JUNE 2022

Cyber War and Ukraine

James A. Lewis

This is 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. 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 2022. Based on publicly available information, Russia launched a broad cyber campaign shortly before the invasion (see the appendix for a list of known events). 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. One company identified eight different families of destructive software used by Russia in these attacks. The primary targets were Ukrainian government websites, energy and telecom service providers, financial institutions, and 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.

Russia's most significant cyber success so far was the disruption of the Viasat Inc's KA-SAT satellite. This created significant damage that spread beyond Ukraine but ultimately did not provide military advantage to Russia. The attack may have been intended to be part of a larger, coordinated cyberattack that proved unsuccessful, or the Russians may not have expected the rapid restoration of service that was provided with outside assistance. The metric for Viasat and for other actions is not whether a cyberattack is effective in terms of network penetration or the disruption of services or data, but whether its effect helps achieve the desired military outcome—in this case, the occupation of Ukraine and the elimination of its elected government. By this metric, the Viasat attack was not a success.

> *A well-prepared and energetic defense can prevail over offense in cyberspace.*

Most of these attacks have been attributed by Ukrainian and Western sources to Russian government entities—chiefly the GRU, Russia's military intelligence service, which has a history of using disruptive cyberattacks. In a few cases, proxy groups (such as the leading ransomware group Conti) were also involved, and in one reported instance, a Brazilian hacker group supportive of Russia attacked Ukrainian universities. All these hacking efforts, whether by the GRU or not, seem to have been poorly coordinated with Russian military actions in Ukraine.

The Value of Cyber Operations

In conflicts involving modern militaries, cyberattacks are best used in combination with electronic warfare (EW), 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. 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' decisionmaking and create social turmoil. 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. 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.

> *Cyberattacks are overrated. While invaluable for espionage and crime, they are far from decisive in armed conflict.*

It takes real effort to make a cyberattack more than a dramatic annoyance. This requires planning, tool development, and reconnaissance, integrated with other offensive capabilities (as with the Israeli airstrike on Syrian nuclear facilities). 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).

Cyber operations in conflict are very useful to conduct espionage, to gain advance knowledge of opponent planning and capabilities, and to mislead. 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. 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.[1]

One apparent weakness of Russian cyber operations has been the seeming lack of coordination between cyber and conventional attacks. At a tactical level, cyberattacks provide benefits when combined with other weapons, including conventional delivery systems, precision-guided munitions, unmanned aerial vehicles, and electronic warfare. This combination can cripple command networks and advanced weapons systems and contribute to the attrition of opposing forces. However, when used in an ad hoc manner, or when uncoordinated with air and ground actions, cyberattacks prove less useful. Coordinating cyber and kinetic actions requires a high degree of planning and staff work that Russia either chose not to do or was incapable of doing. The timing of some Russian cyber operations suggests they were intended to support conventional operations but were unsuccessful.

Cyberattacks can be used to produce or amplify political effect, but it's important to recognize that attacks are as likely to harden defenders' will to resist as they are to sow panic. The most effective cyber tactic is to use hacking and misinformation (as was done in 2016 against the United States) to create confusion and inflame existing discontent, thus distracting governments by creating domestic social and political turmoil. Russia does not seem to have made serious efforts at this in Ukraine—sending texts and emails containing generic threats is juvenile. Unlike Russian actions in 2016, there does not appear to have been advanced planning and work to prepare the ground in Ukraine for political disruption. This is puzzling, given the attention in Russian doctrine to incorporate "pre-conflict" political preparation into attack planning and may indicate a somewhat spontaneous decision to invade Ukraine without careful preparation.

Russian communications were inadequately secured. Corruption may have played a role in Russian communications weaknesses, with funds intended for secure communications equipment diverted to personal use. While Russia's special operations forces have access to sophisticated tactical communications gear using strong encryption (judging from earlier operations in Ukraine), these were in short supply for other units in this invasion. Some Russian units relied on inadequately secured mass-market Chinese equipment. Others relied on Ukraine's commercial telecommunication infrastructure. This reliance creates two major difficulties. First, when the Russians destroyed Ukrainian telecommunications infrastructure, whether inadvertently or intentionally, this hampered their own communications. Second, relying on an opponent's communications system creates numerous possibilities for exploitation. Many speculate that one reason for the high casualty rate among Russian senior officers was that their vulnerable communications allowed their location to be pinpointed.

