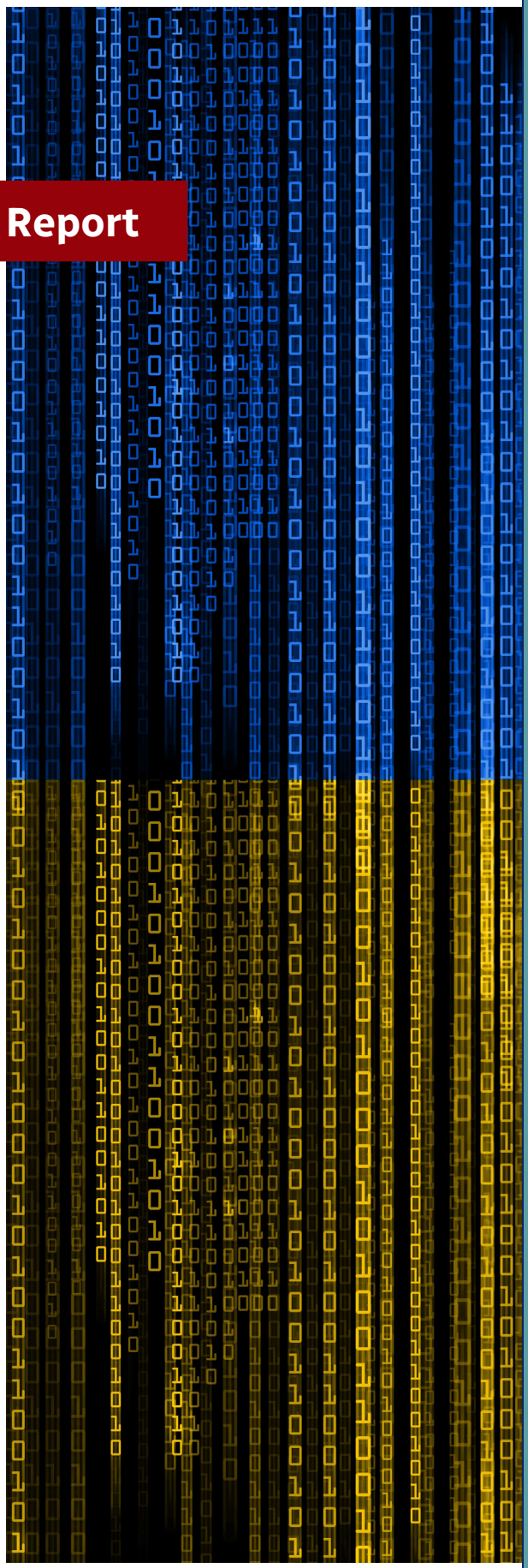


Report

G | M | F

IDEAS LEADERSHIP HOPE

Ukraine's Cyber Defense

Lessons in Resilience

Khrystyna Kvartsiana

ReThink.CEE Fellowship

December 2023

Table of Contents

Summary

Since 2014, Ukraine has faced relentless cyberattacks, with Russian actors repeatedly seeking to identify and exploit vulnerabilities in the country's digital infrastructure. This has showed the rapid evolution of cyber tactics in a modern conflict and the critical importance of early detection and proactive responses to cyber threats. The expanding cyber threat landscape has significantly influenced Ukraine's cyber policy over the last decade. Constant cyberattacks forced the country into a reactive stance, diverting resources from proactive policy development. Its struggle has highlighted the imperative need for strategic planning, resource allocation, and increased public awareness to enhance cyber resilience.

Ukraine's reactive approach to cyber threats, especially from state-sponsored actors, has nonetheless led to the rapid development of its cybersecurity capabilities. This provides the country with the foundation for a more proactive strategy to anticipate and preempt cyber threats. The shift to a proactive cyber defense strategy aligns with broader national security goals as well as the need for responsible conduct in cyberspace.

Russia's full-scale invasion in 2022 was the catalyst for the swift implementation of cyber-defense measures by Ukraine. The character and scale of the cyberattacks prompted a comprehensive approach involving multiple stakeholders and parallel legal and institutional developments. Ukraine capitalized on its digitalization reforms of recent years and tapped help from international technology companies. The invasion increased societal awareness of the importance of cybersecurity and civil society has also been crucial in cyber resilience. Ukraine's experience over the last two years shows the value of investment in cybersecurity infrastructure and public-private partnerships to withstand cyberattacks.

The integration of cyber warfare into conventional military campaigns on such a scale as seen in Ukraine is a groundbreaking development. It helps to optimize the use of resources and achieve far-reaching military and political objectives for both sides. Ukraine's response to Russia's cyber warfare, involving civilian actors through initiatives like the IT Army, poses ethical, legal, and strategic challenges. Functioning with a decentralized structure and not officially affiliated with state institutions, the IT Army engages volunteers worldwide, coordinating efforts to disrupt Russia's financial infrastructure, state services, and propaganda media. Officially there are no specialized cyber troops within the armed forces, but they exist de facto, and their formal creation is under consideration.

Russia's systematic targeting of civilian infrastructure using cyberattacks has also exposed a weakness in international law. This calls for rethinking the responsibility for cybercrimes and introducing more related accountability mechanisms in international law.

Ukraine's experience in dealing with cyber threats has far-reaching implications for cybersecurity policies, international legal frameworks, and the roles of various actors in modern cyber-enabled conflicts. It highlights the need for proactive strategies, international cooperation, and the responsible conduct of all actors in the evolving landscape of cyber warfare.

Introduction

Since the start of Russia's aggression against it, Ukraine has become a crucible for a new breed of warfare—one fought not only with traditional weapons on battlefields but with lines of code and keystrokes in the cyber realm. For almost a decade now, the country has faced an unrelenting wave of cyberattacks, with the invisible battlefront blurring the line between state and nonstate actors and the fighters including not only soldiers but also hackers, volunteers, and private companies. The experience of Ukraine has implications not just for the security of individual countries but for the future of international cyber policy, the role of technology giants in warfare, and the rights and responsibilities of civilians in such conflicts.

This paper analyzes the Russo-Ukrainian cyber battleground, exploring the unique challenges it presents and the lessons it offers. It first looks at the experience of Ukraine with Russia's hybrid warfare before the full-scale invasion of February 2022. It then looks at the change of tactics since then. The next section looks at the different dimensions of Ukraine's cyber resilience and counteroffensive. The paper concludes with some reflections on how Ukraine's experience in dealing with Russia's cyberattacks and the evolving nature of cyber warfare has profound implications for cybersecurity policies, international legal frameworks, and the roles of various actors in modern cyber-enabled conflicts.

Hybrid Warfare Before February 2022

Cyberattacks have been an integral part of Russia's warfare against Ukraine since 2014. These do not involve just distributed denial-of-service (DDoS) attacks against minor targets; Russia has also been targeting critical infrastructure such as banks or electricity grids. The first known significant Russian cyberattack was a DDoS one on the Central Electoral Commission's information system in 2014. It aimed to falsify the results of the presidential election to show a victory by Dmytro Yarosh, the leader of the nationalist organization Right Sector, who was portrayed as a Nazi on Russian television. The attack was revealed thanks to the early dissemination of the fake "results" on Russian media and neutralized by the Computer Emergency Response Team of Ukraine (CERT-UA).

At its summit in Wales in 2014, NATO recognized cyber defense as part of its collective defense mandate. In Ukraine, however, the conversation on cybersecurity and cyber defense was only beginning. In December 2015, three major regional electricity companies—Prykarpattiaoblenergo, Kyivenergo, and Chernivtsioblenergo—were targeted with the Trojan malware BlackEnergy. This cyberattack was among the most successful in cyberspace, resulting in the deactivation of electricity power grids for up to six hours and impacting nearly 225,000 customers.[1] It was undertaken in several phases: from delivering the malware through spear phishing emails to getting corporate credentials months before and exploring vulnerabilities, the malware eventually found its way to the power grid's control system. The KillDisk plug-in was used to destroy entire internal server file systems, which ensured the impact of the cyberattack for a longer period, while a parallel DDoS attack on control centers prevented clients from reporting outages.[2] The Security Service of Ukraine immediately suspected that the Russian government

had coordinated the cyberattack.[3] The US cyber intelligence company iSight Partners later attributed the attack to Sandworm or Unit 74455 of the Main Intelligence Directorate (GRU) of the Russian armed forces.[4]

In December 2016, the central electricity power grid Ukrenergo was the target of a fully automated cyberattack, unlike the December 2015 one in which hackers manually switched the power off.[5] This resulted in an electricity outage of more than one hour in Kyiv and its region. According to one source, the Crash Override malware used in this attack "was programmed to include the ability to 'speak' directly to grid equipment, sending commands in the obscure protocols those controls use to switch the flow of power on and off".[6] This new malware was reported to perform much quicker with significantly less preparation and fewer operators involved. In 2021, the US government attributed this cyberattack to Russian state cyber actors.[7]

