Cyber Warfare in the Ukrainian Conflict — a Determinant of the Outcome of the War?

by Réka Szabó

ITSS Verona Magazine, Vol. 1, no. 1

Spring/Summer 2022

Cyber Warfare in the Ukrainian Conflict — a Determinant of the Outcome of the War?

Réka Szabó

To cite this article: Réka Szabó, *Cyber Warfare in the Ukrainian Conflict — a Determinant of the Outcome of the War?*, ITSS Verona Magazine, Vol. 1, no. 1, Spring/Summer 2022.

Keywords: Ukrainian War, Crimean War, Russia, Cyberwarfare, Unconventional Warfare

ITSS Verona website: https://www.itssverona.it/itss-magazine

LinkedIn: https://www.linkedin.com/company/itss-verona/

Instagram: https://instagram.com/itss_verona?igshid=YmMyMTA2M2Y=

Twitter: https://twitter.com/itssverona

Published online: June 18th, 2022

Abstract: Cyber warfare is being used by both Russia and Ukraine in the current war against Ukraine. This essay sheds light upon the structures and actors — with or without formal ties to the warring states — of the current ongoing cyber warfare, and their influence on the current conventional war. Cyber attacks from the era of the annexation of Crimea and the crisis in the Donbas region are also highlighted, in order to contextualize the current events. Since that time, changes have occurred in cyber warfare strategies and actors; despite these changes, cyber warfare remains a tactic of limited strategic value.

Several patterns of the current war in Ukraine resemble wars in the past in which Russia or the Soviet Union took part. As technology has changed , the methods of warfare have changed, and this has had an impact on how contemporary wars are being waged. Today, it is not only conventional forces that are being deployed by Ukraine and Russia, but cyber tools and tactics as well. . This essay describes the cyber warfare tools and tactics used in the current Ukrainian conflict and presents the structures and actors connected to them.. Antecedents from the era of the annexation of Crimea are also highlighted, to contextualize current events.

Interpreting the use of cyberspace in warfare

Cyberattacks are part of hybrid warfare. As the Center for European Policy Analysis (CEPA) describes it, such warfare "combines military and nonmilitary as well as covert and overt means, such as disinformation, cyberattacks, economic coercion, […] corruption, and irregular and regular forces. […] [these] attempt to undermine target institutions and populations to achieve strategic aims."[1] As a result of globalization and technological development, their "speed, intensity, and scope" have grown in recent times.[2]

There are differences between the Western and Russian attitudes to warfare in cyberspace. The Russian interpretation of cyber warfare — as it is called in the West — is a kind of warfare that is part of the so-called *information confrontation*.[3] This has to be observed through the lens of a geopolitical zero-sum game, in which the national interest is achieved or protected with the involvement of information infrastructures. *Cybersecurity* as a term does not appear in Russian usage. Documents from the Ministry of Defense and other authorities refer to it as *information security* instead. This encompasses more than cybersecurity: it is not solely about "the protection of critical digital networks, but society's cognitive integrity as well."[4] This points out that maintaining narratives about certain events among populations is considered crucial by Russia. By using operations that focus on the cognitive spheres, Russian actors are able to spread disinformation and

[1] CEPA, "Hybrid Warfare of the Future," July 28, 2021, https://cepa.org/hybrid-warfare-of-the-future-sharpening-natos-competitive-edge/.
[2] See note above.
[3] NATO StratCom COE, "Russia's Strategy in Cyberspace" June 2021, accessed April 1, https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf, 4.
[4] See note above, 5-6.

misinformation. As the narratives become entrenched in the population, Russia is able to use them as justification for their foreign policy and claim their strategic aims are legitimate.

In cyber warfare, damage can be done in both physical and cognitive spheres. To achieve suh damages, cyberspace can be used in multiple ways. It embodies software, hardware, and infrastructure as well. *Information war* has a broader scope, and can mean "a wide array of activities […], the spreading of disinformation, electronic warfare, the degradation of navigation support, psychological pressure, and the destruction of adversary computer capabilities."[5] Overall, cyber warfare can be applied for offensive and defensive purposes.

In observing Russian cyber warfare-related practices today, experts[6] claim that the legacy of the Soviet Union is still evident. There are operations in cyberspace that strive for the alteration/influence of policies of other nations, in a secret way, using illegal means. The manipulation of information is a way of doing this. Another example of operations that can be paralleled with Soviet-era methods is the one that encompasses concealment and deception so that the other party makes mistakes because of false pieces of information.

