2023

Russian Cyber Warfare in Ukraine

ANALYSIS & IMPLICATIONS

JUSTIN HEALEY

Table of Contents

Introduction

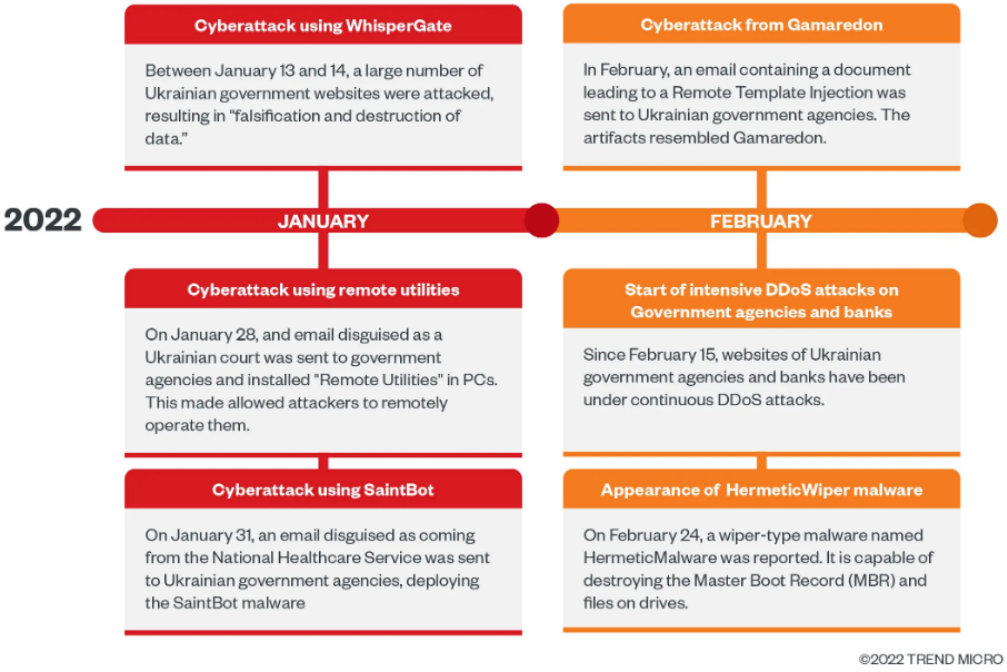
The Initial Invasion

Russia’s ground campaign in Ukraine has been in effect since February 24th, 2022, but Russian cyberattacks against Ukrainian infrastructure date back as far as 2014 (Lewis, 2022). Specifically, in 2015, the Russian military targeted Ukraine’s energy grid with the BlackEnergy malware. As a result of the BlackEnergy attack, the Kremlin succeeded in causing blackouts for approximately 80,000 Ukrainians. A year later, the Russian military targeted Ukrainian energy grids again with a similar malware. During this attack, dubbed “Industroyer,” about one-fifth of Kyiv lost power (Tidy, 2022). These types of attacks continued over the following years. In 2020 there were an estimated 397,000 cyberattacks against Ukrainian services, followed by another 288,000 in the first ten months of 2021 (Fiscal Risks and Sustainability, 2022)

Prior to the Russian ground invasion of Ukraine, it was known that a kinetic invasion of Ukraine would likely be preceded and accompanied by a series of cyberattacks against Ukrainian critical infrastructure. In February 2022, there were four major cyberattacks that occurred around the time of the Russian invasion (Przetacznik & Tarpova, 2022):

1. February 24, 2022 – Ukrainian communication systems and the KA-SAT satellite networks are interrupted one hour before the ground invasion.
2. February 25, 2022 – Ukrainian government websites are targeted with wiper malware, defacing with pro-Russian propaganda, and distributed denial of service (DDoS) attacks.
3. February 25, 2022 – A cyberattack against Romanian border control stations attempts to prevent Ukrainian refugees from entering Romania.
4. February 28, 2022 – Cyberattacks target Ukrainian civilian financial and energy sectors.

According to research performed by researchers at Wordfence, a leader in providing security to WordPress sites, cyberattacks against Ukrainian University and academic websites increased tenfold in the days leading up to the invasion (Maunder, 2022). Out of 282 websites where attacks “had increased dramatically following the invasion,” 229 contained the domain “edu.ua”; i.e., websites for academic institutions in Ukraine.