The cyberattacks intensified in the following years, in particular with the ransomware Petya and the malware NotPetya hitting even more critical infrastructure in 2017. Petya required a user to open a file and download it while NotPetya could spread in computers independently, which explains the latter's quick and far-reaching impact. According to different estimates, including from the Ministry of Infrastructure at the time, NotPetya hit the overwhelming majority of government websites and around 10% of all computers in the country.[8] From there it spread to neighboring countries and eventually globally. More than 10,000 government devices were affected by the malware, including those at the Cabinet of Ministers, the Ministry of Infrastructure, the Tax Service, the Antonov Aircraft State Concern, the national telecom provider Ukrtelecom, Boryspil and Zhulyany airports, the national gas extraction company Ukrgazvydobuvannya, the major electricity provider DTEK, television channels, gas stations, the Kyiv Metro, the national railway company Ukrzaliznytsia, the National Bank of Ukraine and major banks, the national postal service, the Chornobyl nuclear power plant, and hundreds of companies. According to the Cyber-Police Department of the National Police of Ukraine, the NotPetya attack hit more than 2,000 institutions. The US Department of Justice charged six officers of Russia's GRU for this cyberattack in 2020.[9]

These cyberattacks correlated with political events and symbolic dates in Ukraine with a degree of predictability.

While Petya was a ransomware that demanded a payment in Bitcoin to decrypt affected user's files, NotPetya was a malware aiming for destruction. After a sudden restart, an infected device was irreversibly encrypted and basically destroyed. NotPetya's objective was to cause as much damage as possible to the economy and infrastructure of Ukraine, and to those of its supporters. It affected more than 60 countries and caused damage estimated to up to $10 billion.[10] The initial infection occurred through the system of updates of M.E.Doc, Ukraine's authorized support software for reporting taxes, which was installed in almost every Ukrainian taxpaying company.

These cyberattacks correlated with political events and symbolic dates in Ukraine with a degree of predictability. The NotPetya attack took place the day before the Constitution Day national holiday. The massive attack on the Central Electoral Commission servers in 2014 happened on the day of the first democratic election after the Revolution of Dignity. According to Viktor Zhora, the deputy chief of the State Service of Special Communications and Information Protection, the main body responsible for Ukraine's cyber defense,

> Starting with the first attack on the election system in 2014, continuing with an attack on an energy facility in 2015, continuing on an energy company's systems management system in 2016 and ending at the end of 2017, it was a series of cyberattacks that shaped our national cybersecurity policy, which initially was about raising awareness on the importance of cybersecurity at the level of the state and at the level of business. And it also contributed to the strengthening of our capabilities in cyber defense, which is now part of state policy.[11]

As a first response to such cyberattacks, the government created in 2015 the Cyber-Police Department within the National Police of Ukraine, dedicated specifically to countering cybercrimes. The scale and severity of the 2017 cyberattacks prompted the government to take national cybersecurity more seriously, and in that year the Law on the Basic Principles of Ensuring Cyber Security of Ukraine was adopted.[12] It had been introduced in parliament in 2015 and might have been passed much later if not for the NotPetya attack. The law introduced definitions of "cyberattack", "cyber threat", and other essential terms to the legal framework. It also made several key institutions responsible for Ukraine's cybersecurity:

- The State Service for Special Communications and Information Protection of Ukraine, which is responsible for policymaking and implementation
- The National Police of Ukraine, which is responsible for the prevention, detection, stopping, and disclosure of cybercrimes.
- The Security Service of Ukraine, which is responsible for the "prevention, detection, stopping and disclosure of crimes against the peace and security of humanity, which are committed in cyberspace; counter-intelligence and operational-research measures aimed at combating cyber-terrorism and cyber espionage, secretly checks of the readiness of critical infrastructure facilities for possible cyberattacks and cyber-incidents; cybercrime counteraction, the consequences of which may pose a threat to the vital interests of the state; investigation of cyber incidents and cyberattacks regarding state electronic information resources".
- The Ministry of Defense and the General Staff of the Armed Forces, which are responsible for the "preparation of the state to repel military aggression in cyberspace (cyber defense); military cooperation with NATO and other subjects of the defense sphere to ensure the security of cyberspace and joint protection against cyber threats; implementation of measures to ensure cyber protection of critical information infrastructure in conditions of emergency and martial law".
- The intelligence agencies.
- The National Bank of Ukraine.

Though a milestone in laying out the legal basis for institutionalizing cybersecurity policy, the law was for a long time criticized by civil society. The Ukraine Cyber Alliance, for instance, pointed out that the vagueness in direct jurisdictions and enforcement mechanisms was a clear shortcoming of the law. To prove its point that the state's systems were highly at risk, it repeatedly exposed the vulnerabilities of dozens of public institutions.[13] Another criticism from civil society has been aimed at the cautious approach to increasing the scope of competences of law-enforcement agencies, which may have been appropriate in the relatively calm post-Euromaidan period but was not for one of full-scale war.

Besides, the necessary changes to the Criminal Code to reflect the terminology introduced in the law were not made. For example, the Criminal Code does not even mention what "cyberspace" is. Thus, cybercrimes still are being prosecuted under Chapter XVI of the Criminal Code, which refers to "Criminal offenses in the field of use of electronic computing machines (computers), systems and computer networks and telecommunication networks", and in particular Article 363-1, which refers to "interfering with the operation of (computers), automated systems, computer networks or telecom networks by mass distribution of telecommunications messages".

Other articles of the Criminal Code that are to this day the reference for the criminal liability for cybercrimes (though not labeled as such) are: Article 361 (unauthorized interference in the operations of computers, computer networks, or electronic networks), Article 361-1 (intentional creation, use, distribution or sale of malicious software), Article 361-2 (unauthorized sale or distribution of information with limited access), Article 362 (theft, appropriation, extortion of computer information or obtaining it by fraud or abuse of official position), and Article 363 (violation of the rules of operation of automated electronic computing systems).

The slow institutionalization of the cybersecurity legal framework and enforcement apparatus could barely keep up with the intensification of cyberattacks on Ukraine's critical infrastructure.

The slow institutionalization of the cybersecurity legal framework and enforcement apparatus could barely keep up with the intensification of cyberattacks on Ukraine's critical infrastructure. For example, in 2018, the chief of the Cyber-Police Department said the number of cybercrimes in Ukraine has been increasing by an average of 2,500 yearly.[14] The Cyber-Police Department and the Security Service of Ukraine, the two agencies empowered to investigate cybercrimes, occasionally reported the number of intercepted cyberattacks and disclosed cybercrimes but without much detail. For instance, at the end of 2018, the Cyber-Police Department reported that it had investigated more than 11,000 cybercrimes (of which 2,688 related to cybersecurity) and exposed more than 800 people involved in cybercrimes (including 505 under Article 361 and 55 under Article 361-1 of the Criminal Code).[15] But what exactly these acts involved or how many people were sentenced for them was never made public. Overall, Ukraine's investigative institutions reported record numbers of cases based on the cybercrime articles of the Criminal Code. The prosecution services did not make their statistics available under open access but rather only upon requests for public information. Court decisions as a result of criminal proceedings under the cybercrime articles can be found in the State Register of Court Decisions, but it is not clear how many people convicted of cybercrimes were actually sentenced or fined.

According to Dmytro Khutkyy, an expert at the European Digital Development Alliance,

> When government agencies report on the number of deterred or prevented cyberattacks, it's unclear what exactly they mean. Frequently, the used language is ambiguous leaving too much space for interpretations. When they say that N number of cyberattacks was deterred without explaining which ones and how, it can mean multiple things. For example, that Ukrainian e-system withstood a minor cyberattack, or that there was a breach but there was no damage, or the damage was mitigated, or a cyberattack was foreseen and measures

> were taken in advance. We, the public, don't know. Of course, maybe there is a national security rationale in this. In any case, this makes it difficult for analysts to see the full picture at the moment.[16]

After the NotPetya cyberattack, the Security Service of Ukraine regularly reported that it had tracked many cyber incidents back to Russia. For instance, it stated that 480 Russian cyberattacks on state institutions and critical infrastructure had been neutralized in 2019.[17] The majority of these related to information crimes and not cybercrimes as they concerned fake individual accounts on social media that spread separatist propaganda and attempted to destabilize the political situation in Ukraine from within—a characteristic feature of Russian hybrid warfare before 2022. Compared to a complex cyberattack on critical infrastructure, which can take years of preparation,[18] launching with as little as a couple hundred dollars a Facebook page to spread anti-government and pro-Russia propaganda is much more time- and resource-efficient. The cyberattacks on critical infrastructure and the information operations aimed at polarizing the population and spreading pro-Russia narratives served the same purpose of undermining Ukraine's state and national security.