Preparing Cyber Operations

Carrying out successful cyber operations creates a heavy burden for an attacker's workforce, planning, and intelligence support. In this, Ukraine helps highlight one strength of the U.S. military: its capacity for planning and staff work. The creation, decades ago, of regional combatant commanders who control naval, air, ground, and cyber forces can provide a coordinated assault (or defense) informed by long experience. One reason for U.S. losses in the Battle of the Coral Sea (1942) came from having two command structures that did not coordinate to provide adequate reconnaissance. The United States learned from this. It takes planning

[1] A separate discussion will examine the relationship of cyber operations and electronic warfare, which can have both tactical and political effect.

and preparation to maximize the return on a cyberattack, and this is best achieved when cyberattacks are integrated with other offensive capabilities. The emphasis on joint operations that began with Goldwater-Nichols is another strength that can give the United States an advantage in the use of offensive cyber operations. Success is derived from the ability of a commander to deliver effect, inflict damage, and force an opponent to retreat, change plans, or surrender. Cyber operations can play an important part if they are used to prepare the ground and in coordination with other capabilities, something that requires staff work, intelligence support, and planning.

Writings by Russian authors suggest that they know that cyberattacks can disrupt logistics and communications (this was part of their planning for conflict with). Such attacks provide military advantage, and better planned or better executed Russian attacks on Ukraine's logistics and communications could have used cyber means to disrupt Ukrainian command and control, interfere with air defense systems and logistics, and inject uncertainty and doubt into commanders' decisionmaking (on troop location or on supply status, for example). The failure (so far) to disrupt Ukrainian operations, logistics, and communications probably reflects the haphazard nature of Russian planning, flawed assumptions about the reception Russian forces would receive, and the strength of the Ukrainian cyber defenses. As with the ground invasion, there was a miscalculation about the strength and effectiveness of Ukrainian resistance. Russia may be reconsidering the use of cyber offense as it adjusts its initial and flawed strategy. However, if Russian forces now move to strategies similar to what they used in Grozny or Syria—indiscriminate bombardment to level civilian and military targets—this may make cyberattacks, which are less destructive and less certain, a lower priority.

Russia has shown how not to use cyber operations to gain advantage in armed conflict, but its efforts highlight best practices. The most obvious lesson is the need for adequate preparation to generate coordinated, simultaneous strikes on critical targets. The second is to achieve cyber superiority by crippling cyber defenders. The third is to prepare the battlefield politically and psychologically and to control the public narrative of the campaign as much as possible.

Hacktivism

One dilemma for analysis is the tendency to confuse the symbolic actions of hacktivists for actual strategic effect. While celebrated in the media, the various cyber actions against Russian websites by private actors had no effect on Russian military operations, its military capabilities, or, as far as anyone can tell, Putin's strategic calculations. The results of the activities of "hacktivists" and their efforts against Russia are exaggerated. Russia did not change course or alter plans as a result of these hacktivist efforts, nor was the Russian capability to engage in offensive operations, spotty as it may have been, degraded by hacktivist action. Russian public opinion, largely supportive of the war, seems unaffected by hacktivism. By these measures, hacktivism is irrelevant to the course of the war.

> *The various cyber actions against Russian websites by private actors had no effect on Russia military operations.*

At the onset of conflict, thousands of volunteers engaged in cyber actions against Russia and to defend Ukrainian network targets. The most difficult problem with an "army" of thousands of civilian volunteers is coordination. The mechanisms and infrastructure for coordination require advance preparation. Estonia's Cyber Defense Unit is an example of how such groups can be organized to be effective. Estonia assisted Ukraine before the invasion, and it is possible that some of the volunteer cyber defenders were organized in ways that assigned them to priority targets, avoided both duplication of effort and gaps, and made them a more reliable source of auxiliary cyber capability. The lesson for other countries is that volunteers can provide valuable assistance in defense if their efforts are coordinated and a framework for coordination and partnership with government agencies is developed in advance of conflict. Ukrainian civilian efforts to provide intelligence on Russian forces, while dependent on networks, are not exactly "cyber" efforts, but they provided real benefit to defenders.

