PONARS Eurasia
NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Russia's Cyberwar Against Ukraine

A De-Modernized Regime Against a Networked Society

PONARS Eurasia Policy Memo No. 787
July 2022

Tetyana Malyarenko[1] and Borys Kormych[2]
Odessa Law Academy

Russia's war against Ukraine has increased the intensity of Russian cyber operations compared to 2014-2021. However, this increase has not (yet) inflicted significant damage on Ukrainian infrastructure. Analytical reports published after February 2022 offer two competing explanations for Russia's information-technology (IT) attack failure. The first assumes that Russia's cyberwar against Ukraine had already reached its highest possible level of complexity, so there is either too little room for qualitative growth on the Russian side or sufficient resilience on the Ukrainian side. The second explanation is based on published reports from government agencies and private companies, such as Microsoft, which show that Russian cyberattacks have improved and increased since January 2022, but attention and intervention by the United States and other international cyber specialists helped Ukraine neutralize the attacks and successfully counterattack.

Russian cyberattacks against Ukraine thus constitute attacks by a de-modernized totalitarian regime on a modern networked society. This factor, to a certain extent, also explains the relatively low efficacy of Russian cyberwarfare. Nevertheless, in the second phase of the Russian-Ukrainian war that is focused on the conquest of Donbas and characterized by the predominance of non-modern artillery on the battlefield, the role of cyberattacks turned out to be relatively insignificant. Considering this general de-modernized aspect, and accepting the second explanation for Russia's lack of success in cyberspace, we believe that as the Russian-Ukrainian war wears on, cyberwar has every chance of regaining a key role in future operations.

[1] Tetyana Malyarenko is Professor of International Security and Jean Monnet Professor of European Security at the National University Odessa Law Academy. Tetyana Malyarenko gratefully acknowledges funding from the Erasmus+ Programme of the European Union and the Volkswagen Stiftung, IOS Regensburg.
[2] Borys Kormych is Professor and Head of the Department of Maritime and Customs Law at the National University Odessa Law Academy.

The Evolution of the War in the Cyber Domain

Hostile Russian-Ukrainian interactions in cyberspace can be roughly divided into two periods. The first period—**covert proxy attacks**—started in late 2013 with the Euromaidan revolution. Intense cyberattacks, combined with psychological operations on social networks and media under the umbrella of the GRU-linked group "Cyber Berkut," accompanied the kinetic activity of the Russian army and pro-Russian proxies during the Euromaidan Revolution and the war in eastern Ukraine.

However, except for a short period from November 2013 to March 2014, during which cyber and psychological operations supported Russia-backed anti-Maidan activities and the annexation of Crimea, Russia's goal during this first phase was to collect information in preparation for an all-out war against Ukraine. Destructive Russian activities in Ukrainian cyberspace included operations ranging from small-scale cyberattacks and covert data collection to large-scale testing of Ukraine's cyber system's stability in conditions of a state of conventional war.

In turn, Ukraine's goal from 2013-2022 was to strengthen a national cybersecurity system. Since then, digitalization has had a significant impact both on public administration and in Ukrainians' private lives. The share of population using Internet has grown from 41 percent in 2013 to 75 percent in 2020. Ukraine's 2016 Cyber Security Strategy contained measures to create a national cybersecurity system. At the same time, it focused on protection against predominantly non-military threats.

Between the two high-intensity phases of the Russian-Ukrainian war (2014-2015 and 2022), Ukraine suffered at least two massive cyberattacks: one against its power infrastructure, which caused blackouts for large parts of the population in 2015, and another linked to NotPetya ransomware in 2017. NATO STRATCOM believes that both were a rehearsal for a future cyberwar since the scale and cost of the attacks far exceeded their destructive results.

After the two attacks mentioned above, Kyiv boosted its efforts to strengthen its national cyber defense infrastructure. The government established several cyber centers, such as the UA30 within the Situational Center for Ensuring Cybersecurity within the Security Service of Ukraine (SBU). The Ukrainian security strategy's shift in focus from protection against non-military to military threats occurred in the second half of 2021 (see, for example, the 2021 parliament's Cyber Security Strategy). It emphasized building an effective cyber defense, creating cyber troops, countering intelligence and subversive activities, and developing asymmetric deterrence tools, among other areas of focus.[3]

[3] The secretary of the National Defense and Security Council of Ukraine, Oleksiy Danilov, in an interview with Channel 24 on May 26, 2022, acknowledged that Ukraine had begun preparations for a full-scale Russian invasion in mid-2021, including strengthening cybersecurity in the field of the Internet, mobile communications, and television.

