Cyberwar Between Ukraine And Russia

Thanh V. Nguyen
Department of Computer Science
University of New Orleans
New Orleans, LA
tvnguy14@uno.edu

***Abstract*—Vladimir Putin's goal is to restore what he sees as Russia's rightful home among the world's major powers, alongside the United States and China [8]. Ukraine, a nation of 44 million people, was formerly a member of the Soviet Union and has a 1,200-mile border with Russia [8]. Russian cyberattacks on Ukraine have continued ever since Russia's illegitimate takeover of Crimea in 2014, peaking immediately before the 2022 invasion [2]. Russia officially declared war on Ukraine on February 24, 2022 [2]. The public, energy, media, financial, commercial, and nonprofit sectors in Ukraine have suffered the most during this time [2]. Limited cyberattacks by Russia have impacted the supply of food, medicine, and humanitarian aid since February 24 [2]. Their effects have included data theft and deception, notably using deep fake technology, in addition to restricting access to fundamental services [2]. Phishing emails, distributed denial-of-service attacks, data-wiper malware, backdoors, surveillance software, and information thieves are some more hazardous online activities [2]. The hybrid hazards that are so presented have not gone unnoticed by organizations and governments throughout the world [2]. Efforts led by the US, EU, and NATO have been carried out to counter cyber threats and defend critical infrastructure [2].**

***Index Terms*—Cyberwar, Ukraine, Russia, United States, Cyber attacks, malware, phishing, Distributed-Denial-of-Service, Hack,**

I. Introduction

Since at least 2014, Ukraine has consistently been the target of Russian cyberattacks [2]. According to a Politico study, Ukraine is the ideal sandbox for those to try out new cyberweapons, strategies, and tools due to the thousands of assaults that take place there each month [2]. Since February 24th, 2022, the attacks have been on a small scale, with the predicted but failed attack on the energy infrastructure occurring only in the second month of the conflict [2]. Researchers have made assumptions about the cause of this "noticeable lack" of cyberattacks [2]. The reasons include the extensive security measures taken to secure Ukraine's information technology (IT) network and the dependency of Russian armed troops on Ukrainian IT infrastructure [2]. While some analysts believe that Russia's offensive cyber capabilities may have been exaggerated, others believe that Russia may just be waiting for another favorable opportunity to conduct significant assaults [2]. A significant cyberattack would have the ability to spread fast to neighboring nations [2]. On March 21, 2022, US President Joe Biden encouraged American business leaders to improve their cyber-defense capabilities, emphasizing that Ukraine and other countries are at risk from Russia's exploitation of its complete range of cyber capabilities [2].

II. Types of Cyber Attacks

A. Phishing

Phishing attacks are impersonation communications that compromise all kinds of data sources even if they seem to be coming from a reliable source [9]. Attacks can make it easier for people to access their personal information and online accounts, get access to related systems and change or breach them, and in certain circumstances, take over whole computer systems until a ransom is paid [9]. Sometimes cybercriminals are content to steal your personal information and credit card numbers in order to make money [9]. In other instances, scam emails were sent to collect employee login credentials or other information in order to launch more nefarious assaults against a small group of people or a particular business [9].

B. Malware

Any invasive program created by cyber criminals (often referred to as "hackers") to steal data and harm or disrupt computers and software systems is referred to as malware, which is short for "malicious software" [10]. Malware types that are often encountered include viruses, worms, Trojan horses, spyware, adware, and ransomware [10]. Massive quantities of data have been exfiltrated by recent malware assaults [10]. It appears in an unbelievable array of shapes. The most well-known form of malware is arguably a computer virus, which spreads by duplicating itself [13]. Worms also possess this quality [13]. Other forms of malware, like spyware, are called for the actions they carry out: Spyware sends personal data, including credit card details, via the Internet [13].

