cyber Defense Review* 7, no. 3 (2022): 126, https://www.jstor.org/stable/48682327.
[11] Thornton and Miron, 127.
[12] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 9.
[13] Giles, "Russian Cyber and Information Warfare in Practice," 28.

means.[14] Russia gained an edge in their early assault against a Ukrainian defence that had to utilize alternate methods for resilient communications.[15]

Similarly, at the outset of the invasion new malware was directed at Ukraine's government and defence sectors on a scale not previously observed.[16] These initial tools were destructive wipers aimed at first propagating through networks, creating a distraction using a decoy element, and simultaneously deleting the disk and itself.[17] This malware impacted a dozen government and key industry networks, and was tailored for these targets well in advance.[18] These attacks were quickly observed and defended against with the support of premier tech companies in the security space, notably Microsoft, Google/Mandiant, Cloudflare and ESET.[19] Follow-on actions included deploying key services to the cloud where they were removed from physical attacks and defended by cyber security experts.[20] The result were small tactical successes for Russia in the cyber domain to delete data, but the overall impact did not appear to be disabling to service delivery for Ukrainian citizens, nor align to a distinct military battlefield goal. However, it could be argued that these attacks contributed to the cyber-psychological goals of lowering trust in government as well as consuming resources that might have been utilized for defences in other areas.[21]

While C2 systems as well as government and military-related industry were targeted at the outset of the invasion, these attacks quickly tapered off.[22] They were instead replaced in the fall and winter of 2022 by Industrial Control System (ICS) attacks on utilities with a specific focus of those related to the energy sector.[23] On 10 and 12 October a blackout was successfully triggered using access developed months in advance and maintaining presence until a planned strike. This was a multilayered attack where the payload achieved the initial compromise, laterally moved from one network to another, hid from detection, responded to C2 to execute the attack, and finally came back and wiped the IT system supporting the site to cover its tracks.[24] The execution of the event coincided with the campaign of missile attacks on critical

---

[14] Lonergan, Smith, and Mueller, "Evaluating Assumptions About the Role of Cyberspace in Warfighting," 90.
[15] Dan Rice, "The Untold Story of the Battle for Kyiv," Small Wars Journal, May 31, 2022, https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv.
[16] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 11.
[17] ESET, "ESET Research: Ukraine Hit by Destructive Attacks before and during the Russian Invasion with HermeticWiper and IsaacWiper," ESET, March 1, 2022, https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/.
[18] Microsoft Digital Security Unit, "An Overview of Russia's Cyberattack Activity in Ukraine," Special Report: Ukraine, April 27, 2022, 7, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.
[19] Mueller et al., "Cyber Ops Russo-Ukraine War," 9.
[20] Russ Mitchell, "How Amazon Put Ukraine's 'government in a Box' — and Saved Its Economy from Russia," Los Angeles Times, December 15, 2022, https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.
[21] Gavin Wilde, "Why Cyber Attacks on Ukrainians Aren't Working the Way Russia Expected," Emissary, March 11, 2024, https://carnegieendowment.org/emissary/2024/03/why-cyber-attacks-on-ukrainians-arent-working-the-way-russia-expected?lang=en.
[22] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 12–13.
[23] Giles, "Russian Cyber and Information Warfare in Practice," 27.
[24] Ken Proska et al., "Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology," Mandiant, November 9, 2023, https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

infrastructure in the both the local area and throughout Ukraine, which indicated an intent to coordinate with conventional forces on the same targets.[25] This suggests strategic or operational level alignment, but not necessarily at the tactical level where sequencing and geography matter significantly. Instead, this example suggests "pooled interdependence" where both cyber and kinetic strikes occur in their own domains to achieve similar goals but are not sequential or closely coordinated to enable one another.[26] While this was a surgical and well-planned event in the cyber domain, its impact was limited despite it overlapping with a kinetic strike in the same vicinity. Given that both the kinetic and cyber strikes were aiming for the same targets it is not inconceivable that a well-placed missile may have caused a longer outage or perhaps even hidden this massively successful cyber-attack.[27]

## PUBLICIZED FAILURES

Despite the discrete offensive cyber successes described in the above section, Russia has had far more events in their cyber campaign crash and burn against a wall of determined defenders.[28] The disruption of Viasat at the outset of the invasion drove the delivery and integration of SpaceX's Starlink system as an augmentation of the satellite communications means available. This commercial service proved immediately valuable to Ukraine and the preferred means for a variety of critical tasks and users.[29] The Starlink system has numerous advantages making it more resistant to jamming than constellations that operate in higher orbits.[30] Starlink has had to adapt not just to electronic warfare signal jamming, but offensive cyber-attacks to the system like occurred to Viasat. The attack surface includes the user terminals themselves or necessary central services such as authentication.[31] The description by a US defence official regarding SpaceX's speed and resilience to one such attack was "eye-watering".[32] The ability of commercial companies to defend their own systems against state and non-state level offensive cyber has been an important factor in the conflict.