Psychological Operations Linked to Symbolic Politics

In the Russian-Ukrainian hybrid war from 2014-2022 and the high-intensity war that started in February 2022, cyberwarfare has gone hand-in-hand with information warfare and psychological operations. Even though, to date, the main results of the war have been achieved by artillery and infantry in eastern and southern Ukraine, some of the most influential tools in the conflict's military propaganda are victories and defeats at sea. In modern conflicts, as in the past, violence is driven by hostile myths, which Stewart Kaufman referred to as symbolic politics. Both Russia and Ukraine widely employ myths and symbols in their diplomatic efforts to justify their actions in the war to domestic and foreign audiences. However, while modern Russian propaganda appeals to the past, using terms, narratives, and symbols from the Soviet Union during World War II, Ukraine's decommunization policy aims to destroy physical and emotional symbols related to Ukraine's Soviet history.

The Black Sea Fleet in annexed Sevastopol is one key symbol with sacred meaning for Russia. Therefore, for Ukraine, the destruction of targets embodying this symbol is not only a security interest but a propaganda goal. The destruction of the Russian Black Sea Fleet flagship cruiser *Moskva* carried out by a Ukrainian Neptune missile with the help of Western intelligence is of great symbolic significance. Before their defeat, Russian warships were declared key targets of the war, and their destruction was reflected in formal and informal Ukrainian military propaganda. The Russian fleet's capture of the Ukrainian Snake Island created one of this war's most popular patriotic slogans. When told to surrender by radio from the *Moskva*, a Ukrainian marine replied, "Russian warship, go f… yourself." His mobile phone video and phrase instantly went viral and were shared in media, the arts, advertising, and statements of Ukrainian officials. The National Civil Service Agency had to clarify that officials' use of this phrase is not a violation of the code of ethics and that Ukrainians perceived the phrase as a call for unity worldwide. The phrase became a symbol of the struggle against Russian occupiers.

During the hybrid phase of the Russian-Ukrainian war, information and cyberattacks were widely used in the Black Sea theater and intensified a year before the active phase of the war. For example, in 2021, Russian state-sponsored hackers destroyed the Ukrainian Navy's website to obtain data on participants in the Sea Breeze exercise. Later on, Russian state-sponsored hacking initiated a number of attacks on Sea-Breeze Exercise websites. On the other side, while sailing from Odesa to Georgia, the British warship Defender crossed annexed-Crimea's territorial waters. A few days earlier, a Dutch frigate, the HNLMS Evertsen, staged a virtual visit to Sevastopol by falsifying its automatic identification system position.

Open Confrontation in Cyberspace

The second period of the Russian-Ukrainian war in cyberspace—**open confrontation**—started with Russia's military invasion in February 2022. During this phase, the goal of Russian cyberattacks has been to paralyze Ukraine's information systems, which would make it easier to achieve military goals in other areas of war. Russia's invasion was preceded by a massive cyberattack on the Ukrainian government's websites in January 2022. Russian hackers used the sites' known vulnerabilities to gain access to data on 2,6 millions of individuals, businesses and law firms, and government agencies.

As an April 2022 Microsoft report suggests, Russian cyber actors are cooperating with kinetic military activity, supplementing land, air, and sea operations. Thus, Russian national cybersecurity actors work in tandem with military strikes, engaging multiple threats. Russian cyberattacks also attempt to implement information and psychological operations aimed at undermining Ukraine's political will and ability to continue the fight. More than 40 percent of the destructive cyberattacks targeted organizations in critical infrastructure. Another 32 percent were supposed to affect Ukrainian government organizations and various malware families deployed against Ukrainian networks.

The key unknown regarding Russia's cyber activity in Ukraine starting from 2022 is the reason for its low effectiveness. At the time of this writing, none of the Russian cyberattacks have been successful.

