The 5×5—Conflict in Ukraine's information environment

atlanticcouncil.org/content-series/the-5x5/the-5x5-conflict-in-ukraines-information-environment/

March 22, 2023

Conflict Cybersecurity Defense Industry Defense Technologies Disinformation Europe & Eurasia Infrastructure Protection Intelligence Internet National Security Russia Security & Defense Technology & Innovation Ukraine

By Simon Handler

This article is part of The 5×5, a monthly series by the Cyber Statecraft Initiative, in which five featured experts answer five questions on a common theme, trend, or current event in the world of cyber. Interested in the 5×5 and want to see a particular topic, event, or question covered? Contact Simon Handler with the Cyber Statecraft Initiative at .

Just over one year ago, on February 24, 2022, Russia launched a full-scale invasion of neighboring Ukraine. The ensuing conflict, Europe's largest since World War II, has not only besieged Ukraine physically, but also through the information environment. Through kinetic, cyber, and influence operations, Russia has placed Ukraine's digital and physical information infrastructure—including its cell towers, networks, data, and the ideas that traverse them—in its crosshairs as it seeks to cripple Ukraine's defenses and bring its population under Russian control.

Given the privately owned underpinnings of the cyber and information domains by technology companies, a range of local and global companies have played a significant role in defending the information environment in Ukraine. From Ukrainian telecommunications operators to global cloud and satellite internet providers, the private sector has been woven into Ukrainian defense and resilience. For example, Google's Threat Analysis Group reported having disrupted over 1,950 instances in 2022 of Russian information operations aimed at degrading support for Ukraine, undermining its government, and building support for the war within Russia. The present conflict in Ukraine offers lessons for states as well as private companies on why public-private cooperation is essential to building resilience in this space, and how these entities can work together more effectively.

We brought together a group of experts to provide insights on the war being waged through the Ukrainian information environment and take away lessons for the United States and its allies for the future.

#1 How has conflict in the information environment associated with the war in Ukraine compared to your prior expectations?

Nika Aleksejeva, *resident fellow, Baltics, Digital Forensic Research Lab (DFRLab), Atlantic Council*:

“As the war in Ukraine started, everyone was expecting to see Russia conducting offensive information influence operations targeting Europe. Yes, we have identified and researched Russia’s coordinated information influence campaigns on Meta’s platforms and Telegram. These campaigns targeted primarily European countries, and their execution was unprofessional, sloppy, and without much engagement on respective platforms.”

Silas Cutler, *senior director for cyber threat research, Institute for Security and Technology (IST)*:

“A remarkable aspect of this conflict has been how Ukraine has maintained communication with the rest of the world. In the days leading up to the conflict, there was a significant concern that Russia would disrupt Ukraine’s ability to report on events as they unfolded. Instead of losing communication, Ukraine has thrived while continuously highlighting through social media its ingenuity within the conflict space. Both the mobilization of its technical workforce through the volunteer IT_Army and its ability to leverage consumer technology, such as drones, have shown the incredible resilience and creativity of the Ukrainian people.”

Roman Osadchuk, research associate, Eurasia, Digital Forensic Research Lab (DFRLab), Atlantic Council:

“The information environment was chaotic and tense even before the invasion, as Russia waged a hybrid war since at least the annexation of Crimea and war in Eastern Ukraine in 2014. Therefore, the after-invasion dynamic did not bring significant surprises, but intensified tension and resistance from Ukrainian civil society and government toward Russia’s attempts to explain its unprovoked invasion and muddle the water around its war crimes. The only things that exceeded expectations were the abuse of fact-checking toolbox WarOnFakes and the intensified globalization of the Kremlin’s attempts to tailor messages about the war to their favor globally.”