The desirability of being able to find a cyber method of degrading Starlink has been a contributing factor leading to other operations enabled by co-operative intelligence collection efforts in the land and cyber domains. Russia deliberately tried to acquire Ukrainian tablets that run the Delta battle command app. With access to captured equipment and to the network, the GRU distributed malware named Infamous Chisel – a collection of seven layered elements along

---

[25] Proska et al.
[26] Max Smeets, "The Strategic Promise of Offensive Cyber Operations," *Strategic Studies Quarterly* 12, no. 3 (2018): 98, https://www.jstor.org/stable/26481911.
[27] Andy Greenberg, "Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike," *Wired*, November 9, 2023, https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/.
[28] James Andrew Lewis, "Cyber War and Ukraine," Center for Strategic & International Studies, June 16, 2022, 7, https://www.csis.org/analysis/cyber-war-and-ukraine.
[29] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 43.
[30] Lucas Laursen, "Satellite Signal Jamming Reaches New Lows - IEEE Spectrum," IEEE Spectrum, May 18, 2023, https://spectrum.ieee.org/satellite-jamming.
[31] Becky Bracken, "Killnet Gloats About DDoS Attacks Downing Starlink, White House," Dark Reading, November 29, 2022, https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov.
[32] Anonymous, "The Satellites That Saved Ukraine," *The Economist* (London, United Kingdom: The Economist Intelligence Unit N.A., Incorporated, January 7, 2023), 14, https://www.proquest.com/docview/2761511645/abstract/E9CFC18579894DE7PQ/1.

with the supporting C2 infrastructure – to search for specific items and exfiltrate them.[33] The primary data that it looked for were items of military value, but one tool specifically sought configurations related to Starlink. This attack was reportedly stopped before it was able to attain a foothold on the network and achieve its aim.[34] This follows other similarly denied attempts to gain access using other routes with lower equity phishing attacks.[35] While the Ukrainian cyber services are certainly doing their part in securing this system they are not doing so alone, as several NATO nations are participating in the defensive cyber operations for the network.[36]

A final example of Russia's publicly acknowledged cyber failings relates to attempts to disrupt power infrastructure in Ukraine. The ICS example above in the success section achieved its tactical goal with a very detailed, layered, and novel approach, potentially based on lessons learned from this earlier attack from April 2022. The Industroyer2 malware recycled some source code from the Industroyer attack several years prior and appeared rushed to deployment after achieving the prerequisite access.[37] The successful defence was a collective effort between the system operators, Ukrainian Computer Emergency Response Team (CERT-UA), and two industry partners in Microsoft and ESET keeping the power on for 2 million civilians.[38] Multiple cyber-attacks on the power grid have been disclosed with few seeing success. Those with significant resource and time investments achieved results as opposed to those with lower equity exploits. In the end, the cyber approach to power disruption was significantly supplanted in terms of effects by kinetic strikes once it was apparent that a quick victory over Ukraine would not be achieved.[39]

## INTERNAL REASONS FOR LACK OF OPERATIONAL SUCCESS

Multiple different experts using compiled public data on cyber incidents assess most events during the conflict were directed towards efforts to collect intelligence or cyber-psychological shaping as opposed to deliver effects through degradation or destruction.[40] The targets also factor into the choice of operations, with most of the Russian cyber activity directed at private non-state actors, state entities and local government, with little focus on the military.[41] A limitation of all this data is that it is based on public reporting, and many actors are not

