The Ongoing Cyberwar Between Ukraine and Russia

Edward Kevin Winata
Binus International University
Central Jakarta, Indonesia
edward.winata@binus.ac.id

***Abstract*—This section represents a preliminary review of cyber operations in the Ukraine conflict based on publicly available information. Ukraine was not the first "cyber war"—the term itself makes little sense—but it was the first major conflict involving large-scale cyber operations. The so-far inept Russian invasion, where cyber operations have provided little benefit, raises questions about the balance between defense and offense in cyberspace, the utility of offensive cyber operations, and the requirements for planning and coordination. Better-than-expected Ukrainian defenses seem to be one hallmark of this invasion and the primary reason why Russian cyber efforts have had limited effect.**

It is likely that Ukraine, forewarned by Russian cyber actions that began as early as 2014, was better prepared as a result. It was also assisted in its cyber defense by friendly countries and private actors with whom it had developed cooperative relationships before the conflict [1]. This preparation allowed it to deflect many Russian offensive cyber operations, suggesting that a well-prepared and energetic defense can have the advantage over offense in cyberspace.

Russia had previously used cyberattacks against Ukraine to destroy or damage infrastructure and data. It attempted to do so again in the year of 2022. Based on publicly available information, Russia launched a broad cyber campaign shortly before the invasion. Some reporting showed a huge increase in exploits on the first day. The intent appears to have been to create disorder and overwhelm Ukrainian defenses. Russia sought to disrupt services and install destructive malware on Ukrainian networks included phishing, denial of service, and taking advantage of software vulnerabilities [2]. One company identified eight different families of destructive software used by Russia in these attacks. The primary targets were Ukrainian government websites, energy and telecommunication service providers, financial institutions such as banks and hedge fund managers as well as media outlets, but the cyberattacks encompassed most critical sectors. This was a wide-ranging attack using the full suite of Russian cyber capabilities to disrupt Ukraine, but it was not a success [3].

***Index Terms*—inept, hallmark, cyberspace, phising, encompassed, metric.**

I. Background

In conflicts involving modern militaries, cyberattacks are best used in combination with electronic warfare, disinformation campaigns, antisatellite attacks, and precision-guided munitions. The objective is to degrade informational advantage and intangible assets such as data, communications, intelligence assets, and weapons systems to produce operational advantage [4]. The most damaging actions would combine precision-guided munitions and cyberattacks to disable or destroy critical targets. Cyber operations can also be used for political effect by disrupting finance, energy, transportation, and government services to overwhelm defenders' decision making and create social turmoil [5]. Russia has been unable to achieve any of these objectives at meaningful scale.

It may offend the cyber community to say it, but cyberattacks are overrated. While invaluable for espionage and crime, they are far from decisive in armed conflict. A pure cyberattack, as most analysts note, is inadequate to compel any but the most fragile opponent to accept defeat [6]. No one has ever been killed by a cyberattack, and there are very few instances of tangible damage. Logical damage from attacks on software and data such as the Iranian action against Aramco are frequent, but these attacks usually do not create strategic advantage—which can be defined as forcing an opponent to make changes or concessions it would not have otherwise made—since they have not been used at scale and in a sustained manner, but rather in an uncoordinated and sporadic fashion. Sustained and systematic efforts are required to damage an opponent's ability to resist.

It takes a significant effort to make a cyberattack more than a dramatic annoyance. This requires highly detailed and thorough planning, tool developments and pre-reconnaissance, integrated with other offensive capabilities(as with the Israeli airstrike on Syrian nuclear facilities) [7]. The test of effectiveness lies in the results, measured by the extent of damage and whether the cyber operation forced an opponent to change plans or make concessions. Also, unlike a successful attack using a kinetic weapon, cyberattacks do not assure destruction (a radar hit by a missile can be seen to be a smoking ruin, but from the outside, a successful cyberattack on a radar may not look different from one that fails, and any damage may not be permanent) [8].

Cyber operations in conflict are very useful to conduct espionage, to gain advance knowledge of opponent planning and capabilities, and to mislead [9]. There was reportedly a surge of Russian action to penetrate North Atlantic Treaty Organization (NATO) networks at the onset of the conflict, a sensible precaution from the Russian perspective, given its fear of the possibility of a NATO intervention [10]. An attacker must weigh the loss of the benefits of espionage against the potential gain from a disruptive attack. In many cases, the benefits of espionage outweigh those of attack.

