Tallinn Workshop Report

Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)

Monica Kaminska, James Shires, and Max Smeets

July 2022

Tallinn Workshop Report

Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)

Monica Kaminska, James Shires, and Max Smeets

ECCRI Tallinn Workshop Report, July 2022
eccri.eu

Tallinn Workshop 2022

What key lessons can we draw from the 2022 Russian invasion of Ukraine about the role of cyber operations in military conflict? How do Russian cyber operations differ in wartime compared to peacetime activity? And what cyber activity can we expect in the months ahead?

On the 30th of May, the European Cyber Conflict Research Initiative (ECCRI) held a roundtable in Tallinn discussing these questions about the impact of cyber operations during the war in Ukraine. The event included cyber threat intelligence and incident response practitioners, corporate representatives, academics, and officials from key governments and international institutions. It was invite-only and held under the Chatham House Rule to enable those attending to be as frank as possible. Nonetheless, we thought it useful – in consultation with all attendees – to make several lines of discussion public.

Russian “Reserve” Cyber Capability

Since late February 2022, Russia has conducted a variety of cyber operations. We have witnessed multiple variants of data destruction malware, known as ‘wipers’, being deployed against a wide range of targets. Russia has also stepped up its cyber espionage operations in Ukraine and continued its influence operations targeting a variety of audiences. Reporting from Microsoft suggests that these cyber operations are coordinated with conventional military operations.

A key point was to what extent we have observed the full extent of Russian cyber efforts during the war in Ukraine. Some attendees suggested that if Russian cyber actors had possessed the ability to conduct operations with more severe effects than those publicly observed, they would have used this capability at the start of the invasion. Therefore, Russian actors were not operating with any “reserve” capability in the sense of “ready-to-go" cyber operations. This does not imply that more disruptive or destructive cyber attacks will not occur in future, as Russian cyber actors continue to develop their access to Ukrainian information infrastructure.

Other attendees disagreed, suggesting that some known tools had not been seen in the conflict, possibly because only one cyber actor within the Russian system, Unit 74455 Main Directorate of the General Staff of the Armed Force, also known as Sandworm, had taken the lead in conducting cyber effect operations. These attendees noted especially that Russian cyber operations for espionage outside Ukraine continued, and that Ukraine positions became the subject of intelligence collection for other targets. This shows that, even if no further cyber escalation had been possible in Ukraine itself, Russia is capable of conducting multiple cyber campaigns concurrently and still possesses the ability to widen the scope of its targets.

Operational Tempo and “Burning” Tools

Many attendees stressed the uniquely high operational tempo of Russian cyber operations during the war in Ukraine. It seems that cyber capabilities have been developed, deployed, detected, and mitigated at an unprecedented pace, with several important consequences.

First, Russian cyber operations have been relatively unsophisticated, sometimes reworking known malware, with consequently high visibility. The attribution of specific tactics, techniques, and procedures to specific threat actors, however, is complicated for several reasons, including extensive earlier reporting on Russian cyber actors (including by the U.S. CISA), which led to their re-tooling.

Second, Ukraine cyber defenders have engaged in constant “fire-fighting” to prevent disruption and have been unable to follow usual incident response procedures in removing the adversary from networks altogether.

Third, it appears that Russian cyber operations in the war in Ukraine are centralized, with Unit 74455 conducting the effect operations, even if they build on broader intelligence capabilities. For example, this includes deploying wipers on systems where other actors have achieved the initial access.

Fourth, the high operational tempo has potential effects on the human element of cyber operations. Josiah Dykstra and Celeste Lyn Paul, from the U.S. Department of Defense, conducted four surveys to study human fatigue and performance in cyber operations. They showed how over the course of a cyber operation, with an average length of just over 5 hours, operator fatigue and frustration increased significantly due to the required cognitive demands. Considering the persistent pace of operational activity coming from Russia, the “brain drain” from Russian emigration after the war, and the difficulty in maintaining and motivating sufficiently skilled personnel over longer periods of time, we can expect a great deal of Russian employee burnout.