---

[33] NCSC, "UK and Allies Support Ukraine Calling out Russia's GRU for New Malware Campaign," August 31, 2023, 18, https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/infamous-chisel/NCSC-MAR-Infamous-Chisel.pdf.
[34] Security Service of Ukraine, "Cyber Operation of Russian Intelligence Services as a Component of Confrontation on the Battlefield," Technical, August 8, 2023, 14, https://ssu.gov.ua/uploads/files/DKIB/technical-report.pdf.
[35] Daryna Antoniuk, "Military Operations Software in Ukraine Was Hit by Russian Hackers," The Record, December 19, 2022, https://therecord.media/military-operations-software-in-ukraine-was-breached-by-russian-hackers.
[36] Giles, "Russian Cyber and Information Warfare in Practice," 14–15.
[37] ESET, "Industroyer2: Industroyer Reloaded," April 12, 2022, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.
[38] Kevin Collier, "Ukraine Says Russian Cyberattack Sought to Shut down Energy Grid," NBC News, April 12, 2022, https://www.cnbc.com/2022/04/12/ukraine-says-russian-cyberattack-sought-to-shut-down-energy-grid.html.
[39] Lonergan, Smith, and Mueller, "Evaluating Assumptions About the Role of Cyberspace in Warfighting," 91,94.
[40] Lonergan, Smith, and Mueller, 88–89; Mueller et al., "Cyber Ops Russo-Ukraine War," 8.
[41] Mueller et al., "Cyber Ops Russo-Ukraine War," 8.

incentivised to reveal the volume and effect of the activity directed at them in order to maintain operational security.[42]

Other explanations have been proposed that relate to deliberate choices on the types and targets of cyber operations due to the organizational aspect of Russian cyber resources. Kier Giles and Gavin Wilde propose that the most mature cyber elements are integrated in the departments inclined to support intelligence gathering and general subversion, as opposed to the less capable group allocated within the GRU.[43] This aligns with observations indicating a shift from multifunctional and novel malware at the outset of the conflict to a preponderance of simpler wipers with lower development costs and fewer instances of complex attacks on specific targets due to limitations on capacity.[44] This capacity issue was considered in analysis to be a significant differentiator between peacetime, grey zone and war: while the scale of offensive cyber activity was unprecedented – even if it was sustainable at that tempo beyond the initial stage – it was still a very small proportion of the overall campaign in Ukraine once the invasion began in earnest.[45] This also comes back to doctrine and intent. Battlefield electronic support for Russia is primarily an EW task, as opposed to a cyber one, which is why they have invested in significant EW integration at the operational and tactical level.[46]

A final consideration is that Russia is holding back more sophisticated offensive tools and exploits for a more significant escalation. These equities may not have been considered necessary for a quick drive to victory initially. After shifting tactics to kinetic attrition inside Ukraine they could have been held in reserve with the thought they might be better employed against targets in NATO where Russia does not have a conventional advantage.[47] This aligns with the view that Ukraine is one front in a larger conflict with the West. Russian state and non-state attributed cyber actors have maintained, or stepped up, the number of cyber activities outside of Ukraine, implying concentration of force is not a guiding principle for Russia in their offensive cyber plans.[48]

## UKRAINIAN (AND FRIENDS) DEFENCE

A consistent theme of cooperation arises when reviewing the cyber operations in the Russia – Ukraine war. Ukraine has had eight years since the invasion of Crimea to observe and react to persistent cyber activity on their networks and have clearly invested in their own

---

[42] Grossman et al., "Cyber Dimensions of the Russia-Ukraine War," 18; Giles, "Russian Cyber and Information Warfare in Practice," 12.
[43] Giles, "Russian Cyber and Information Warfare in Practice," 26; Wilde, "Russia's Unmet Expectations," 11.
[44] Grossman et al., "Cyber Dimensions of the Russia-Ukraine War," 14.
[45] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 36.
[46] Ariel Levite, "Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict" (Washington, DC: Carnegie Endowment for International Peace, April 18, 2023), 12, https://carnegieendowment.org/research/2023/04/integrating-cyber-into-warfighting-some-early-takeaways-from-the-ukraine-conflict?lang=en.
[47] Thornton and Miron, "Winning Future Wars," 128–29.
[48] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 37; Levite, "Integrating Cyber Into Warfighting," 15–16.

resilience.[49] Ukraine's investment, however, did not occur in a vacuum. It has been augmented and reinforced from both states and private industry.

