EUROPEAN CYBER CONFLICT RESEARCH INITIATIVE

Workshop Report

The Cyber Dimensions of the Russia-Ukraine War

Taylor Grossman, Monica Kaminska, James Shires, and Max Smeets

April 2023

The event and workshop report were generously supported by the UK National Cyber Security Centre as part of broader efforts to enhance the UK’s thought leadership engagement in cyber security.

Introduction

On the 28th of February 2023, the European Cyber Conflict Research Initiative (ECCRI) held a workshop to reflect on wartime cyber operations in Ukraine. The event included cyber threat intelligence practitioners, academics, and officials from key governments and international institutions. The workshop was invite-only and held under the Chatham House Rule to allow participants to share their frank thoughts and reflections. In consultation with the attendees, ECCRI has written this report to highlight key lines of discussion.

This workshop report builds upon a previous report by ECCRI on wartime cyber operations in Ukraine, based on a closed-door workshop held in Tallinn in May 2022, just three months after the full-scale invasion of Ukraine.

Table of Contents

The Cyber Dimensions of the Russia-Ukraine War

In the twelve months since Russia's large-scale invasion of Ukraine in February 2022, influential narratives have developed around a supposedly "missing" cyber element. In the first few weeks, observers and analysts were quick to claim that cyber operations were absent from early battles. Some interpreted this as evidence of the ineffectiveness of cyber operations in kinetic conflict, while others warned of the coming "cyber war". Since then, reporting from threat intelligence practitioners and researchers has shed light on multiple cyber dimensions of the ongoing conflict, weakening early scepticism.

Key takeaways from the report:

- In line with its doctrine of information confrontation, Russia employed a variety of cyber operations during the war at an unprecedented scale.
- The primary goals of wartime operations – sabotage, influence, and espionage – have remained constant. Cyber operations provide new opportunities to achieve age-old objectives.
- Cyber activity in Ukraine is associated with kinetic activity bursts and lulls.
- The GRU has adopted a flexible approach with "pure wipers" that are easy to manipulate and launch without draining significant resources.
- Western observers may overestimate coordination between Russian-aligned criminals and the Russian government.
- Distinguishing between cyber criminal and political activist groups is becoming increasingly difficult.
- Initiatives such as the IT Army risk blurring important principles of distinction between combatants and non-combatants.
- Responsibilities for cyber defence are shifting between public and private actors, with industry delivering capacity at scale.
- While Ukraine has benefited from unity of purpose across many different Western actors, this conflict may not provide a good roadmap for the future.

Organising for Cyber: The Russian State

Russian cyber operations do not stem from a single unit or agency, but rather from a complicated bureaucratic morass. Participants highlighted the differing approaches that the Russian Federal Security Service (FSB) and the Main Directorate of the General Staff of the Armed Forces (GRU) adopt toward cyber operations, while noting that doctrinal and operational distinctions remain poorly understood. Although the FSB was originally focused on domestic affairs, it has increasingly shifted its attention abroad. The FSB is in charge of intelligence collection and counterintelligence and was long the primary Russian actor in cyberspace. Meanwhile, the GRU has become a much more prominent actor.

GRU's Leading Role in Cyber Operations

Recently, the GRU has taken a leading role in cyber operations, investing significant capability and capacity in an information operations force (*voyska informatsionnykh operatsiy,* or VIO).[1] The VIO was established in May 2014 within the GRU.[2] Since the February 2022 invasion, the GRU has sustained an operational tempo that is much higher than anything previously seen. As several participants agreed, the GRU has worked to combine informational technical effects (sabotage, destruction, etc.) with influence operations to achieve psychological impact. While it is hard to meaningfully measure the impact of these activities, participants agreed that the GRU is operating at an unprecedented volume of activity.

Some participants noted that the GRU is plagued by bureaucratic in-fighting, but that it also has needed to prove itself to Russian leadership. The GRU's mandate in

[1] See: Bilyana Lilly and Joe Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," in *20/20 Vision: The Next Decade* (12th International Conference on Cyber Conflict, Tallinn, Estonia, 2020).

[2] See: "Istochnik v Minoborony: V Vooruzhennykh Silakh RF Sozdany Voyska Informatsionnykh Operatsiy [Source in the Ministry of Defense: Information Operations Troops Created in the Armed Forces of the Russian Federation]," *TASS*, May 12, 2014, https://tass.ru/politika/1179830; cited in Lilly and Cheravitch, "The Past, Present, and Future of Russia's Cyber Strategy and Forces," 140–42.

cyberspace has grown rapidly in the past decade, and participants thought that the organisation feels it must justify this expansion. Throughout the last year of the war in Ukraine, the GRU has operated with amazing speed and flexibility, despite inconsistencies in its doctrine.

In the past, the West has viewed Russia as a reckless actor with a high tolerance for risk in cyberspace. In some ways, as several participants noted, this history of Russian cyber operations may be undermining the country's own trust in its operators. This incongruity makes the GRU's position even more fragile and can perhaps explain the high volume of swift attacks we are seeing today, as GRU operatives attempt to demonstrate proof of concept to Russian leadership.

Cyber Professionalism in the Russian Military

How well does the Russian military understand what their cyber operators can and cannot do? In other words, how does the Russian military understand itself? Participants agreed that when conducting cyber activities, the operational realities within the Russian state are complex and multifaceted. Attendees generally agreed that while some units are well-drilled and exhibit professionalism, others are much less formalised.

At least on paper, Russian practitioners should be familiar with how different organisational components work independently and together when conducting cyber operations. However, this may not translate well into practice. Information confrontation groups were formed specifically to work on integrating Russian cyber operations and were first used in an exercise in 2016.[3] This timeline supposedly gives the Russian military up to six years of established practice prior to the full-scale invasion. Information confrontation centres also appear to exist within each of Russia's military districts and are integrated within the VIO.[4] At least in theory, these components have been exercising together and have developed some degree of

[3] See: "Армия России Впервые Отработала Информационное Противоборство На Учениях «Кавказ-2016»," *Zvezda*, September 14, 2016, https://tvzvezda.ru/news/201609141221-va0s.htm.

[4] See: Joe Cheravitch, "The Role of Russia's Military in Information Confrontation," Occasional Paper (Arlington, Virginia: CNA, June 2021); "Центры Информационных Операций ГРУ ГШ в Ваших Руках," *Слив ТОП* (blog), July 22, 2022, https://sliv.top/2022/07/22/czentry-informaczionnyh-operaczij-gru-gsh-v-vashih-rukah/.

cross-functional coordination. However, several participants were sceptical of whether these new centres and practices have made significant headway in formalising and professionalising Russian cyber forces.

Coordination is particularly difficult for the GRU, which maintains a broad and disparate ecosystem of external parties. Not all GRU cyber expertise is in-house; rather, the GRU leans heavily on contractors, "hacktivists", and other state-affiliated actors. As several participants pointed out, this ecosystem is rapidly expanding as the war effort continues, making coordination and centralisation even more difficult.

Coordination is particularly difficult for the GRU, which maintains a broad and disparate ecosystem of external parties.

Participants agreed that in terms of targeting decisions for cyber operations, nothing seems to be off limits for the GRU. The GRU is not concerned with international humanitarian law (IHL) or other international law; rather, GRU targeting is driven by leadership demands. Participants generally agreed that if asked to do so, the GRU would not hesitate to target a non-governmental organisation (NGO) or even a hospital in a cyber operation. However, some attendees noted that the GRU may avoid such targets because of fears of possible escalation with NATO. Attendees also debated whether the GRU might place some targets off limits for cyber operations because they could not guarantee that cyber operations could achieve a narrow and decisive effect. The GRU may want to calibrate its cyber operations in such a way that they can be controlled and sustained, rather than spreading beyond the organisation's control. In this way, the GRU and other Russian military actors may act cautiously for strategic reasons, rather than out of a sense of moral or normative obligation.