C. Distributed-Denial-of-Service (DDoS)

Distributed Denial of Service (DDoS) assaults are another name for distributed network attacks [11]. This kind of attack makes use of the precise capacity restrictions that are applicable to all network resources, including the technology supporting a company's website [11]. With the intention of surpassing the website's capacity to handle numerous requests and preventing the website from operating properly, the DDoS attack will generate repeated requests to the targeted online resource [11]. Attacks known as distributed denial-of-service (DDoS) are complex attempts to overwhelm the network with unnecessary data [12]. When a DDoS assault occurs, critical

infrastructure either experiences a decline in network quality or a complete service interruption [12].

III. Cyberwar between Ukraine and Russia

This is an overview of the cyber war between Ukraine and Russia in 2022. Most of the information is based on a report, "Cyber War and Ukraine," written by James A. Lewis and published by CSCI, which analysis the cyber activities in the Ukraine crisis based on news that is readily accessible to the public [1]. Despite not being the first cyber war, the conflict in Ukraine was the first considerable one to use major cyber operations [1]. The ineffective Russian assault raises concerns about the proper ratio of cyberspace offensive and defense [1]. An obvious characteristic of this invasion seems to be better-than-expected Ukrainian resistance [1]. Ukrainian cyber defenses surprisingly held up and limited the impact of the Russian cyber offense [1]. Russia is known to be one of the biggest cyber threats and for Ukraine's cyber defense being able to counter, some can argue that Russia may have lost a step or wasn't well prepared for the cyberattack [4]. We are witnessing the evolution of cyber war, and this is just a glimpse of what's to come.

Due to Russian cyber activities that started as early as 2014, Ukraine was perhaps better equipped because of the warning [1]. Friendly nations and private players with whom it had established cooperative contacts before the war also helped it in its cyber defense [1]. This preparedness enabled it to block several Russian offensive cyber operations, indicating that in cyberspace, a strong defense may prevail over an offensive one [1].

In the past, Russia had attacked Ukraine's infrastructure and data through cyberattacks [1]. In 2022, another attempt was made to accomplish so [1]. According to evidence readily available, Russia started a significant cyber effort just before the attack [1]. According to certain reports, there was a sharp rise in exploits on the first day [1]. It appears that the goal was to destabilize Ukrainian defenses and overwhelm them [1]. By using phishing, distributed denial-of-service (DDoS) attacks, and exploiting software flaws, Russia attempted to interfere with services and introduce dangerous malware onto Ukrainian networks [1]. Eight separate families of damaging software that Russia utilized in these assaults have been discovered by one business [1]. Although the assaults affected many of the crucial industries, the principal targets were "Ukrainian government websites, energy and telecom service providers, financial institutions, and media outlets," said Lewis [1]. This was a comprehensive attack that attempted to destabilize Ukraine utilizing the full range of Russian cyber capabilities, but it was unsuccessful [1].

The success of the KA-SAT satellite from Viasat Inc. was Russia's biggest cyber victory to date [1]. Although this caused considerable harm that went beyond Ukraine, it ultimately did not give Russia a military edge [1]. The Russians would not have anticipated the fast service restoration that was made possible with outside aid, or the assault may have been meant to be a component of a broader, coordinated hack that was unsuccessful [1]. The measure for Viasat and other acts is whether a cyberattack helps achieve, in this example, the takeover of Ukraine and the overthrow of its elected government [1]. It is not whether a cyberattack is successful in terms of network penetration or the interruption of services or data [1]. By this standard, the Viasat attack failed [1].

According to Ukrainian and Western sources, the GRU, Russia's military intelligence branch, which has a history of launching disruptive cyberattacks, is primarily responsible for many of these operations [1]. Proxy organizations were occasionally engaged, and in one accused case, a Brazilian cyber group that supports Russia attacked Ukrainian colleges [1]. Whether or not the GRU was involved, all of these cyber attempts appear to have been badly planned with Russian military operations in Ukraine [1].