The conditions under which hacktivism might have an effect vary according to the political situation of the target country. A government that feels vulnerable to attack or invasion may fear that hacktivism is the precursor to more drastic actions, an indicator of opponent intent. A country that is politically vulnerable with a discontented population will be more vulnerable. In contrast, an authoritarian state that is not particularly sensitive to what its population thinks, has well-developed propaganda and social control tools, and is willing to use forceful measures to suppress any opposition will not feel that hacktivism poses much of a threat. It is easy for Western observers to underestimate the success of Russian (and Chinese) media control and propaganda, but these have been successful in building public support and outweigh the effect of hacktivism.

External Targets

Ukraine is not the only possible target for cyber action, and Russia appears to have considered cyber operations against the United States and allies. The United States has not been attacked, as Putin may have calculated that cyber action against it or its allies would broaden conflict without benefiting Russia and make the war even more difficult to manage. This could change as Putin becomes more frustrated with the failure of his initial plans, but the fundamental strategic considerations remain the same—a cyberattack on the United States would be unlikely to advance Russia's goals in Ukraine and would increase the chances of failure. This consideration will likely continue to shape any Russian cyber action.

One element of Russia's initial calculations appears to have been that Western political leadership and societies are risk averse, would choose inaction, and would succumb to threats. This has so far proven erroneous (and explains Russia's need to intensify pressure by uttering nuclear threats). However, Putin may yield to temptation and launch a damaging cyber operation against the United States or its allies. If he continues to follow a risk-minimization approach, this temptation would be to repeat something like the **Colonial Pipeline ransomware attack**, which panicked American consumers and created political stress for the Biden administration while offering a shred of deniability. Moscow could attribute the action to criminals, deny culpability, and promise to take action against them. This would even support the short-lived Russian effort to renew cyber talks with the United States.

Russia could unleash something like **NotPetya**, which cost the global economy millions of dollars (without providing benefit to Russia). More damaging attacks against nations in the "near abroad," like Moldova, are also a possibility. The considerations for possible action are to create political turmoil in the victim country, stay below the level of use of force to reduce the risk of retaliation, and provide some degree of deniability, no matter how flimsy. As sanctions continue to uncouple the Russian economy from the West, the cost of such attacks may decrease for Russia, removing a disincentive for cyber action. Wars are not won by playing punishing pranks, even pranks that are expensive for the victim. The key question for any Russian decision is whether it increases the likelihood that Russia will make progress toward its goals in Ukraine. Malicious actions like NotPetya do not.

A disruptive cyberattack against U.S. critical infrastructure probably makes little sense from the Kremlin's perspective. It would not force the United States to stop supporting Ukraine, it would not degrade U.S.

military capabilities, and it would create political pressure for a more forceful U.S. response. Russian leaders lost respect for the United States after the defeats in Iraq and Afghanistan (although the Biden administration is beginning to make them reconsider this), but that does not mean they want to start a war with the United States. Russia's preference is to make progress on its goals in Ukraine while avoiding expanded conflict with NATO or the United States. A limited cyberattack against the United States would only make Russia's situation worse by broadening the conflict, and while the Kremlin enjoys the use of bellicose threats, it has been much more circumspect in its actions.

A better tactic for Russia might have been to inflame existing discontent in democratic nations (as was done in 2016) in advance of the invasion, to distract governments by creating domestic problems. The Russians do not seem to have attempted this, and in Europe they face a substantial barrier created by their lack of credibility and the hostility the invasion has engendered in European populations.