Cyberattack using WhisperGate

Between January 13 and 14, a large number of Ukrainian government websites were attacked, resulting in "falsification and destruction of data."

Cyberattack using remote utilities

On January 28, and email disguised as a Ukrainian court was sent to government agencies and installed "Remote Utilities" in PCs. This made allowed attackers to remotely operate them.

Cyberattack using SaintBot

On January 31, an email disguised as coming from the National Healthcare Service was sent to Ukrainian government agencies, deploying the SaintBot malware

Cyberattack from Gamaredon

In February, an email containing a document leading to a Remote Template Injection was sent to Ukrainian government agencies. The artifacts resembled Gamaredon.

Start of intensive DDoS attacks on Government agencies and banks

Since February 15, websites of Ukrainian government agencies and banks have been under continuous DDoS attacks.

Appearance of HermeticWiper malware

On February 24, a wiper-type malware named HermeticMalware was reported. It is capable of destroying the Master Boot Record (MBR) and files on drives.

©2022 TREND MICRO

A timeline of cyber-attacks leading up to the Russian ground invasion of Ukraine in 2022.
Source: Trend Micro (2022)

Importance & Implications

It is worth noting that Russia's cyber campaign against Ukraine has not yielded any disruptions greater than those caused by conventional and kinetic weapons (Bateman, 2022). For this reason, Russian cyber demonstrations should not be taken as a threat that is any larger than their conventional army, rather as a growing capability that the Federal Security Service (FSB) and Russian Military are developing.

The majority of the cyber attacks against Ukraine by the Russian military have been offensive operations designed to inflict damage against critical infrastructure or military targets. However, the Russian government may have better success, and a greater impact, by shifting their focus towards intelligence gathering and "hack-and-leak" operations against Ukrainian targets (Bateman, 2022). Additionally, the Russians are notorious for supporting cyber criminals and hacking groups – for example, APT29, "Cozy Bear," is a hacking group that is generally believed to be associated with and funded by the Russian Government, specifically Russia's Foreign Intelligence Service (SRV). The FBI, NSA, and Cybersecurity & Infrastructure Security Agency (CISA) released an advisory that publicly blamed APT29 for the SolarWinds supply chain attack in 2020 (U.S. DoD, Cybersecurity Advisory, 2021).

Another key component of cyber warfare is psychological cyberwarfare, i.e., targeting the morale of civilian and military personnel and executing a campaign that attempts to demoralize or bring down the spirits of your adversaries. With the rise of social media and development of new groundbreaking technologies, such as artificial intelligence (AI) and deepfakes, the Russians are able to have a much more drastic yet subtle influence and psychological warfare campaign. Although there is little clear evidence on the effect that Russian cyber attacks have had on the morale of Ukrainian citizens and military forces, the concern is real. This report further analyzes the psychological effect of cyberwarfare on Ukrainian citizens and troops in the Psychological Cyber Warfare sub-section of Potential Consequences.

As with conventional warfare, cyberwarfare can be extended to physical and/or digital destruction; for example, Black Energy and Industroyer were Russian cyberattacks on the Ukrainian energy grid that caused blackouts in Kyiv in 2015 and 2016 respectively. The Russians also knocked out Ukrainian satellite communications systems as a supplement to their 2022 ground invasion. This was done not with missiles, but with malware, allowing for a more discrete, immediate, and risk-averse offensive.

Potential Consequences

Psychological Cyber Warfare

Psychological warfare is the use of propaganda, military, economic, or political acts against an enemy intended to reduce the morale of the enemy (Britannica). Political propaganda and misinformation are historical trademarks of any Russian conflict or involvement, and the Russian media is heavily influenced by the Kremlin – this has been known for decades – but this control has spiraled in lieu of the "special operation" in Ukraine. Russia's cyber campaign in Ukraine has been, in part, an attempt to spread misinformation and demoralize the Ukrainian people.