Russia's Audience

Understanding Russia's intentions through its behavior in cyberspace continues to prove challenging. Russian doctrine does not draw clear distinctions between information operations and cyber effects operations; rather, Russia's primary objective is to have a cognitive effect on its intended target by shaping the information space. Russia certainly wants to destabilise Western institutions and create distrust in

Western populations. Yet, measuring the effects of Russian operations can be extremely difficult, and few Western governments have a mature model for dealing with the effects of Russian disinformation and information operations.

Western governments are too often parochial in their understanding of information operations, dismissing Russian disinformation that does not appear to deeply resonate in their own constituencies. Russia, however, may not be interested in shaping attitudes in the UK or the US; instead, Russia seems to be focusing on changing minds in the Global South, where it sees it could have greater impact. Several participants pointed out that while Western governments have held firm in sanctioning Russia, very few countries in Africa, Latin America, and Southeast Asia have joined the sanctions regime. This situation may have been influenced by Russian information operations; several participants pointed to this outcome as a possible symptom of Internet fragmentation in action.

Russia is also seeking out allies in the United Nations Open-Ended Working Group (OEWG), courting smaller states to back up its proposals and help curtail efforts by the United States and others. One participant noted that Russia has explicit instructions for states about what they hope will emerge (and what they hope will not emerge) from these forums. While Russia attempts to create distrust in Western institutions, it is also attempting to insulate its own Internet architecture. Attendees agreed that internet fragmentation is a real possibility, as Russia intends to create its own sovereign system.[5]

[5] On Internet fragmentation, see: Kevin Kohler, "One, Two, or Two Hundred Internets? The Politics of Future Internet Architectures," Cyberdefense Report (Zurich: CSS, ETH Zurich, August 2022), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-08-One-Two-or-Two-Hundred-Internets.pdf; on the UN processes, see: Taylor Grossman, "Norms vs. Realities: Cyber at the UN," *CSS Analyses in Security Policy*, no. No. 313 (November 2022), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse313-EN.pdf; Valentin Weber, "The Dangers of a New Russian Proposal for a UN Convention on International Information Security," *Net Politics, Council on Foreign Relations* (blog), March 21, 2023, https://www.cfr.org/blog/dangers-new-russian-proposal-un-convention-international-information-security?utm_medium=social_owned&utm_source=tw.

Coordinating Kinetic and Cyber Operations

The volume of Russian-attributed or supported cyberattacks occurring in Ukraine is unprecedented: the Russians are maintaining a very high operational tempo. Participants identified several distinct types of Russian-attributed cyber operations that have occurred in Ukraine, including denial-of-service or distributed denial-of-service attacks (DoS or DDoS), destructive attacks or cyber effects operations, data weaponisation, and disinformation.[6]

Wipers have become a common feature of the invasion. Threat intelligence organisations have reported at least 16 wipers since the start of the invasion.[7] Interestingly, none have been self-spreading, with the exception (in some instances) of HermeticWiper, an early wiper explored in more depth below. These newer wipers have operated quite differently from NotPetya, which spread far beyond its initial targets and helped solidify Russia's reputation as a reckless cyber actor.[8] Russia also appears to be rectifying the mistake it made with AcidRain, the wiper used against ViaSat that spread to Western targets within the first few hours of the invasion.[9]

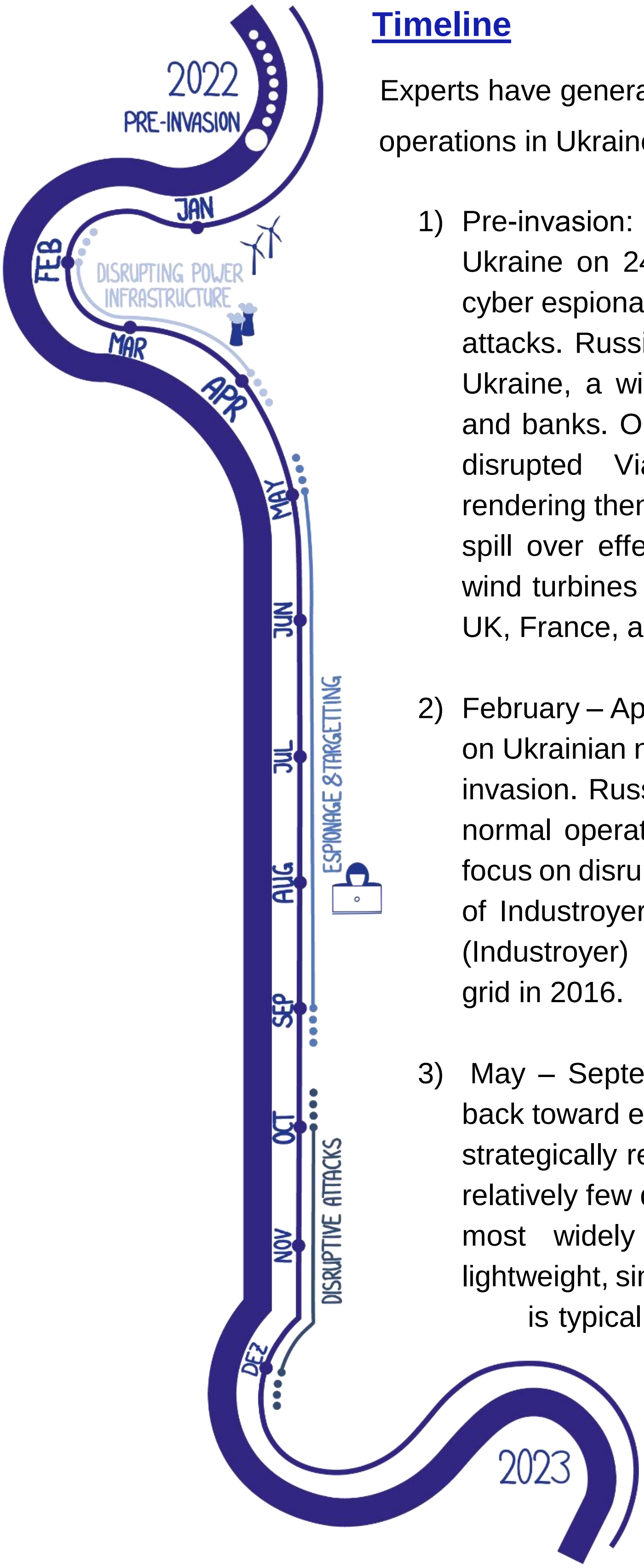
[6] A few attendees also asserted that we need to be careful with our language: the phrase "cyberattack" is used to encompass a wide range of activities. Web defacement, for example, is very different from an attack on a cyber-physical system, and so on.

[7] See: Andy Greenberg, "Ukraine Suffered More Data-Wiping Malware Last Year than Anywhere, Ever," *Wired*, February 22, 2023, https://www.wired.com/story/ukraine-russia-wiper-malware/; "A Year of Wiper Attacks in Ukraine," *We Live Security by ESET* (blog), February 24, 2023, https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/; Geri Revay, "The Year of the Wiper," *Fortiguard Labs Threat Research* (blog), January 24, 2023, https://www.fortinet.com/blog/threat-research/the-year-of-the-wiper.

[8] Also see: Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Random House, 2020).

[9] See also: Rob Joyce, "Nation State Threat Actors and How to Detect and Prevent Threats Before They Happen" (Mandiant Worldwide Information Security Exchange, Washington, DC, October 18, 2022), https://www.youtube.com/watch?v=b0jRdcywc7U; Juan Andres Guerrero-Saade and Max van Amerongen, "AcidRain - A Modem Wiper Rains Down on Europe," *Sentinel Labs* (blog), March 31, 2022, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/; Katrina Manson, "The Satellite Hack Everyone Is Finally Talking About," *Bloomberg*, March 1, 2023, https://www.bloomberg.com/features/2023-russia-viasat-hack-ukraine/.

Timeline



Experts have generally seen several distinct phases of cyber operations in Ukraine:

1) Pre-invasion: prior to Russia's full-scale invasion into Ukraine on 24 February, Russia primarily conducted cyber espionage to pre-position forces ahead of kinetic attacks. Russia also launched HermeticWiper against Ukraine, a wiper that targeted government agencies and banks. On the day of the invasion, a cyberattack disrupted Viasat KA-SAT modems in Ukraine, rendering them unusable. The Viasat incident also had spill over effects into other countries, shutting down wind turbines in Germany and causing outages in the UK, France, and elsewhere.

