

Insights from the Ukrainian Cyber Battlefield

Is the Private Sector a Game Changer?

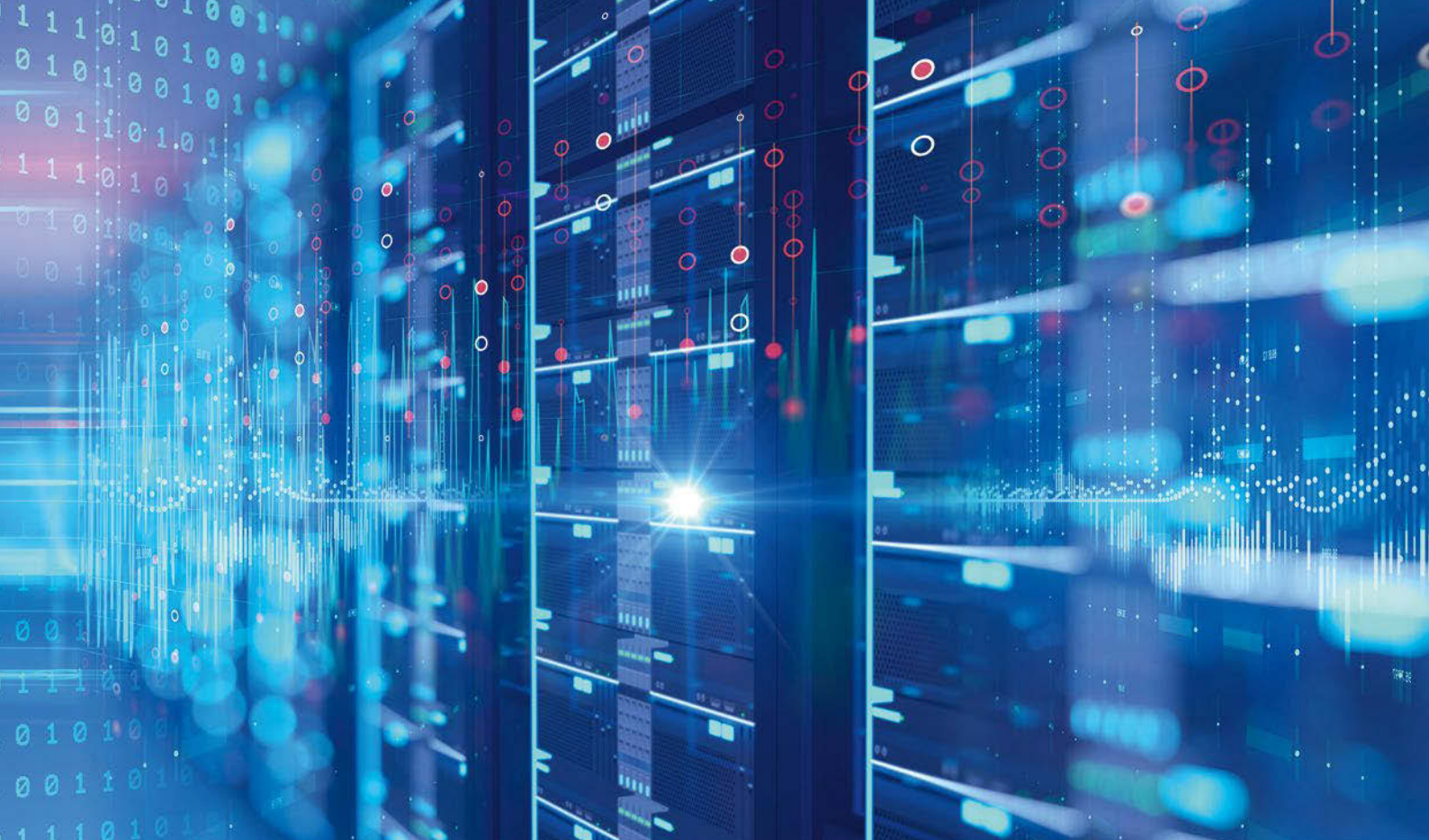
By Lieutenant Colonel Antonios Chochtoulas, GR Air Force, JAPCC