Less than a month after the unsuccessful initial ground invasion by Russian forces in Ukraine, Russian hackers posted a deepfake video of Ukrainian President Volodymyr Zelensky on a Ukrainian news site (Bergengruen, 2023). In the video, Zelensky is shown urging his people to give up, and that "There is no need to die in this war … I advise you to live." The video was promptly taken down and very publicly debunked and refuted by Ukrainian and other Western officials. Nonetheless, it was one of many attempts by the Russian military and affiliated groups at demoralizing the Ukrainian citizens and troops.

It appears that, as Putin tries to degrade the Ukrainian people and empower his own through control of the media and digital information in Moscow, he may be having the opposite effect. In an article discussing Russian media influence and control, CNN compares the control and access to digital information in Russia to the Iron Curtain (Picheta, 2023). The same article describes an interview with a Moscow resident, who describes how she supported the invasion in the beginning but is now completely against it. She cites the lack of transparency and misinformation from the Kremlin, as well as moral reasons for her change of heart. This is an increasingly common narrative.

The Russians had been targeting Ukrainian civilian infrastructure for years before the ground invasion. However, as winter approaches, the Russian military and affiliated hacking groups have turned more of their attention towards electricity and internet civilian infrastructure (Miller, 2023). By targeting the energy sector, the Russians hope to terrorize the Ukrainian people – there is no other reason to target civilian infrastructure. Whether the aim is to freeze the Ukrainian people to death or demoralization, the attacks have caused intense fear.

Ukrainian officials reported that they thwarted a Russian cyber-attack on *civilian* energy grids at the beginning of the invasion in April of 2022 (Pearson, 2022). The attack was blamed on the hacking group Sandworm, which is believed to be closely tied to the Russian military and, although this attack targeted physical infrastructure, it was likely in part an attempt to show Ukrainian civilians that Russia is targeting them too – to instill fear and decrease morale.

Destructive Cyber Warfare

The Russian Government is focused on spreading propaganda, instilling fear, and pushing their narrative across Ukraine; simultaneously, hacking groups, such as Sandworm and Cozy Bear, have been hammering away at Ukrainian civilian and military infrastructure for nearly a decade. In 2015, when Russia illegally annexed Crimea, the Ukrainian power grid was hit with a sophisticated version of the Black Energy malware. The Ukrainians, along with the United States and other allies, blamed hacking group APT 28 or "Fancy Bear." Fancy Bear is known to be linked to the Russian SVR and military (Miller 2021). A similar attack, later named Industroyer, occurred in 2016. This attack was attributed to a hacking group named Sandworm, which is also believed to be linked to the Russian SVR.

In 2022, when Russia conducted a ground invasion of Ukraine, there were hundreds of cyber-attacks targeting Ukrainian civilian and military infrastructure, but only several had a considerable impact. Appearing to follow past campaigns, multiple attacks specifically targeted Ukrainian energy providers and infrastructure. In the first week of the invasion, there were 22 major destructive cyber-attacks targeting services in Ukraine (Microsoft Special Report, 2022). The threat actors are modifying the malware, adding obfuscation, and increasing sophistication with every major attack to attempt to avoid detection. The most common attack vector is phishing, where access is exploited to introduce trojans and other malware.

Threat Actors

The Russian Foreign Intelligence Service (SVR), Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), and Federal Security Service (FSB) all conduct intelligence, military, and espionage activities on behalf of the Russian Federation. For the purposes of cyber warfare, these groups rarely carry out operations themselves; rather, they recruit elite hacking groups to attack foreign targets so the Federation can maintain plausible deniability.

Note: this is not a complete list, rather is a list of the most prominent/active criminal hacking groups associated with the Russian Federation.

APT 29 (Cozy Bear, Dark Halo, Nobelium)

APT 29 is a prominent player in the cyber activities of the Russian SVR and FSB (Council on Foreign Relations). APT 29 primarily targets governments and affiliated agencies; they were blamed for the 2015 attacks against the White House, Department of State, and the Pentagon. Additionally, the 2020 supply chain attack on SolarWinds was attributed to Cozy Bear, where the group was able to compromise thousands of networks, including those of several top-level U.S. government agencies.

