II. Space attacks and cyberattacks in Ukraine

NIVEDITA RAJU AND LORA SAALMAN

Ukraine became the front line of a range of attacks against space systems and cyberattacks, following the Russian invasion in February 2022. Space systems were the targets of both electronic attacks and cyberattacks.[1] One such cyberattack had significant impact as tens of thousands of internet customers across Europe, including emergency services in France and wind turbines in Germany, were unable to communicate. It was reported that 'more than 40 per cent of the destructive cyberattacks [involving Ukraine] were aimed at organizations in critical infrastructure sectors that could have negative second-order effects on the government, military, economy, and people'.[2] With some of the attacks blurring the line between cybercrime and cyberwarfare and impacting both military and civilian sectors across state borders, the war in Ukraine underscores the issues that must be addressed by international space and cyber governance.[3]

This section reviews attacks on space assets and cyberattacks that targeted Ukraine in 2022. It looks at cyberattacks on, in turn, space assets, government and finance institutions, telecommunications networks and power facilities.[4]

Cyberattacks on space assets

Coinciding with the early hours of the invasion of Ukraine on 24 February 2022, a cyberattack targeted a single consumer-oriented partition of the KA-SAT satellite broadband network, which is operated by Skylogic, a subsidiary of French satellite operator Eutelsat, on behalf of the US satellite communications company Viasat.[5] During the distributed-denial-of-service (DDoS) attack, high volumes of focused, malicious traffic were detected emanating from several modems and other customer equipment physically located within Ukraine.

[1] On electronic attacks (e.g. signals jamming of space assets), which are not discussed here, see e.g. EU Aviation Safety Agency (EASA), 'Global navigation satellite system outage leading to navigation/surveillance degradation', Safety Information Bulletin no 2022-02R1, 17 Mar. 2022; and Nilsen, T., 'More Russian GPS jamming than ever across border to Norway', *Barents Observer*, 9 July 2022.

[2] Microsoft, Digital Security Unit, 'Special report: Ukraine—An overview of Russia's cyberattack activity in Ukraine', 27 Apr. 2022, p. 4.

[3] While there is no universally accepted definition of cyberwarfare or cybercrime, the United Nations Office on Drugs and Crime (UNODC) defines cyberwarfare as 'cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack' and cybercrime as an 'act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime'. UNODC, 'Cyberwarfare'; and UNODC, 'Cybercrime in brief'.

[4] On other aspects of the war in Ukraine see chapter 1, section V, chapter 2, section I, chapter 5, section I, chapter 8, section V, chapter 10, section I, and chapter 12, section III, in this volume.

[5] Viasat, 'KA-SAT network cyber attack overview', 30 Mar. 2022.

The impact across Europe was significant. While this cyberattack was almost certainly designed to disrupt the Ukrainian military's satellite communications, it also caused far-reaching civilian disruptions. Viasat reported that the cyberattack had an impact on 'several thousand customers located in Ukraine and tens of thousands of other fixed broadband customers across Europe'.[6] It disrupted emergency services in France and interrupted remote monitoring and control of 5800 wind turbines in Germany.[7] Victor Zhora, deputy head of the Ukrainian State Service of Special Communications and Information Protection (SSSCIP), confirmed that the attack targeted Ukraine's satellite communications and suggested that it 'partially succeeded'.[8] While Russia did not claim responsibility for the attack, several states, including member states of the European Union (EU), the United Kingdom and the United States, attributed the attack to Russia.[9]

The vectors of the cyberattack remain in dispute. Viasat contends that the malware executed 'legitimate, targeted management commands' and 'overwrote key data in flash memory on the modems, rendering the modems unable to access the network, but not permanently unusable'.[10] In contrast, Sentinel Lab researchers suggest that the cyberattack used the KA-SAT management mechanism in a supply chain attack to push the AcidRain wiper, which is designed to overwrite key data in a modem's flash memory, rendering it inoperable.[11] They noted AcidRain wiper's developmental similarities to VPNFilter malware, which was previously attributed to Russia's Sofacy Group—also known as Advanced Persistent Threat (APT) 28, Sandworm (see below), Strontium, X-Agent, Pawn Storm, Fancy Bear and Sednit.[12] Their findings suggest that, rather than the attacks temporarily disabling these systems (as Viasat suggested), they were destructive and likely to have Russian sources.

[6] Viasat (note 5).

[7] French National Assembly, National Defence and Armed Forces Committee, 'Compte rendu: Audition, à huis clos, de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale' [Report: Closed doors hearing of Mr Stéphane Bouillon, secretary-general for defence and national security], Report no. 5, Extraordinary session of 2021–22, 13 July 2022; and Enercon, 'Over 95 per cent of WECs back online following disruption to satellite communication', 19 Apr. 2022.

[8] Victor Zhora (@VZhora), Twitter, 10 May 2022, <https://twitter.com/VZhora/status/1524080689452359680>.

[9] Council of the European Union, 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', Press release, 10 May 2022; British Foreign, Commonwealth and Development Office, 'Russia behind cyberattack with Europe-wide impact an hour before Ukraine invasion', Press release, 10 May 2022; and Blinken, A. J., US secretary of state, 'Attribution of Russia's malicious cyber activity against Ukraine', Press statement, US Department of State, 10 May 2022.