Introduction

Russia's invasion of Ukraine on 24 February shocked the entire world and created the most significant security crisis in Europe since the Second World War. Along with traditional kinetic warfare, Russia has conducted large-scale cyber operations in Ukraine before and after the invasion. Since the start of the invasion, at least six different state-linked hacker groups have conducted nearly 240 cyber operations against Ukrainian civilian and military targets. By examining Russia's cyber offensive, we can draw insights on cyber resiliency from Ukraine's response.

Malicious software combined with malicious tools and advanced hacking techniques were used against Ukraine's public infrastructure, universities, and the private sector. Advanced Persistent Threat (APT) groups linked with Russian intelligence agencies are the actors behind this ongoing campaign. A cyber-attacker is designated as an APT when it attacks a network or a system in a targeted manner over a long period of time. Typically, this actor is well trained and often linked to or even controlled by a state.

Despite its reputation in cyber warfare, Russia did not manage to deliver decisive cyber strikes against



Ukraine's Information Technology (IT) infrastructure. The attacker's methods and tools were previously effective, but this time the outcome differed from what many expected. In addition to reduced effectiveness, the volume of Russian cyberattacks was less than defence and cyber experts expected.

Ukraine's success so far in defending against Russia's cyber offensive can be attributed to three elements: the government's preparations in the years before the war, cyber defence assistance from NATO and EU countries, and the involvement of private companies like Microsoft, Amazon, and SpaceX, which offered commercial solutions like digital cloud services and Starlink which provided critical communications infrastructure.

This article is based on publicly available information. Its purpose is to present, in short, the major cyber incidents of this war and to provide insights on the Ukrainian government's successful defence, with support from foreign countries and private companies, against Russian cyberattacks. It will further identify the lessons learned and provide recommendations to NATO and non-NATO countries on how to enhance their cyber resilience.

Historical Background

Russia has systematically used cyberattacks against Ukraine. Hackers linked with Russian intelligence agencies have conducted cyber offensive operations in Ukraine at least since Russia's 2014 annexation of Crimea. Their targets included government sites, universities, power companies, the banking sector, and other critical infrastructure. In those early days, Russia aimed to cause public frustration and weaken their political adversaries in the Ukrainian political system. In some cases, the attackers deployed malicious software never used before, making Ukraine a testbed for new cyber weapons.¹

Starting in 2014, the pro-Russian hacktivist² group *CyberBerkut*, linked to the foreign military intelligence agency of the General Staff of the Russian Armed Forces, commonly known as the GRU, compromised the Ukrainian central election system by installing malware in the system to undermine trust in the election process and cause political instability.³ In addition, on the day of the elections, *CyberBerkut* launched a massive Distributed Denial-of-Service (DDoS) attack campaign to delay the final election tally and discredit the election process in the eyes of the public. The

attack was unsuccessful, as it did not delegitimize the winner. Ukrainian cybersecurity personnel removed the malware from the system on time, preventing it from releasing false results. However, the final vote tally was delayed for two hours.

'Since the start of the invasion, at least six different state-linked hacker groups have conducted nearly 240 cyber operations against Ukrainian civilian and military targets.'

In 2015, *Sandworm*, an APT group linked to the GRU, managed to conduct the first-ever publicly acknowledged cyberattack on a power grid.⁴ The attackers managed to remotely gain control of the Supervisory Control and Data Acquisition (SCADA) systems in three Ukrainian energy distribution companies and disrupt the power supply in an equal number of Western Ukraine provinces. About 225,000 people were left without electricity for up to six hours.⁵ In 2016, almost a year after the previous attack, the Ukrainian energy grid was targeted again. This time the attackers deployed the *Industroyer* malware, which became the biggest threat to industrial control systems since Stuxnet.⁶ *Industroyer* was used to remotely gain control of electricity substation switches and circuit breakers. This was accomplished by installing a backdoor into the target system that exploited the protocols used by Industrial Control Systems (ICS) throughout the critical infrastructure. This cyberattack affected a large part of Ukraine's capital and was attributed to the *Electrum* APT group, which is directly associated with *Sandworm*.⁷