Russian official statements are a poor indicator of intent, since they are designed to manipulate Western opinion and appeal to the nationalist sentiments of Russia's domestic audience. They often bear only a tenuous relationship to fact. Russia believes U.S. strategic thinking is risk averse. Its own strategic culture places greater reliance on the use of exaggerated threats. Threats are a Russian diplomatic tactic, and the difficulty in differentiating between ploy and plan increases the uncertainty that is normal in warfare. The concern is that these threats may increasingly reflect a Russian leadership that is willing to consider ideas (nuclear weapons use, cyberattacks on the West) that were once thought taboo or would seem unreasonable to a rational policymaker.

Control of the Narrative

The battle for control of the narrative largely occurs in a digital space and can be shaped by cyber actions. Russian attention to controlling the narrative about the invasion, to deflect criticism and win public support, reflects long-standing Russian doctrine on the importance of the political and psychological context of conflict. It informs both cyber and electronic warfare (EW) operations. This effort has had mixed results and the narrative contest remains undecided. It was unsuccessful in Ukraine and among Ukraine's supporters. Putin has lost in the Western democracies and Ukraine but has won in Russia and is at least holding his own with non-Western audiences in China (abetted by China's own propaganda and narrative control efforts), India, Africa, the Middle East, and some Latin American countries. This success outside of Ukraine is more a reflection of the damage done to U.S. credibility under previous administrations rather than the skill of Russian propaganda.

> *Putin has lost in the Western democracies and Ukraine but has won in Russia and is at least holding his own with non-Western audiences.*

The Russians deployed a number of mobile and relatively modern EW systems in theater that have information warfare capabilities, such as the Leer-3. Leer-3 comes with drones that can be used to jam telecommunications and provide capabilities similar to Western Stingray systems to capture mobile phone traffic and monitor social media for exploitation and psychological warfare (including sending mass text messages to mobile phone numbers it collects).

Reflecting its larger propaganda failure, Russia was unable to craft compelling content for a Ukrainian audience. A standard Russian tactic is to hack databases or emails and then leak them for damaging effect.

Sometimes this stolen data is falsified to amplify effect. This tactic did not work for Russia in its invasion. One lesson is that despite its skill and experience in disinformation, Russia struggled to rebut declassified Western intelligence that rapidly undercut Russian assertions. Nor was Russian propaganda sufficient to hide the undeniable evidence of aggression, violations of international law, and horrific human rights violations that were publicly available from many nongovernmental sources. Propaganda is most effective when it exploits existing beliefs, discontent, or skepticism, but when these preconditions do not exist, even constant repetition is insufficient to have persuasive effect.

Another lesson from Ukraine is that future wars will need to take into account the ubiquity of mobile phone cameras, public access to satellite imagery, and even communications intercepts using online services like WebSDR. These public, nongovernmental sources of information undercut any effort to control the narrative while providing real intelligence advantage. What used to be considered secret intelligence is becoming a publicly available good. Governments have not lost their monopoly of the use of force, but any monopoly they had on controlling information from war zones has largely disappeared. In theater, civilians can provide valuable information on opponent forces. Civilian actors can use digital and mobile technologies to greatly expand the amount of information available to the force they support and complicate efforts to falsify or disrupt it. Only the strictest censorship can hope to control the narrative and many news sources lie outside the scope of censorship. Russian efforts to jam cellular telephony or interfere with internet access in Ukraine were also unsuccessful. Planning how to degrade or control civilian communications spread across a decentralized global network networks will also need to become part of cyber offensive operations.

The use of private messaging services like Signal and Telegram (used by Russians and Ukrainians) can provide a degree of end-to-end encryption to preserve and secure communications. Use of these services gave Ukraine an advantage, both in social cohesion and in tactical intelligence. The Russian inability to deny access to messaging services was a significant intelligence failure and points to a larger issue. Global connectivity means that third-party, non-belligerent services can provide services that are difficult for an attacker to disrupt unless they are willing to attack neutral third parties. This can make key services difficult to deny and strengthen the ability to resist.