The public discourse in Ukraine on national cybersecurity developed over eight years of cyberattacks and threats from Russia. However, the resulting institutional transformation was slow, partly because other necessary reforms, such as the ones against corruption, took up a lot of space on the national agenda. The second milestone with regard to national cybersecurity after the passing of the 2017 law was the adoption in 2021 of a Cybersecurity Strategy,[19] which the newly elected government pushed. Although the law did not elevate cybersecurity to the importance given it by NATO, its implementation plan formulated key objectives prioritizing cyber defense and included indicators with clear targets. Among other things, the strategy envisaged the creation by 2023 of cyber troops in the armed forces, with the appropriate financial, personnel, and technical resources to deter armed aggression in cyberspace and to repulse an aggressor.[20] At the time of writing, the creation of cyber troops within the General Staff of the Armed Forces was being actively discussed, and a draft law was about to be registered in the parliament (see further below).

Counteracting cyberattacks was done primarily by volunteers as the perception of cybersecurity as an integral part of national security was still in the making, along with corresponding legislation and institutions. This resembled the support to the weak armed forces in 2014, when thousands of volunteer combatants went to the Donetsk and Luhansk regions to reinforce the country's defense against the Russian invasion.

One volunteer group involved is the Ukrainian Cyber Alliance (UCA), a hacktivist movement that emerged as a response to Russian cyber aggression in the spring of 2014. It has conducted countless cyber operations against Russian agencies and top officials, aiming to expose Russia's invasion of Donbas at a time when the international community would refer to the situation there as an internal conflict, a civil war, or a separatist uprising. In one instance, the UCA leaked nearly one gigabyte of emails belonging to Vladislav Surkov, advisor to Russia's President Vladimir Putin, which contained confirmation of the presence of Russian regular armed forces in Donbas, direct orders from the Russian government to the leaders of the "Donetsk People's Republic" with regard to the political destabilization of Ukraine, a list of recommended candidates for appointments in the separatist "government", and communications from alleged "people of Donbas" drafted in the Kremlin.[21]

Russia also changed the disposition of the Internet connectivity infrastructure serving Crimea and Donbas. One study showed that the Border Gateway Protocol—which enables the global routing system of the Internet—had been modified "in order to divert the local Internet traffic from continental Ukraine—drawing a kind of 'digital frontline' consistent with the military one."[22] Controlling Internet routes can lead to having ultimate power over traffic and being able to block news sources, social media, or any web sources. According to Louis Pétiniaud, one of the authors of that study, Crimea and Donbas, being under Ukraine's sovereignty were progressively de facto integrated in the Russian Runet. The same pattern can be observed with other "separatist" entities in the region: Abkhazia is fully integrated in the Russian network, while the rest of Georgia, just like the rest of Ukraine, is connected to the EU networks.[23]

Since February 2022, Russia has repeated this in the parts of Ukraine that it has occupied, such as Berdiansk, Mariupol, and Kherson. Kherson, for example, as all Ukrainian cities, used to be connected to the Internet through Kyiv. Since June 1, 2022, the Russian authorities rerouted the occupied city's Internet traffic through their state-controlled network in Crimea and connected it to Moscow's network.[24] In most cases, the rerouting of Internet traffic has happened at the same time as the blocking of mobile phone networks, so that the population under occupation immediately loses connection to alternative information sources and to relatives and friends in the rest of Ukraine. In this, cyber warfare is closely interlinked with information warfare, tightening the grip of censorship and surveillance.

Full-Scale Invasion and Change of Tactics

Russia's cyberattacks on Ukraine go hand in hand with its war plans, aiming to spread panic, to terrorize the civilian population, and to undermine the government and state institutions. For a long time before January 2022, Ukraine was the second-ranked target of cyberattacks in the world after the United States. Since then, it has been the first-ranked.[25]

On January 14, 2022, right after unsuccessful security talks between Russia and the United States, government websites, including those of the Ministry of Education and the Ministry of Foreign Affairs, were defaced with a xenophobic message saying: "Ukrainians! … All information about you has become public. Be afraid and expect worse. It's for your past, present and future".[26] The statement included images of Ukraine's map, national flag, and emblem crossed out as banned. The content of this message clearly aligned with Putin's justification for the invasion, as reflected later in the atrocities carried out by the Russian army in occupied cities and the statements of Russian propaganda such as by RIA Novosti on what "Russia should do with Ukraine".[27]

According to the Security Service of Ukraine, Russia has been orchestrating fake messages about the planting of mines across the country since the occupation of Crimea in 2014.[28] In January 2022, simultaneously as the Kremlin deployed 150,000 troops along Ukraine's borders with Belarus and Russia, the national police reported receiving 1,000 such messages, a twelvefold increase from previous years.[29] Though not strictly speaking a cybercrime or information crime, these messages play on human fears to intimidate people, to provoke their disbelief in the

state's capacity to protect them, and to destabilize the country. They are a tool in the psychological pressure operations employing predominantly mass propaganda and disinformation that Russia has been waging in Ukraine and elsewhere since 2014.

Russia's campaign to create informational uncertainty around the shooting of Malaysian Airlines flight NH17 in July 2014—with Ukrainian and Western social media bombarded with countless opinions aiming at encouraging people's feeling that there was no true version of the event[30]—was a precursor to the information attacks against Ukraine happening daily since the full-scale invasion. Constant fake news, deepfakes, rapid-fire lying, and disparaging outgroups are being used to undermine Ukrainian society's morale and resistance. Google reported a 250% increase in Russia-backed cybercriminals targeting Ukrainian users in 2022 compared to 2020.[31] These tools are particularly difficult to thwart when they are coupled with frequent bombings that keep people shocked and their mind vulnerable.

However, Ukraine's experience of countering information warfare over the last eight years has significantly increased the level of digital literacy in society and reinforced fact-checking journalism and communication capacities. Ukrainians therefore often successfully apply techniques against information warfare. Having learned that Russian propaganda channels frequently foreshadow the actions of Russian army, the authorities have used strategies warning the public about possible planned information attacks.

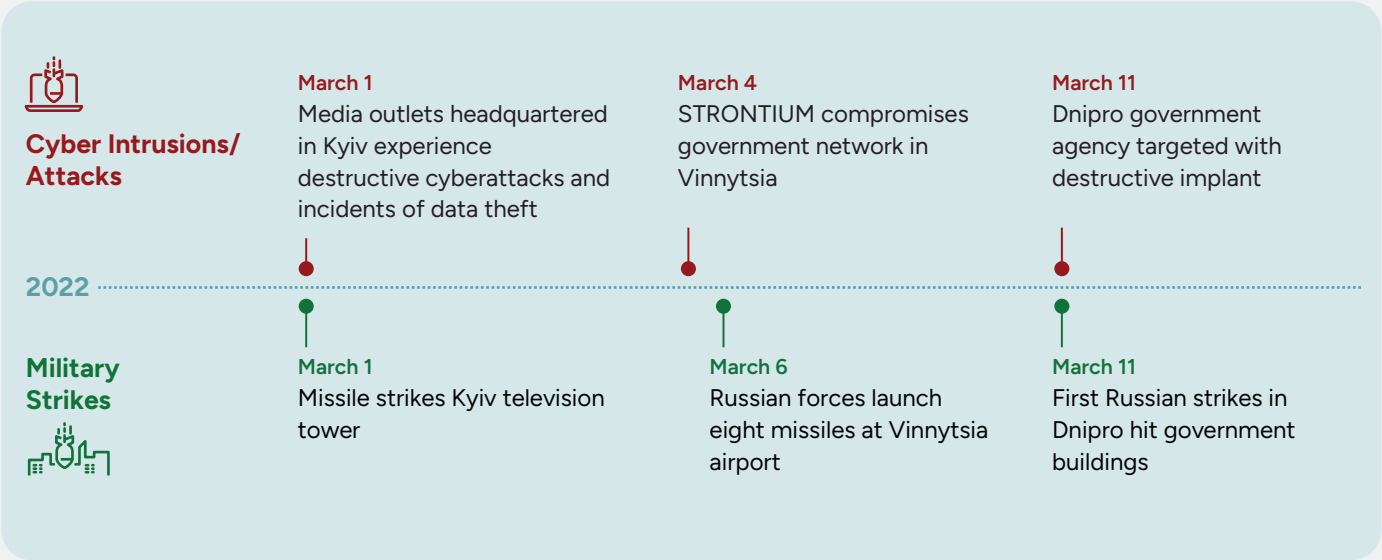
In the first days of the full invasion, after false news about President Volodymyr Zelenskyi fleeing Kyiv and calling on the armed forces to surrender went viral on Russian media, the government communicated to the public that it had expected such an information attack and that there would be more. Shortly after the announcement, accounts on Ukraine's social media started sharing a deepfake video of Zelenskyi announcing his resignation and calling on the army to surrender,[32] but this did not work. Following announcements by the Main Directorate of Ukraine Intelligence, Ukrainians were prepared for the numerous attacks on civilian infrastructure that were part of informational-psychological operations.