2) February – April: Several distinct wipers were deployed on Ukrainian networks at the beginning of the full-scale invasion. Russia appeared to be attempting to disrupt normal operations of the government, with a specific focus on disrupting power infrastructure with the launch of Industroyer2, a new variant of an earlier malware (Industroyer) that had targeted the Ukrainian power grid in 2016.

3) May – September: Russian cyber operations turned back toward espionage, attempting to gain footholds in strategically relevant networks. During this period with relatively few destructive attacks, CaddyWiper was the most widely deployed wiper. CaddyWiper is a lightweight, simple, and easily reconfigurable wiper that is typically spread through Microsoft group policy administration settings.

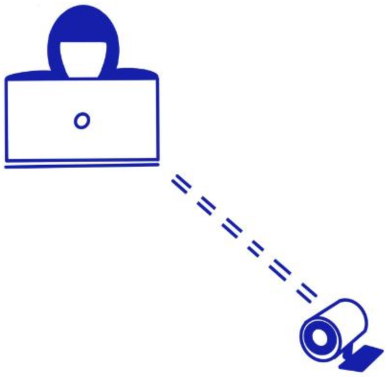
4) October – End of 2022: we witnessed a renewed campaign of destructive cyberattacks, including a spike in the use of wipers.

Generally, the phases laid out above correspond with the broad phases of Russia's kinetic campaign in Ukraine.[10] Cyber effects operations, cyber espionage operations, and information operations are supporting kinetic activities in different ways.

Coordination or Coincidence?

When it came to deciphering the connections between specific cyber and kinetic operations, however, participants disagreed in their conclusions. Participants generally affirmed that the launch of HermeticWiper on 23 February was timed to coincide with the kinetic invasion.[11] In this instance, extensive planning likely took place to allow for such close coordination of attacks. However, in the case of the Viasat attack, attendees disagreed. Some participants believed that the incident was a clear example of strategic level coordination, while others were less convinced.

Major shifts in kinetic activity have coincided with new uses of cyber operations.[12] As the war shifted to the Donbas and into the Eastern front, for example, Russian operators began hacking into webcams along the Ukrainian border in what appeared to be surveillance activity.[13] Russia also began targeting several situational awareness applications Ukraine



[10] See: Roncone and Wolfram, "Cyber War on the Edge: A Balance of Access and Action"; as covered in Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless"; "A Year of Russian Hybrid Warfare in Ukraine" (Microsoft Threat Intelligence, March 15, 2023), https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf; Dan Black, "Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences" (The International Institute for Strategic Studies, 2023); "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape" (Google, February 2023), https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

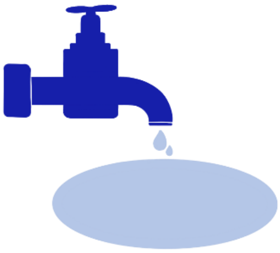
[11] See: Juan Andres Guerrero-Saade, "HermeticWiper | New Destructive Malware Used in Cyber Attacks on Ukraine," *Sentinel Labs* (blog), February 23, 2022, https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/.

[12] See: "Russia's Cyber Tactics: Lessons Learned 2022" (State Service of Special Communications and Information Protection of Ukraine, March 2023), https://cip.gov.ua/en/news/cyberwar-lessons-weak-it-ecosystems-allow-the-enemy-to-access-sensitive-data-in-ukraine.

[13] See: Joyce, "Nation State Threat Actors and How to Detect and Prevent Threats Before They Happen"; Ofir Dor, "How Threat Intelligence Became Key to Microsoft's Computer Security," *Globes*, September 1, 2022, https://en.globes.co.il/en/article-how-threat-intelligence-became-key-to-microsofts-computer-security-1001423167 (John Lambeth, head of MSTIC, notes that Russia hacked into webcames along the border in January 2022); Maggie Miller, "Russia's Cyberattacks Aim to 'terrorize' Ukrainians," *Politico*, January 11, 2023, https://www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561.

had launched to facilitate communication, including Delta App.[14] Delta App is used by the Ukrainian military to share battlefield information, integrating a variety of sources including surveillance satellites, sensors, and intelligence from a network of participants (including troops and civilians).

As Ukraine began its counteroffensive, Russia appeared to ramp up its targeting of critical infrastructure, particularly against the energy sector. Three wipers were launched in parallel that targeted water infrastructure and other critical national infrastructure. For several of these attacks, Russia appeared to use intrusions attained months prior; some participants asserted that Russia deliberately held on to this information for months to coordinate its cyber activities with its kinetic operations.[15]



In cyberspace, activity can be both opportunistic and strategic.

However, other attendees were more skeptical of the timing analysis above, claiming that much seeming coordination is simply chance or opportunism. Attendees agreed that in cyberspace, opportunistic activity can also be strategic: in most cases, it is beneficial to get access wherever and whenever you can. Participants also conceded that it is unlikely we will ever know for certain how much of what we see is the result of opportunism or strategic planning, or perhaps a combination of both.

Often, observers expect Russia to leverage kinetic and cyber operations through combined arms: where different combat arms of a military are integrated to achieve mutually complementary and sustaining efforts. However, as one participant pointed out, combined arms operations are incredibly difficult. Instead, Russia appears to be experimenting with different methods of integration, pairing cyber and kinetic operations together in a variety of distinct supporting and coordinated relationships.

[14] See: “Cyberattack on Delta System Users Using RomCom/FateGrab/StealDeal Malware (CERT-UA#5709)” (CERT-UA, December 18, 2022), https://cert.gov.ua/article/3349703.
[15] See: Black, “Russia’s War in Ukraine: Examining the Success of Ukrainian Cyber Defences.”

What can we expect moving forward?

Russian cyber operations will keep evolving as the war continues. Participants agreed that we have already seen some evolution in Russian cyber activity, as operators respond to on-the-ground developments. The GRU has adopted a much more flexible approach, launching "pure wipers" (without worming capabilities) that are easy to change and manipulate quickly, and can be built and launched without draining significant resources from the traditional development ecosystem that supports cyberattacks. Indeed, the GRU has shifted toward using CaddyWiper in recent months, likely because it is easy to use and quick to develop and then discard.[16]

The GRU has adopted a fast-paced, flexible approach to cyber operations, launching "pure wipers" that are easy to change and manipulate quickly.

Looking to the future trajectory of the conflict, participants anticipated the increased use of throwaway or single-use wipers because of the strengths outlined above. Participants tended to agree that we are unlikely to see multifunctional wipers like NotPetya emerge in the coming months in Ukraine, although they disagreed on the reasons why this will likely be the case. Some attendees argued that the GRU simply does not have the resources to launch the kind of development cycles needed to create a complex wiper at this point in its war efforts. Others, meanwhile, believed Russia may be saving more sophisticated malware for the future. Finally, a few participants wondered if Russia's shift toward pairing down modular activities is a result of decisions around equities, taking a more cautious approach as to when to "burn" its best capabilities.[17] Industroyer2, for example, is only one module from

[16] See: Daryna Antoniuk, "A Deeper Look at the Malware Being Used on Ukrainian Targets," *The Record*, April 21, 2022, https://therecord.media/a-deeper-look-at-the-malware-being-used-on-ukrainian-targets; Gabby Roncone and John Wolfram, "Cyber War on the Edge: A Balance of Access and Action" (CyberwarCon, Arlington, Virginia, November 10, 2022), https://www.cyberwarcon.com/cyber-war-on-the-edge; as cited in Andy Greenberg, "Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless," *Wired*, November 10, 2022, https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/.

[17] There might be similar considerations for Russia with respect to the use of zero-day exploits. See: James Sadowski and Casey Charrier, "Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace," *Mandiant* (blog), March 20, 2023, https://www.mandiant.com/resources/blog/zero-days-exploited-2022.

Industroyer1.[18] Regardless, participants generally concurred that we are likely to see more generic payloads going forward.