Cyberattacks used in the current conflict can be classified into three main categories. One group is called wipers. Such attacks delete information from networks or block data. Another type of cyberattack is DDoS (Distributed Denial of Service) attacks. These impede the access of websites, by "overwhelming a system via an excessive number of 'requests' — people trying to access a website — in a short space of time."[7] Defacement attacks, on the other hand, operate on the psychological or cognitive level: they eliminate or modify pieces of information from websites, thus facilitating the dissemination of disinformation and fake news.[8]

Russian cyber warfare actors

Several actors have been active in cyber wars since the annexation of Crimea, ranging from actors connected to the Russian state to volunteers. Similar to conventional proxy wars, some actors

[5] NATO StratCom COE, "Russia's Strategy in Cyberspace," 7.
[6] NATO StratCom COE, "Russia's Strategy in Cyberspace," 11.
[7] Deutsche Welle, "Ukraine: Cyberwar Creates Chaos, 'it Won't Win the War' | DW | 03.03.2022," DW.COM, accessed April 1, 2022, https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197..
[8] See note above.

can be called proxies in cyberspace as well. Although there is no scholarly agreement on the definition yet, according to Tim Maurer (New America Foundation), one can be the following: "actors using force against a third party to the benefit of the state."[9] This includes private actors as well, which are prominent in the current war, according to the expert.

While it is difficult to trace actors and find connections between them, Russian state actors have unquestionably been taking part in cyber warfare, or, as they call it, *information confrontation*. The Federal Security Service (FSB), the former Committee for State Security (KGB), is one of these. It is responsible for counter-intelligence and intelligence connection, and "securing Russia's domestic information space"[10] Turla, a cyber espionage group, engaging in espionage campaigns in several countries, including the United States, is claimed to be linked to FSB.

Another significant state actor is the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU or GU). This external intelligence agency is responsible for offensive cyber operations, signal intelligence, and cryptography, and hack and leak operations in the presidential elections in the United States in 2016. It "uses cyberspace not only for espionage but also for sabotage and information operations."[11] There are hacktivist groups that can be linked to the GRU, like CyberBerkut and the Sandworm Group, and APT28 (APT stands for *advanced persistent threat*).

The other external intelligence agency is the Foreign Intelligence Service (SVR). It "steals information for traditional espionage purposes."[12] APT29 is the group connected to it, and it targeted the United States, the Netherlands, and Norway.

The Internet Research Agency (IRA) is a private organization but it also has ties to the Kremlin. It has several departments which are responsible for comments, infographics, videos, and other outputs which are centrally guided and support the Kremlin's side.[13]

---

[9] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine", http://195.222.11.251/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf

[10] NATO StratCom COE, "Russia's Strategy in Cyberspace," 17.

[11] NATO StratCom COE, "Russia's Strategy in Cyberspace," 19.

[12] See note above.

[13] NATO StratCom COE, "Russia's Strategy in Cyberspace," 2.

The so-called *patriotic hackers* take part in cyberattacks. These people are not "part of the state machinery," but they "might act based on their attachment to the state either independently or be given direction by the state."[14] There are *cyber criminals,* too, "who are either paid by intelligence services or, if willing to put their skills to the service of the state, will have their prison sentences significantly reduced."[15] The deployment of the latter group is cost-effective and it is also easy to deny their ties to the government. There is, however, proof that cyber criminals were connected to the FSB.

Cyber warfare during the crises in Crimea and the Donbas region

Russia used cyber warfare before the annexation of Crimea, and actors connected to the Russian state (proxies) played a significant role in the preparation of the annexation and the destabilization of Ukraine. Just like the Gamaredon group, IRA became active before the annexation of Crimea.[16] The troll farm disseminated pro-Kremlin messages in Russia and other countries, contributing to the public support of military operations in Crimea..[17] Other groups connected to the GRU initiated attacks against Ukraine, too: APT28 interfered in the 2014 presidential elections. CyberBerkut did the same, with the use of malware that damaged the systems responsible for vote counting.[18] This group conducted "cyber-espionage, information operations, and disruptive computer network intrusions, including DDoS"[19] not only targeting Ukraine but NATO and Germany as well. As the cyber war continued during the crises in Crimea and eastern Ukraine, the Sandworm group carried out cyber attacks on critical infrastructure, [20] resulting in blackouts in the country.[21]