Western governments and alliances aided Ukraine to secure their networks prior to the full-scale invasion and continue to do so. Notable cyber powers including the US and UK have made supporting Ukraine's networks a priority while capable nations, such as Canada, have dedicated a significant share of their capacity to provide direct support.[50] NATO and the EU have also taken on a role for information sharing and response.[51] This means that Russia is not just attacking the same actor they had been competing against previously. Given the many sophisticated state level cyber organizations involved, this has turned into a team sport for which states aligned against Russia's aggression in the Ukraine are motivated to both gain intelligence and develop responses.

That partnership expands well beyond that of states and into private industry support. The example of Starlink as a service provision that can remain resilient under attack was provided earlier in the section on publicized failures, but it is not the only one participating in the "collective defense". Tech companies have provided services out of pocket or funded by governments and grants that Ukraine could not likely afford to contract on their own.[52] The cloud and cybersecurity service provision have been assessed as being highly important to the success of the defence against Russian offensive cyber.[53] The scale of this support is beyond the scope of the paper to review, but corporations have been a dominant actor that operate on the front lines of the cyber conflict, and it is valuable to question if this near universal response is replicable in any future scenario.[54]

## INFORMING CANADA'S MILITARY OFFENSIVE CYBER AMBITIONS

There are four key observations to draw from the analysis of the examples of Russian cyber activity noted above:

- Offensive Cyber Operations (OCO) and initiative. The examples of successful coordination between offensive cyber and conventional operations by Russia were either directly tied with the opening invasion itself or the collective shift to increase civilian suffering leading into the winter of 2022. These are points at which Russia had the initiative or had planned out a deliberate strategy on how to take it back. While there are many indications that the Russian military executed the invasion with little advance warning or coordination between arms and supporting elements, this is not reflective of the evidence in the cyber domain.[55] These periods exemplified the opportunities to plan for OCO as a coordinated supporting activity to the physical domain and are a model to follow.

---

[49] Giles, "Russian Cyber and Information Warfare in Practice," 10–11.
[50] Giles, 14–15.
[51] Mueller et al., "Cyber Ops Russo-Ukraine War," 10.
[52] Giles, "Russian Cyber and Information Warfare in Practice," 16–17.
[53] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 42–43.
[54] Taylor Grossman et al., "Public-Private Collaboration in Ukraine and beyond - Binding Hook," *Binding Hook* (blog), April 4, 2024, https://bindinghook.com/articles-binding-edge/public-private-collaboration-in-ukraine-and-beyond/.
[55] Giles, "Russian Cyber and Information Warfare in Practice," 9–10.

- Deliberate vs dynamic targeting. This observation considers both capacity limitations and the advance timelines of successful events. The requirement for spending significant time on intelligence collection and detailed analysis is to ensure that there is high likelihood of the desired effect being achieved and no unintended spillover beyond the target.[56] In lieu of specific targets that must have synchronous and dependent effects to succeed – enabled through tactical and operational level coordination of multi-domain effects – Russia chose to aim offensive cyber operations against similar strategic targets assigned to the conventional forces. This has shown little value in its "pooled interdependence" as the kinetic strikes have been vastly more impactful.[57]

- Reversable and temporary effects on the battlefield have value. There is additional significance when considering multi-national companies are participating on the front line of the cyber domain.[58] This unique element of this conflict leads to risks in escalation and target legitimacy for further study as corporations cannot be considered non-combatants in the cyber domain. While in open war, kinetic weapons destructive effects are preferred so long as they have sufficient reach and the collateral damage risks can be accepted. Democratic countries like Canada have more incentive to develop options for non-kinetic "fires" that can create deceive, degrade, disrupt, or deny effects through the cyber domain. These are unique attributes that can be applied to conventional operations in ways that Russia has not often pursued beyond the outset of the conflict.

- Implications of joint cyber operations between CAF and CSE. Canada's defence policy update provided guidance on how government wants a unified approach to cyber operations between the foreign signals intelligence (Communications Security Establishment) and military (Canadian Armed Forces) organizations.[59] Russian efforts have privileged intelligence and security efforts over military ones possibly due to their organizational arrangement. For Canada to make this synergy between CSE and CAF function during conflict several processes can benefit from review of the Russian OCO efforts in Ukraine since 2022. The first is deliberate information sharing to ensure these joint cyber activities are synced with strategic, operational, and tactical military goals. Secondly, prioritization practices will require development to avoid access fratricide between efforts for intelligence exploitation and offensive cyber effects supporting the battlefield.[60] A methodology will also need to be created for assessing which exploits and tools are available to burn for target effects. Finally, deliberate planning must be undertaken to keep persistent access and equities in reserve, as they take a long time to develop and have limited re-usability once deployed and discovered.[61]