IV. The Importance of Cyber Acts

Cyberattacks work best when combined with electronic warfare (EW), misinformation movements, antisatellite assaults, and precision-guided weapons when disagreements concerning current armies [1]. The goal is to generate operational advantages by undermining informational gain, intangible resources (like data), connections, intelligence resources, and weapon systems [1]. The most harmful acts would combine cyberattacks with bombs aimed to damage or killing crucial targets [1]. Cyber operations may also be used to undermine decision-making by defenders and stir up civil unrest by interfering with government, energy, transportation, and financial systems [1]. None of these goals have been accomplished by Russia on a considerable level [1].

Some may think cyberattacks are overrated, while those in the cyber community may take offense to that saying [1]. Cyberattacks such as spying and criminal activities are helpful, but not all effective in military battles [1]. The battle on the ground is getting people killed. As far as we know, cyberattacks haven't gotten anyone killed, and they rarely cause noticeable harm [1]. Most analysts agree that a pure cyberattack is insufficient to force any but the weakest foe to concede defeat [1]. Cyberattacks are viewed as a way to harass and delay your opponent from their plans. Attacks on software and data often result in understandable damage, but these attacks typically do not produce a calculated benefit (which can be defined as compelling an enemy to implement adjustments or concessions it would have not otherwise made), as they have instead been used sporadically and incoherently [1]. To weaken an opponent's resistance, consistent and careful work is needed [1]. Cyberattacks require a lot of planning to execute certain tasks, functions do not run from the push of one big red button.

Making a hack more than a spectacular inconvenience requires serious work. Good preparation, tool designs, and observations are needed, along with other offensive capabilities [1]. The success of a cyber operation is determined by its impact on the target and if it requires an opponent to alter actions or make a consideration [1]. Additionally, cyberattacks do not guarantee damage, unlike a successful strike with a

physical weapon [1]. A satellite can be seen getting struck by a missile resulting in smoke and explosions, but a successful cyberattack on a satellite may go unnoticed and damage can be restored [1].

In times of conflict, cyber operations are highly helpful for conducting surveillance and learning in advance about the plans and capabilities of the opposition to trick and game plan against them [1]. There were reports of Russian attempts to breach North Atlantic Treaty Organization (NATO) networks at the beginning of the conflict, which made sense because Russia was concerned about NATO interfering [1]. An attacker must compare the possibility of profit from a disruptive assault to the loss of the advantages of spying. The advantages of espionage frequently exceed the disadvantages of an attack [1].

The apparent insufficient coordination among cyber and conventional strikes has been one drawback of Russian cyber operations [1]. When used in conjunction with conventional delivery methods, precision-guided missiles, unmanned aircraft, and electronic warfare, cyberattacks are helpful strategically [1]. This combination has the potential to impair modern weapon systems and command networks while increasing the longevity of opposing troops [1]. Cyberattacks, however, are less effective when utilized carelessly or when they are not planned alongside air and ground operations [1]. A significant amount of preparation and staff effort is needed to coordinate cyber and kinetic strikes, which Russia either refused to execute or was unable to accomplish [1]. Some Russian cyberattacks may have been timed to complement conventional operations, but they didn't work out that way [1].

The security of Russian communications was lacking. Because money meant for safe communication systems was redirected to personal use, corruption may have contributed to Russia's communications problems [1]. According to prior operations in Ukraine, Russia's special operations personnel have access to advanced tactical communications equipment with effective encryption, while other groups in this invasion lacked similar equipment [1]. Some Russian forces depended on cheap Chinese equipment that wasn't properly controlled [1]. Others depended on the industry-grade telecommunications network in Ukraine [1]. Two significant problems result from this dependency [1]. First, whether on purpose or accidentally, the Russians' communications were limited when they damaged the Ukrainians' telecommunications networks [1]. Furthermore, depending on an enemy's communications networks generate a variety of potential exploits [1].

V. Preparing Cyber Operations

It is difficult for an attacker's staff, planning, and intelligence support to conduct successful cyber operations [1]. In doing so, Ukraine's results highlighted one asset of the American military, which is its talent for teamwork and preparation [1]. The development of regional combatant commanders with command over navy, air, ground, and cyber forces decades ago allows for a coordinated attack (or defense) based on extensive experience [1]. The fact that the United States had two command organizations that did not work together to provide appropriate scouting contributed to American casualties in the Battle of the Coral Sea (1942) [1]. The US learned from their mistakes. The ideal way to merge cyberattacks with other offensive weapons is to optimize the return on a cyberattack, which requires organizing and preparation [1].