[10] Viasat (note 5).

[11] Guerrero-Saade, J. A. and van Amerongen, M., 'AcidRain—A modem wiper rains down on Europe', Sentinel Labs, 31 May 2022.

[12] US Department of Justice, 'Justice Department announces actions to disrupt Advanced Persistent Threat 28 botnet of infected routers and network storage devices', 23 May 2018. On other activities connected with Strontium see section IV in this chapter.

Cyberattacks on government and industry

Even prior to Russia's invasion of Ukraine, in January 2022 Microsoft identified a destructive malware operation, known as WhisperGate, aimed at multiple organizations in Ukraine.[13] These wiper attacks masqueraded as ransomware, threatening to encrypt the master boot record (MBR)—the first sector on a hard drive containing code necessary to start the operating system—unless a ransom were paid. However, multiple forensic laboratories determined that the intended aim was to destroy the MBR.[14] By 15 February, while Russian troops were massing at the Ukrainian border, DDoS attacks affected the Ukrainian Ministry of Defence and armed forces, with further DDoS attacks targeting the websites of two banks, Privatbank and Oschadbank.[15]

Several hours before the launch of the invasion on 24 February, offensive and destructive cyberattacks were directed against Ukraine's digital infrastructure. Notable among these was FoxBlade—also known as Hermetic Wiper and with alleged links to Russian military intelligence (see below)—which, like the WhisperGate wiper, served as decoy ransomware.[16] It destroyed systems and information across more than 12 organizations in the governmental, ICT, energy, agricultural and financial sectors in Ukraine, and also appeared in Latvia and Lithuania.[17]

The vectors of cyber intrusion and attack expanded even further in March 2022, when an open-source backdoor named GoMet affected a large software-development company whose software is used in various Ukrainian state organizations.[18] This suggests a supply chain attack in which systems are compromised through a third-party service provider.

By August 2022, cyber intrusions shifted again, towards data exfiltration. Ukrainian government agencies were infected by a phishing campaign—a form of 'social engineering' in which the targets are deceived into revealing sensitive information or installing malware—allegedly conducted through

[13] 'Destructive malware targeting Ukrainian organizations', Microsoft Security Blog, 15 Jan. 2022.

[14] Mandiant, 'Evacuation and humanitarian documents used to spear phish Ukrainian entities', 20 July 2022; and Microsoft, 'Special report' (note 2).

[15] Ukrainian State Service of Special Communications and Information Protection (SSSCIP), 'Cyberattacks on the sites of military structures and state banks', 15 Feb. 2022.

[16] Constantinescu, V., 'New FoxBlade malware hit Ukraine hours before invasion, Microsoft says', BitDefender Blog, 1 Mar. 2022; Microsoft Security Intelligence, 'DoS:Win32/FoxBlade.A!dha', 23 Feb. 2022; and Guerrero-Saade, J. A., 'HermeticWiper—New destructive malware used in cyber attacks on Ukraine', Sentinel Labs, 23 Feb. 2022.

[17] Microsoft, 'Special report' (note 2); and Uchill, J., 'Ransomware may have been a decoy to launch new wiper malware seen in Ukraine cyberattacks', SC Media, 24 Feb. 2022.

[18] Schultz, J., 'Attackers target Ukraine using GoMet backdoor', Talos Threat Spotlight Blog, 21 July 2022.

Gamaredon (also known as Actinium), an APT linked to the Russian Federal Security Service (Federal'naya Sluzhba Bezopasnosti, FSB).[19]

In October 2022, Prestige ransomware targeted organizations in the transportation and logistics industries in both Ukraine and Poland.[20] This laid the foundations for these key economic sectors to be degraded by the Iridium group, which is allegedly connected to the Sandworm hacking unit (Unit 74455) of Russia's military intelligence agency, the Main Directorate of the General Staff of the Armed Forces (Glavnoe Razvedyvatel'noe Upravlenie, GRU).[21] This unit is also thought to be linked to the deployment of the wipers FoxBlade, CaddyWiper and Industroyer2 in Ukraine.[22]

Cyberattacks on telecommunications

From February 2022 Kyivstar, a Ukrainian ICT operator which provides mobile service to almost 26 million people, highlighted its fight against a barrage of cyberattacks and physical attacks (including missile strikes) that destroyed almost 10 per cent of its base stations.[23] Notably, this combination of attacks coincided with Russian efforts to divert internet traffic in occupied parts of Ukraine through its own networks.[24] This meant that Russian authorities could monitor, exfiltrate and manipulate data in Ukraine.[25] Kyivstar alleged that phishing attacks tripled, combined with a doubling of DDoS attacks aimed at overwhelming company websites with online traffic, attempted exfiltration of data on phone calls and cyber intrusions into third parties to gain access to Kyivstar networks.[26]

By March 2022 cyberattacks on telecommunications firms again grew in scope as Ukrtelecom, an internet service provider, was the target of a 'massive cyberattack'.[27] Connectivity collapsed to 13 per cent of pre-conflict levels. While Ukrtelecom resumed some service on the day of the attack, it emphasized that, 'to continue providing services to Ukraine's Armed Forces and other military formations as well as to the customers', it had limited

[19] Malhotra, A. and Venere, G., 'Gamaredon APT targets Ukrainian government agencies in new campaign', Talos Threat Spotlight Blog, 15 Sep. 2022; and Mandiant (note 14).