Ukraine has also sought to use such information warfare methods against Russia to gain an advantage on the battlefield. In the military counteroffensive of October 2022, for example, the government planted fake information in the media about plans to strike Russian positions in the south of Ukraine, following which the military moved instead in Kharkiv and the east, liberating 12,000 square kilometers of territory.

When it comes to cyber warfare, the main techniques used by Russia since the start of the full invasion have included cyber espionage, malware and ransomware attacks on critical infrastructure, spear phishing and data breaches, deep fakes, and defacing.

In February 2022, one day before the invasion began, a wiping Trojan malware called Foxblade, developed by the same group that had deployed NotPetya in 2017, hit 19 Ukrainian public institutions. Around an hour before the invasion, ViaSat, one of the world's largest commercial satellite Internet providers, which is used by Ukraine's government, banks, and armed forces, was attacked with the destructive wiper malware WhisperGate. This caused a significant disruption in communications when the first Russian missiles were launched at Ukraine. The EU and

Figure 1. Cyber Intrusions or Attacks and Military Strikes Events



Source: Microsoft, Special Report Ukraine 'Overview of Russia's Cyber Activity in Ukraine', April 2022.

the United States officially attributed this attack to Russia. According to Washington, the operation started one month prior to the invasion.[33] The cyberattacks continued throughout the year, with 1,148 out of 2,194 incidents dealt with by CERT-UA identified as being of paramount importance.[34]

The critical transformation in Russian cyber warfare that took place with the full-scale invasion was the combination of kinetic weapons and cyberattacks against critical infrastructure, including cyber infrastructure. The first missiles on February 24, 2022 targeted the Governmental Center of Data Processing that, with most of public services having been digitalized, held hundreds of state registers and was a critical target. However, this attack did not produce the desired result as, one week before the invasion, the parliament had adopted a law allowing the movement of public data to the cloud outside of Ukraine's borders. Figure 1 illustrates the correlation between military strikes and cyber intrusions or attacks.

Cyber Espionage

Since February 2022, Russia has invested more in cyber espionage. It has been spying on digital technologies used by Ukrainians, from social media to video game chats or dating apps, to collect valuable information on strategic objects.[35] Pictures of newly destroyed buildings on social media have been a source of information for the Russian military, helping it to improve targeting in subsequent missile launches. Ukraine's government has repeatedly instructed civilians in wartime digital hygiene rules to address this threat. It has encouraged people to think before posting any images of rockets hitting targets or of movement of the Ukraine armed forces, just as it had called for a more responsible, fact-checking approach when sharing information. Posting information on the movement of the armed forces or on international military aid was criminalized under the new amendments to the Criminal

Code, with penalties between three and eight years of imprisonment. By the end of 2022, around 200 criminal proceedings had been initiated under this provision since the law's adoption.[36]

Cyber espionage on public officials, diplomats, and experts with access to sensitive information is the most dangerous threat, according to a CERT-UA analysis of Ukraine's cyber landscape in 2022.[37] These attacks, which are most difficult to identify and have the potential for critical consequences, are often attributed to the group InvisiMole, which is linked to Russia's Foreign Intelligence Service. To conduct this cyber espionage, Russia uses mostly spear phishing campaigns, trying to infect computers with malware through emails or other ways to gather data.[38]

Spear phishing campaigns aimed at data exfiltration and cyber espionage were identified as a priority in Russian cyber warfare in the second half of 2022, accounting for 70% of all operations, and eventually outpaced destructive cyberattacks.[39] Google registered major spikes in such campaigns between May and July 2022, with more than 4,000 emails with fake Microsoft updates targeting technology, retail, and governmental organizations on May 23, and more than 10,000 spam emails impersonating the state tax service between June 19 and 21.[40]

At the start of the full-scale invasion, the first cyberattacks were directed at media and communication agencies as part of Russia effort to achieve a Blitzkrieg war victory in three days. "Many media outlets were hacked from within and started posting fake news in the first days of invasion, with admin credentials having been stolen way before February 2022", says Pavlo Belousov, a digital security expert at the Internews Ukraine Digital Safety School. However, within weeks, once Russia had failed to capture Kyiv, the focus of cyberattacks switched to government institutions and the energy sector. On March 30, for instance, CERT-UA registered a mass email campaign targeting citizens and organizations, sent out allegedly from the Ministry of Education and Science regarding access to "electronic educational journals". An attached file was infected with a malware called MarsStealer, designed to collect information about infected computers by stealing authentication data from Internet browsers, plug-ins of crypto-wallets, software-based multifactor authentication, and files as well as by taking screenshots. This attack was tracked to the group UAC-0041, which consists of the Russian hacktivist groups AgentTesla and XLoader.[41] Nearly all state institutions, including the General Staff of the Armed Forces, have been impersonated by cybercriminals sending spear phishing emails to other institutions.[42]

The new tactics of Russia's cyber warfare have proved to be more sophisticated and quickly adaptable to Ukraine's information climate. For instance, following the liberation of Bucha and Irpin, when the world was shocked by the atrocities committed by the Russian army, Ukraine's public servants received emails with the subject "Information about war criminals of the Russian Federation". Taking advantage of a moment when Ukraine's collective consciousness was overwhelmed with this news, these emails spread a contaminated file labeled "Military criminals destroying Ukraine (home addresses, photos, phone numbers, pages in social networks).lnk" that, if opened, would eventually provide the attackers with remote access to the victim's computer.[43] Ukraine's authorities attributed the attack to the hackers' group Armageddon, which is linked to Russia's Federal Security Service.

The increase in intensity and severity of cyberattacks in 2022 accelerated the adjustment of Ukrainian legislation addressing cybercrime. On February 1, 2022, the president signed Decree No. 37 on the Plan of Realization of Cybersecurity Strategy. The plan contains ten objectives: effective cyber defense; effective countering of intelligence-subversive activities in cyberspace and cyber-terrorism, effective countering of cybercrime, developing asymmetric instruments of deterrence, national cyber preparedness and robust cyber defense; professional development, cyber-aware society, and scientific and technical support of cybersecurity; safe digital services; strengthening coordination; forming a new model of relations in cybersecurity; and pragmatic international cooperation. Under these, the plan assigns 94 tasks to be completed by various law-enforcement agencies and special state agencies with law-enforcement functions within maximum three years of its adoption.[44] The implementation of the plan was supposed to start with developing a system of indicators for the state of cybersecurity; for the development of the national cybersecurity system; for the state of cyber protection of critical information infrastructure, state information resources and information, but this has not happened so far. Many deadlines are unmet, and the implementation of some tasks has already started, (for example, training with NATO cyber teams) or is yet to begin (for example, creating cyber troops). A comprehensive monitoring assessment of the plan is needed to track progress.

In April 2022, the parliament adopted Law 7182 on Amendments to the Criminal Code of Ukraine to Increase the Effectiveness of Fighting Cybercrime in Martial Law. The law changed the articles concerning cybercrimes in the Criminal Code to bring their terminology in compliance with the 2020 Law on Electronic Communications.[45] It also reinforces the sanctions for the creation of malicious software or applications, which now is punishable by three years of imprisonment.[46]

* * *

Russia's cyber actors and propaganda have been one of the top Kremlin priorities for decades and they have become an integral part of its military effort. The list of actors involved in Russian cyber operations is long and complex, including legitimate and criminal private entities alongside traditional security services, the military, and top political decision-makers. According to Viktor Zhora, its deputy chief, the State Service of Special Communications and Information Protection of Ukraine (SSSCIPU) has identified nearly 80 actors responsible for various types of cyberattacks and information attacks against the country's government, citizens, and civilian infrastructure. He says: "Most of these groups are related to the enforcement agencies of the Russian Federation, and the identification of real persons who sat at the keyboard and carried out these criminal orders is just a technical matter".[47] Based on constant monitoring and analysis of the approaches, techniques, and servers used, the SSSCIPU has singled out key actors of the Russian cyber offensive (See Figure 2).