Participants also agreed that we will likely see more commercial ransomware being used in Ukraine. These tools are easy to obtain and can achieve useful effects cheaply and quickly. Since October 2022, we have already witnessed this shift toward commercial ransomware, and most participants agreed that this trend will continue. The ability to bootstrap criminal capabilities to provide new attack opportunities will prove increasingly important, as operator burnout threatens to become a real challenge for Russia.[19]

Commercial ransomware will likely become more common in Ukraine.

Several participants noted that FSB-associated group Turla has also been more active recently in conducting espionage activities in Ukraine.[20] One participant argued that other intelligence services do not appear to be engaging in cyber effects operations, at least at the present.

Changes in Russian military leadership have often led to changes in cyber strategy. General Valery Gerasimov**,** who has served as Chief of the General Staff of the Russian Armed Forces since 2012, is once again in charge of the Russian war effort. In an effort to elevate the leadership of the war effort, Gerasimov replaced General Sergei Surovikin in January 2023.[21] Gerasimov certainly faces significant pressure to

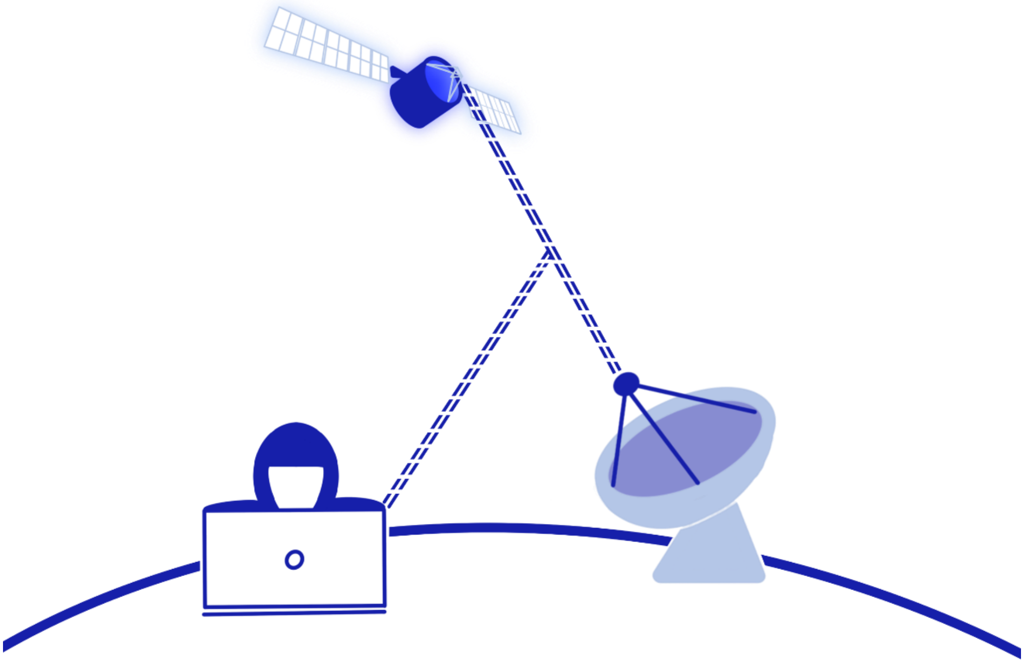
[18] See: Daniel Kapellmann Zafra et al., "INDUSTROYER.V2: Old Malware Learns New Tricks," *Mandiant* (blog), April 25, 2022, https://www.mandiant.com/resources/blog/industroyer-v2-old-malware-new-tricks; Anton Cherepanov and Robert Lipovsky, "Industroyer: Biggest Threat to Industrial Control Systems since Stuxnet," *We Live Security by ESET* (blog), June 12, 2017, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/; Alan Haji, "Industroyer - Crash Override (2016)," *Cyberlaw CCDCOE Wiki*, June 4, 2021, https://cyberlaw.ccdcoe.org/wiki/Industroyer_%E2%80%93_Crash_Override_(2016).

[19] Also see: Clint Watts, "Is Russia Regrouping for Renewed Cyberwar?," *Microsoft* (blog), March 15, 2023, https://blogs.microsoft.com/on-the-issues/2023/03/15/russia-ukraine-cyberwarfare-threat-intelligence-center/.

[20] See: Sarah Hawley et al., "Turla: A Galaxy of Opportunity," *Mandiant* (blog), January 5, 2023, https://www.mandiant.com/resources/blog/turla-galaxy-opportunity.

[21] Peter Beaumont and Pjotr Sauer, "Russia Replaces General in Charge of Ukraine War in Latest Military Shake-Up," *The Guardian*, January 11, 2023, https://www.theguardian.com/world/2023/jan/11/russia-replaces-general-in-charge-of-ukraine-war-in-latest-military-shake-up.

achieve results, and his appointment could impact the kinds of cyber activities we see Russia pursuing. In the past, Gerasimov has been a strong proponent of using information operations to influence both people and institutions.[22]



Regarding future targeting, some participants pointed to Starlink, though overall attendees were divided as to whether the satellite constellation would become a significant target of Russian activity, or whether the international media attention has overblown its strategic value. Both could perhaps be true.

[22] Lilly and Cheravitch, “The Past, Present, and Future of Russia’s Cyber Strategy and Forces,” 134.

Limits to Visibility and Analysis

Throughout the discussion, attendees reflected on the limitations of cyber intelligence and the constraints on analysing cyber operations without deeper awareness of the full range of military activity in Ukraine. In this sense, participants agreed that we may be too myopic in our attempts to understand cyber and kinetic integration. Cyber operations do not simply serve as a kinetic equivalent: rather, cyber operations can fit into conflict in many ways, and we need to think about the enabling effects of cyber activities rather than simply their substitution effects. Even if we were able to determine that every kinetic attack was preceded by and coordinated with a cyberattack, what would that necessarily tell us?

We need to think about the enabling effects of cyber activities rather than simply their substitution effects.

Several participants also noted that if observers and practitioners rely too heavily on cyber activity as evidence of coming kinetic activity, they could become easily diverted. Take, for example, the Normandy Landings in WWII: the Allies planted a significant number of false indicators to persuade the Axis powers that the landing would happen in a different place entirely, leaving Normandy lightly defended. One could imagine how cyber activity could become a ruse in much the same way, diverting attention from more serious pending attacks. Participants agreed that while we do need to understand linkages between cyber and kinetic operations, we should be very careful with what such information ultimately tells us about an adversary's overall strategy. The confluence of intelligence, industry insights, and academic expertise is critical to making sense of cyber operations, particularly amidst the fog of war.

Furthermore, western observers still have quite limited visibility into the military planning of Russia, and many cyber incidents have been unreported. This is particularly true for the threat intelligence sector, where the day-to-day focus is almost exclusively on cyber operations, and it can be hard to have an accurate picture of the entire conflict.[23] Furthermore, threat intelligence professionals do not always have the requisite skillset or priorities to track the conflict's full evolution both digitally and kinetically. Threat intelligence organisations are focused on incident response engagement and tracking APTs, and not necessarily on conventional military activities unless they are in some way directly related to cyber activities they are already tracking. However, as several participants pointed out, traditional state intelligence organisations also struggle to obtain visibility. Both communities should leverage each other's strengths to paint a complete picture of Russian activities.

Threat intelligence professionals do not always have the requisite skillsets or priorities to track the conflict's full evolution both digitally and kinetically.

Finally, Ukraine is creating another interesting and often subtle barrier to full visibility: it is curating the kind of information that Western companies and governments can see. While the Ukrainian government has talked openly about some cyber incidents that have targeted civilian infrastructure, it has offered little visibility into its offensive cyber activity on the military side. As one participant observed, Ukraine's operational security has been very tight since the onset of the war.

[23] Also see: "De Russische aanval op Oekraïne: een keerpunt in de geschiedenis" (AIVD & MIVD, February 2023), https://www.defensie.nl/binaries/defensie/documenten/publicaties/2023/02/20/publicatie-aivd-en-mivd-24-2/Brochure_24-2+De+Russiche+aanval+op+Oekraine_TG_web.pdf;; Alexander Martin, "Dutch Intelligence: Many Cyberattacks by Russia Are Not yet Public Knowledge," *The Record*, February 22, 2023, https://therecord.media/dutch-intelligence-russia-cyberattacks-many-not-yet-public-knowledge.