> *What used to be considered secret intelligence is becoming a publicly available good.*

Cyber Defense

For cyber defense, the conflict in Ukraine is instructive. Cyberattacks need not be unstoppable for a prepared and determined defender. Russia found itself at a disadvantage because Ukraine appears to have learned from the damaging cyberattacks carried out by Russia in 2014 and 2016. The most important elements of Ukrainian defense were preparation and hardening of likely targets, partnerships and assistance from foreign cyber actors, and rapid reaction to nullify attacks, detected by monitoring of critical networks. Countries large and small can copy this for their own cyber defenses.

Ukrainian agencies played the leading role in defense, but defense did not rely entirely on governmental or even Ukrainian assets. Ukraine had a network of partners (both governments and companies) who were able to provide training and assistance, including remote monitoring and mitigation, before the invasion and after it began. Tech companies provided invaluable assistance. Collective action that blended national and foreign, government and private, gave Ukraine an advantage in monitoring and in rapid reaction to block attacks and repair or eliminate vulnerabilities. Russian attackers were often frustrated in their attempts and even when successful, the success was short lived. The lesson is to develop relationships and integrate partners through actions that go beyond meetings and seminars to include planning and exercises well in advance of any attack.

Ukraine published a national cybersecurity strategy in 2016 and established a degree of redundancy and resilience for data and expanding the use of encryption before the invasion. It implemented some basic cyber "hygiene" measures after 2015. Cyber hygiene before an attack is important, but the most important element of defense is the ability to identify and react quickly. Ukraine (with external assistance) undertook real-time monitoring of critical networks and systems to detect exploits early on and then act quickly to counter them. This requires continuous monitoring, an area where many countries could improve performance. Any network perimeter can be breached, and all software has exploitable flaws. It is the ability to respond immediately and effectively to cyber intrusions that seems to be the key to a successful defense. This requires continuous monitoring, an area where many countries could improve.

Ukraine reportedly used a third-party hosting arrangement to move some data and services outside of the geographic boundaries of the conflict. If nothing else, this complicated and constrained Russian planning. Small countries can design digital infrastructure and data architecture that takes advantage of extraterritorial third-party service providers to minimize exposure, increase resilience, and complicate an attacker's task. The commercial operations behind the internet do not always follow geographic boundaries. This diffusion will increase as governments move to rely on cloud services and other remote services (including software as a service and satellite connectivity). Attacking these remote services located in noncombatant countries poses the risk of repercussion an attacker may prefer to avoid.

> *Small countries can design digital infrastructure and data architecture that takes advantage of extraterritorial third-party service providers to minimize exposure, increase resilience, and complicate an attacker's task.*

Larger countries like the United States could face problems of scale in copying this kind of defense if Russia or China decided to launch cyber operations against them similar to what was attempted in Ukraine. The United States is a "target-rich" environment, and it is not yet organized or resourced to duplicate Ukraine's success. However, this sort of direct attack is still unlikely, while many of the lessons from the Ukrainian conflict are applicable. The most important of this may be to prepare now for cyberattacks against critical infrastructure (an area where the United States has made progress) and crucial data (where it may be less prepared). That makes the issue for the United States how to apply lessons and best practices for national defense learned in Ukraine in situations short of armed conflict.

Preliminary Conclusions

No defense is perfect, but Ukraine's efforts have so far been able to thwart the Russian cyberattacks. This combination of defensive measures is a package that can be duplicated by other nations. The conclusions so far from Ukraine are that for offensive operations, planning for cyber operations must be integrated into broader campaign planning and gauge where and when their use is beneficial. A combined arms approach, where cyber is integrated with other offensive capabilities, will gain the full benefit, since cyberattacks are an imperfect substitute for kinetic action and must be used in a sequence linked to other modes of attack.