Emma Schroeder, *associate director, Cyber Statecraft Initiative, Digital Forensic Research Lab (DFRLab), Atlantic Council*:

“The information environment has been a central space and pathway throughout which this war is being fought. Russian forces are reaching through that space to attack and spread misinformation, as well as attacking the physical infrastructure underpinning this environment. The behavior, while novel in its scale, is the continuation of Russian strategy in Crimea, and is very much living up to expectations set in that context. What has surpassed expectations is the effectiveness of Ukrainian defenses, in coordination with allies and private sector partners. The degree to which the international community has sprung forward to provide aid and assistance is incredible, especially in the information environment where such global involvement can be so immediate and transformative.”

Gavin Wilde, *senior fellow, Technology and International Affairs Program, Carnegie Endowment for International Peace*:

"The volume and intensity of cyber and information operations has roughly been in line with my prior expectations, though the degree of private and commercial activity was something that I might not have predicted a year ago. From self-selecting out of the Russian market to swarming to defend Ukrainian networks and infrastructure, the outpouring of support from Western technology and cybersecurity firms was not on my bingo card. Sustaining it and modeling for similar crises are now key."

#2 What risks do private companies assume in offering support or partnership to states engaged in active conflict?

Aleksejeva: "Fewer and fewer businesses are betting on Russia's successful economical future. Additionally, supporting Russia in this conflict in any way is morally unacceptable for most Western companies. Chinese and Iranian companies are different. As for Ukraine, supporting it is morally encouraged, but is limited by many practicalities, such as supply chain disruptions amid Russia's attacks."

Cutler: "By providing support during conflict, companies risk becoming a target themselves. Technology companies such as Microsoft, SentinelOne, and Cloudflare, which have publicly reported their support for Ukraine, have been historically targeted by Russian cyber operations and are already familiar with the increased risk. Organizations with pre-conflict commercial relationships may fall under new scrutiny by nationally-aligned hacktivist groups such as Killnet. This support for one side over the other—whether actual or perceived—may result in additional risk."

Osadchuk: "An important risk of continuing business as usual [in Russia] is that it may damage a company's public image and test its declared values, since the continuation of paying taxes within the country-aggressor makes the private company a sponsor of these actions. Another risk for a private company is financial, since the companies that leave a particular market are losing their profits, but this is incomparable to human suffering and losses caused by the aggression. In the case of a Russian invasion, one of the ways to stop the war is to cut funding for and, thus, undermine the Russian war machine and support Ukraine."

Schroeder: "Private companies have long provided goods and services to combatants outside of the information environment. The international legal framework restricting combatants to targeting 'military objects' provides normative protection, as objects are defined as those 'whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage' in a manner proportional to the military gain foreseen by the operation. This definition, however, is still subject to the realities of conflict, wherein combatants will make those decisions to their own best

advantage. In the information environment, this question becomes more complicated, as cyber products and services often do not fall neatly within standard categories and where private companies themselves own and operate the very infrastructure over and through which combatants engage. The United States and its allies, whether on a unilateral of supranational basis, work to better define the boundaries of civilian 'participation' in war and conflict, as the very nature of the space means that their involvement will only increase."

Wilde: "On one hand, it is important not to falsely mirror onto others the constraints of international legal and normative frameworks around armed conflict to which responsible states strive to adhere. Like Russia, some states show no scruples about violating these frameworks in letter or spirit, and seem unlikely to be inhibited by claims of neutrality from companies offering support to victimized states. That said, clarity about where goods and services might be used for civilian versus military objectives is advisable to avoid the thresholds of 'direct participation' in war outlined in International Humanitarian Law."

#3 What useful lessons should the United States and its allies take away from the successes and/or failures of cyber and information operations in Ukraine?

Aleksejeva: "As for cyber operations, so far, we have not seen successful disruptions achieved by Russia of Ukraine and its Western allies. Yes, we are seeing constant attacks, but cyber defense is much more developed on both sides than before 2014. As for information operations, the United States and its allies should become less self-centered and have a clear view of Russia's influence activities in the so-called Global South where much of the narratives are rooted in anti-Western sentiment."