Russia's cyber warfare against Ukraine has targets far beyond the country's borders, violating the digital sovereignty of states that actively condemn Russian aggression and provide aid to Ukraine. Along with the rise of targeting of Ukrainian users by Russia-backed cybercriminals, Google reported that the targeting of NATO countries increased by 300% in 2022.[48] In April 2023, for example, the pro-Russian hacktivist group Killnet released stolen data that supposedly pertains to 4,639 individuals associated with NATO. The database of leaked documents that was released on its encrypted Telegram account includes the names, phone numbers, and

Figure 2. Key Russian Cyber Actors

Actors	Government Agency Link	Method and Tools	Targets
UAC-0010/Gamaredon/Actinium (Responsible for the greatest number of cyberattacks)	Federal Security Service (FSB)	Cyber espionage (malware via spear phishing emails)	Key government organizations, state-owned enterprises, security, defense sector
UAC-0082/Sandworm/IRIDIUM (Responsible for cyber espionage and destructive activity)	Main Intelligence Directorate (GRU)	Malware: Industroyer2; HermeticWiper, IsaacWiper, CaddyWiper (for Windows users); AwfulShred, SoloShred (for Linux users)	Critical Infrastructure organizations (for example, energy facilities, logistics companies, media)
UAC-0028/APT28/STRONTIUM/ Fancy Bear		Spear phishing, stealers, re-use of passwords	The military
UAC-0035/InvisiMole	Foreign Intelligence Service (SVR)	Cyber espionage, Bring Your Own Vulnerable Driver (BYOVD)	Individual diplomats and Ministry of Foreign Affairs
UAC-0029/APT29/NOBELIUM/ Cozy Bear		Cyber espionage, tools unknown	Political parties, governments, international organizations, think tanks and nongovernmental organizations
Belarusian group UAC-0105/ GhostWriter		Credentials harvesting, malware campaigns	

Source: State Service of Special Communications and Information Protection of Ukraine. Russia's Cyber Tactics: Lessons Learned 2022

email addresses of the victims, along with their city and country of residence. Numerous email addresses in the database are associated with domain names belonging to defense organizations in countries such as Australia,

the United Kingdom, and the United States. This leak coincided with the visit of NATO Secretary General Jens Stoltenberg to Kyiv.[49]

Despite the inherent difficulty in identifying with absolute certainty the actors behind different kinds of cyberattacks, Ukrainian and Western institutions are confident that they have traced several to actors in other countries than Russia. In one major incident concerning a cyberattack on the Ministry of Defense, the SSSCIPU identified groups affiliated with China and Iran as being involved alongside Russian actors.[50] In another, on February 15, 2022, the state digital service Diia was attacked not only from Russia but also from China, Czechia, and Uzbekistan, according to the authorities.[51] China is also believed to have been responsible for cyberattacks on Ukraine's military and nuclear infrastructure on the night before the February 2022 invasion, based on the similarity between the attackers' methods and those of the People's Liberation Army.[52]

In summary, since the February 2022 full invasion, Russia's cyber warfare tactics have used all available tools depending on its priorities at any given moment. These have been well-designed and tailored to their multiple targets—whether the Ukraine's population or government; its energy, financial, or media sectors; the government of its NATO allies or the Western public. This cyber warfare is waged by multiple actors, involving state and private ones and hacker groups linked to the three key Russian intelligence agencies.

Cyber Resilience and Counteroffensive

The complex character and large scale of the Russian cyberattacks on Ukraine after the February 2022 full invasion required a comprehensive approach to defending its cyberspace. This approach has involved multiple stakeholders and parallel developments.

Institutional Development

According to Oleksandr Fedienko, a member of the Parliamentary Committee on National Defense, "On the systemic level, the fundamental change in providing cybersecurity in Ukraine has not happened yet. We have a set of separate decisions and pending processes that are still to form a complete picture".[53] One such decision was the amendment of the Law on the Basic Principles of Ensuring Cyber Security of Ukraine with regard to "active counteraction of aggression in cyberspace" in July 2022.[54] Paragraphs were added to Article 1 mandating the following:

- "a system of active countermeasures against aggression in cyberspace"; referring to "a set of organizational, legal, scientific and technical measures aimed at increasing the level of cyber defense of the state by influencing the information and communication systems of the aggressor state, sources of origin of cyber threats and cyber-attack".
- "active countermeasures against aggression in cyberspace", referring to "actions aimed at increasing the level of cyber defense by neutralizing cyberattacks of the aggressor state, its systems and networks, as well as the sources of cyber threats and cyber-attacks that are used to harm the national security of Ukraine".

Article 8 of the law was also amended to enhance the responsibility of the State Service for Special Communications and Information Protection of Ukraine by giving it the authority to formulate and implement state policy in the field of active counteraction of aggression in cyberspace.[55] Despite the amendments, the law does not fulfil any function other than setting the frame and defining the key state institutions responsible for cybersecurity, Fedienko says.[56]

In this framework, the SSSCIPU has drafted a law "on the introduction of changes to some laws of Ukraine regarding urgent measures to strengthen capabilities for cyber protection of state information resources and objects of critical information infrastructure".[57] The draft law was introduced in the parliament in September 2022 and passed the first reading. Essentially, it seeks to establish a system of essential and concrete cybersecurity measures, such as the creation of cyber defense units in every company and institution, and to enhance the power of the SSSCIPU. The latter has led to some criticism. For instance, the Ukrainian Union of Industrialists and Entrepreneurs has objected to authorizing the SSSCIPU to carry out inspections of any enterprises regardless of the size or type of business.[58] The National Agency of Corruption Prevention has said the draft law entails corruption risks related to the "centralization" of power in cybersecurity in one institution, as it would give the SSSCIPU access to all information systems.[59] Fedienko says these criticisms have been addressed in the new draft of the law, which, at the time of writing, was ready for its second reading in the parliament.[60] Besides, following the EU granting Ukraine the status of candidate for membership, the harmonization of the country's legislation with the 2022 EU directive on "measures for a high common level of cybersecurity" is increasingly being discussed.[61] The directive provides a framework for strengthening the resilience of essential services and digital networks against cyberattacks. Given Ukraine's dependence on information and communication technologies in various sectors—including energy, healthcare, and finance—compliance with the directive is crucial to safeguarding national security and ensuring the uninterrupted functioning of critical services in the face of evolving cyber threats. Moreover, aligning with it would also facilitate international cooperation in cybersecurity efforts, which is essential for Ukraine's EU integration.

The "State in a Smartphone" During Wartime

The successful and timely transfer of government data to the cloud in early 2022 helped preserve the system of digital public services provision that has become in many cases the only alternative for citizens during the war. Ukraine having started in 2019 the ambitious reform process of digitalization of all public services—the "state in a smartphone" was Zelenskyi's slogan when he came to power—significantly facilitated this, as it had made most public documents and services accessible online and increased society's level of digital literacy. For many people fleeing the war zone, online documents were the only ones available.

The state digital service Diia has become a powerful tool to cope with new societal issues caused by the war—such as the internal displacement of people and damage to residential buildings—and thus for strengthening resilience. In the early days of the invasion, DIIA added to the functions of the application new features, including, to report the movement of Russian troops, to buying war bonds or to donate for buying drones for the armed forces, to report damage to one's house, and to apply for social aid for internally displaced people. The number of people using the Diia application rose from 14.5 million at the start of the full invasion to 18.9 million by April 2023.

According to Mstyslav Banik, head of e-services at the Ministry of Digital Transformation, "People's paradigm has changed—they now expect everything only in the application".[62] The spread of digitalization reform across the whole of the country has continued despite the war.[63]

New digital applications aimed at addressing the new reality in Ukraine continue rolling out; for example, the Air Alarm app that notifies users about air raids has become an indispensable tool for Ukrainians. The State Land Cadaster developed an automated system that enables citizens to access from remote locations essential property information such as location, area, and profile. With the extent of the actual or threat of physical destruction of residential buildings, this is of utmost importance for individuals who have invested in property and also with Ukraine's eventual rebuilding efforts in mind.

Another significant measure to strengthen Ukraine's resilience to the Russian invasion was the legalization of cryptocurrencies through the adoption in February 2022 and implementation of the Law on Virtual Assets. The law enabled the exchange of cryptocurrency in Ukraine and, crucially, its use for donations. Elliptic, a blockchain analytics company, reported that over $212 million's worth of cryptocurrency was donated to support the war effort within a year, approximately $80 million of which directly to the government.[64] This has been an effective way to quickly mobilize and send funds to addressing consequences of the war.

The Ministry of Digital Transformation has become one of the central actors in coordinating the country's cyber resistance community. Having transferred the government data to the cloud, it kept Diia running, and it has initiated most of the deals with big technology companies like Amazon, Microsoft, and Space X.

The role of civil society has also been crucial in Ukraine's cyber resilience. It has for years tried to raise awareness and strengthen society's capacities in digital and information security. Pavlo Belousov, expert of the Internews Ukraine Digital Safety School, says that the full-scale invasion transformed the perception of cybersecurity of media outlets, civil society organizations, public authorities, and the military. According to him,

> If two years ago we had to convince people that digital security is important, including the importance of passwords, and we were going to people inviting them for a training, now we don't need to convince anyone and people come to us instead. Moreover, they come with specific requests and understanding what they need because everyone understands that digital security equals physical security.

The IT Army

The IT Army of Ukraine, the country's only known cyber threat actor at the time of writing, was created in answer to a call by Mykhailo Fedorov, the minister of digital transformation, on the first day of the full invasion. It defines itself as "a worldwide IT community united to resist the Russian invasion of Ukraine".[65] At its peak, in March 2022, its Telegram channel had 307,165 users, connecting Ukrainian and foreign volunteer hackers to coordinate efforts aimed at disrupting the work of Russia's financial infrastructure, state services, and propaganda media.