Ukraine was able to engage in the cyber war against Russia and proxies were present, too. The volunteer group called Ukrainian Cyber Forces with Eugene Dokukin had an unquestionable role in it. They used DDoS attacks, leaked documents, and engaged in other activities. Maurer

[14] NATO StratCom COE, "Russia's Strategy in Cyberspace," 21.
[15] See note above.
[16] GLOBSEC, "Where Is Cyberwar? Preliminary Takeaways from Russia's War on Ukraine,", accessed April 1, 2022, https://www.globsec.org/news/where-is-cyberwar-preliminary-takeaways-from-russias-war-on-ukraine/.
[17] See note 14.
[18] See note 16.
[19] See note 11.
[20] See note 16.
[21] See note 11.

claims that during this conflict, significant cyber capabilities were privately owned, and these were used by states. Some were patriotic hacker groups in Ukraine, for example, Cyber Hundred and Null Sector initiated DDoS attacks against the Kremlin's websites and the Russian central bank.[22] Anonymous also engaged in activities by that time.

Despite the engagement of several hacktivist groups in the conflict, "the amount of cyber proxy activity has remained relatively low" on the Ukrainian side, and actions on both sides were "limited to DDoS attacks, web defacements, and the occasional leaking of government files."[23]

Cyber warfare in the current war in Ukraine

As in the era of the crises in Crimea and eastern Ukraine, cyber warfare is being used in the current Ukrainian conflict; , however only to a limited extent. Russia appears to have changed their cyber strategy, compared to previous years. According to Josephine Wolff, associate professor of cybersecurity policy at Tufts University, a shift has happened in their strategy, resulting in more covert operations in the cyber domain. This means the increased use of "tactics like credential harvesting, supply chain compromises, and infiltrating critical service provider platforms," and the decreased application of "techniques like traditional phishing and denial-of-service attacks."[24] Russia's shift to more covert operations means that it is relying less heavily on techniques like traditional phishing and DDoS attacks. Instead, the focus is on more advanced intrusion tactics like credential harvesting, supply chain compromises, and infiltrating critical service provider platforms. Wolff also draws attention to elevated activity by the SVR and the "the relative inactivity of the GRU in the cyber domain since 2018."[25] Cybersecurity expert Matthias Schulze claims that Russia is unable to combine conventional war with cyber tactics and the separately existing cyber warfare has only a psychological effect that will not be a determining factor in the eventual outcome of the war. He describes the Russian cyber war efforts as "cyberattacks connected to espionage and

[22] Tim Maurer, "Cyber Proxies and the Crisis in Ukraine," in *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers (Tallinn: NATO CCD COE Publications, 2015), http://195.222.11.251/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf, 81.

[23] See note above, 85.

[24] Josephine Wolff, "Understanding Russia's Cyber Strategy," Foreign Policy Research Institute, July 27, 2021, https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/.

[25] See note above.

disinformation, or wiper attacks," and believes that "there is no indication that any of these attacks have helped Russia strategically on the battlefield."[26]

Several explanations exist for the limited cyber activities. One is that bombardment was enough for the destruction of infrastructure in Ukraine, and additional cyber attacks were simply not useful or effective anymore. Another claim is that the military actions were planned to last only for days, and for the implementation of cyberattacks, simply put, more time would be needed. Following the third train of thought, a possible failure occurred on the Russian side in the execution of successful attacks, thanks to the cooperation between Ukraine, the United States, and NATO. Lastly, it is also possible that Russia uses cyber capabilities as deterrence.[27]

On the other hand, this does not mean that activities in cyberspace are not going to intensify later. One reason for this is that "cyber warfare does not lend itself to a linear plan of attack with defined inputs and outcomes,"[28] as in conventional wars with kinetic military actions. Furthermore, what makes the current war different from others and what shows the importance of the cyber domain — even if it is not decisive in the overall war yet - is the size of the *cyber armies.* According to estimates, more people are participating in cyber warfare now than the number of soldiers engaging in conventional warfare on the ground.