Unit 74455 (Sandworm, Telebots, VooDoo Bear)

Unit 74455, more commonly known as Sandworm, has been linked to the Russian GRU (Starks 2022). Sandworm was responsible for the 2015 WannaCry (NotPetya) incident, Industroyer in 2017, as well as a more recent attempted attack against Ukrainian civilian infrastructure in April of 2023. Sandworm is believed to have carried out interference in the 2017 French presidential election and the 2018 Winter Olympic Games cyberattack.

Berserk Bear (Energetic Bear, Crouching Yeti)

Berserk Bear is a Russian FSB affiliated hacking group that targets entities in Western Europe and Western Hemisphere (CISA Advisory AA22-110A). Berserk Bear tends to seek out critical infrastructure and defense industrial base organizations. This group has been known to conduct extensive reconnaissance and phishing campaigns, including scanning outward facing infrastructure, conducting brute force attacks, and attempting web-based cyber-criminal activities (drive by downloads, defacing, etc.).

Conclusions

Summary & Analysis

The Russian Federation has not had much success in Ukraine thus far – it appears that, at least in terms of cyberwar, Ukraine has been a testing ground for the SVR, FSB and GRU. The Russian Government has used Ukraine to test what tactics work, what is worth it, and how far they can go without retaliation. By recruiting elite hacking groups to do their dirty work, the Russian Government maintains plausible deniability, while simultaneously fueling their propagandic message. So far, the Russians have been primarily targeting infrastructure – energy grids, water supplies – a large amount of which is civilian infrastructure.

Plausible Deniability & Testing the Waters

It is known that the Russian Government recruits elite hacking grounds to carry out attacks on foreign targets. By doing so, the Russian Federation maintains plausible deniability, i.e., a "prove it" stance, while gaining the media's attention in the West. Even if their attacks in Ukraine so far have not been overly successful (as far as we know), the pure fact that they are *trying* means that cyber is a growing interest and capability of the Russian Government – this capability, as of now, is proxied through third-party hacking groups. Nonetheless, the attacks are on behalf of the Kremlin, whether they originate in the Federation or are sponsored by It. All this time, they have been testing their capabilities (rather, the capabilities of the groups they recruit), finding the line of retaliation, and testing what they can realistically get away with.

Impact on Infrastructure

From the annexation of Crimea in 2014 through the ground invasion of Ukraine in 2022, the Russians have notoriously sponsored cyber-attacks around the globe, namely BlackEnergy (2015), Industroyer (2016), Olympic Destroyer (2018), and numerous others since the war began in 2022.

The question remains whether these attacks illustrate a need for future concern of Russian state-sponsored cyber-attacks, and whether previous attacks have been impactful against their physical targets. The attacks against the Ukrainian power grid, for example, were by definition "successful," but whether they were impactful is questionable. The hackers managed to cause slight chaos in Kyiv on more than one occasion, but the effects were short lived and quickly remedied. In short, Russian state sponsored attacks on infrastructure have been successful but have not had a major physical effect on their targets. Rather, the attacks on infrastructure have allowed the Kremlin to paint themselves as a world cyber-power, find out the best ways to remain anonymous, and find the line at which victims would respond.

Psychological Impact

Russian cyberattacks arguably cause more psychological damage and spread more propaganda than they have a physical impact. In other words, previous Russian cyberattacks have spread the message “we [the Russian Federation] are developing these amazing cyber-capabilities and you all should be scared,” even though they have not had incredibly devastating physical effects.

The psychological effects of cyberwar can be politically influential and help create a false curtain around the level of capability of an actor. This is precisely what the Russian Federation has been aiming for. If they were aiming for physical destruction, they would use kinetic weapons. If they were aiming for intelligence, they would target more classified networks and organizations (the only major example of this was SolarWinds in 2020). Instead, Russian cyber-attacks in Ukraine have largely targeted *civilian infrastructure*, namely power grids, as well as defacing government websites.

By targeting civilian infrastructure, the Russians are able to do what they have always strived to do – that is, look scary. As we saw with the ground invasion, the Russian army was no where near as capable or sophisticated as the world thought. That is not to say the ground invasion has “failed,” that is a different conversation, but rather to say that the Russians tend to be almost all bark and almost no bite; their cyber demonstrations in Ukraine have been no different than their masking of their kinetic abilities. The Kremlin aims to cause fear and to be feared. Targeting civilian infrastructure causes the media to paint exactly the picture that the Kremlin wants and provokes average citizens to fear Its cyber capabilities, even if those capabilities are not much more advanced than any other world power’s, if at all.