---

[56] Dr Herbert Lin, "Russian Cyber Operations in the Invasion of Ukraine," *Cyber Defense Review* 7, no. 4 (Fall 2022): 38–39, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/CDR_V7N4_Fall_2022.pdf?ver=1u4jRWNzOClxpmZ8653DmA%3d%3d; Levite, "Integrating Cyber Into Warfighting," 6.

[57] Bateman, "Russia's Wartime Cyber Operations in Ukraine," 22.

[58] Giles, "Russian Cyber and Information Warfare in Practice," 48,52.

[59] Government of Canada, "Our North, Strong and Free: A Renewed Vision for Canada's Defence," Reports and Publications, April 8, 2024, 26, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

[60] Wilde, "Russia's Unmet Expectations," 11.

[61] Levite, "Integrating Cyber Into Warfighting," 17.

## CONCLUSION

The conflict between Russia and Ukraine is now into its third year and its story pertaining to cyber operations is not complete. What information on this topic that has made it into the public domain has confirmed some expectations, challenged others, and brought to light unexpected results. Canada has lessons to learn in developing its own capability from how Russia operated in this domain of warfare. Russian efforts to coordinate conventional and cyber operations were limited by doctrine and organizational principles, where prime resources have been dedicated to other targets and theatres with desired effects of coercion or intelligence collection. Those that did succeed in complementing the military were noted when Russia had the initiative and was able to invest time to leverage access for deploying novel and carefully crafted payloads. Their choice largely was to apply these efforts against the same target types as the conventional battle and were minimally successful in their ability to supplement traditional fires. Adding to the challenge Russia faced was that the cyber environment they were operating in was not defended by just Ukraine, but rather collectively shielded by other significant state cyber powers and titanic industry partners that chose a side in the war. Further research will need to go into how this aspect changes interpretations of Law of Armed Conflict and International Humanitarian Law.

**BIBLIOGRAPHY**


Anonymous. "The Satellites That Saved Ukraine." *The Economist*, London, United Kingdom: The Economist Intelligence Unit N.A., Incorporated, January 7, 2023. https://www.proquest.com/docview/2761511645/abstract/E9CFC18579894DE7PQ/1.

Antoniuk, Daryna. "Military Operations Software in Ukraine Was Hit by Russian Hackers." The Record, December 19, 2022. https://therecord.media/military-operations-software-in-ukraine-was-breached-by-russian-hackers.

Bateman, Jon. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." Carnegie Endowment for International Peace. Accessed May 5, 2024. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657

Bracken, Becky. "Killnet Gloats About DDoS Attacks Downing Starlink, White House." Dark Reading, November 29, 2022. https://www.darkreading.com/threat-intelligence/killnet-gloats-ddos-attacks-starlink-whitehouse-gov.

Collier, Kevin. "Ukraine Says Russian Cyberattack Sought to Shut down Energy Grid." NBC News, April 12, 2022. https://www.cnbc.com/2022/04/12/ukraine-says-russian-cyberattack-sought-to-shut-down-energy-grid.html.

Digital Security Unit, Microsoft. "An Overview of Russia's Cyberattack Activity in Ukraine." Special Report: Ukraine, April 27, 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

ESET. "ESET Research: Ukraine Hit by Destructive Attacks before and during the Russian Invasion with HermeticWiper and IsaacWiper." ESET, March 1, 2022. https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/.

———. "Industroyer2: Industroyer Reloaded," April 12, 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.

Giles, Keir. "Russian Cyber and Information Warfare in Practice: Lessons Observed from the War on Ukraine." Royal Institute of International Affairs, December 14, 2023. https://doi.org/10.55317/9781784135898.

Government of Canada. "Our North, Strong and Free: A Renewed Vision for Canada's Defence." Reports and Publications, April 8, 2024. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.

Greenberg, Andy. "Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike." *Wired*, November 9, 2023. https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/.