In our opinion, many attempts to analyze the reasons for this low efficacy overlook the role of Ukrainian society's horizontal structures, which have repeatedly shown their effectiveness at critical moments, including the Revolution of Dignity and the first stages of the Russian invasion of 2014. For example, the Android-based military automated tactical management system *Kropyva* was developed by patriotic associations back in 2015 and later officially employed by the Ukrainian Ministry of Defense. *Kropyva* helped drastically increase the effectiveness of Ukrainian artillery. Moreover, the *Kropyva* case shows how, over the past eight years, many participants in horizontal structures have transitioned to the public sphere and are applying lessons learned from the interaction between horizontal structures to combat the Russian invasion of 2022.

The first example of such horizontal interaction countering Russian cyber threats is also connected with military IT systems, including *Kropyva*. On February 24, 2022, just an hour before the invasion, Russian government hackers targeted the U.S. satellite company Viasat, resulting in a significant loss of communications for the Ukrainian military. Two days later, Ukraine's Minister of Digital Transformation tweeted Elon Musk, asking him to provide Starlink Internet to Ukraine. Musk replied just hours later: "Starlink service is now active in Ukraine. More terminals en route." Thousands of Starlink terminals were delivered to Ukraine and deployed, bypassing all registration and certification procedures and eventually helping to restore communications both for civilians and the military.

The second example is Ukraine's so-called IT Army, which emerged from the Ukrainian Ministry of Digital Transformation's social media posts calling for volunteers willing to join cyber operations against Russian invaders. It is suggested that the IT Army consists of two parts:

1) a continuous global call to action that mobilizes anyone willing to participate in coordinated DDoS attacks against designated—primarily civilian—Russian infrastructure targets; and

2) an in-house team likely consisting of Ukrainian defense and intelligence personnel that has been experimenting with and conducting ever-more complex cyber operations against specific Russian targets.

Even though this initiative came from officials, one should consider that this phenomenon has its roots in the traditions of self-organization developed during the Revolution of Dignity and the subsequent war with Russia in the Donbas. In particular, the IT Army is more of a coordination entity of independent actors, both private and public. Coordination is carried out through communication platforms like Telegram channels and not through control centers.

Conclusions

Since February 2022, Russian cyberwarfare in Ukraine has followed the same course as Russia's politico-military approach to Ukraine in general. First, it started with declared hybrid warfare, in which cyberattacks would be a significant component and a low-intensity special operation. It has progressed to a non-modern war in which cyber warfare plays a seemingly minor role.

We suggest this stems from a shortage of modern weapons and technologies in Russia. For example, during the war in Ukraine, it turned out that electronic devices made in France are widely used in the production of Russian tanks, Orlan drones, and aircraft. Communication and information technologies in cyberspace independently and in support of military operations on air, land, and sea turned out to be Russia's greatest weakness in the Ukrainian war. This was not just the result of Russia's general technological weakness, exemplified by an observation from the head of the Committee of the Council of Federations of Russia, Andrey Klishas, that Russia's import substitution program had failed completely. It was also caused by the increase in U.S. intelligence sharing with Ukraine, the participation of U.S. military hackers in offensive and defensive operations in support of Ukraine, and the cooperation between the White House, the Department of Homeland Security, and Microsoft to help Ukrainian government agencies and other organizations defend their cyberspace.

Unlike conventional forms of Russian-Ukrainian warfare, in which the United States and allies avoid intervention to keep the war from escalating, gray-zone conflict in cyberspace makes it possible to defeat Russian cybersecurity actors without being a party to the conflict. However, cyberwarfare with the participation of the United States and other international cybersecurity actors has been limited. Since the Russian-Ukrainian war is dragging out, cyberwar has every chance of regaining its key role in future operations.

Acknowledgments

Tetyana Malyarenko gratefully acknowledges funding from the Erasmus+ Programme of the European Union and Volkswagen Stiftung; Jean Monnet Module "The EU's comprehensive approach to security: tackling evolving threats, building a strong security ecosystem" [Project 101047745 – EUSEC]; and Jean Monnet Project "Towards a More Secure Digital Europe: Multilevel Governance for Countering Online Disinformation and Hybrid Threats" [619924-EPP -t-2020-l-uA-EppJMo-pRoJECT].

Borys Kormych gratefully acknowledges funding from the Jean Monnet Module "The EU's comprehensive approach to security: tackling evolving threats, building a strong security ecosystem" [Project 101047745 – EUSEC].

PONARS EURASIA NEW APPROACHES TO RESEARCH AND SECURITY IN EURASIA

Elliott School of International Affairs
THE GEORGE WASHINGTON UNIVERSITY