It is important to note that, despite their apparent efforts, Russian cyberattacks have seemingly had an opposite effect than that they intended. There are examples of Russian citizens who supported the war, but quickly changed their minds once they discovered Putin was hiding the truth. At the same time, Russian propaganda and continuous attacks have only infuriated the Ukrainian people, rather than demoralize them, and caused them to fight even harder.

References

(2022). *Fiscal Risks and Sustainability.* Office for Budget Responsibility , Stationary Office . London, U.K.: HH Associates Ltd. . Retrieved April 18, 2023, from https://obr.uk/docs/dlm_uploads/Fiscal_risks_and_sustainability_2022-1.pdf

Bateman, Jon. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." *Carnegie Endowment* , 16 Dec. 2022, carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

Bergengruen, Vera. "Inside Russia's Year of Ukraine Propaganda." *Times Magazine* , 22 Feb. 2023, time.com/6257372/russia-ukraine-war-disinformation/.

"Connect the Dots on State-Sponsored Cyber Incidents - the Dukes." *Council on Foreign Relations*, www.cfr.org/cyber-operations/dukes. Accessed 22 May 2023.

Defense Media , U.S. Department of Defense , Apr. 2021. https://media.defense.gov/2021/Apr/15/2002621240/-1/-1/0/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF/CSA_SVR_TARGETS_US_ALLIES_UOO13234021.PDF. Accessed 18 May 2023.

Lewis, J. A. (2022, June 16). *Cyber War and Ukraine* . Retrieved from Center for Strategic & International Studies : https://www.csis.org/analysis/cyber-war-and-ukraine

Maunder, M. (2022, March 1). *Ukraine Universities Hacked as Russian Invasion Started* . Retrieved from Wordfence : https://www.wordfence.com/blog/2022/03/ukraine-universities-hacked-by-brazilian-via-finland-as-russian-invasion-started/

Miller, Christina. "Throwback Attack: Blackenergy Attacks the Ukrainian Power Grid." *Industrial Cybersecurity Pulse*, 15 Aug. 2022, www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-blackenergy-attacks-the-ukrainian-power-grid/.

Miller, Maggie. "Russia's Cyberattacks Aim to 'terrorize' Ukrainians." *POLITICO*, 11 Jan. 2023, www.politico.com/news/2023/01/11/russias-cyberattacks-aim-to-terrorize-ukrainians-00077561.

Microsoft Digital Security Unit. Special Report: *An overview of Russia's cyberattack activity in Ukraine.* 27 April 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Pearson, James. “Ukraine Says It Thwarted Russian Cyberattack on Electricity Grid.” *Reuters*, 12 Apr. 2022, www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/.

Picheta, Rob. “‘It’s All a Lie’: Russians Are Trapped in Putin’s Parallel Universe. but Some Want Out.” *CNN*, 27 Feb. 2023, www.cnn.com/2023/02/27/europe/russia-propaganda-information-ukraine-anniversary-cmd-intl/index.html.

Przetacznik, J., & Tarpova, S. (2022). *Russia's war on Ukraine: Timeline of cyber-attacks.* Brussels, Belgium : European Parliamentary Research Service.

“Psychological Warfare.” *Encyclopædia Britannica*, www.britannica.com/topic/psychological-warfare. Accessed 18 May 2023.

“Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (AA22-110A).” *Cybersecurity and Infrastructure Security Agency CISA*, 16 May 2023, www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a.

Starks, Tim. “Analysis | Russian Sandworm Hackers Deployed Malware in Ukraine and Poland.” *The Washington Post*, 11 Nov. 2022, www.washingtonpost.com/politics/2022/11/11/russian-sandworm-hackers-deployed-malware-ukraine-poland/.

Tidy, J. (2022, March 22). *The three Russian cyber-attacks the West most fears*. Retrieved from British Broadcasting Company : https://www.bbc.com/news/technology-60841924

Trend Micro Research. “Cyberattacks Are Prominent in the Russia-Ukraine Conflict.” *Trend Micro*, 3 Mar. 2022, www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html.