As an aside, cyber offense would benefit from increasing the lethality and predictability of cyberattacks to improve their utility in offense. Cyberattacks already perform well in speed, range, and precision (to the extent those variables apply) and may offer greater possibilities for surprise, but their destructive capabilities are still limited. When a missile destroys a power plant, the smoking rubble can be observed. It is more difficult to tell if a cyberattack has succeeded or how permanent the effect will be. This will require emphasizing the use of cyberattacks to focus on disrupting command mechanisms, weapons software, and information as much or more than physical destruction. An attacker's decision to use cyberattacks must calculate whether their use makes the conflict more or less manageable and weigh this against how much use contributes to achieving strategic effect.

For offense, a campaign plan needs to include a realistic and specific assessment of the benefits and costs of cyber operations, including the cost to intelligence collection and the political effect on both combatants and external parties—realistic because of the limitations of cyberattacks, specific because very often a cyber operation will require a tailored quality determined by the nature of the target network and the intended effect. At a minimum, this will require both reconnaissance of the target network and "weapons" design (writing code for use in the attack) well in advance of any attack, along with testing and "refreshing" attack tools.

To the extent that cyberattacks harm civilians, including degrading their access to online services and social media, this will create a degree of repugnance. The international community is less tolerant of collateral damage or deliberate attacks on civilian targets, and these can have damaging political consequences for an attacker. Planning for offense must take into account the politics of cyberattacks over connected civilian networks. Russia did not, and this was another mistake.

The conflict in Ukraine can inform the United States and its allies on how to defend against offensive cyber operations directed against it by opponents, but China or even Iran may have also learned from the Russian experience. For cyber actions, Ukraine is probably not a safe precedent for conflict with any possible attack by China. China is better equipped and likely to have better planning. The United States may also not want to count on ineptitude among these opponents, even if they share authoritarian (and thus potentially idiosyncratic) decisionmaking.

Cyber operations failed to advance Russian goals—the occupation of Ukraine and the replacement of its elected government. Some of the mistakes that Russia made are becoming clear. Ukraine was not the first cyber war nor was cyberattack particularly useful to the Russians. The Ukrainian defenders and their partners did a good job of reacting quickly to deflect Russian efforts to disrupt networks. They do not appear to have faced a well-thought-out plan of attack integrated into broader campaign planning. This may be the most important lesson for cyber warfare from Ukraine: preparation and planning on how to integrate cyber operations with other modes of attack to achieve maximum effect makes cyberattacks useful. ■

James A. Lewis *is senior vice president and director of the Strategic Technologies Program at the Center for Strategic and International Studies in Washington, D.C.*

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).

Appendix: Cyber Incidents against Ukraine[2]

October 2021: Hackers created the IssacWiper malware on or before October 19, 2021, according to the code's timestamp, which they then deployed to Ukrainian government networks in February 2022.

November 2021: Hackers began development of cloned Ukrainian government websites with malware embedded in links on the fake sites. Researchers linked this activity to actors with ties to the Russian GRU and believe this activity has a connection to the second distributed denial-of-service (DDoS) attack in February 2022 against the Ukrainian banking sector and government websites.

December 2021: Hackers developed the HermeticWiper malware, according to the code's oldest timestamp, used in a February 2022 attack against financial organizations and Ukrainian government contractors.

December 2021: A hacking group targeted the State Migration Service of Ukraine with a phishing attack. In November 2021, the Ukrainian Security Service linked members of the group researchers believe carried out this attack to the Russian Federal Security Service (FSB).

December 2021: Hackers with suspected ties to the Russian GRU began development of malware used in March and April phishing attacks.

December 2021: A group with suspected ties to the Russian FSB compromised the network of a nuclear safety organization. Hackers stole data from this organization through March 2022.

January 2022: Hackers deployed destructive malware (WhisperGate), masquerading as ransomware, on numerous Ukrainian government, nonprofit, and information technology organizations' systems. Researchers linked this attack to hackers with suspected ties to the Russian GRU.

January 2022: Hackers targeted around 70 Ukrainian government websites, taking down several and defacing the Foreign Ministry website. The defacement included a threatening message to Ukrainians and a notice of the exposure of personal data, which was later refuted by Ukraine's Center for Strategic Communications and Information Security.