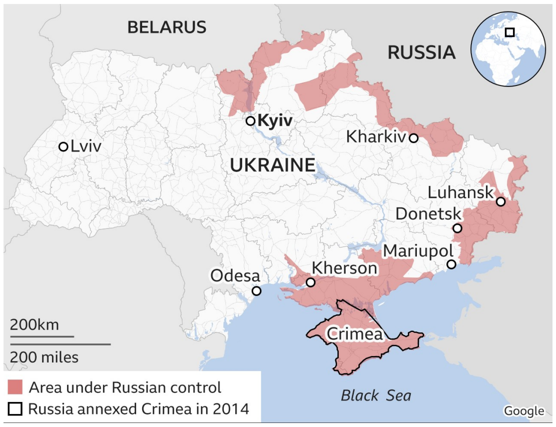

Fig. 1. Ukrainian Regions That Are Under Control By Russian Armed Forces

II. Offensive and Defensive Strategies

A. Russia's Cyber Warfare Capabilities

For years, Russia's military and intelligence establishment has been honing their skills in cyber warfare. They have carried out numerous cyber operations against a number of states(Ukraine, George, Estonia and even the United States). At the same time, they seem to enjoy a symbiotic relationship with deniable proxy groups such as CozyBear and FancyBear [11]. These and other groups carry out cyberattacks without significant consequences from the Russian state but are strongly believed to act for the Russian government when told to do so.

This array of Russian hackers who work directly for the state and / or under the implicit protection of the state have likely embedded malware and backdoors in numerous Ukrainian energy, communications and weapons systems, making Ukraine vulnerable to a cyber first strike. Such a kind of attack will likely be accompanied by a coordinated social influence campaign that spreads disinformation and misinformation to sow further confusion amongst the Ukrainian military and population [12]. Without NATO assistance, the combination of Russian military might, cyber assets and social media influence campaigns will likely lead to quick wins for Russia, should a kinetic conflict with Ukraine erupt in the upcoming weeks.

B. Ukraine's Cyber Warfare Capabilities

Prior to the invasion of Ukraine, Russian hackers identified a vulnerability in Microsoft's leading data management software. This was similar to a weakness in network software that allowed Russian hackers to unleash the NotPetya malware on Ukrainian networks in 2017 [13]. The attack caused an estimated 10 billion dollars in damage worldwide.

Ukraine's government had sought to build the most digitally advanced state in Eastern Europe as one of their greatest milestones in the country's cyber capability improvements. This objective has always been related with the enhancements of more features and controls.

Alongside their own efforts, public- and private sector partners have been involved in strengthening their cyber systems. USAID has provided cybersecurity support through a program that has been in place since 2020 [14]. This initiative has helped Ukraine bolster its cyber defences and address weak points.

Just days before Russian tanks began crossing into Ukraine in February 2022, Russian hackers used a vulnerability in the market-leading data management software SQL to place on Ukrainian servers in the form of malware that erases stored data [15]. However, over the last five years Ukrainian institutions have significantly strengthened their cybersecurity. Most notably, Ukrainian organizations have shifted away from pirated enterprise software, and they integrated their information systems into the global cybersecurity community of technology firms and data protection agencies.

III. Implemented Tools

The conflict between Russia and Ukraine is raging not only in the physical realm but also on the cyber front, where governments, hacktivist groups and individuals are trying to enforce their specialties and role inside.

Cyberwarfare by Russia includes denial of service attacks, dissemination of disinformation and propaganda, participation of state-sponsored teams in political blogs, internet surveillance using SORM technology, persecution of cyber-dissidents and other active measures [16]. According to investigative journalist Andrei Soldatov, some of these activities were coordinated by the Russian signals intelligence, which was part of the FSB and formerly a part of the 16th KGB department.