The IT Army does not easily fit in any institutional category primarily because it fulfills an offensive function against Russian targets in cyberspace—something that in principle is not a part of Ukraine's official war effort, which is based on defense. In the words of one academic, "out of necessity, the IT Army subsequently evolved into a hybrid construct that is neither civilian nor military, neither public nor private, neither local nor international, and neither lawful nor unlawful".[66] The data breaches carried out by the IT Army also have the potential to support and accelerate the process of investigating Russian war crimes.

The first founding document of the IT Army established two priority targets: Russian online banking services and logistics companies.[67] Eventually, it claimed to be attacking many more important targets, including the Federal Security Service, national and regional mass media, and the public-procurement system Roseltorg. In July 2022, the Ministry of Digital Transformation reported that the IT Army had hit 6,000 targets, using predominantly DDoS attacks.[68]

Though created at the government's call, the IT Army is not part of any public institution, so its activities can be compared to those of volunteer combatants in the field. It can be joined by anyone regardless of professional background. Its targets' IP addresses and ports[69] are posted by the community administrators but can also be proposed by the community members. While it has been impossible so far to identify who are the members of this group, by analyzing the sharing of Telegram posts on proposed targets published in the IT Army channel, one expert identified the group's link with other cyber actors such as Ukrainian Reaper, KiberBull, Cyber Palyanitsa, Studentcybergroup, DDoS Attack Cyber Cossacks, Anonymous-Ukraine, DDoS joint group, and UA Cyber Shield. All these groups at some point have engaged in the IT Army operations.[70] With its grassroots-like decentralized structure, website, and Telegram channel for coordination, the IT Army is a successful example of volunteer mobilization. It has achieved many results, including shutting down the websites of the Moscow stock exchange and Sberbank (Russia's largest bank), gaining access to 6,000 files regarding Gazprom's financial and economic activities,[71] and reportedly many others, like defacing the website of Miranda Media, the Russian Internet provider in Crimea.[72]

There is no evidence that this is done in coordination with Ukrainian governmental institutions, although such cooperation would not be proscribed by law. Neither the ministry that encouraged the IT Army's creation nor any other governmental institution acknowledges any connection to it. The official government line is that Ukraine pursues a solely defensive cyber strategy. But just as it is hard to decide what is defensive in war—for example, when it comes to striking at Russian airfields from where fighter jets take off to bomb Ukraine's civilian infrastructure—it is even harder to draw such lines in the cyberspace.

Given the scale of the IT Army's cyber operations, the government's involvement is very probable but there is no clear evidence of it. According to the SSSCIPU's Viktor Zhora, "Those volunteer groups who are countering Russian aggression in a cyberspace in a counteroffensive way, in our opinion, are weakening the enemy's ability to attack us, for which we are grateful. But this activity is voluntary, it is not coordinated by the state".[73] However, one person who joined the armed forces has told about coordination with government agencies that tool place when he was acting still a volunteer hacker.[74]

International nonstate hacktivist movements also work alongside the IT Army in operations against Russia. The Belarus Cyber Partisans, for example, have claimed to have held two successful attacks: one on Belarus's national railway for transporting Russian troops and one on Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor).[75] The latter was also attacked by the international collective Anonymous, which took 360,000 files from it.[76] In July 2022, Anonymous claimed to have successfully hacked over 2,500 websites from Russia and Belarus so far.[77]

Since the intensification of kinetic warfare in the last year, the number of subscribers of the IT Army Telegram channel has significantly decreased; as of September 2023, it had 163,937 followers. Nevertheless, it still actively recruits new volunteers and Ukrainian governmental institutions such as the Ministry of Education and the Parliament encourage citizens to sign up for it.

Cyber Troops

The operations of the IT Army of Ukraine volunteers against targets in Russia technically put these actors in danger as they become participants in the war. There is no international convention that specifically regulates cyber warfare, and it is international humanitarian law that technically applies. Some experts interpret the latter to mean that the IT Army is a legitimate target for the Russian government when it targets Russian civilian infrastructure such as transport or communications companies.[78] Nonetheless, the question of the international protection of such volunteers remains open. One of the ways to grant them the same rights as military personnel during war is to recruit them in the armed forces as cyber troops. The parliamentarian Oleksandr Fedienko says that they

> should be military, should be recognized as combatants protected by international and our national legislation. Attacks on infrastructure conducted by Russians are an element of military operations. Active countermeasures to this—that is, cyber-combat—I am sure, consists in conducting similar special operations on their critical infrastructure facilities.[79]

The creation of specialized cyber troops within the armed forces is an idea that has been under consideration since 2010 but the full invasion and the fundamental transformation of the armed forces in last two years has shed new light on this issue. Officially there are still no cyber troops in the armed forces, but they exist de facto. There are some teams within the armed forces as well as in the General Directorate of Intelligence but not a separate unit under the chief of the General Staff. These cyber teams currently only work to protect the systems of the respective state institutions, rather than to serve national goals in the broader cyberspace.[80]

The state institutions responsible for cyber defense are not authorized by law to respond to Russian cyberattacks on critical infrastructure with reciprocal ones—their responsibility is only to deter, prevent, and strengthen the resistance of national information systems. At least officially, they are not threat actors and cannot carry out offensive cyber operations. However, there have been repeated media reports of successful cyberattacks. For example, in May 2023, the hacktivist group Twelve claimed responsibility for the cyberattack on the Donvard armored vehicles factory in Russia, but sources close to the General Directorate of Intelligence said it was involved.[81]

The draft law on cyber troops, which was still due to be introduced in the parliament at the time of writing, is partly inspired by the US Army Cyber Forces' Defend Forward concept. According to this, cyber troops operate in cyberspace outside of the country to strike at enemies and to neutralize risks before they appear inside the country.[82] According to Vadym Lednei, a cyber warfare specialist of the General Staff of the Armed Forces who helped write the draft law, the main functions of the cyber forces should include cyber intelligence, planning and conducting defensive and offensive cyber operations, supporting information and psychological operations in cyberspace, and organizing measures to prepare the state for cyber defense against military aggression, with coordination among executive authorities, local governments, and other defense institutions.[83]

Technology Companies

The government turned to major international technology companies such as Amazon, Google, Microsoft, and SpaceX to reinforce Ukraine's cybersecurity and critical communications infrastructure in 2022. Safeguarding from kinetic attacks government data stored on servers in Ukraine—considered high-priority targets by Russia—was a crucial challenge in maintaining the uninterrupted functioning of the government and economy. Until recently, however, storing government data outside the country's borders was illegal. This changed five days before the full-scale invasion with the adoption of the Law On Cloud Services, which enabled the transfer of government data to the cloud, including servers outside Ukraine.

Microsoft provided $107 million to shift government data as well as a significant portion of the country's computing infrastructure to the cloud.[84] Amazon transferred 10 petabytes of government data to the cloud, including bank information, land registers, and essential data from 27 ministries, 18 universities, and dozens of private companies.[85] For instance, one of Ukraine's major banks, PrivatBank, moved all of its operations to the cloud. Shortly after the full-scale invasion, Google included the websites of Ukraine's government and embassies in its project Shield,[86] which provides free protection against DDoS attacks, so that they could stay online and continue offering critical services.[87]

SpaceX enabled countrywide access to its Starlink satellite Internet service and delivered the first batch of terminals by February 28. As of January 2023, Ukraine had received 30,000 Starlink terminals, of which about 14,500 were from the Polish government, 5,000 from the US Agency for International Development, SpaceX, and donors, and 5,000 by other EU governments.[88]

Satellite Internet has become essential to provide service in most areas, especially those close to the front line and de-occupied ones, where broadband connection had been disrupted due to shelling. It has been largely used in the newly liberated territories to restore connection immediately for isolated families while the operators restore the mobile networks.[89]

As the only satellite Internet provider that could keep the Internet functioning in Ukraine in the face of Russian attacks, Starlink has become a game-changer on the battlefield too, providing Ukraine with a competitive advantage by letting it apply highly technological warfare methods alongside conventional kinetic attacks. However, depending on such critical military infrastructure that is owned by one private company already had

undesired implications for Ukraine when its owner, Elon Musk, limited Ukraine's armed forces access to the Starlink service within 100 km around occupied Crimea's coast, preventing from executing an attack on the Russian fleet in Sevastopol.[90]

Conclusion

Since 2014, Ukraine has been a testing ground for Russia's cyberattacks. These have allowed Russian actors to study and exploit vulnerabilities within the country's digital infrastructure and systems. They were able to develop and refine their cyber weaponry, gaining a significant advantage when launching the full-scale invasion. This experience underscores the critical importance of early detection and proactive responses to cyber threats, as it demonstrates the rapid evolution and adaptation of cyber tactics in modern conflicts.