Cyber capabilities have been developed, deployed, detected, and mitigated at an unprecedented pace, with several important consequences.

However, some attendees stressed that we do not have a reliable baseline of how many operators, developers and other expertise is available to Russia, nor do we have a good assessment of their existing “arsenal” of customized tooling. This makes it hard to judge loss of capability in absolute terms: the high operational tempo and burning tools might seriously impact their overall arsenal, or it could represent the quick development and relatively easy sacrifice of a smaller percentage of lower-value tools.

Strategic Value of Cyber Operations

The debate on the strategic value of cyber operations has gone through different stages, ranging from the claim that "cyberwar will not happen" and the argument that cyberspace does not contribute to methods of interstate conquest or coercion, to the idea that cyberspace creates new strategic effects between the situations of war and peace.

Questions remain about the strategic utility of cyber operations during the 2022 Russian invasion of Ukraine. Attendees emphasised the psychological effects of the two most significant cyber incidents in the conflict: the Industroyer 2 operation and the “VIASAT hack” (although the accuracy and utility of this label also came under scrutiny). The integration of information operations on both sides has also been highly influential – e.g. the release of SIGINT by Western nations in the lead-up to and early days of the invasion. However, the idea that Ukraine is winning the narrative war is parochial. Globally, the Russian narrative has a lot of support in some quarters. Moreover, there have been many leaks and dumps of information by Russian actors and frequent compromises of the Ukrainian Ministry of Foreign Affairs and the emergency services, with significant psychological effects on the ground.

Attendees stressed that we should not single out cyber operations individually but ask how they contribute to overall strategy and forms of competition in international security. More specifically, there has been a great deal of academic and policy writing about the need to focus on how cyber operations are linked into broader campaigns, to assess their cumulative impact in peacetime. Attendees discussed the need to maintain this campaign focus for cyber activity in wartime as well. The question

We should not single out cyber operations individually but ask how they contribute to overall strategy and forms of competition in international security.

is less how a single wiper has influenced the 2022 invasion of Ukraine, and more how the persistent use of disruptive cyber capabilities has provided strategic value to Russian war efforts.

Attendees were divided as to whether cyber operations have in fact provided strategic value in this way. Some saw cyber operations as a form of largely low-level political subversion with the aim of, say, dividing Western support for economic sanctions against Russia, or undermining alternative energy sources. These attendees perceived the strategic utility and effects of political subversion via cyberspace to be severely limited, owing to operational and other challenges. Others disagreed, arguing that cyber "unpeace" can significantly harm political, economic, and social interests regardless of its inability to conquer territory or its difficulty of coercing state behaviour.

Finally, discussions of the strategic value of cyber operations revolved around the naivety of the target. Subversive cyber operations may work well against a naive adversary but can unintentionally galvanise a more coordinated and effective response, both nationally and internationally, as their target learns from earlier operations.

Conceptual and Legal Clarity

Attendees pointed out that there is a lot of conceptual confusion and murkiness in the cyber studies field – for example regarding the distinctions between hybrid war, unpeace, and grey zone conflict. The terms of art carry different connotations and are susceptible to different interpretations. Unpeace, for example, is often conflated with grey zone conflict – but they are different, because grey zone conflict can involve territorial violations and limited violence (e.g. political assassinations), whereas

unpeace is distinctly nonviolent and non-territorial. Moreover, unpeace is not necessarily coercive, but instead is seeking to undermine societies and governments from within.

Actors are also often unhelpfully unclear. For example, the EU's response to the VIASAT incident referred to norms of responsible state behaviour, which are peacetime norms, and, in the same statement, referred to the incident as part of a wider "war". Clearly, analysts and policymakers struggle to make sense of where cyber actions fit within the legal rulebook.