January 2022: Hackers targeted a Western government agency operating in Ukraine with a phishing attack. The actors uploaded a resume with malware to a Ukrainian job posting platform and submitted it to the government agency. Researchers attributed this attack to a hacking group previously linked to the Russian FSB by the Ukrainian Security Service.

February 2022: Hackers targeted a Ukrainian energy company with espionage malware through a phishing attack. The Computer Emergency Response Team of Ukraine (CERT-UA) attributed these attacks to a group with a history of targeting Ukrainian government organizations since at least March 2021 and with suspected ties to the Russian GRU.

February 2022: Hackers sent phishing emails on behalf of Ukrainian state bodies with malware masquerading as Ukrainian language translation software. Researchers attributed this attack to a group with ties to the Russian GRU.

February 2022: Hackers targeted the Ukrainian banking sector and government websites with a series of DDoS attacks, temporarily taking the websites offline. The United States, United Kingdom, and Australia attributed the attacks against financial institutions to the Russian GRU.

[2] The author would like to thank Georgia Wood for assembling this list.

February 2022: *The Times* reported that Chinese hackers targeted vulnerabilities in over 600 critical infrastructure institutions and the Defense Ministry in Kyiv in an attempt to compromise data and disrupt services. Their source claims to be from the Ukrainian Security Service, but the service denies this attribution.

February 2022: Hackers targeted websites belonging to the Ukrainian banking sector and the Ukrainian government with a DDoS attack, rendering some sites inaccessible. This was the second DDoS attack against Ukrainian banks and government websites in two weeks.

February 2022: Hackers deployed a destructive malware (HermeticWiper) to destroy around 300 systems across more than a dozen financial, government, energy, information technology, and agricultural organizations in Ukraine. Researchers linked this attack to a Russian GRU-affiliated group.

February 2022: Hackers deployed a file encryptor on the network of an agricultural company. Researchers assessed this was likely to target grain production in Ukraine and attributed the attack to a group with suspected ties to the Russian GRU.

February 2022: Hackers targeted the *Kyiv Post* with a DDoS attack, forcing its website offline. The *Kyiv Post* published news on social media platforms until connectivity was restored.

February 2022: Hackers deployed a destructive malware (IsaacWiper) on a Ukrainian government network.

February 2022: Hackers targeted European government members involved in coordinating logistics of refugees fleeing Ukraine with a phishing attack. The actors used a compromised email belonging to a Ukrainian armed service member.

February 2022: Hackers targeted satellite communications company Viasat with destructive malware, disabling modems communicating with Viasat Inc's KA-SAT satellite. The attack impacted connectivity across Ukraine and Europe, as the satellite provides internet access to customers in multiple countries. The United Kingdom, United States, and European Union attributed this attack to Russia.

February 2022: A hacking group, linked by researchers to the Belarusian government, targeted high-profile Ukrainians through a phishing attack. Hackers aimed to gain access to the individuals' social media accounts and post misinformation about Ukrainian forces.

February 2022: Hackers targeted a Ukrainian border control station with destructive malware that forced officials to process people fleeing into Romania manually.

March 2022: Hackers targeted at least 30 Ukrainian university websites. Researchers believe this attack came from a Brazilian-based group that publicly supports Russia.

March 2022: Hackers targeted telecom provider Triolan on March 9 and February 24, impacting network connectivity. A source from Triolan claimed the hackers reset the company's computer settings to factory level and some equipment required physical access to restore, which was difficult due to the ongoing crisis.

March 2022: A suspected Russian-linked hacker targeted a major broadcasting company with a destructive malware (DesertBlade).

March 2022: Hackers targeted charities, nongovernmental organizations, and other aid organizations providing assistance for Ukraine with malware intending to disrupt services.

March 2022: Hackers targeted Ukrainians with a phishing attack to deploy malware that compromises user data. The email promised payment "in the amount of 15,000" from the government as support during "this difficult time."

March 2022: A suspected Russian-linked hacker targeted a Ukrainian research institution. False Russian weapons conspiracies featured this institution in the past.

March 2022: A suspected Russian nation-state actor stole data from a nuclear safety organization.