Overall, Ukraine's experience in dealing with Russia's cyberattacks and the evolving nature of cyber warfare has profound implications for cybersecurity policies, international legal frameworks, and the roles of various actors in modern cyber-enabled conflicts. Adaptation and effective responses to these challenges are imperative as Ukraine and other countries navigate the complex terrain of cyberspace in an era of evolving threats and opportunities.

The ever-expanding cyber-threat landscape in the last decade was the major factor in shaping Ukraine's cyber policy. The constant barrage of cyberattacks forced the country to adopt a reactive stance, diverting valuable resources and attention from proactive policy development. Limited resources and a lack of widespread public and governmental attention to cybersecurity hindered progress in building robust cyber defenses. This struggle highlights the need for strategic planning, resource allocation, and increased public awareness to enhance Ukraine's cyber resilience.

Having to react to numerous cyberattacks, especially from state-sponsored actors, targeting critical infrastructure and government systems has necessitated the rapid development of cybersecurity capabilities to defend against these threats. As a result, Ukraine has gained valuable experience in understanding the tactics, techniques, and procedures used by cyber adversaries. This can serve as a foundation for a more proactive strategy from now on. Instead of solely focusing on defensive measures, Ukraine can use its knowledge to anticipate and preempt cyber threats. This might involve actively monitoring for emerging threats, gathering threat intelligence, and even engaging in offensive cyber operations to deter potential attackers, as the example of the US Defend Forward concept suggests. Furthermore, a proactive cyber strategy aligns with Ukraine's broader national security goals, especially in the context of Russia's hybrid warfare. By proactively addressing cyber threats, Ukraine can strengthen its deterrence posture, sending a clear message that cyberattacks will be met with robust responses. However, such a shift also requires careful consideration of legal and ethical implications, international cooperation, and the need for responsible conduct in cyberspace. Balancing proactive cyber defense with responsible behavior will be essential to ensure that Ukraine's eventual cyber troops operate within established norms and uphold international standards.

The cyber warfare between Russia and Ukraine is unique due to its scale and the diverse range of actors involved. Beyond government entities, it encompasses volunteers, hacktivists, and private companies. The involvement of major international technology companies introduces a novel and concerning dimension, granting them with a powerful position in international security while they are not subject to the mechanisms of checks and balances that governments are under. The example of Elon Musk unilaterally influencing the outcome of Ukraine's attempted operation in Crimea underscores the substantial influence that these companies can exert the course of war. Therefore, Kyiv has been looking for alternatives to Starlink for a long time. At the start of the summer of 2023, the Swedish company Satcube transfered 100 terminals to Ukraine[91] and other companies like Iridium, Globalstar, OneWeb, SES, ORBCOMM, Eutelsat, Telesat, Inmarsat, and Thuraya that provide satellite Internet services are entering the market.

Russia's full-scale invasion served as a catalyst for the swift implementation of cyber defense measures by Ukraine's government. The crisis prompted a much-needed increase in societal awareness regarding the importance of cybersecurity. Ukraine's resilience during the war can be attributed in part to its well-developed digital infrastructure and the highly digitized nature of its public services. This underscores the value of investment in cybersecurity infrastructure and public-private partnerships to ensure the ability to withstand cyberattacks.

The integration of cyber warfare into conventional military campaigns in Ukraine since January 2022 represents a groundbreaking development with lasting implications. This unprecedented hybrid conflict, unmatched in scale, is likely to persist beyond an eventual conclusion of conventional military hostilities. Russia has systematically targeted civilian infrastructure, using cyberattacks as a pivotal component of its military agenda. These actions have exposed a gap in international law, which does not effectively address such integrated tactics. There is a need to rethink the responsibility for and to introduce in international law the notions of cybercrimes and accountability mechanisms for them, which, unlike war crimes, currently do not exist. The Berkeley Human Rights Center calling on the International Criminal Court (ICC) to launch a war-crime prosecution against Russian hackers responsible for the NotPetya attack has laid the groundwork for change.[92] Having initially received limited attention, this issue gained traction when in 2022 Ukraine submitted a request to the ICC to prosecute Russian cybercrimes as war crimes. Recent statements by the ICC prosecutor indicate that such prosecutions under the court's jurisdiction are increasingly probable.[93]

Ukraine's countering of Russia's cyber warfare has established a precedent by involving civilians as participants, notably through initiatives like the IT Army. This poses multifaceted ethical, legal, and strategic challenges. It calls into question the roles and, more importantly, the rights of civilians in cyber conflicts, highlighting the need for clear international norms and regulations in this evolving domain. The participation of civilian volunteers and tech experts in cyber-defense efforts has created a new dynamic that demands careful consideration to safeguard civilian populations and ensure the responsible use of digital capabilities in warfare.

Endnotes

1 US Cybersecurity and Infrastructure Security Agency, Cyber-Attack Against Ukrainian Critical Infrastructure, July 20, 2021.
2 Khan, R. et al, Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid, 4th International Symposium for ICS & SCADA Cyber Security Research, October 2016.
3 Polityuk, P., "Ukraine to probe suspected Russian cyber-attack on grid," Reuters, December 31, 2015.
4 US Department of Justice, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, October 19, 2020.
5 Greenberg, A., "'Crash Override': The Malware That Took Down A Power Grid," Wired, June 13, 2017.
6 Dragos report, CRASHOVERRIDE: Threat to the Electric Grid Operations June 13, 2017.
7 US Cybersecurity and Infrastructure Security Agency, Alert (TA17-163A). CrashOverride Malware. July 25, 2017.
8 Greenberg, A., The Untold Story of NotPetya, the Most Devastating Cyberattack in History, Wired, August 22, 2018.
9 US Department of Justice, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, October 19, 2020.
10 Greenberg, The Untold Story of NotPetya, the Most Devastating Cyberattack in History.
11 Interview with Viktor Zhora, deputy chairman and chief digital transformation officer at the State Service of Special Communication and Information Protection of Ukraine.
12 Article 5, Law of Ukraine "On the basic principles of ensuring cyber security of Ukraine", 2017.
13 InformNapalm, #FuckResponsibleDisclosure – flashmobe of IT-professionals from UCA forces Ukrainian state institutions care about informational security, November 19, 2017. [In Ukrainian.]
14 ZN.UA, "Number of cyber crimes in Ukraine increases by 2,5 thousand a year," January 15, 2018. [In Ukrainian.]
15 Department of the Cyber Police of Ukraine, Conclusions of the year 2018 in numbers. [In Ukrainian.]
16 Interview with to Dmytro Khutkyy, European Digital Development Alliance.
17 Security Service of Ukraine, SBU: In 2019, half a thousand cyber attacks on state bodies and critical infrastructure were neutralized January 25, 2020. [In Ukrainian.]
18 Maigre, M., NATO's Role in Global Cyber Security, German Marshall Fund of the United States, April 6, 2022.
19 President of Ukraine, Decree of the President Of Ukraine No. 447/2021 On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine, August 2021.
20 National Security and Defense Council of Ukraine, Decision About the Cyber Security Strategy Implementation Plan of Ukraine from December 30, 2021, February 1, 2022. [In Ukrainian.]
21 Toler, A. and Haring, M., Russia Funds and Manages Conflict in Ukraine, Leaks Show, Atlantic Council, April 24, 2017.
22 Douzet F. et al, Measuring the Fragmentation of the Internet: The Case of the Border Gateway Protocol (BGP) During the Ukrainian Crisis, 12th International Conference on Cyber Conflict, October 2020.
23 Interview with Louis Pétiniaud, GEODE.
24 Satariano, A., "How Russia Took Over Ukraine"s Internet in Occupied Territories," The New York Times, August 9, 2022.
25 Boltryk, E. and Manzhelo A., "Ukraine ranks first in the world regarding the number of cyberattack since 14th of January 2022 – Deputy Chief of SSCIPU," Interfax Unraine, May 23, 2023. [In Ukrainian.]
26 Harding, L., "Ukraine hit by 'massive' cyber-attack on government websites," The Guardian, January 14, 2022.