[20] Microsoft, 'New "Prestige" ransomware impacts organizations in Ukraine and Poland', 14 Oct. 2022.

[21] Microsoft, 'Special report' (note 2).

[22] On Sandworm see e.g. Holt, R., 'Sandworm: A tale of disruption told anew', WeLiveSecurity by ESET, 21 Mar. 2022; and US Cybersecurity and Infrastructure Security Agency, 'New Sandworm malware Cyclops Blink replaces VPNFilter', Alert no. AA22-054A, 23 Feb. 2022.

[23] Satariano, A., 'How Russia took over Ukraine's internet in occupied territories', *New York Times*, 9 Aug. 2022; and Bergengruen, V., 'The battle for control over Ukraine's internet', *Time*, 18 Aug. 2022.

[24] On the alleged coordination between cyberattacks and physical attacks see Khmelova, I., *Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions* (SSSCIP: Kyiv, 2022).

[25] Satariano (note 23).

[26] Miller, M., 'Ukraine's largest telecom stands against Russian cyberattacks', Politico, 7 Sep. 2022.

[27] Condon, S., '"Massive cyberattack" against Ukrainian ISP has been neutralized, Ukraine says', ZDNet, 28 Mar. 2022.

services to the 'majority of private users and business-clients', indicating the toll on civilian users.[28] In this ongoing compromise of telecommunications firms, in June 2022 the SSSCIP's Computer Emergency Response Team of Ukraine (CERT-UA) warned of emails containing a document file that would load a DarkCrystal remote-access trojan that again targeted Ukrainian telecommunications operators and service providers.[29]

Cyberattacks on power facilities

In April 2022 CERT-UA worked with ESET, a Slovakia-based international cybersecurity company, to analyse an intended cyberattack against Ukrainian high-voltage electrical substations that some have attributed to Sandworm.[30] The cyber intrusion, which occurred in February with an intended deployment date in April, employed malware against industrial control systems (ICSs), which monitor, control and regulate automated processes of industrial systems. Forensics revealed this malware—named Industroyer2—to be an updated version of the Industroyer malware used in 2016 to sever power supplies in Ukraine, also allegedly linked to Sandworm.[31] The Industroyer2 cyberattack allegedly used other destructive malware, including CaddyWiper, OrcShred, SoloShred and AwfulShred. While this particular cyberattack failed, it suggested the potential for similar future attacks on critical infrastructure and power supply.

Farid Safarov, a Ukrainian deputy minister of energy, attributed the attempted cyberattack to Russia, alleging that it sought to prevent Ukraine connecting to the 'Pan European electrical grid'.[32] Pointing to the humanitarian costs of such an outage, Zhora of the SSSCIP emphasized that the attack was intended to harm civilian targets: 'It was supposed to start working in a way to cause electricity outages [in] a number of areas in Ukraine that [would] deprive the civil population of electricity and I stress the point that this civil infrastructure was targeted to disrupt electricity supply.'[33] Further, in the weeks that followed, Russian hackers allegedly broke into a Ukrainian power company and temporarily shut down nine electricity substations,

[28] Condon (note 27).

[29] SSSCIP, 'Hackers attack Ukrainian telecom operators and service providers', 25 June 2022.

[30] ESET Research, 'Industroyer2: Industroyer reloaded', WeLiveSecurity by ESET, 12 Apr. 2022.

[31] US Department of Justice, Office of Public Affairs, 'Six Russian GRU officers charged in connection with worldwide deployment of destructive malware and other disruptive actions in cyberspace', Press release, 19 Oct. 2020.

[32] Uchill, J., '"The criminals are guided by the Russian Federation": Ukraine responds to Industroyer2', SC Media, 12 Apr. 2022. See also Blaustein, A., 'How Ukraine unplugged from Russia and joined Europe's power grid with unprecedented speed', *Scientific American*, 23 Mar. 2022.

[33] Uchill, '"The criminals are guided by the Russian Federation"' (note 32).

according to a non-public document reportedly shared with *MIT Technology Review*.[34]

Conclusions

The sustained attacks on ICT systems and critical infrastructure in Ukraine—which also affected users across Europe—highlight both the cyber and physical costs of such attacks on the civilian population, possibly in breach of international humanitarian law. Further, the confluence of these various cyber intrusions and attacks demonstrate that destructive impacts crossed national and industry borders, military and civilian sectors, and—in the form of wipers masquerading as ransomware—technological boundaries. Such attacks also evidence the convergence of cybercrime tactics and cyberwarfare aims. These trends indicate an urgent need to advance governance in both the space and cyber domains, discussed in sections III and IV, respectively.

[34] O'Neill, P. H., 'Russian hackers tried to bring down Ukraine's power grid to help the invasion', *MIT Technology Review*, 12 Apr. 2022.