It is important to point out that these cyber warfare-related activities are not necessarily limited to Russia, Ukraine, and neighboring countries. There are implications for political and military developments at the international level as well. It can spread further to other countries and has already done so, in the form of malware attacks, for instance. There is also a possibility that Russia could launch a "direct cyberattack on another country's critical infrastructure."[29] At this point, such an action is not considered likely since it would lead to an escalation of the war and could lead to the direct involvement of NATO. NATO Secretary-General Jens Stoltenberg affirmed

[26] Deutsche Welle, "Ukraine: Cyberwar Creates Chaos, 'it Won't Win the War' | DW | 03.03.2022," DW.COM, accessed April 1, 2022, https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197.
[27] POLITICO, "The World Holds Its Breath for Putin's Cyberwar," accessed April 1, 2022, https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440
[28] See note 16.
[29] See note 26.

that cyberattacks can trigger Article 5.[30] It should be noted that Ukraine is now a contributing participant of NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), and its cyber resilience has increased against Russian attacks in the cyber domain.[31]

The main actors in cyberspace and their activities in the current war

Observing cyber attacks by Russia or its proxies, actors already active during the Crimean crisis appear, but other actors have engaged as well, not to mention the volunteer hacktivists whose identity often remains unrevealed.

Russian-affiliated actors were using cyber warfare before the invasion. In January, a wiper malware attacked Ukrainian systems, such as the networks of the Foreign Ministry.[32] After the invasion, activities in the cyber domain intensified. GRU is believed to have been "behind a cyberattack on a satellite broadband service that disrupted Ukraine's military communications."[33] The Russian APT28, which is also connected to GRU, "engaged in a credential phishing campaign targeting users of the popular Ukrainian media company UKRNet."[34] Other attacks can be traced back to the Russian state, for example, DDoS attacks on the Ukrainian Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs, Security Service, and Cabinet of Ministers, and on bank, government, and military websites. The Gamaredon group was also active; it attacked Ukrainian organizations with malware, including surveillance software.[35]

Russia, similarly to its activities during the annexation of Crimea, used fake news to strengthen the Russian narrative about events. Disinformation has been a significant part of cyber warfare, aimed at undermining public opinions. According to Meduza, Russian media portrayed a Ukrainian refugee from Mariupol as a testimony of atrocities committed by Ukrainian soldiers

[30] C-Span, "NATO Chief Says Cyberattacks Can Trigger Article 5," accessed April 1, 2022, https://www.c-span.org/video/?c5003322/nato-chief-cyberattacks-trigger-article-5.

[31] CCDCOE, "Ukraine to be accepted as a Contributing Participant to NATO CCDCOE", https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/

[32] Council on Foreign Relations, "Tracking Cyber Operations and Actors in the Russia-Ukraine War," accessed April 5, 2022, https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

[33] "Russian Military behind Hack of Satellite Communication Devices in Ukraine at War's Outset, U.S. Officials Say," The Washington Post, accessed April 5, 2022, https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/.

[34] See note 32.

[35] See note above.

against civilians, and who blames the mayor of the city for having abandoned the people. The video containing such fake pieces of information was distributed by the FSB.[36] Bot farms, supported by the Russian state, were also active on social media and distributed fake news about the war. Not only Russia-based actors have had a huge part in cyberattacks in this war. The Belarus APT Group launched disinformation campaigns (by hacking social media platforms of high profile Ukrainians) and phishing campaigns with malware, against ”European government personnel involved in managing the logistics of refugees fleeing Ukraine.”[37]

The Ukrainian state seems to be more prepared for this current state of cyber warfare, compared to the Crimean and eastern Ukrainian crisis. To counter Russian cyberattacks, the Ukrainian cyber-security authority, the Ministry of Digital Transformation was created in 2019. They recruited volunteers for a unit, the *IT Army.* This is an unprecedented escalation in the history of cyber warfare. Currently, there are hundreds of thousands of members on its Telegram channels.[38] They target websites of “infrastructure businesses, such as energy giant Gazprom, the country’s banks, the power grid, and railway system,[39] and official government websites”[40] and Russian-aligned sites with DDoS attacks.[41] This tactic is most helpful as a defensive measure,[42] but there have been “attempts to disrupt transport and power networks,” too.[43]

Other hacker groups have also engaged in the war on the Ukrainian side, including Anonymous, “a decentralized community of tech activists who collaborate in small groups on projects they call *operations*.”[44] Anonymous declared cyber war against Russia already on the day

---

[36] “‘Anybody Would Be Scared’ Russian State News Aired a Refugee’s Testimony about ‘Atrocities’ Committed by Ukraine’s Azov Battalion. The Video Came from the FSB. — Meduza,” accessed April 5, 2022, https://meduza.io/en/feature/2022/03/30/a-refugee-s-video-testimony-about-atrocities-committed-by-the-azov-battalion-made-the-rounds-on-russian-state-news-it-came-from-the-fsb.