Fig. 2. Russian Investigative Journalist Andrei Soldatov

A. Wiper Malwares

According to Aqua Security, part of Ukraine's cyber experts hired by the government, the military campaign was preceded by a sophisticated cyberattack launched by Russia against multiple Ukrainian organisations. It included highly destructive wiper malwares named IsaacWiper and HermeticWizard, which are new and recently developed variants [17]. The attack, alongside the military campaign, aimed to make an impact on the conflict.

The malware was installed on hundreds of machines in Ukraine and was followed by a wave of distributed denial-of-service attacks. The new wipers can corrupt the data on a machine and make it inaccessible. In addition to the worm ability of spreading across a local network to infect more machines, they can also launch a ransomware attack and encrypt files on the compromised machine.

Back in 2017, Russia-linked hackers launched NotPetya, another kind of malware targeting financial softwares used by businesses in Ukraine. But the malware's use of a common vulnerability allowed it to spread worldwide, destroying access to almost all records at companies such as the Danish shipping giant Maersk — and causing an estimated 10 billion dollars in damages globally.

B. Assault On Ukraine's Electricity Providers

In 2015 Ukraine's electricity grid was disrupted by a cyber-attack called BlackEnergy, which caused a short-term blackout for 80,000 customers of a utility company in western Ukraine [18].

Then, nearly exactly a year later another cyber-attack known as Industroyer took out the power for about one-fifth of Kyiv province, the Ukrainian capital, for about an hour.

While The US and EU had named and blamed Russian military hackers for these attacks, experts believe that no cyber-attack against a power grid has resulted in an extended interruption of power supply. Executing cyber-attacks on complex engineering systems in a reliable way is extremely difficult and achieving a prolonged damaging effect is sometimes impossible due to in-built protections.

Some of them had also hypothesized that this event could backfire on Russia too, as the West is most likely to have a decent foothold and remote control in Russian networks as well.

C. Assault On Ukraine's Artillery Equipment

From 2014 to 2016, according to CrowdStrike, an U.S. based cyber tech company which has been monitoring the war for some time, Russian APT Fancy Bear(Cyber espionage team hired by the government) used Android malware to target the Ukrainian Army's Rocket Forces and Artillery. They distributed an infected version of an Android app whose original purpose was to control targeting data for the D-30 Howitzer artillery [19]. The app, used by Ukrainian officers, was loaded with the X-Agent spyware and posted online on military forums.

CrowdStrike claims the attack was successful, with more than 80 percent of Ukrainian D-30 Howitzer and multiple air crafts not usable anymore, the highest percentage loss of any artillery pieces in the army(a percentage that had never been previously reported and would mean the loss of nearly the entire arsenal of the biggest artillery piece of the Ukrainian Armed Forces). According to the Ukrainian army, this number is incorrect and that losses in artillery weapons were way below those reported and that these losses have nothing to do with the stated cause.

Fig. 3. Ukraine's D-30 Howitzer Artillery Cannon

D. Defacement Attacks and Fake News

Defacement attacks delete information on a website or change the information that appears there. It is a basic misinformation tactic that can mislead the general public into thinking fake information is reliable. And that fake information can spread fast.

It is also one of the oldest war tactics and it's called obfuscation, when actors in a war flood a civilian population with misleading information. Its effect are largely psychological, but very effective.

Other types of cyberwar are more open and official. For instance Meta, the company that owns the social media platform Facebook, has blocked 90 percent of Russian media on its platforms. In a counter maneuver, both Russia and Ukraine has been limiting access to Facebook. This leads to some Ukrainian citizens's reports about their social media accounts being restricted unexpectedly [20].

It has become difficult to tell what is real or fake concerning public news, and it is happening on both sides.

IV. Successfully Breached Systems

As to what the previous section had mentioned, it is a truth that one of the successful breach attempts made by Russia concerns Ukraine's electrical company systems which occurred as early as February 2022. As for how the intruders made their way into the company's internal systems, until the present moment, it is currently not yet known.

Ukrainian officials declined to name the company that suffered the breach and the region its substations are in, citing fears of continuing cyber attacks.

Ukrainian companies in finance and media have also been subject to regular cyber attacks since the war began. Ukrainian internal agency recalls that since Russia's invasion began, it had recorded three times as many attacks as it had tracked in the previous year.