The worst cyber incident in Ukraine occurred in 2017, when the Russian APT group *Telebots*, also linked to *Sandworm*, deployed the destructive *NotPetya* malware against Ukraine's financial and energy sectors. *NotPetya* took its name from its resemblance to the ransomware *Petya*, which struck in early 2016 and extorted victims for the key to unlock their files. This time, *NotPetya*, regardless of whether the victim paid,

sabotaged 10 % of the computers in Ukraine so they could not boot.⁸ It spread all over Ukraine's financial sector through a popular tax preparation program. Although the attack targeted companies inside Ukraine, the malware got out of control and affected multinational companies across Europe and the United States (US). The exact impact on the Ukrainian economy is unclear, but the estimated global economic losses exceeded \$10 billion.⁹

The day before Russia's invasion, a massive cyberattack using the *HermeticWiper* malware was launched on Ukraine's government machines and the financial, aviation, IT, and energy sectors.¹⁰ Although there is no hard evidence connecting the orchestrators of this attack to Russia, the timing and methodology used strongly suggest it. The next day, within hours of the invasion, another significant cyberattack took place against the Viasat's KA-SAT network, widely used by the Ukrainian military and police.¹¹ The attack combined DDoS attacks with the *AcidRain* malware, which was specially designed against telecommunication equipment. As a result, most Viasat modems were inoperable and the broadband internet service for hundreds of thousands of Ukrainians and the military was disrupted. A side effect of this attack was that *AcidRain* crossed borders and impacted other European countries, as in the *NotPetya* case.¹²

The following major incident was recorded in April 2022, when Ukraine's energy infrastructure was attacked by the *Industroyer2* malware, the successor of *Industroyer*, specifically targeting high-voltage electrical substations.¹³ The *CaddyWiper* malware was also deployed along with *Industroyer2* to delete the traces of the attack. Notably, unlike its predecessor, *Industroyer2* was used as a stand-alone weapon, requiring no intervention from a remote-stationed operator. This is a significant upgrade because such a weapon could be implanted in a corporate network and stay idle, waiting for the right time to attack. Such behaviour complicates the cyber defenders' role in preventing an attack. This attack appears to be the work of *Sandworm*, which also delivered the 2016 *Industroyer* attack, but this time no power outages were reported. The successful outcome was

due to the immediate response of Ukraine's cyber defence authorities, who have gained significant experience in recent years, and the assistance from Microsoft and ESET.¹⁴

Collaboration with the Private Sector

The Ukrainian government and armed forces overcame the initial shock of the invasion and successfully addressed these non-kinetic attacks. Ukraine's Computer Emergency Response Team (CERT-UA) worked with private companies to minimize the effects of Russia's cyber offensive and keep all the critical systems running with minimal interruption. A week



before the invasion, when war seemed imminent, the Ukrainian government got worried about the security of their data and searched for ways to protect it. Until then, Ukrainian law required particular government and public sector data to be stored on servers physically located in the country. The government changed the law, allowing sensitive government and private sector data to be transferred to cloud servers outside the country.¹⁵ Next, under pressure from the events, the Ukrainian government made a public call for help. Amazon Web Services and Microsoft, the world's biggest cloud service providers, were among the first companies to respond to that call.

In the following days and weeks, these companies provided help, support, and the means (IT equipment and data centres outside Ukraine) for data migration from across all sectors of Ukraine. Thus, vast amounts of data were moved to the cloud. Most Ukrainian ministries, universities, and private companies have benefitted from this collaboration.¹⁶ In effect, Ukraine traded data sovereignty for improved cyber defence against Russian kinetic and non-kinetic attacks. Due to this strategy, not only was the Ukrainian government able to function properly through today, but the population was able to continue a relatively normal online life during the war: banks remained open, universities could still provide education, most public services were available, etc. All of these significantly impacted the nation's morale and certainly helped sustain Ukraine's resistance to the invasion.