[37] CyberPeace Institute, “Ukraine: A Timeline Of Cyberattacks,” February 24, 2022, https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

[38] POLITICO, “‘We Are the First in the World to Introduce This New Warfare’: Ukraine’s Digital Battle Against Russia,” accessed April 1, 2022, https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880.

[39] See note 32.

[40] “Ukraine’s Volunteer ‘IT Army’ Is Hacking in Uncharted Territory,” accessed April 1, 2022, https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

[41] See note 38.

[42] See note 40.

[43] BBC, “Ukraine Says It Is Fighting First ‘Hybrid War,’”, March 4, 2022, sec. Technology, https://www.bbc.com/news/technology-60622977.

[44] Dale Beran, “The Return of Anonymous,” The Atlantic, August 11, 2020, https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/.

of the outbreak of the war, and stated that it had hacked the database of the Russian Ministry of Defense, state TV channels,[45] websites,[46] and the Central Bank of Russia so that several files and confidential documents became publicly available.[47] They launched DDoS attacks[48] and hacked cameras and broadcasters, too, and disseminated information about the war.[49] Files of Roskomnadzor, a Russian state media regulator agency, were leaked by Anonymous as well. Another pro-Ukrainian hack group is called the Belarusian Cyber Partisans. Their cyberattacks aimed at impeding the use of railways in Belarus for Russian military means. Similarly, the malware RURansom wiper was used by hacktivists supporting Ukraine). It "functions as a wiper, and offers victims no opportunity to pay to have their systems decrypted" and also checks "victim's systems for a Russian IP address."[50]

There have been attacks from both sides where the hackers' or groups' identities are unknown. Malware was used against charity organizations, NGOs, for example, "in order to spread confusion and cause disruption".[51] The origin of malware used against Ukrainian government networks is also as yet unknown. Similarly, DDoS attacks of unknown origin were launched against the Kyiv Post to impede the publishing of news.[52] Undetectable attacks occurred on the Ukrainian side as well: Vkontakte – the largest social media platform in Russia – was hacked, and data about the war was shared on it,[53] in the form of private messages for the users.[54]

---

[45] The Guardian, "Anonymous: The Hacker Collective That Has Declared Cyberwar on Russia | Ukraine," accessed April 1, 2022, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

[46] See note 43.

[47] India Today, "Hacker Group Anonymous Targets Russia's Central Bank, Threatens to Release Secret Documents - World News," accessed April 1, 2022, https://www.indiatoday.in/world/russia-ukraine-war/story/russia-ukraine-war-anonymous-collective-hacked-the-central-bank-of-russia-1928830-2022-03-24.

[48] See note 40.

[49] India Today, "Hacker Group Anonymous Targets Russia's Central Bank, Threatens to Release Secret Documents - World News."

[50] See note 32.

[51] CyberPeace Institute, "Ukraine: A Timeline Of Cyberattacks,", February 24, 2022, https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

[52] See note above.

[53] The Times, "Russian Social Media 'Hacked by Western Intelligence Agency'," accessed April 1, 2022, https://www.thetimes.co.uk/article/ukraine-war-russian-social-media-hacked-by-western-intelligence-agency-qzcf293sz.

[54] HVG, "Tech: Feltörték Az „orosz Facebookot", És 12 Millió Címre Írták Meg, Mi Is Történik Ukrajnában," accessed April 1, 2022, https://hvg.hu/tudomany/20220321_vkontakte_kozossegi_media_hackertamadas_hackerek_ukrajna_haboru.

Conclusion

So far, we are seeing an unprecedented level of cyber activity occurring alongside conventional warfare. Although the intensity is still relatively low, some experts predict that the cyber domain has the potential to intensify the current conflict.[55] If the war continues, it is logical to presume that states and their proxies are going to use all their efforts, even on the cyber level, to gain an advantage. By learning from mistakes, engaging with more sophisticated technologies, and combining conventional war and cyber tactics, actors could become more determinant, and set a precedent for future wars in which the cyber domain is strategically crucial.

[55] See note 45.