Cutler: "Prior to the start of the conflict, it was strongly believed that a cyber operation, specifically against energy and communication sectors, would act as a precursor to kinetic action. While a WannaCry or NotPetya-scale attack did not occur, the AcidRain attack against the Viasat satellite communication network and other attacks targeting Ukraine's energy sector highlight that cyber operations of varying effectiveness will play a role in the lead up to a military conflict."

Osadchuk: "First, cyber operations coordinate with other attack types, like kinetic operations on the ground, disinformation, and influence operations. Therefore, cyberattacks might be a precursor of an upcoming missile strike, information operation, or any other action in the physical and informational dimensions, so allies could use cyber to model and analyze multi-domain operations. Finally, preparation for and resilience to information and cyber operations are vital in mitigating the consequences of such attacks; thus, updating defense doctrines and improving cyber infrastructure and social resilience are necessary."

Schroeder: "Expectations for operations in this environment have exposed clear fractures in the ways that different communities define as success in a wartime operation. Specifically, there is a tendency to equate success with direct or kinetic battlefield impact. One of the biggest lessons that has been both a success and a failure throughout this war is the role

that this environment can play. Those at war, from ancient to modern times, have leveraged every asset at their disposal and chosen the tool they see as the best fit for each challenge that arises—cyber is no different. While there is ongoing debate surrounding this question, if cyber operations have not been effective on a battlefield, that does not mean that cyber is ineffective, just that expectations were misplaced. Understanding the myriad roles that cyber can and does play in defense, national security, and conflict is key to creating an effective cross-domain force.

Wilde: "Foremost is the need to check the assumption that these operations can have decisive utility, particularly in a kinetic wartime context. Moscow placed great faith in its ability to convert widespread digital and societal disruption into geopolitical advantage, only to find years of effort backfiring catastrophically. In other contexts, better trained and resourced militaries might be able to blend cyber and information operations into combined arms campaigns more effectively to achieve discrete objectives. However, it is worth reevaluating the degree to which we assume offensive cyber and information operations can reliably be counted on to play pivotal roles in hot war."

More from the Cyber Statecraft Initiative:

#4 How do comparisons to other domains of conflict help and/or hurt understanding of conflict in the information domain?

Aleksejeva: "Unlike conventional warfare, information warfare uses information and psychological operations during peace time as well. By masking behind sock puppet or anonymous social media accounts, information influence operations might be perceived as legitimate internal issues that polarize society. A country might be unaware that it is under attack. At the same time, as the goal of conventional warfare is to break an adversary's defense line, information warfare fights societal resilience by breaking its unity. 'Divide and rule' is one of the basic information warfare strategies."

Cutler: "When looking at the role of cyber in this conflict, I think it is critical to examine the history of Hacktivist movements. This can be incredibly useful for understanding the influences and capabilities of groups like the IT_Army and Killnet."

Osadchuk: "The information domain sometimes reflects the kinetic events on the ground, so comparing these two is helpful and could serve as a behavior predictor. For instance, when the Armed Forces of Ukraine liberate new territories, they also expose war crimes, civilian casualties, and damages inflicted by occupation forces. In reaction to these revelations, the Kremlin propaganda machine usually launches multiple campaigns to distance themselves, blame the victim, or even denounce allegations as staged to muddy the waters for certain observers."

Schroeder: “It is often tricky to carry comparisons over different environments and context, but the practice persists because, well, that is just what people do—look for patterns. The ability to carry over patterns and lessons is essential, especially in new environments and with the constant developments of new tools and technologies. Where these comparisons cause problems is when they are used not as a starting point, but as a predetermined answer.”

Wilde: “It is problematic, in my view, to consider information a warfighting ‘domain,’ particularly because its physical and metaphorical boundaries are endlessly vague and evolving—certainly relative to air, land, sea, and space. The complexities and contingencies in the information environment are infinitely more than those in the latter domains. However talented we may be at collecting and analyzing millions of relevant datapoints with advanced technology, these capabilities may lend us a false sense of our ability to control or subvert the information environment during wartime—from hearts and minds to bits and bytes.”