The Role of Cyber Criminal Actors and Hacktivists

The landscape of cyber actors in Ukraine has become ever murkier, with criminals and political activists adopting visible roles in the conflict. Western observers often ascribe too much coordination between Russian state organisations and criminal groups, yet the Kremlin does exert informal pressures on the enterprises operating within its borders. Meanwhile, the line between criminal and hacktivist is shifting, with some major organisations becoming increasingly politicised, while others claim political allegiances largely out of convenience. New types of actors are also taking the stage: the IT Army of Ukraine has brought individuals from around the world onto the digital battlefield.

Coordination Between State and Cyber Criminal Actors

How do we organise information on non-state actors in cyberspace in a way that is meaningful, in relation to state actors? And which non-state actors have actually had strategic effect? Western observers frequently assume too much coordination between Russian-aligned criminal actors and the Russian government. In the case of the Colonial Pipeline ransomware attack, for example, American audiences were quite ready to believe that the action was a Russian state operation. Similarly, in Ukraine, observers have been quick to tie criminal actors to the Russian government, assuming that the targeting of Ukrainian institutions and companies was intentional and strategic.

The reality, however, is much more complex. Russia is generally a safe harbour state for cyber criminals, and the Russian state has played a key role in permitting ransomware to become a major global threat. Several participants noted that while the Russian government has general parameters that it does not allow criminal groups to trespass – for example, not targeting Russia-based organisations – state actors do not usually directly channel criminal activities. A few attendees argued that in many cases, ransomware groups conduct operations with political impact almost accidentally, with the targeting decisions based on potential financial gain.

Yet, the linkages between criminal groups and the Kremlin are not always clear-cut. Some participants asserted that while Russia may not directly control criminal actors operating within its borders, the Kremlin still has considerable influence over these groups: the Russian government can very quickly create linkages with criminal actors if and when it so chooses. Groups are also hybridising: state and non-state actors are beginning to blend together in interesting ways. Hybridisation can also make it difficult for outside observers to differentiate between groups.

Cyber Crime & Political Activism

Participants generally agreed that distinguishing between cyber criminal groups and political activist groups in the current climate is increasingly difficult. Some groups claim to pursue "hacktivism," but seem to be more interested in financial gain than in making political statements. Other criminal groups have even fractured over political differences. The Conti group, for example, split after leaked information publicised a division in support for Russia's activities in Ukraine.[24] Similarly, leaks regarding the group TrickBot's activities have also caused internal disputes and reorganisation.[25]

Participants also noted that the goals of several criminal groups seem to have shifted from denying access to information for financial gain, to stealing that information for state intelligence purposes. These groups have pivoted toward infiltration and information gathering as their primary goal. GameOver Zeus malware, for example, was once thought to be a tool for economic gain; more recently, it has been used to gather up strategic and sensitive intelligence in Georgia and other countries in the region. Additionally, several "hacktivist" groups like Killnet and NoName seem to advertise completed activities even if they weren't altogether successful.[26] Several

[24] See: Matt Burgess, "Leaked Ransomware Docs Show Conti Helping Putin From the Shadows," *Wired*, March 18, 2022, https://www.wired.co.uk/article/conti-ransomware-russia.

[25] See: Davey Winder, "Inside The Russian Cybergang Thought To Be Attacking Ukraine -- The Trickbot Leaks," *Forbes*, July 15, 2022, https://www.forbes.com/sites/daveywinder/2022/07/15/inside-the-russian-cybergang-thought-to-be-attacking-ukraine-the-trickbot-leaks/.

[26] For more on these groups, see: Antoaneta Roussi, "Meet Killnet, Russia's Hacking Patriots Plaguing Europe," *Politico*, September 9, 2022, https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/; Sam Sabin, "Pro-Russian Hacktivist Group Is Only Getting Started,

participants wondered if there is increasing coordination in the use of DDoS and wiper campaigns across these "hacktivist" groups.

Throughout the day, the Belarusian Cyber Partisans were cited as a remarkable non-state actor in this growing ecosystem.[27] The hacking group gained notoriety for their role in major cyber attacks, including one that disrupted the Belarusian railway system, preventing Russian ground artillery and troop movement into Ukraine. The Belarusian Cyber Partisans have used ransomware creatively and have also developed sophisticated and strategic coordination. The group can best be characterised as a digital resistance movement. Unlike other non-state hacking groups that support Ukrainian resistance, such as Anonymous, the Cyber Partisans are a small, tightly knit group with strong ties to Belarus.[28] They also have a stated mission and a proper strategy, in contrast with other hacktivist groups which tend to be less well organised.

The Use of Ransomware in the Conflict

Ransomware continues to be a significant and troubling development, as states struggle to respond in ways that disrupt and deter groups. Early in 2022, the REvil ransomware group faced consequences from the Russian state: 14 alleged members were arrested by the FSB, and the group's activities were essentially shuttered.[29] However, as several participants noted, REvil had ceased to be a major operation several months prior. Participants remained sceptical that these arrests indicated any real shift in Russian state attitudes toward cyber criminal activity.

Experts Warn," *Axios*, February 3, 2023, https://www.axios.com/2023/02/03/killnet-russian-hackers-attacks; Tom Hegel and Aleksandar Milenkoski, "NoName057(16) - The Pro-Russian Hacktivist Group Targeting Nato," *Sentinel Labs* (blog), January 12, 2023, https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/.

[27] The previous ECCRI workshop report on cyber operations in Ukraine also covered the Belarusian Cyber Partisans. See: Monica Kaminska, James Shires, and Max Smeets, "Cyber Operations during the 2022 Russian Invasion of Ukraine: Lessons Learned (so Far)" (European Cyber Conflict Research Initiative, July 2022), https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf.

[28] Also see: Juan Andres Guerrero-Saade, "The Last Remaining Cover for Action" (CyberwarCon, Arlington, Virginia, November 16, 2021), https://www.youtube.com/watch?app=desktop&v=uLCVhh8gfIQ&ab_channel=CYBERWARCON; Max Smeets, "Collective Resistance in the Digital Domain: The Cyber Partisans as an Exemplar" (H-Diplo RJISSF Forum, Forthcoming).

[29] See: Matt Burgess and Lily Hay Newman, "Russia Takes Down REvil Hackers as Ukraine Tensions Mount," *Wired*, January 14, 2022, https://www.wired.com/story/russia-revil-ransomware-arrests-ukraine/.

At the same time, governments experiencing tough sanctions regimes often have an added incentive to give criminal actors expanded room to manoeuvre. We have seen this occur in North Korea; several participants suggested that Russia may be following a similar playbook, creating a more lenient environment for criminal activity to offset the financial pressures it faces from Western sanctions following the full-scale invasion of Ukraine.

Ransomware is also becoming increasingly politicised. In several instances, Ukrainian and allied networks were attacked, data was encrypted, but no ransom demands followed. These attacks are reminiscent of earlier cases before the war, such as NotPetya, where the goal of attackers was to cause damage and disruption rather than to reap financial gain. More generally, the number of reported instances of ransomware has declined; however, we do not yet know if that reflects a real decline in ransomware attacks, or the changing environment for reporting. Many governments and officials have begun stressing the dangers of paying ransoms, including violating sanctions. This shifting public atmosphere could make victims less willing to report instances when they are affected, particularly if they do choose to pay the ransom. The number of insurance claims from ransomware has also declined, but again it is difficult to know whether this really reflects a reduction in ransomware incidents or a reluctance to report.

The IT Army of Ukraine and Civilian Capabilities

We are seeing civilians directly participate in this armed conflict through digital activity. Participants agreed that the most significant example of this phenomenon is the IT Army of Ukraine, which has directly facilitated the proliferation of cyber capabilities at an individual level.