March 2022: Hackers targeted the Vinasterisk network according to the operator, impacting connectivity in western Ukraine.

March 2022: Hackers deployed a destructive malware (CaddyWiper) in Ukrainian organizations. Researchers linked this attack to a group affiliated with the Russian GRU.

March 2022: Hackers targeted Ukraine 24, a media company out of Kyiv, to report that President Zelensky announced a surrender to Russia. President Zelensky later posted a video stating the message was fake.

March 2022: Hackers targeted the systems of Ukrainian state authorities with a phishing attack. According to CERT-UA, the attack came from a group associated with the Luhansk People's Republic (LPR).

March 2022: Hackers targeted several Ukrainian news outlets, defacing the platforms with symbols banned in Ukraine. The Security Service of Ukraine stated they identified the networks and servers used by the attackers.

March 2022: Hackers deployed a destructive malware (DoubleZero) targeting Ukrainian enterprises.

March 2022: Hackers targeted the Ukrainian Red Cross website, forcing it to suffer an outage for several hours.

March 2022: Hackers targeted Ukrainian organizations with a phishing attack. The malware uploads a backdoor that allows hackers to access and control system data. CERT-UA attributed these attacks to a group previously announced by the Ukrainian Security Service to have ties to the Russian FSB.

March 2022: Chinese hackers targeted Ukraine in a phishing attack, according to researchers. The email includes a malware-ridden document masquerading as coming from the National Police of Ukraine.

March 2022: Hackers targeted a transportation and logistics provider based in western Ukraine. Researchers linked this attack to a suspected Russian GRU-affiliated group.

March 2022: Hackers used WordPress sites to target 10 websites with DDoS attacks, including Ukrainian government agencies, think tanks, and financial sites.

March 2022: Hackers targeted Ukrtelecom, one of the largest telecom providers in Ukraine, forcing connectivity in the country to drop to 13 percent of pre-war levels. Specialists from the State Service of Special Communications and Information Protection of Ukraine restored connectivity within several hours of the attack.

March 2022: Hackers targeted Ukrainian organizations and individuals with a phishing attack. The scam email claimed to be from the Ministry of Education and Science of Ukraine, and the malware gives the hacker access to sensitive data and user identification information.

April 2022: Hackers targeted the Telegram accounts of Ukrainian government officials with a phishing attack in an attempt to gain access to the accounts.

April 2022: A group targeted several Ukrainian media organizations in an attempt to gain long-term access to their networks and collect sensitive information. Microsoft took control of seven internet domains the group used to mitigate these attacks. The group has connections to the Russian GRU.

April 2022: Hackers targeted a Ukrainian energy facility, but CERT-UA and private sector assistance largely thwarted attempts to shut down electrical substations in Ukraine. Researchers believe the attack came from the same group with suspected ties to the Russian GRU that targeted Ukraine's power grid in 2016, using an updated form of the same malware.

April 2022: Hackers targeted Ukraine's national post office with a DDoS attack, days after releasing a new stamp honoring a Ukrainian border guard. The attack impacted the agency's ability to run its online store.

April 2022: Hackers created a fake Ukraine 24 Facebook page, prompting users to enter their personal data and payment information.

April 2022: Hackers used a compromised Ukrainian government email in a phishing attack. CERT-UA linked this attack to hackers with suspected ties to the Russian GRU.

April 2022: Hackers targeted Ukrainian state authorities with a phishing attack.

May 2022: Hackers launched a phishing attack allegedly on behalf of CERT-UA with malware that compromises user data. CERT-UA attributed this attack to actors with ties to the Russian GRU.

May 2022: Hackers launched a phishing attack to gain access to authentication data. The email warns recipients of an impending chemical attack to convince users to open its malware-ridden attachment.

June 2022: Hackers targeted Ukrainian state organizations with a phishing attack.

June 2022: Hackers targeted media organizations in Ukraine with a phishing attack. CERT-UA attributed the attack with an "average level of confidence" to a suspected Russian GRU-linked group.