Russian authors' writings imply that they are aware of how logistics and communications might be disrupted by hackers, which is used as a game plan to conflict with [1]. This approach benefits the military, and better planned/executed Russian attacks on Ukraine's logistics and communications. This also can utilize cyber means to disturb Ukrainian control and command, interfere with air defense systems and supplies, and cast doubt and confusion about the commanders' judgment [1]. The ineffectiveness of Russian efforts to interfere with Ukrainian operations, supplies, and communications is largely attributable to Russia's sloppy preparation, inaccurate expectations of the response Russian forces would get, and the effectiveness of Ukrainian cyber defenses [1]. Like the ground invasion, it was assumed that Ukrainian resistance would be weak and ineffective [1]. Russia may be changing its mind about using cyberattacks as it tweaks its first, unsuccessful plan. But, if Russian troops suddenly use tactics such as those they utilized in Grozny or Syria—random bombing to destroy both military and civilian targets—this may deprioritize cyberattacks, which are less damaging and unpredictable [1].

Although Russia's actions emphasize effective practices, they also demonstrate how not to employ cyber operations to your advantage in armed combat [1]. The highlighting lesson is the importance of thorough planning in order to generate simultaneous, coordinated attacks on vital targets [1]. The other is to weaken online defenses in order to gain the upper hand in the digital sphere [1]. The third step is to prepare the battlefield while exerting as much public narrative control as you can mentally and politically [1].

VI. Hacktivism

Hacktivism, which derives from the terms "hack" and "activism," is the action of hacking, or tapping into a computer system, for goals that are politically or socially motivated [7]. They basically hack for some purpose. The potential to mistake hacktivists' symbolic gestures for real strategic influence is an analytical problem [1]. Despite receiving global attention, none of the private actors' different cyberattacks on Russian websites had any impact on Russian military activities, its military power, or, as far as anybody can determine, Putin's strategic calculations [1]. The effects of "hacktivists'" actions and the risks they take against Russia are overestimated [1]. By these standards, hacktivism has very little impact on how the battle would unfold [1].

Thousands of volunteers took part in cyber warfare at the start of the conflict against Russia to guard Ukrainian network targets [1]. Coordination is the most challenging issue when dealing with an "army" of thousands of citizen volunteers [1]. Management techniques and infrastructure must be prepared in advance [1]. A good illustration of how such teams might

be structured for maximum effectiveness is Estonia's Cyber Defense Unit [1]. Prior to the invasion, Estonia supported Ukraine and certain of the volunteered cyber defenders were likely arranged in a manner that routed them to priority targets [1]. This minimized gaps and work duplication, making Ukraine a more dependable supply of extra cyber power [1]. The takeaway for other nations is that if volunteers' activities are structured and a system for partnership and collaboration with federal agencies is created ahead of the war, they may offer essential support in defense. Despite relying on networks, Ukrainian civilians attempted to offer information on Russian forces, which doesn't count as "cyber" activities [1]. But they respectfully did support defenders [1]!

The political scene of the target nation affects the circumstances in which hacktivism may be effective [1]. A government that worries about invasion or assault can worry that hacktivism is a prelude to more serious acts or a sign of enemy intent [1]. A nation that has frustrated people and is politically weak will be more susceptible [1]. Hacktivism, on the other hand, will not be seen as posing much danger by an authoritarian government that is not concerned with what its citizens believe and developed misinformation and socialization tools, which are ready to use force to repress any resistance [1]. Although Russian (and Chinese) media management and propaganda have been successful in gaining popular support and outweighing the impact of hacktivism, it is common for Westerners to underestimate their effectiveness [1].

This section indicates that hackers are being overlooked as not much of a threat. There is so much untapped potential for what hacking can do to a nation as technology continues to grow better at a rapid rate. Spreading misinformation has great power to control the masses, and we all have to be aware of how to handle it together as a team.