The IT Army has met with a lot of success in large part because it has figured out a way to gamify the response to the conflict. In its recruiting efforts, the IT Army has romanticised the role of volunteers. The IT Army leadership has also provided clear, step-by-step outlines of how to target and achieve effects. Several attendees noted that the information given to IT Army volunteers is often more sophisticated and streamlined than the kinds of information seen in other, seemingly more professionalised hacking organisations.

Civilians are directly participating in the war in Ukraine by joining the digital battlefield.

The IT Army has also skirted the boundaries of several important cyber norms. Participants agreed that we need to be careful with the kinds of precedents we may be setting. The IT Army has targeted critical national infrastructure which could potentially constitute a violation of International Humanitarian Law (IHL), depending on the exact operation and outcome.[30] In addition to the IT Army, Ukraine has also pressured telecommunications companies and internet governance NGOs to stop routing Russian traffic, which goes against the Western norm of a free and open internet. In the case of ICANN, the organisation responsible for coordinating the namespaces and numerical spaces of the internet, Ukrainian arguments were unsuccessful, but other venues were more receptive. An Estonian company named Hacken put out a call to collect zero-days in Russian infrastructure, another action which is concerning in conflict.[31]

Such phenomena also blur important principles of distinction between combatants and noncombatants: civilians have certain protections, but they relinquish those

[30] On the IT Army, see: Stefan Soesanto, "The IT Army of Ukraine: Structure, Tasking, and Ecosystem" (Center for Security Studies, ETH Zurich, June 2022); on cyber operations and IHL, see: Kubo Mačák and Tilman Rodenhäuser, "Towards Common Understandings: The Application of Established IHL Principles to Cyber Operations," *Humanitarian Law & Policy, ICRC* (blog), March 7, 2023, https://blogs.icrc.org/law-and-policy/2023/03/07/towards-common-understandings-the-application-of-established-ihl-principles-to-cyber-operations/; "Cyber Operations and Armed Conflict: The Principle of Proportionality" (ICRC, March 2023), https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/04_proportionality-0.pdf.
[31] Soesanto, "The IT Army of Ukraine: Structure, Tasking, and Ecosystem."

protections if they join a military confrontation.[32] Untrained civilians are also more likely to use tools incorrectly, causing an attack to spread beyond its intended target or create other collateral damage.

Finally, participants asked what would happen with these civilian operators at the end of the war – a group of trained actors with no set boundaries of activity. In the past, countries have had to deal with civilians leaving and joining terrorist organisations, becoming radicalised, and then returning to their native countries. Many governments have developed systems to deal with this potential threat. With cyber operations, however, an actor can conduct attacks at a distance. How do we track these individuals and make sure they do not cause damage at home? Individuals can be drawn into hacking activities quite easily; often, it is only a matter of putting out a call, providing some tools, and pointing at a target for a DDoS attack. Drawing an individual into the IT Army of Ukraine is much simpler than the radicalisation processes we have seen in the past, and there is no good existing legal framework for dealing with this issue.

[32] For more on cyber operations and the principle of distinction in IHL, see: "Cyber Operations and Armed Conflict: The Principle of Distinction" (ICRC, March 2023), https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf; Mačák and Rodenhäuser, "Towards Common Understandings: The Application of Established IHL Principles to Cyber Operations."

The Role of the Private Sector

In recent years, the technology industry has clearly become a strategic player in geopolitics. The ongoing war in Ukraine has highlighted the various ways in which technology companies can become enmeshed in international politics. Although a contested point amongst some companies themselves, participants noted industry's decision to commit resources to the conflict as a strategic one, noting that the outbreak of a war changes markets, shifting the roles expected of key service providers. While private sector companies may share core values with governments, there are also clear limitations in how far this alignment can naturally proceed.

Participants agreed that the private sector has undoubtedly been playing an active role in aiding the Ukrainian government. Public-private cooperation has been evident since the very beginning: one participant noted that in the hours leading up to the invasion, senior government officials were able to coordinate directly with industry partners to spread threat intelligence about a new wiper that had just appeared in Ukraine, alerting all 30 NATO allies. Indeed, private sector actors seem to have taken up the mantle of "collective defense", even using the term in their own reporting on the conflict.[33]

While private sector companies may share core values with governments, there are also clear limitations in how far this alignment can naturally proceed.

Historical Analogues

Participants turned to history to try and parse the developing relationship between government and industry in the Ukraine conflict. In the past, private companies have had a key role to play in conflict settings; often, the roles of industry are significantly different in wartime than in peacetime. Several participants raised the analogue of maritime escorts, whereby private actors worked closely with navies to maintain

[33] See, for example: "Defending Ukraine: Early Lessons from the Cyber War" (Microsoft, June 22, 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

shipping routes during wartime. Others noted the rise of privateering as a useful analogy: the government provided niche capabilities to support private actors, who were then leveraged to help combat the rise of piracy. *Letters of marque* provided privateers with authority from their national government to engage in otherwise illegal activities and target rogue ships on the high seas. Are we moving towards this model in cyberspace?[34]

Yet, history also shows us that empowering the private sector to take on security and defense roles normally left to government actors can go very wrong. Several attendees stressed that blurring the lines of responsibility between government and industry can be advantageous in the short-term but can have profoundly destabilising effects in the long run. For example, US reliance on private military and security companies in Iraq in the 2000s raised significant questions about the duties and legal responsibilities of the host state. The Montreux document, developed by the Swiss Government and the International Committee of the Red Cross (ICRC) in 2008, is one international attempt to settle some of these open questions.[35] Other participants looked even further to the past, pointing to the rise of Italian mercenary armies in the fourteenth century as an example of private sector activity eroding the trust and integrity of government functions. Many participants agreed that the international community is facing a similar situation of uncertainty, where growing dependence on industry is casting doubt on whether national governments can protect and defend citizens. Greater clarity as to the status of actors under international law is needed, as this raises fundamental questions as to what security means within the confines of a conflict. How is security configured, and who decides what is good for the future?

Who Has the Lead in Defending Ukraine?

Several attendees stressed that private companies have indeed been the major players in this conflict: governments have supported industry in Ukraine, and not the

[34] For more on cyber activity and privateering, see: Florian Egloff, "Cybersecurity and the Age of Privateering," in *Understanding Cyber Conflict: Fourteen Analogies*, ed. George Perkovitch and Ariel E. Levite (Washington, DC: Georgtown University Press, 2017); Florian J. Egloff, "Cybersecurity and Non-State Actors: A Historical Analogy with Mercantile Companies, Privateers, and Pirates" (DPhil, University of Oxford, 2013).

[35] "The Montreux Document: On Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies during Armed Conflict" (ICRC and Swiss Federal Department of Foreign Affairs, August 2009).

other way around. One participant noted that this represents a profound shift in responsibilities that needs to be recognised by both the public and private sectors, with industry delivering effect to its own determinations, and doing so at scale.

Participants discussed the range of criteria that determined the private sector's involvement in the conflict, noting that industry responses also differed by country. Industry is ultimately beholden to shareholders and driven by market forces; these incentive structures are distinct from the drivers of government and need to be acknowledged when assessing private sector roles and responsibilities. Several participants argued that major tech companies are de facto political actors; indeed, these corporations often gain political influence through their cyber intelligence capacities. One attendee noted that industry reports shape how the public understands policy and can even shift government positions and attitudes towards threat actors.

Commercial impacts also matter. Withdrawing from the Russian market in the early days of the conflict affected companies differently: some companies faced significant financial setbacks, despite cultural proximities with Ukraine and a shared sense of solidarity. Many Ukrainian technology companies also had major operations in Russian territory. Western sanctions regimes also forced companies to withdraw hastily, often with extreme financial repercussions. Participants also noted that these speedy withdrawals from Russia shifted the kind of threat telemetry and market visibility companies had into the region. Companies needed to quickly adapt to a very different vantage point, with previous sources of data completely cut off.