27 Center of Civic Liberties, RIA NOVOSTI has clarified Russia's plans vis-à-vis Ukraine and the rest of the free world in a program like article: What Russia should do with Ukraine?, April 4, 2022. [In Ukrainian.]
28 Ibid.
29 Petrenko, I., "Analysis | The alleged mining of Ukrainian schools : what one needs to know and is it really done from Russia," Liga Life, February, February 1, 2022. [In Ukrainian.]
30 Lewandowsky, S. et al., The Debunking Handbook, 2020.
31 Huntley, S., Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape, Google, February 16, 2023.
32 The Telegraph, "Deepfake video of Volodymyr Zelensky surrendering surfaces on social media", March 17, 2022.
33 Blinken, A., "Attribution of Russia's Malicious Cyber Activity Against Ukraine", US Department of State, May 10, 2022.
34 Buniak, V., "CERT-UA registered above 300 cyberattacks in two months — SSCIPU," March 26, 2023. [In Ukrainian.]
35 Litvitska, L., "FSB collects data from Volyn residents through computer games and websites - SBU," Suspilne, April 22, 2022. [In Ukrainian.]
36 Free Speech in Wartime, Prohibition on publishing the movement of the Ukrainian Armed Forces and military aid, March 4, 2022.
37 Buniak, V., CERT-UA identified more than 300 cyber attacks in two months, — SSSCIPU. [In Ukrainian.]
38 Bezverkhyi, A., "InvisiMole Cyber Espionage Group Resurfaces to Attack Ukrainian Government Entities Via Targeted Spear Phishing: CERT-UA Warning", SOC Prime, March 22, 2022.
39 State Service of Special Communications and Information Protection of Ukraine, Russia's Cyber Tactics: Lessons Learned in 2022 — SSSCIP analytical report on the year of russia's full-scale cyberwar against Ukraine, March 2023.
40 Huntley, Fog of War.
41 State Service of Special Communications and Information Protection of Ukraine, Five hacker groups that attack Ukraine the most, April 22, 2022. [In Ukrainian.]
42 Ukrinform, Ukrainians informed about spam emails with viruses from allegedly the Chief of General Command, October 21, 2022. [In Ukrainian.]
43 CERT-UA, CERT-UA Cyberattack of UAC-0010 group (Armageddon) on state institutions of Ukraine (CERT-UA#4378), April 4, 2022. [In Ukrainian.]
44 President of Ukraine, Decree of the President Of Ukraine No. 447/2021 on the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine, August 26, 2021.
45 In Articles 361 and 361-1 of the Criminal Code, the words "electronic computing machines (computers), automated systems, computer networks or telecommunications networks" are replaced by the words "information (automated), electronic communication, information and communication systems , electronic communication networks," with the aim of bringing the terminology of the Criminal Code into compliance with the terminology of the Law on Electronic Communications and other legislation of Ukraine in the field of cybersecurity.
46 Berezyna, D., Changes for the counteraction against cyber crimes are being introduced to the criminal code, Tokar, March 22, 2022. [In Ukrainian.]
47 Interview with Viktor Zhora.
48 Huntley, Fog of War.
49 Schappert, S., Pro-Russian KillNet targets thousands with ties to NATO, CyberNews, April 21, 2023.
50 State Service of Special Communications and Information Protection of Ukraine, Russia's Cyber Tactics. [In Ukrainian.]
51 DEV.UA, «DIIA» attacked from RF, China, as well as Czechia and Uzbekistan, February 15, 2022. [In Ukrainian.]
52 Milmo, D., "China accused of cyber-attacks on Ukraine before Russian invasion," The Guardian, April 2, 2022.
53 Interview with Oleksandr Fedienko, member of the Parliamentary Committee on National Defense.
54 Verkhovna Rada, Law of Ukraine "On the introduction of changes to some laws of Ukraine on ensuring the formation and implementation of state policy in the field of active countermeasures against aggression in cyberspace", July 2022.
55 Ibid.

56 Interview with Oleksandr Fedienko.

57 Verkhovna Rada, The Law of Ukraine "On the introduction of changes to some laws of Ukraine regarding urgent measures to strengthen capabilities for cyber protection of state information resources and objects of critical information infrastructure", January 2023.

58 Economichna Pravda, "Too much power for the SSSCIPU : Ukrainian Union of Industrialists and Entrepreneurs criticised draft law 8087," July 11, 2023.

59 Prylypiv, I. "The State Service for Special Communications can be given extraordinary powers with corruption risks," Economichna Pravda, June 9, 2023.

60 Interview with Oleksandr Fedienko.

61 Official Journal of the European Union, Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2), December 27, 2022.

62 Diia.gov.ua, "Mstyslav Banik: how the attitude of Ukrainians to Diya changed during the full-scale war," April 3, 2023. [In Ukrainian.]

63 Ministry of Digital Transformation of Ukraine, Results of digital transformation in the regions of Ukraine, March 23, 2023.

64 Eliptic Connect, "Crypto Donations to Ukraine and Russia: Breaking Down the Numbers," March 3, 2023.

65 IT Army of Ukraine.

66 Soesanto, S. The IT Army of Ukraine Structure, Tasking, and Ecosystem, Center for Security Studies, ETH Zürich, June 2022.

67 Ibid.

68 Kazymyrov, M., Who and What the Ukraine IT Army is Made of? Report of Zurich Security Studies Center, DEV.UA, June 29, 2022. [In Ukrainian.]

69 The virtual points within an operating system where network connections start and end.

70 Soesanto, The IT Army of Ukraine.

71 Render-Katolik, A., The IT Army of Ukraine, Center for Strategic and International Studies, August 2023.

72 Kunder, N., "IT Army of Ukraine claims to have destroyed Russian Miranda-media!," The Tech Outlook, August 25, 2022.

73 Interview with Viktor Zhora.

74 Tidy, J., "Ukrainian cyber front. How hackers wage their war against Russia," BBC News, April 15, 2023.

75 Palczewski, S., "Year of war in Ukraine. Belarusian Cyberpartisans against Putin," Defense 24, February 24, 2023.

76 Horne, L. B. and Best, E., "Release: Roskomnadzor (820 GB)", Distributed Email of Secrets, March 10, 2022.

77 Pitrelli, M., "Hacktivist group Anonymous is using six top techniques to 'embarrass' Russia," CNBC, July 28, 2022.

78 Healey, J., and Grinberg O., "'Patriotic Hacking' Is No Exception," Lawfare, September 27, 2022.

79 Polishchuk, V., "At the time of creation of an effective system of cyber defense of the state - Oleksandr Fedienko", ArmyInform, October 21, 2022.

80 Interview with Olksandr Fedienko.

81 Bezpalko, U. and Kucheriavets, M., "GUR carried out a large-scale cyber attack on the defense plant of the Russian Federation, - sources," RBC-UKRAINE, May 30, 2023.

82 Interview with Olksandr Fedienko.

83 Global Cyber Cooperative Center, Interview with Vadym Ledney, cyber warfare specialist of the General Staff of the Armed Forces of Ukraine, January 17, 2023.

84 Gralla, P., "How Microsoft is helping Ukraine's cyberwar against Russia," Computerworld, January 24, 2023.

85 Amazon, Safeguarding Ukraine's data to preserve its present and build its future, June 9, 2022.

86 Project Shield, Protecting free expression from digital attacks, November 17, 2023.

87 Huntley, Fog of war.

88 Slovo i Dilo, Which countries and organizations have transferred Starlink terminals to Ukraine, January 16, 2023.

89 Telegram, Mykhailo Fedorov, July 9, 2022.

90 Isaacson, W., "How Am I in this War? The untold story of Elon Musk's support for Ukraine," Washington Post, September 7, 2023.

91 Dagens Nyheter, "Svenskt satellitinternet ska koppla upp Ukraina," [Swedish satellite internet will connect Ukraine] August 8, 2023.

92 Freeman L., et al, The Gravity of Russia's Cyberwar against Ukraine, OpinioJuris, April 19, 2023.

93 Geneva Internet Platform, ICC's new mandate: investigating and prosecuting cyberwar crimes, September 8, 2023.

Disclaimer

The views expressed in GMF publications and commentary are the views of the author(s) alone.

As a non-partisan and independent research institution, The German Marshall Fund of the United States is committed to research integrity and transparency.

About the Author(s)

Khrystyna Kvartsiana is a ReThink.CEE Fellow at the German Marshal Fund of the United States with expertise in digitalization, democracy, and Ukraine-EU relations, gained in Ukrainian and EU civil society organizations and think tanks. She is the Representative in Ukraine of ALDA—European Association for Local Democracy, and she works on developing multilateral decentralized cooperation between Ukrainian and EU cities. She is also a fellow of the Salzburg Global Seminar, Ukraine Forum. She holds a master's degree in sustainable development from Université Paris 1 Panthéon-Sorbonne, KU Leuven, and University of Padua, and another one in political science from Kyiv-Mohyla Academy.

About the ReThink.CEE Fellowship

As Central and Eastern Europe faces mounting challenges to its democracy, security, and prosperity, fresh intellectual and practical impulses are urgently needed in the region and in the West broadly. For this reason, GMF established the ReThink.CEE Fellowship that supports next-generation policy analysts and civic activists from this critical part of Europe. Through conducting and presenting an original piece of policy research, fellows contribute to better understanding of regional dynamics and to effective policy responses by the transatlantic community.

Cover photo credit: Ground Picture | Shutterstock

About GMF

The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of the Second World War, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.

Ankara • Belgrade • Berlin • Brussels • Bucharest

Paris • Warsaw • Washington, DC

gmfus.org