VII. Control of the Narrative

The struggle for narrative dominance takes place mostly online and can be influenced by online behavior [1]. Longstanding Russian teaching on the significance of the political and psychological backdrop of combat is reflected in Russia's focus on shaping the narrative about the invasion in order to quell criticism and secure the public's support [1]. It provides information for electronic and electronic warfare (EW) activities [1]. The outcome of this endeavor has been iffy, and the narrative competition is still up in the air [1]. Both in Ukraine and among Ukraine's supporters, it failed [1].

The Leer-3 is one of many transportable, somewhat contemporary EW devices that the Russians have used in the theater that is capable of information warfare [1]. Leer-3 comes with drones that have similar capabilities to Western Stingray systems for capturing mobile phone traffic, monitoring social media for exploitation and psychological manipulation, and sending bulk text messages to mobile phone numbers it collects [1]. These drones could also be used to block signals for telecommunications as well as provide capabilities similar to those of the Stingray systems [1].

Russia was unable to provide engaging content for the Ukrainian audience, which reflects its bigger propaganda failure [1]. Hacking email accounts or databases and then leaking the information is a common Russian practice [1]. This stolen information is occasionally changed to increase its influence, but Russia's invasion strategy did not succeed using this approach [1]. Russia failed to dispute exposed Western intelligence that quickly contradicted Russian allegations, despite its talent and experience in misinformation, which is a lesson to be learned [1]. Russian propaganda was also unable to cover up the overwhelming proof of aggression, transgressions of international treaties, and horrendous human rights abuses that were made available to the public through several nonprofit sources [1].

Another takeaway from the conflict in Ukraine is the need to consider how common mobile phone cameras, open access to satellite images, and telecommunications intercepts like WebSDR will all be in future conflicts [1]. While offering genuine intelligence advantages, these accessible, nongovernmental sources of information undermine any attempts to control the narrative [1]. What was formerly thought of as top-secret intelligence is now a product that is offered to the general public [1]. Governments still retain the right to employ force, but they no longer have much of a monopoly on intelligence coming from conflict areas [1]. Civilians in the theater can offer useful intelligence on the enemy troops [1]. Digital and mobile technology may be used by civilian individuals to increase the quantity of information accessible to the force they help and make it difficult to mislead it [1]. Only the strongest censorship has any chance of influencing the narrative, but many news sources are not subject to it [1]. Russian attempts to jam mobile phones or obstruct internet service in Ukraine were likewise ineffective [1]. Cyber offensive operations will also need to consider ways to restrict or manage civilian communications scattered all over a decentralized global network [1].

Private messaging apps like Telegram and Signal, which are popular in Russia and Ukraine, can help protect and secure messages to some extent [1]. Utilizing these services offered Ukraine a benefit in terms of tactical information as well as social cohesiveness [1]. An important intelligence failure and a symptom of a bigger problem was the Russians' inability to block access to messaging platforms [1]. Due to widespread connection, non-combatant third parties can offer services that are challenging for attackers to interfere with unless they are prepared to strike unbiased third parties [1]. This can improve the capacity for resistance and make it more difficult to refuse vital services [1].

VIII. Cyber Defense

Ukraine's crisis offers valuable lessons for cyber protection [1]. Cyberattacks don't have to be unavoidable if the defense is prepared and persistent [1]. Ukraine managed to learn from the destructive cyberattacks that Russia launched in 2014 and

2016, which put Russia at a disadvantage [1]. The planning and hardening of potential targets, cooperation and support from foreign cyber players, and the quick response to counter the assaults that were found by monitoring critical networks were the essential parts of the Ukrainian defense [1]. Both large and small nations may use this as a model to guide their cyber security [1].