Budget discrepancies help tell part of the story. One attendee noted that the UK Foreign, Commonwealth & Development Office (FCDO) has broken down a lot of institutional obstacles to lend support to the defense of Ukrainian cyberspace. In November 2022, the FCDO announced a £6.35 million aid package through its Ukraine Cyber Programme.[36] While this is a significant contribution, it pales in

[36] "UK Boosts Ukraine's Cyber Defenses with £6 Million Support Package," *UK Foreign, Commonwealth & Development Office* (blog), November 1, 2022, https://www.gov.uk/government/news/uk-boosts-ukraines-cyber-defences-with-6-million-support-package.

comparison to private sector contributions: Microsoft announced the same month that it had committed more than $400 million to support Ukraine since the war began in February.[37] These kinds of major differences in resource allocation are worth noting and understanding more fully.

Several participants argued that while private industry may want to act altruistically, this kind of behavior is ultimately not sustainable over the long run. In Ukraine, private companies shared a remarkable degree of unity of purpose with government actors; in other situations, this may not be the case. Industry actors need to protect their own interests, which often diverge from government incentives. Private sector actors are also limited in how they can respond in times of crises – they can't print money or raise taxes, and thus need to look out for their long-term sustainability.

Public-Private Partnerships: Getting the Level of Engagement Right

Other participants, however, stressed that governments cannot count on companies to engage in national security issues; the public sector needs to be prepared to properly compensate corporations for services rendered in times of crisis. The issue of sustainability was a frequent spectre in the day's conversation: participants struggled to define how private sector companies could support government efforts if a conflict or crisis were to continue for prolonged periods of time.

Governments cannot count on companies to engage in national security issues. The public sector needs to be prepared to properly compensate corporations for services rendered in times of crisis.

Generally, participants agreed that national governments need to set the roles and expectations of the private sector in wartime environments. Governments can usefully be enablers of industry – but this needs to be done in a way that differentiates between peacetime and conflict settings; this is not solely about building trust, but also about building long-term predictability or strategic stability.

[37] Brad Smith, "Extending Our Vital Technology Support for Ukraine," *Microsoft* (blog), November 3, 2022, https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/.

Participants also noted that while collective action between the public and private sectors in Ukraine has been successful, it has been ad hoc in nature. Significant questions remain around the financial, legal, and political aspects of industry's support to Ukraine: what has been the ambition in cooperating? Is strategic alignment better, or do ad hoc approaches work? Would the use of formal contracts or retainers by governments be effective? Several attendees suggested that what may be missing is a coordinator or central mechanism to facilitate connection points. NATO has a rapid response capability that it has used in Ukraine; participants wondered how this capacity can be built up and used by other allies in times of crises, perhaps through a virtual rapid response program that could harness national and private capabilities as part of a broader collective effort.

There are many ways to structure public-private sector partnerships: participants agreed that both public and private sector actors need to be clear from the start about the level of engagement they want to sustain. Top-down collaboration vehicles can be inefficient, weighed down by unnecessary bureaucracy, lack of transparency on the part of governments (with the US intelligence community being known for expecting full cooperation from the private sector, without much reciprocation), or governments sharing insights too broadly for them to remain valuable. Many attendees agreed that scale is generally a problem: trust does not necessarily scale, and while there are excellent pockets of information sharing and collaboration across industry and government, these close-knit communities cannot be easily replicated in larger structures. Coordination models could prove more useful. Cited examples included

the UK Industry 100 program operated by the NCSC and the CyberPeace Builders program.[38]

Can Companies Remain Neutral?

Some participants raised the idea that for larger tech companies, sitting on the side lines is not a viable option. Companies like Amazon, Google, Microsoft, and Facebook have significant transnational footprints and play key roles in shaping the international environment in which they operate. If a major technology company decides not to become involved in a conflict, that has significant ramifications for public visibility into the conflict and for the kinds of support mechanisms that can be offered to those affected. Several participants agreed that big technology companies do not have the luxury of staying apolitical because ultimately, the technology they produce is not apolitical.

Participants also pointed to gaps in involvement: some major tech companies and Internet Service Providers (ISPs) have made gestures of collaboration but have not actually taken concrete steps towards aiding the crisis.

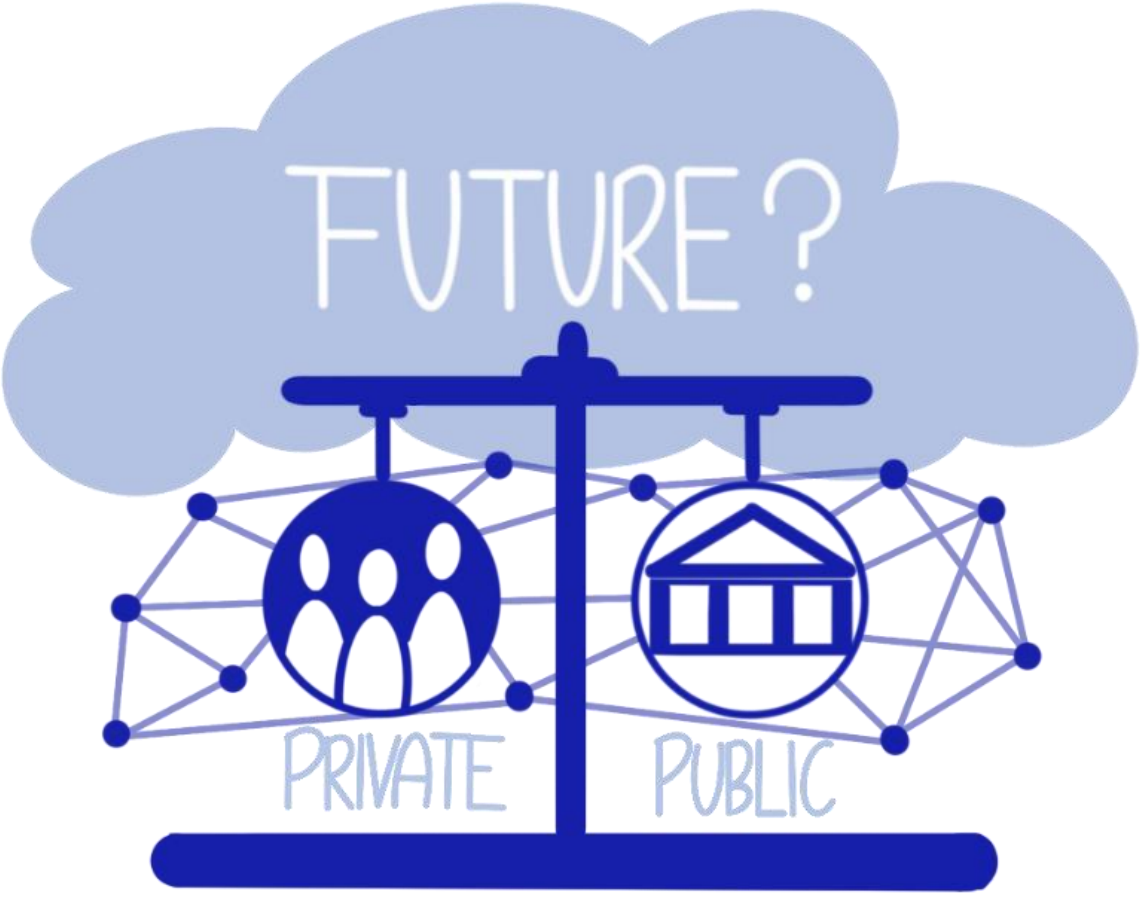
Other participants asserted that at the level of the individual, people do want to help. The threat intelligence industry is full of highly motivated people who want to help protect and defend against potential harms in cyberspace. Indeed, while we often focus on organisations when we look at public-private partnerships, individuals tend to be less risk averse getting involved, and less motivated about personal incentives. Several participants proposed involving individuals rather than companies and working from the ground-up to build collaboration.

Participants raised several further questions on the role of the private sector. In Silicon Valley, the focus has been on the future role of the private sector: how do companies feel about being agents of government action? In Washington, DC, policymakers have latched onto potential parallels with rising tensions with China: can companies replicate the support rendered in Ukraine in Taiwan? Meanwhile, in many European

[38] "Industry 100," UK National Cyber Security Centre, n.d., https://www.ncsc.gov.uk/section/industry-100/about; "CyberPeace Builders," CyberPeace Institute, n.d., https://cyberpeaceinstitute.org/cyberpeace-builders/.

capitals, people are wondering about long-term reliance on private actors: do we now live under a cyber umbrella run by Google and Amazon Web Services?