Another interesting aspect was the cooperation of CERT-UA with private cybersecurity companies to monitor and identify potential cyberattacks. Even before the 2022 *Industroyer2* attack, researchers from Microsoft¹⁷ and ESET¹⁸ were remotely monitoring the networks in Ukraine and performing real-time data

analysis to identify potential malicious activity. In addition, during Ukraine's cyber operations the first confirmed utilization of Artificial Intelligence (AI) was recorded. According to Microsoft president Brad Smith, Ukraine successfully used AI to detect, identify, and defeat a Russian cyberattack without human intervention.¹⁹ This has definitely contributed to the Ukrainian success.

Resilient and secure communications are essential for any military operation. After the cyberattack against Viasat's satellite communications infrastructure the Ukrainian military was left without satellite communications. This situation undermined the country's entire defence. The gap was quickly filled by another US private company, SpaceX, which offered Ukraine free access to its Starlink satellite internet services. Ukraine quickly adopted the service as a replacement for the compromised government military communications system, which has proven extremely useful and successful. The system has also proven its resilience against signal jamming, as SpaceX's CEO Elon Musk stated recently.²⁰

Considerations

The lack of verifiable information about successful Russian cyberattacks during the war complicates



the picture. Ukraine is likely not publicly revealing the full extent of the impacts of Russian cyber offensives on its infrastructure, lest Russia has a clear picture of the efficiency of its cyber operations. Nevertheless, the last Russian drone campaign from October against the Ukrainian energy infrastructure may signify that Russia could not use a cyberattack towards that goal. On the other hand, Russia might be keeping some of its cyber capabilities in reserve for future operations or is already working on a new yet undisclosed cyber offensive. In either case, Ukraine's years of preparation seem to have paid off.

Data is at the core of the information age, and events like the 2017 *NotPetya* cyberattack have shown that cyberspace does not have ordinary borders. Collateral damage from cyberattacks can occur far beyond the original target.

Malicious software might quickly spread across countries and affect government and business data worldwide. The public and private sectors cannot overlook the potential damage of such a crisis. New strategies that could enhance resilience against such attacks must be implemented. As the Ukrainian example shows, the benefits of data migration to out-of-country clouds may overcome disadvantages such as loss of data sovereignty and may be a solution. Another consideration is that big

corporate data centres that provide cloud services are more difficult for APT groups to compromise than local ones.

The Alliance is confronted by cyber, space, hybrid, and other asymmetric threats and the malicious use of Emerging and Disruptive Technologies (EDT).²¹ EDTs, such as AI and space-based broadband internet services, are not only expected to be game changers in future warfare but have already been tested and proved on the battlefield. Global competition becomes more intense as EDTs change the character of conflict and acquire strategic importance. However, notwithstanding the opportunities brought to the fore by EDTs, they also threaten the Alliance. By leveraging emerging technologies, adversaries could achieve technological primacy and, through that, influence the outcome on the battlefield.

Conclusion

Following the 2022 NATO Madrid Summit, the Alliance decided to use national assets to build and exercise a rapid response cyber capability to respond in the event of a significant cyberattack. Building on the lessons learned from the war in Ukraine, the Alliance should develop new capabilities in the fields of data storage and cyber resilience. Such developments could only happen with the collaboration of the private sector, and the EU and other political entities could participate and benefit too. Data migration should also be considered for the military domains, although most military data and communications are classified. In the future, quantum cryptography could allow the exchange of classified data in a military cloud that could be geographically distributed across allied countries' data centres.

On the other hand, as private companies become part of the conflict, nations should take the proper measures to protect them in cyberspace. National authorities should provide the proper framework for cybersecurity cooperation with the private sector and work closely to address cyberattacks effectively. Furthermore, national laws and policies should increase resources to investigate, disrupt, and prosecute malicious cyber activity, and impose higher penalties for cybercrime and insider enablers. Nations should also leverage diplomatic and economic tools against nations that provide cover for malicious cyber actors. Nations should also dedicate additional funding and set higher standards for strengthening SCADA and other vulnerable industry systems against cyber threats.