Finally, some attendees suggested that Russia's understanding of NATO's Article 5 on collective defence seems to be shaping the boundaries of Russian actions. For example, in the case of NotPetya, we now know with the benefit of hindsight that the operation was not meant to spread outside of Ukraine and affect NATO members (such as Denmark).

Generalizability of the Russia-Ukraine War

Participants suggested that Ukraine may not be a good "test case" for the development of cyber conflict theory. With Russia's invasion in 2014, Ukraine became a classic situation of sovereignty violation and use of force. Cyberspace took a secondary role next to the use of conventional military means. Thus, all major Ukraine cyber attacks over the last 8 years have occurred within a war. In Crimea, for example, cyber means and territorial control are not separate, as Russian or sympathetic actors control key internet routing infrastructure. Thus, Ukraine might not offer many lessons for great power conflict "in cyberspace".

Even in terms of cybered conflict, there was a surprising lack of what attendees referred to as "netwar". The Russian military did not conduct a network-centric war in their initial invasion, and relied on old, often analogue hardware. This makes visions (and fears) of a revolution in military affairs less relevant and negates the possible downsides of hackable military infrastructure. At the same time, some attendees noted that the Ukrainian Ministry of Defense has not been forthcoming about cyber operations impacting military hardware.

The vulnerability and exploitation of national civilian and military communications infrastructure was raised several times during the roundtable. Some attendees suggested that both Russian and Ukrainian forces had been forced onto insecure communications systems due to cyber operations, enabling greater SIGINT collection and even individual targeting. Relatedly, the ownership of such infrastructure was also a point of discussion.

Tech Companies and the Threat Intelligence Community

Some big technology companies have been extremely active in supporting Ukraine against cyber operations, whether by increasing the resilience of Ukrainian cyber infrastructure, or contributing to the awareness of Russian cyber operations. Not least, Microsoft has worked proactively to help

Ukrainian cybersecurity officials defend against Russian attacks, and published several threat intelligence reports.

On the one hand, this raises the question of how far this is a unique moment, where competitors in the threat intelligence industry put aside their differences and work together on shared threats. It also raises the question of "burden-sharing", as some big tech companies are effectively "semi-state actors" and so may be better placed to withstand cyber operations in comparison to Ukrainian domestic actors; if so, should such tech companies take on the burden of defence?

Similarly, tech companies defend more computer systems and networks than many states, so it is important that intelligence flows to them as well as from them. It was noted that not all tech companies have contributed equally, with some taking a much more public stance than others. The long-term consequences of such strong alignment with one side in this conflict are not well understood, whether by those in such companies or outside it.

Some attendees highlighted that there are probably a lot of "Western" and specifically Five Eyes cyber operations in Ukraine that are not publicly reported by threat intelligence firms. Indeed, General Nakasone has confirmed that the US Cyber Command has conducted a "series of operations across the full spectrum; offensive, defensive, [and] information operations" in response to the Russian invasion. But the nature and impact of these activities has not been independently substantiated by commercial threat intelligence companies.

Also, there has been commercial threat intelligence reporting on Chinese espionage activities in Ukraine and the region. For example, Google's Threat Analysis Group discovered an ongoing cyber operation in Ukraine from a Chinese hacking group, known as APT31, targeting Gmail users affiliated with the United States government. Yet, attendees noted that there remain significant blind spots in how Chinese cyber actors are able to exploit the war in Ukraine for intelligence collection.

Tech companies defend more computer systems and networks than many states, so it is important that intelligence flows to them as well as from them.

Role of Other Non-State Actors

First, following the Russian invasion of Ukraine, several non-state hacking groups have pledged allegiance to either side of the war. For example, the Conti team, responsible for numerous ransomware attacks, announced its full support of Russia. As the group states: "The Conti Team is officially announcing a full support of Russian government. If anybody will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy."