Although Ukrainian agencies took the lead in defense, it wasn't totally dependent on the government or even Ukrainian resources. Before and after the invasion, Ukraine had a network of partners (including both businesses and governments) that could offer instruction and support, such as remote monitoring and prevention [1]. Tech firms were a tremendous help, and Ukraine benefited from the collective effort that included domestic, international, public, commercial, surveillance, and counters to prevent attacks and patch or remove vulnerabilities [1]. Russian invaders frequently encountered failure in their endeavors, and even when they did, the success was brief [1]. The message is to build partnerships and teamwork through activities that go beyond conferences and seminars, such as planning and training sessions ahead of any attempts [1].

Before the invasion, Ukraine issued a national cybersecurity policy in 2016, establishing a level of duplicates and persistent data while increasing the usage of encryption [1]. After 2015, it adopted several fundamental "cyber hygiene" safeguards, which are crucial for any assault [1]. Though, the ability to recognize and respond promptly is the most crucial component of security [1]. Real-time monitoring of crucial networks and systems was implemented by Ukraine (with outside help) in order to promptly identify vulnerabilities and stop them [1]. Continuous monitoring is necessary for this, an area where many nations might do better [1]. Every software program has vulnerabilities that may be used to penetrate any network border [1]. The secret to a successful defense appears to be the skill to react quickly and efficiently to cyberattacks [1]. This involves constant surveillance, which many nations might get better at [1].

According to reports, Ukraine moved some data and services beyond the area affected by the fighting via a third-party hosting agreement [1]. This made things difficult for Russia's planning. Small nations can create digital infrastructure and data architecture that makes use of extraterritorial third-party service providers to reduce exposure, boost resilience, and make it more difficult for attackers to carry out their mission [1]. The businesses that run the internet don't always respect national borders [1]. As governments transition to relying on cloud services and other online services, this dissemination will grow [1]. The danger of consequences associated with attacking these distant systems in non-combatant nations may be something an attacker would like to avoid [1].

If Russia or China wanted to execute cyberattacks on the United States similar to those that were attempted in Ukraine, larger nations like the United States might run into scaling issues when attempting to replicate this type of protection [1]. Although the United States has a large number of potential targets, it is not yet structured or equipped to match Ukraine's achievements [1]. This kind of frontal assault is still improbable, even though several of the lessons learned during the fight in Ukraine are still relevant [1]. The most significant of them could be to get ready right away for cyberattacks on vital infrastructure (a field in which the United States has managed to improve) and needed information (which can be less organized) [1].

IX. Conclusion

Although no security is foolproof, Ukraine's measures have successfully stopped Russian cyberattacks [1]. Other countries can replicate this set of defensive measures. The lessons learned thus far from Ukraine indicate that for military actions, cyber operations planning must be incorporated into larger campaign planning and evaluated for where and when it is advantageous to deploy them [1]. While cyberattacks are an unsatisfactory alternative to physical activity and must be utilized in a sequence connected to other types of attack, a joint force approach that integrates cyber with other offensive weapons would benefit fully [1].

Aside from that, to enhance the effectiveness of cyberattacks as weapons of war, lethality and predictability should be increased [1]. While cyberattacks may present more opportunities for surprise and currently perform well in terms of speed, distance, and accuracy (to the degree that those factors apply), their destructive power is still constrained [1]. The burning debris left behind after a missile kills a power facility is seen [1]. It is more challenging to determine whether a cyberattack was successful and how long-lasting the consequences would be [1]. In order to do this, it will be important to emphasize the employment of cyberattacks with a focus on impeding command systems, weapon systems, and data as much as possible [1]. When deciding whether to utilize cyberattacks, an attacker must consider if doing so would make the conflict easier to manage or harder to control, as well as how much usage will help achieve strategic effect [1].

For offense, an advertising plan requires providing an intricate and detailed assessment of the advantages and disadvantages of cyberattacks, such as the expense of intelligence gathering and the political impact on both soldiers and outside parties [1]. This assessment must be accurate due to the constraints of cyberwarfare and detailed because a cyber operation frequently requires a customized quality based on the characteristics of the directed system and the planned outcome [1]. This will necessitate at the very least investigation of the target network, "weapons" creation (creating programs for use during the attack), testing, and "refreshing" attack tools well enough in preparation for any attack [1].