#5 What conditions might make the current conflict exceptional and not generalizable?

Aleksejeva: “This war is neither ideological nor a war for territories and resources. Russia does not have any ideology that backs up its invasion of Ukraine. It also has a hard time maintaining control of its occupied territories. Instead, Russia has many disinformation-based narratives or stories that justify the invasion to as many Russian citizens as possible including Kremlin officials. Narratives are general and diverse enough, so everyone can find an explanation of the current invasion—be it the alleged rebirth of Nazism in Ukraine, the fight against US hegemony, or the alleged historical right to bring Ukraine back to Russia’s sphere of influence. Though local, the war has global impact and makes countries around the world pick sides. Online and social media platforms, machine translation tools, and big data products provide a great opportunity to bombard any internet user in any part of the world with pro-Russia massaging often tailored to echo historical, racial, and economic resentments especially rooted in colonial past.”

Cutler: “During the Gulf War, CNN and other cable news networks were able to provide live coverage of military action as it was unfolding. Now, real-time information from conflict areas is more broadly accessible. Telegram and social media have directly shaped the information and narratives from the conflict zone.”

Osadchuk: “The main difference is the enormous amount of war content, ranging from professional pictures and amateur videos after missile strikes to drone footage of artillery salvos and bodycam footage of fighting in the frontline trenches—all making this conflict the most documented. Second, this war demonstrates the need for drones, satellite imagery, and open-source intelligence for successful operations, which distances it from previous conflicts and wars. Finally, it is exceptional due to the participation of Ukrainian civil society in

developing applications, like the one alerting people about incoming shelling or helping find shelter; launching crowdfunding campaigns for vehicles, medical equipment, and even satellite image services; and debunking Russian disinformation on social media."

Schroeder: "One of the key lessons we can take from this war is the centrality of the global private sector to conflict in and through the information environment. From expedited construction of cloud infrastructure for the Ukrainian government to Ukrainian telecommunications companies defending and restoring services along the front lines to distributed satellite devices, providing flexible connectivity to civilians and soldiers alike, private companies have undoubtedly played an important role in shaping both the capabilities of the Ukrainian state and the information battlespace itself. While we do not entirely understand the incentives that drove these actions, an undeniable motivation that will be difficult to replicate in other contexts is the combination of Russian outright aggression and comparative economic weakness. Companies and their directors felt motivated to act due to the first and, likely, free to act due to the second. Private sector centrality is unlikely to diminish and, in future conflicts, it will be imperative for combatants to understand the opportunities and dependencies that exist in this space within their own unique context."

Wilde: "My sense is that post-war, transatlantic dynamics—from shared norms to politico-military ties—lent significant tailwinds to marshal resource and support to Ukraine (though not as quickly or amply from some quarters as I had hoped). The shared memory of the fight for self-determination in Central and Eastern Europe in the late 1980s to early 1990s still has deep resonance among the publics and capitals of the West. These are unique dynamics, and the degree to which they could be replicated in other theaters of potential conflict is a pretty open question."

***Simon Handler** is a fellow at the Atlantic Council's Cyber Statecraft Initiative within the Digital Forensic Research Lab (DFRLab). He is also the editor-in-chief of The 5×5, a series on trends and themes in cyber policy. Follow him on Twitter @SimonPHandler.*

The Atlantic Council's **Cyber Statecraft Initiative**, under the Digital Forensic Research Lab (DFRLab), works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology.

learn more
Related Experts: Nika Aleksejeva, Roman Osadchuk, and Emma Schroeder

Image: Russian bombardment of telecommunications antennas in Kyiv. Credit: Ministry of Internal Affairs of Ukraine (licensed under the Creative Commons Attribution 4.0 International License)