Grossman, Taylor, Monica Kaminska, James Shires, and Max Smeets. "The Cyber Dimensions of the Russia-Ukraine War." European Cyber Conflict Research Initiative, April 19, 2023. https://eccri.eu/wp-content/uploads/2023/04/ECCRI_REPORT_The-Cyber-Dimensions-of-the-Russia-Ukraine-War-19042023.pdf.

Grossman, Taylor, Monica Kello, James Shires, and Max Smeets. “Public-Private Collaboration in Ukraine and beyond - Binding Hook.” *Binding Hook* (blog), April 4, 2024. https://bindinghook.com/articles-binding-edge/public-private-collaboration-in-ukraine-and-beyond/.

Laursen, Lucas. “Satellite Signal Jamming Reaches New Lows - IEEE Spectrum.” IEEE Spectrum, May 18, 2023. https://spectrum.ieee.org/satellite-jamming.

Levite, Ariel. “Integrating Cyber Into Warfighting: Some Early Takeaways From the Ukraine Conflict.” Washington, DC: Carnegie Endowment for International Peace, April 18, 2023. https://carnegieendowment.org/research/2023/04/integrating-cyber-into-warfighting-some-early-takeaways-from-the-ukraine-conflict?lang=en.

Lewis, James Andrew. “Cyber War and Ukraine.” Center for Strategic & International Studies, June 16, 2022. https://www.csis.org/analysis/cyber-war-and-ukraine.

Lin, Dr Herbert. “Russian Cyber Operations in the Invasion of Ukraine.” *Cyber Defense Review* 7, no. 4 (Fall 2022): 31–46. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_fall/CDR_V7N4_Fall_2022.pdf.

Lonergan, Erica D., Margaret W. Smith, and Grace B. Mueller. “Evaluating Assumptions About the Role of Cyberspace in Warfighting: Evidence from Ukraine*.” In *2023 15th International Conference on Cyber Conflict: Meeting Reality (CyCon)*, 85–102, 2023. https://doi.org/10.23919/CyCon58705.2023.10182101.

Mitchell, Russ. “How Amazon Put Ukraine’s ‘government in a Box’ — and Saved Its Economy from Russia.” Los Angeles Times, December 15, 2022. https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data.

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. “Cyber Operations during the Russo-Ukrainian War: From Strange Patters to Alternative Futures.” On Future War, July 13, 2023. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

NCSC. “UK and Allies Support Ukraine Calling out Russia’s GRU for New Malware Campaign,” August 31, 2023. https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/infamous-chisel/NCSC-MAR-Infamous-Chisel.pdf.

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.” Mandiant, November 9, 2023. https://www.mandiant.com/resources/blog/sandworm-disrupts-power-ukraine-operational-technology.

Rice, Dan. “The Untold Story of the Battle for Kyiv.” Small Wars Journal, May 31, 2022. https://smallwarsjournal.com/jrnl/art/untold-story-battle-kyiv.

Security Service of Ukraine. “Cyber Operation of Russian Intelligence Services as a Component of Confrontation on the Battlefield.” Technical, August 8, 2023. https://ssu.gov.ua/uploads/files/DKIB/technical-report.pdf.

Smeets, Max. “The Strategic Promise of Offensive Cyber Operations.” *Strategic Studies Quarterly* 12, no. 3 (2018): 90–113. https://www.jstor.org/stable/26481911.

Soldatov, Andrei, and Irina Borogan. “Russian Cyberwarfare: Unpacking the Kremlin’s Capabilities.” CEPA, September 8, 2022. https://cepa.org/comprehensive-reports/russian-cyberwarfare-unpacking-the-kremlins-capabilities/.

Thornton, Rod, and Marina Miron. “Winning Future Wars: Russian Offensive Cyber and Its Vital Importance: In Moscow’s Strategic Thinking.” *The Cyber Defense Review* 7, no. 3 (2022): 117–35. https://www.jstor.org/stable/48682327.

Wilde, Gavin. “Cyber Operations in Ukraine: Russia’s Unmet Expectations.” Washington, DC: Carnegie Endowment for International Peace, December 12, 2022. https://carnegieendowment.org/research/2022/12/cyber-operations-in-ukraine-russias-unmet-expectations?lang=en.

———. “Why Cyber Attacks on Ukrainians Aren’t Working the Way Russia Expected.” Emissary, March 11, 2024. https://carnegieendowment.org/emissary/2024/03/why-cyber-attacks-on-ukrainians-arent-working-the-way-russia-expected?lang=en.