There will be some resentment about the amount that cyberattacks hurt individuals, including limiting their access to social media and internet services [1]. The rest of the world is much less forgiving of intentional assaults on targeted attacks or collateral damage, which can have negative political repercussions for the invader [1]. The policy of cyberattacks linked to civilian networks must be considered while planning

an offensive strategy [1]. Russia didn't do so which was a big miscalculation on their part [1].

Although China or perhaps Iran may have learned from the Russian practice, the crisis in Ukraine might teach the United States and its partners how to protect themselves from offensive cyber operations launched against it by rivals [1]. Ukraine is certainly not a reliable example of confrontation with any potential attack by China in terms of cyber operations [1]. China is more prepared and is probably better planned [1]. Even if these adversaries share an authoritarian style of decision-making, the United States might not wish to rely on incompetence among them [1].

Russian objectives—the takeover of Ukraine and the overthrow of its chosen government—were not enhanced by cyber activities [1]. Some of Russia's errors are now becoming obvious [1]. Neither the first cyberwar nor a cyberattack especially helpful to Russia occurred in Ukraine [1]. It was well done by the Ukrainian defense and their allies to respond rapidly to divert Russian attempts to sabotage networks [1]. They don't seem to have encountered a well-thought-out plan of assault that was part of a larger campaign strategy [1]. The most essential lesson learned from Ukraine's experience with cyber warfare may be this: to be effective, cyberattacks must be planned and coordinated with other forms of assault [1].

X. Small Timeline of Cyber Events in Ukraine

- In October 2021, according to the code's date, hackers developed the IssacWiper malware before or on October 19, 2021 [1]. In February 2022, they released it against Ukrainian government networks [1].
- In November 2021, hackers started creating phony websites for the Ukrainian government that contained links to malicious software [1]. Researchers think this behavior is related to the second distributed denial-of-service (DDoS) attempt against the Ukrainian banking industry and government websites in February 2022 [1]. They have linked this activity to individuals with connections to the Russian GRU [1].
- In December 2021, the earliest date on the code indicates that the HermeticWiper virus was created by hackers and was utilized in a February 2022 strike against financial institutions and Ukrainian federal workers [1].
- In December 2021, a hacker collective launched a phishing attempt on the Ukrainian State Migration Service [1]. Members of the gang believed by researchers to have carried out this assault were connected towards the Russian Federal Security Service in November 2021 by the Ukrainian Security Service (FSB) [1].
- In December 2021, Malware used in phishing attempts in March and April started to be developed by hackers with connections to the Russian GRU [1].
- In December 2021, the network of a nuclear safety agency was attacked by a gang thought to have connections to the Russian FSB [1]. Up to March 2022, this organization's data was stolen by hackers [1].
- January 2022: Destructive malware (WhisperGate), disguising as ransomware, was installed by hackers on the networks of various Ukrainian government, charitable, and IT organizations [1]. Researchers believe that hackers with links to the Russian GRU were responsible for this attack [1].
- In January 2022, hackers attacked over 70 websites belonging to the Ukrainian government, shutting down a number of them while also altering the one for the Foreign Ministry [1]. The defacement contained a message that threatened Ukrainians and a notification that personal information had been exposed; these statements were later debunked by the Ukrainian Center for Strategic Communications and Information Security [1].
- In January 2022, hackers used a phishing assault to target a Western government organization working in Ukraine. [1] The actors sent a malware-infected CV to the government agency after uploading it to a Ukrainian employment board [1]. This assault was traced by researchers to a hacker cell that the Ukrainian Security Service had previously connected to the Russian FSB [1].
- In February 2022, hackers used a phishing assault to target a Ukrainian energy firm with espionage software [1]. These assaults were linked by the Computer Emergency Response Team of Ukraine (CERT-UA) to a gang that has a history of attacking Ukrainian government institutions since at least March 2021 and is thought to have links to the Russian GRU [1].
- In February 2022, hackers disseminated malware-infected phishing emails purporting to be from Ukrainian government agencies [1]. This attack was linked by researchers to a group connected to the Russian GRU [1].
- In February 2022, hackers launched a number of DDoS assaults against the government and financial websites in Ukraine, momentarily putting the websites down [1]. Attacks on financial institutions were ascribed to the Russian GRU by the US, UK, and Australia [1].
- In February 2022, the Times reported that Chinese hackers attempted to breach data and disrupt services by targeting weaknesses in over 600 major infrastructure organizations and the Defense Ministry in Kyiv [1]. They cite the Ukrainian Security Service as their source, although the agency disputes this [1].
- In February 2022, hackers launched a DDoS attack against websites linked to the Ukrainian financial industry and the government, making some of the sites unusable [1]. In the last two weeks, there have been two DDoS attacks against the websites of Ukrainian banks and the government [1].
- In February 2022, hackers in Ukraine used a devastating malware called HermeticWiper to take out 300 systems at over a dozen banking, governmental, energy, IT, and agricultural enterprises [1]. This assault was connected to the Russian GRU by researchers [1].
- In February 2022, an agricultural company's network had a file encryptor installed by hackers [1]. Researchers