After the announcement, a security researcher with the twitter handle 'Contileaks' published years of Conti's internal communications online (the Conti team has been hit before when a former employee published their attack playbook). Considering the severity of the leaks, there is a good chance that the

Conti team will reorganise and its employees will move to other ransomware groups. That said, attendees agreed that Western governments still do not have a strategic answer to this criminal activity from Russia and some other Eastern-European countries.

Second, the Ukrainian government has not yet established a military cyber command. The government called on people across the world to join its volunteer IT Army. The IT Army likely consists of a small in-house team that includes Ukrainian intelligence and defence officials, and a larger group of individuals across the world participating in coordinated DDoS attacks against Russian networks and systems. The attendees discussed how further strategic thinking on the part of Ukraine is much needed to understand this set-up can be leveraged in the future - as well as its dangers as a blueprint for non-state participation in future conflicts.

Several non-state hacking groups have pledged allegiance to either side of the war.

Third, attendees discussed the role of domestic or regional resistance organizations, with a particular focus on the Cyber Partisans. The Cyber Partisans have claimed responsibility for several major cyber attacks, including a high-profile operation against the Belarusian railway system that reportedly halted Russian ground artillery and troop movement into Ukraine. The Cyber Partisans do not participate in the IT Army's activities or execute operations outside of Belarus's borders. The group is, however, willing to share best practices about the targeting of Russian forces. Two key aspects came up in the discussion: first, these regional resistance movements are potentially a much more influential and authentic means of resistance; second, the legality of their activity.

Conclusion

This ECCRI roundtable explicitly sought to go beyond stale binary narratives of "missing" cyber operations and looming cyberwar. As the summary above suggests, it demonstrated that the state of the art in cyber conflict research has much to offer for the analysis of cyber capabilities in the Russia-Ukraine war, with nuanced theoretical positions drawing on the latest empirical data as and when it becomes publicly available. However, the roundtable's discussion also cautions observers of cyber conflict (wherever they sit) to remain aware of the broader context of this activity, in three ways.

First, the roundtable urges us to consider cyber incidents or operations in relation to the overall cyber landscape, whether through a "campaign" lens or through reflecting more on adversary target selection and aims, media bias, and collection limitations.

Second, the roundtable warns us to thoroughly integrate the study of cyber conflict with its "conventional" cousins. To our great sadness, the war in Ukraine starkly demonstrates the horrific human cost of war, and growing awareness of human rights violations and massacres only brings this terrible picture further into focus. Cyber operations occur as part of this wider deployment of lethal force, and we must resist the temptation to analyse them in isolation, as somehow detached from the suffering caused by war.

Third, and finally, the roundtable reminds us to be humbly aware of the constraints of (especially public) research on this subject. This summary is of lessons learned *so far*, with the recognition that future events might easily upend our understanding of cyber conflict to date. Equally importantly, reporting and analysis of cyber operations is skewed for many reasons – commercial, geopolitical, normative – and these blind spots influence our conclusions, sometimes without us being aware of it. This is unavoidable, but organisations like ECCRI exist to enhance the public understanding of cyber conflict in as independent, objective, and rigorous a manner as possible.

Monica Kaminska is a postdoctoral researcher at The Hague Program on International Cyber Security at the Institute of Security and Global Affairs, University of Leiden.

James Shires is an assistant professor in Cybersecurity Governance at the Institute of Security and Global Affairs, University of Leiden.

Max Smeets is the director of ECCRI and a senior researcher at the Center for Security Studies (CSS) at ETH Zurich.

Careful, objective, and open research on cyber conflict

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.

The Tallinn Workshop is funded by the William & Flora Hewlett Foundation. The William & Flora Hewlett Foundation is a nonpartisan, private charitable foundation that advances ideas and supports institutions to promote a better world, and specifically among others responsive government.

Published in 2022 by the European Cyber Conflict Research Initiative.

https://eccri.eu/
ECCRI is a UK Charitable Incorporated Organization (No. 1190782).