Russian intruders have also broken into communications systems, including satellite communication services and telecommunication companies. Investigations into those breaches are continuing, although cyber security analysts and U.S. officials believe Russia is responsible. Other government hacker associations, including one affiliated with Belarus, have broken into media companies' systems and social media accounts of some of Ukraine's high-profile military officials, trying to spread disinformation that claimed Ukraine planned to surrender [21].

Acknowledgment

Not applicable.

References

[1] Connell, Michael, and Sarah Vogler. Russia's approach to cyber warfare. CENTER FOR NAVAL ANALYSES ALEXANDRIA VA ALEXANDRIA. United States, 2016. [Online].

[2] Limnéll, Jarno. "The exploitation of cyber domain as part of warfare: Russo-Ukrainian war." International Journal of Cyber-Security and Digital Forensics 4.4 , 2015, pp. 521-533. [Online].

[3] Maschmeyer, Lennart and Myriam Dunn Cavelty. "Goodbye Cyberwar: Ukraine as Reality Check." Policy Perspectives 10, 2022. [Online].

[4] Libicki, Martin C. "Correlations between cyberspace attacks and kinetic attacks." 2020 12th International Conference on Cyber Conflict (CyCon). Vol. 1300. IEEE, 2020. [Online].

[5] Jonsson, Oscar, and Robert Seely. "Russian full-spectrum conflict: An appraisal after Ukraine." The Journal of Slavic Military Studies 28.1, pp. 1-22. 2015. [Online].

[6] Springer, Paul J. Cyber Warfare: A Reference Handbook: A Reference Handbook. Abc-Clio, 2015. [Online].

[7] Libicki, Martin, and Kenneth Geers. "The Cyber War that Wasn't." Cyber war in perspective: Russian aggression against Ukraine, pp. 49-54. 2015. [Online].

[8] Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible digital front: Can cyber attacks shape battlefield events?." Journal of Conflict Resolution 63.2, pp. 317-347. 2019. [Online].

[9] Astrov, Vasily, et al. Possible Russian invasion of Ukraine, scenarios for sanctions, and likely economic impact on Russia, Ukraine and the EU. No. 55. Policy Notes and Reports, 2022. [Online].

[10] Fitton, Oliver. "Cyber operations and gray zones: Challenges for NATO." Connections 15.2, pp. 109-119. 2016. [Online].

[11] Giles, Keir. The next phase of Russian information warfare. Vol. 20. Riga: NATO Strategic Communications Centre of Excellence, 2016. [Online].

[12] Tashev, Blagovest, Michael Purcell, and Brian McLaughlin. Russias Information Warfare: Exploring the Cognitive Dimension. Marine Corps Center for Advanced Operational Culture Learning Quantico United States, 2019. [Online].

[13] Andrew, James, and Kenneth Geers. "'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine." In Cyber war in perspective: Russian aggression against Ukraine, pp. 39-48. NATO CCDCOE, 2015. [Online].

[14] Cunningham, Conor. "A Russian Federation Information Warfare Primer." The Henry M. Jackson School of International Studies. 2020. [Online].

[15] Hemsley, Kevin, and Ronald Fisher. "A history of cyber incidents and threats involving industrial control systems." International Conference on Critical Infrastructure Protection. Springer, Cham, 2018. [Online].

[16] Rusnáková, Soňa. "Russian new art of hybrid warfare in Ukraine." Slovenská politologická revue 17.3-4, pp. 343-380. 2017. [Online].

[17] Khan, Rafiullah, et al. "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid." 4th International Symposium for ICS and SCADA Cyber Security Research 2016 4. 2016. [Online].

[18] Cherepanov, Anton, and Robert Lipovsky. "Blackenergy–what we really know about the notorious cyber attacks." Virus Bull. October. 2016. [Online].

[19] Baezner, Marie. Cyber and Information warfare in the Ukrainian conflict. No. 1. ETH Zurich, 2018. [Online].

[20] Oxford Analytica. "Meta's Russia strategy could have global repercussions." Emerald Expert Briefings oxan-es. 2022. [Online].

[21] Lilly, Bilyana, and Joe Cheravitch. "The past, present, and future of Russia's Cyber strategy and forces." 2020 12th International Conference on Cyber Conflict (CyCon). Vol. 1300. IEEE, 2020. [Online].