determined that this assault was likely to pursue Ukraine's grain production and linked it to a group thought to have links to the Russian GRU [1].

- In February 2022, hackers launched a DDoS assault against the Kyiv Post, taking down its website [1]. Up until access was restored, The Kyiv Post disseminated stories on social media sites [1].
- In February 2022, hackers infected a Ukrainian government network with the damaging software IsaacWiper [1].
- In February 2022, hackers used phishing to target European government personnel involved in organizing logistics for refugees fleeing Ukraine [1]. The actors made advantage of a hijacked email account that belonged to a Ukrainian serviceman [1].
- In February 2022, malicious software was used by hackers to disable modems connecting to Viasat Inc.'s KA-SAT satellite, which is used for satellite communications [1]. As the satellite serves consumers in several nations, the strike had an impact on connections throughout Europe and Ukraine. Russia was blamed for this assault by the United States, the European Union, and the United Kingdom [1].
- In February 2022, a cyber organization that experts have connected to the Belarusian government used phishing to target prominent Ukrainians [1]. Hackers wanted to access people's social media accounts so they could spread false information about Ukrainian soldiers [1].
- In February 2022, hackers used malicious software to attack a Ukrainian border check station, forcing staff to manually process fugitives trying to enter Romania.

REFERENCES

[1] Lewis, James A. "Cyber War and Ukraine." CSIS, 16 June 2022
[2] Przetacznik, Jakub, and Simona Tarpova. "Russia's War on Ukraine: Timeline of Cyber-Attacks." European Parliament, June 2022
[3] "Ukraine: A Timeline of Cyberattacks." CyberPeace Institute, 24 Feb. 2022
[4] Wolff, Josephine. "Everyone Is Still Waiting for the Cyberwar." TIME Magazine, vol. 199, no. 11/12, Mar. 2022, pp. 31–32. EBSCOhost
[5] Gralla, Preston. "Russia Is Losing the Cyberwar against Ukraine, Too." Computerworld (Online Only), May 2022, p. 4. EBSCOhost
[6] Sparkes, Matthew. "Why Hasn't Russia Waged an All-out Cyberwar against Ukraine?" New Scientist, vol. 253, no. 3378, Mar. 2022, p. 9. EBSCOhost
[7] "What Is Hacktivism?" Check Point Software, 1 Oct. 2019
[8] Bilefsky, Dan, et al. "The Roots of the Ukraine War: How the Crisis Developed." The New York Times, The New York Times, 12 Oct. 2022
[9] "What Is Phishing?" Cisco, 11 Oct. 2019
[10] "What Is Malware." Cisco, 4 June 2022
[11] "What Is Malware and How to Defend Against It?" Kaspersky, 5 July 2022
[12] "What Is Phishing?" Cisco, 11 Oct. 2019
[13] "What Is Malware and How to Defend Against It?" Kaspersky, 5 July 2022