Bibliography

Beran, Dale. “The Return of Anonymous.” The Atlantic, August 11, 2020. https://www.theatlantic.com/technology/archive/2020/08/hacker-group-anonymous-returns/615058/.

CCDCOE. ”Ukraine to be accepted as a Contributing Participant to NATO CCDCOE.” Accessed April 1, 2022. https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/.

CEPA, “Hybrid Warfare of the Future,” July 28, 2021. https://cepa.org/hybrid-warfare-of-the-future-sharpening-natos-competitive-edge/.

Council on Foreign Relations, “Tracking Cyber Operations and Actors in the Russia-Ukraine War.” Accessed April 5, 2022. https://www.cfr.org/blog/tracking-cyber-operations-and-actors-russia-ukraine-war.

C-SPAN. “NATO Chief Says Cyberattacks Can Trigger Article 5.” Accessed April 1, 2022. https://www.c-span.org/video/?c5003322/nato-chief-cyberattacks-trigger-article-5.

CyberPeace Institute. “Ukraine: A Timeline Of Cyberattacks,” February 24, 2022. https://cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks/.

Deutsche Welle. “Ukraine: Cyberwar Creates Chaos, ‘it Won’t Win the War’ | DW | 03.03.2022.” DW.COM. Accessed April 1, 2022. https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197.

GLOBSEC. “Where Is Cyberwar? Preliminary Takeaways from Russia’s War on Ukraine.” Accessed April 1, 2022. https://www.globsec.org/news/where-is-cyberwar-preliminary-takeaways-from-russias-war-on-ukraine/.

“Hacker Group Anonymous Targets Russia’s Central Bank, Threatens to Release Secret Documents - World News.” Accessed April 1, 2022. https://www.indiatoday.in/world/russia-ukraine-war/story/russia-ukraine-war-anonymous-collective-hacked-the-central-bank-of-russia-1928830-2022-03-24.

HVG. “Tech: Feltörték Az „orosz Facebookot”, És 12 Millió Címre Írták Meg, Mi Is Történik Ukrajnában.” Accessed April 1, 2022. https://hvg.hu/tudomany/20220321_vkontakte_kozossegi_media_hackertamadas_hackerek_ukrajna_haboru.

Maurer, Tim. “Cyber Proxies and the Crisis in Ukraine.” Essay. In *Cyber War in Perspective: Russian Aggression against Ukraine*, edited by Kenneth Geers, 79–86. Tallinn: NATO CCD COE Publications, 2015. http://195.222.11.251/uploads/2018/10/Ch09_CyberWarinPerspective_Maurer.pdf.

Meduza. "'Anybody Would Be Scared' Russian State News Aired a Refugee's Testimony about 'Atrocities' Committed by Ukraine's Azov Battalion. The Video Came from the FSB." Accessed April 5, 2022. https://meduza.io/en/feature/2022/03/30/a-refugee-s-video-testimony-about-atrocities-committed-by-the-azov-battalion-made-the-rounds-on-russian-state-news-it-came-from-the-fsb.

NATO StratCom COE, "Russia's Strategy in Cyberspace" June 2021, Accessed April 1. https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf

POLITICO. "The World Holds Its Breath for Putin's Cyberwar." Accessed April 1, 2022. https://www.politico.com/news/2022/03/23/russia-ukraine-cyberwar-putin-00019440.

POLITICO. "'We Are the First in the World to Introduce This New Warfare': Ukraine's Digital Battle Against Russia." Accessed April 1, 2022. https://www.politico.com/news/magazine/2022/03/08/ukraine-digital-minister-crypto-cyber-social-media-00014880.

The Guardian. "Anonymous: The Hacker Collective That Has Declared Cyberwar on Russia." Accessed April 1, 2022. https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia.

The Times. "Russian Social Media 'Hacked by Western Intelligence Agency'." Accessed April 1, 2022. https://www.thetimes.co.uk/article/ukraine-war-russian-social-media-hacked-by-western-intelligence-agency-qzcf293sz.

The Washington Post, "Russian Military behind Hack of Satellite Communication Devices in Ukraine at War's Outset, U.S. Officials Say." Accessed April 5, 2022. https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say/.

Wired. "Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory." Accessed April 1, 2022. https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/.

Wolff, Josephine. "Understanding Russia's Cyber Strategy." Foreign Policy Research Institute, July 27, 2021. https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/.