Furthermore, while Ukraine has benefited from the best efforts of many different actors, participants warned that this conflict may not provide a good roadmap for the future. The process of private sector support has been ad hoc; in the future, actors will need to be more careful and strategic from the start. Other attendees also wondered whether the triumphalism surrounding private sector activity in Ukraine was overstated: do we really know what kind of activities are having a clear material impact for Ukraine?



Civil-Military (Dis)Integration?

Cyberspace continues to be a contested realm, where the lines between civilian and military infrastructure are often blurred. In the case of public-private collaboration, these blurred categorisations become even trickier to deal with. Countries cannot simply hand control of cyberspace over to the military in times of crisis or armed conflict – too much infrastructure is in private hands.

Yet, the principle of distinction between civilian and military targets is a cornerstone of international humanitarian law (IHL), and fundamental to aid work writ large. As more and more armed forces capitalise on private cloud and satellite capabilities, we are likely to see the further disintegration of this principle. Private sector employees could also become parties to the conflict if their corporations take on certain roles and responsibilities normally served by government functions.

Companies that take political stands are also politicising their technical platforms. Several participants noted that this complicates the work of humanitarians, as countries party to a conflict may resist the use of certain technical platforms because of the political attitudes adopted by the company's leadership. This politicisation could lead to further fragmentation, as certain tech platforms can only be used in some geographical areas but not others.

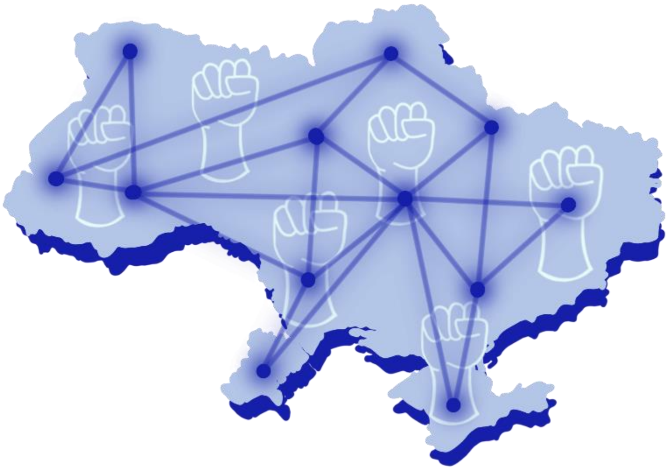
Conclusions

This ECCRI workshop sought to unpack the major narratives that have formed around the conflict in Ukraine, moving beyond initial assumptions into nuanced, intelligence-backed assessments of ongoing cyber activities and critical policy questions. It was the second such event since the invasion in February 2022. We have certainly learned much about Russian targeting and collection strategies over the course of the past year of warfare: participants generally agreed that while Russian forces may not have been well-prepared before the invasion began, they have acted with remarkable speed and flexibility since, sustaining an unprecedented operational tempo in Ukraine.

The workshop also reinforced important limitations in our current understanding of the conflict. Participants agreed that we still have limited visibility into the realities on the ground; any conclusions drawn must be accompanied with caution. Attendees stressed that lessons learned from Ukraine may not be easily applied to other conflict situations. Many observers are intent to draw parallels with the growing tension in Taiwan; however, participants overwhelmingly agreed that such attempts gloss over key details and attributes of the current conflict. Ukraine has a very particular geography: it is a large country that shares land borders with several important allies, granting overland access to defenders. Russia also appears to have significantly underprepared for the invasion, a mistake the country (and others) are unlikely to repeat in the future. Taiwan is a very different case, facing a very different kind of adversary, and we would do well to remember that.

Furthermore, we tend to ascribe a narrative of offense dominance to cyberspace: the defender needs to succeed in securing every front, while the attacker needs only one lucky break. However, Ukraine's ability to withstand constant cyberattacks from Russian actors has demonstrated the power of resilient systems. Participants agreed that Ukraine's ability to withstand a constant barrage of cyberattacks from Russia clearly demonstrates the importance of cyber resilience.[39] Ukraine has learned many lessons since the annexation of Crimea in 2014, including how to build and leverage resilient systems. Ukraine has also capitalised on its deep familiarity with Russian tactics to build more robust protections. Several attendees noted that resilience should be at the heart of any country or alliance's defensive strategy and is particularly important for NATO moving forward.

Ukraine has proved masterful at controlling the Western narrative surrounding the war and has held together a broad coalition of support from the West. Some attendees were surprised by the extent to which the invasion solidified Ukrainian resilience to information operations. Others noted that the invasion has also dramatically reinforced distrust among Ukraine's allies towards Russia, with many Western countries more aligned on this than in years prior.



The defender gets a vote.

Furthermore, to sustain a remarkable network of supporters from the West, Ukraine has potentially restrained itself so as not to lose the moral high ground. Some participants argued that Ukraine could have gone much further in some of the country's cyberattacks, wreaking havoc on the Russian internet, but has instead avoided such destructive actions. Other participants raised the issue of the Russian TV hack as evidence of a miscalculation on the part of pro-Ukrainian activists: the hack

[39] "How Technology Helped Ukraine Resist during Wartime," *Microsoft - CEE Multi-Country News Center*, January 20, 2023, https://news.microsoft.com/en-cee/2023/01/20/how-technology-helped-ukraine-resist-during-wartime/.

seems to have bolstered support for Russia, possibly doing more harm than good for the Ukrainian war effort.[40]

Overall, Ukrainian forces have also responded with incredible resilience and determination, demonstrating that defense in cyberspace counts for much more than previously appreciated. The country’s mass digital mobilisation, particularly through outlets like the IT Army, have changed the geographies of cyber conflict and will likely have major repercussions on the ways cyber operations are constructed in the future. Ukraine has inspired a unique unity of purpose among Western actors and driven collective action in mobilising cyber defences at pace and scale. Even so, we may be setting some concerning precedents for future cyber conflict.

[40] See: Daryna Antoniuk, “Pro-Ukraine Hackers Claim Attack on Russian TV Broadcasts,” *The Record*, September 13, 2022, https://therecord.media/pro-ukraine-hackers-claim-hack-on-russian-tv-broadcasts.

Acronyms and Abbreviations

CISA – U.S. Cybersecurity and Infrastructure Security Agency

DDoS - Distributed Denial of Service attack

DoS - Denial of Service attack

DoD – U.S. Department of Defense

FSB – Federal Security Services of the Russian State

FCDO – UK Foreign, Commonwealth & Development Office

GRU – Main Intelligence Directorate of the Russian Armed Forces

ICANN – International Corporation for Assigned Names and Numbers

ICRC – International Committee of the Red Cross

IHL - International Humanitarian Law

IL - International Law

IO – International Organisation

ISP – Internet Service Provider

NCSC – UK National Cyber Security Centre

NGO – non-governmental organisation

VIO - *voyska informatsionnykh operatsiy,* or information operations force

About the Authors

Taylor Grossman is a senior researcher in the Cyberdefence Project with the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

Monica Kaminska is Assistant Professor of International Security and Technology at the Institute of Security and Global Affairs at Leiden University.

James Shires is a senior research fellow in cyber policy at Chatham House.

Max Smeets is the director of the European Cyber Conflict Research Initiative and a senior researcher at the Center for Security Studies (CSS) at ETH Zurich.

About ECCRI

The European Cyber Conflict Research Initiative (ECCRI) promotes the interdisciplinary study of cyber conflict and statecraft in Europe and beyond. ECCRI exists to make rigorous, objective research on cyber conflict and statecraft accessible to policy-makers and the general public.

ECCRI encourages and supports high-quality original research, as well as enabling researchers to communicate their findings to policy-makers and the general public.

ECCRI is a UK Charitable Incorporated Organization. ECCRI's Registered Charity Number is 1190782.

The views expressed in this publication are those of the authors, and do not reflect the views of ECCRI or any other institution.

Published in 2023 by the European Cyber Conflict Research Initiative.

Illustrations by Christine Musch