The Alliance continues to face distinct threats from all strategic directions and must adapt to the evolving threats in cyberspace. NATO and its allies require strong and resilient cyber defence to fulfil their core tasks of deterrence and defence, crisis prevention and management, and cooperative security.²² As Ukraine's cyber defence shows, collaboration with the private sector is a proven method to defend our networks and operations against adversaries indiscriminately wielding sophisticated cyber weapons. Having in mind that 'resilience is a national responsibility and a collective commitment', we should enhance the Alliance's cyber resilience through nationally-developed goals and capabilities to achieve Alliance's objectives.²³ ●

1. <https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/> (accessed 18 October 2022).
2. Derived from combining the words 'Hack' and 'Activism', hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes.
3. <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> (accessed 18 October 2022).
4. <https://www.cisa.gov/uscert/ncas/alerts/aa22-110a> (accessed 20 October 2022).
5. Whitehead, D.E. et al., 'Ukraine cyber-induced power outage: Analysis and practical mitigation strategies', 70th Annual Conference for Protective Relay Engineers (CPRE), 2017, pp. 1–8.
6. <https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/> (accessed 19 October 2022).
7. <https://www.gov.uk/government/news/uk-exposes-series-of-russian-cyber-attacks-against-olympic-and-paralympic-games> (accessed 31 October 2022).
8. https://www.eset.com/us/about/newsroom/corporate-blog/petya-ransomware-what-we-know-now/?utm_source=welivesecurity.com&utm_medium=referral&utm_campaign=autotagging&utm_content=ukraine-crisis-digital-security-resource-center&utm_term=en (accessed 1 November 2022).
9. Greenberg, A., 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', *Wired*, 22 August 2018.
10. [https://cyberlaw.ccdcoe.org/wiki/HermeticWiper_malware_attack_\(2022\)](https://cyberlaw.ccdcoe.org/wiki/HermeticWiper_malware_attack_(2022)) (accessed 4 November 2022).
11. <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview> (accessed 4 November 2022).
12. <https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/> (accessed 7 November 2022).
13. <https://cert.gov.ua/article/39518> (accessed 7 November 2022).
14. <https://cip.gov.ua/en/news/viktor-zhora-vzyav-uchast-u-profilnii-konferenciyi-z-kiberbezpeki-black-hat-usa-2022-u-las-vegasi> (accessed 15 November 2022).
15. <https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future> (accessed 10 October 2022).
16. <https://www.infosecurity-magazine.com/interviews/interview-microsoft-migrating-data/> (accessed 10 October 2022).
17. 'Defending Ukraine: Early Lessons from the Cyber War', Microsoft, 2022.
18. ESET Threat Report, T1, 2022.
19. <https://www.ekathimerini.com/opinion/interviews/1197775/building-defenses-for-cyberwarfare/> (accessed 14 November 2022).
20. <https://spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites/> (accessed 4 November 2022).
21. Madrid Summit Declaration, NATO, 2022.
22. NATO, Cyber defence. https://www.nato.int/cps/en/natohq/topics_78170.htm (accessed 17 November 2022).
23. NATO 2022 Strategic Concept. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-factsheet-strategic-concept-en.pdf (accessed 17 November 2022).

Lieutenant Colonel Antonios Chochtoulas

graduated from the Hellenic Air Force (HAF) Academy in 1999. He holds a Master of Science in Computer Science, and his subject matter expertise is Cybersecurity and Systems Administration. He initially served as a programmer and, after that, as a Database and System Administrator of HAF's proprietary Logistics Information System. Throughout his career in HAF, he was involved in several Cybersecurity projects and participated in Cyber military exercises. Currently, he is the Cyberspace SME at the JAPCC.

