European Repository of Cyber Incidents

Major Cyber Incidents

KA-SAT 9A

Other incident names: Viasat, AcidRain

Description

The GEO satellite broadband services of the US communications company Viasat (KA-SAT 9A network) were disrupted in parts of Europe when the Russian military offensive against Ukraine commenced in February 2022. While the attack caused widespread disruptions to Ukrainian satellite-based communications in the early hours of the Russian invasion on 24 February 2022, it also affected the KA-SAT networks in large parts of Western Europe. The threat intelligence company SentinelOne found some "non-trivial developmental similarities" between components of AcidRain and the VPNFilter malware. This malware is widely acknowledged as being deployed by the Russian APT Sandworm, which is affiliated with the Russian military intelligence agency GRU; however, SentinelOne refrained from explicitly attributing AcidRain to Sandworm. On a political level, several governments supported the generic attribution of the KA-SAT hack to Russia, referring to US and UK intelligence findings published on 10 May 2023. So far, the Viasat incident is widely viewed as the most disruptive cyber operation of the Russian war against Ukraine, although it is understood to have had a limited impact on the conventional military campaign.

Timeframe
24 February to 15 March 2022

Initiator
Russian Military Intelligence: GRU
(likely Sandworm)

Incident Type
Wiper: Disruption, Hijacking with Misuse

Affected Target
Telecommunications infrastructure (Satellite Internet) in Ukraine and wide swaths of Europe

Background

The attack occurred concurrent with the onset of the Russian military offensive against Ukraine, which included a series of cyberattacks. Marking the culmination of the years-long Russian aggression against Ukraine, the Russian ground offensive advanced from four different directions in the early morning of 24 February 2022. This ground offensive was supported by missiles, rockets, and artillery fire against Ukrainian towns and infrastructure. At the time, computer network exploitation ("cyber espionage") and digital attacks against Ukrainian civilian, military, and critical infrastructure targets had been intensifying since late 2021. [1]

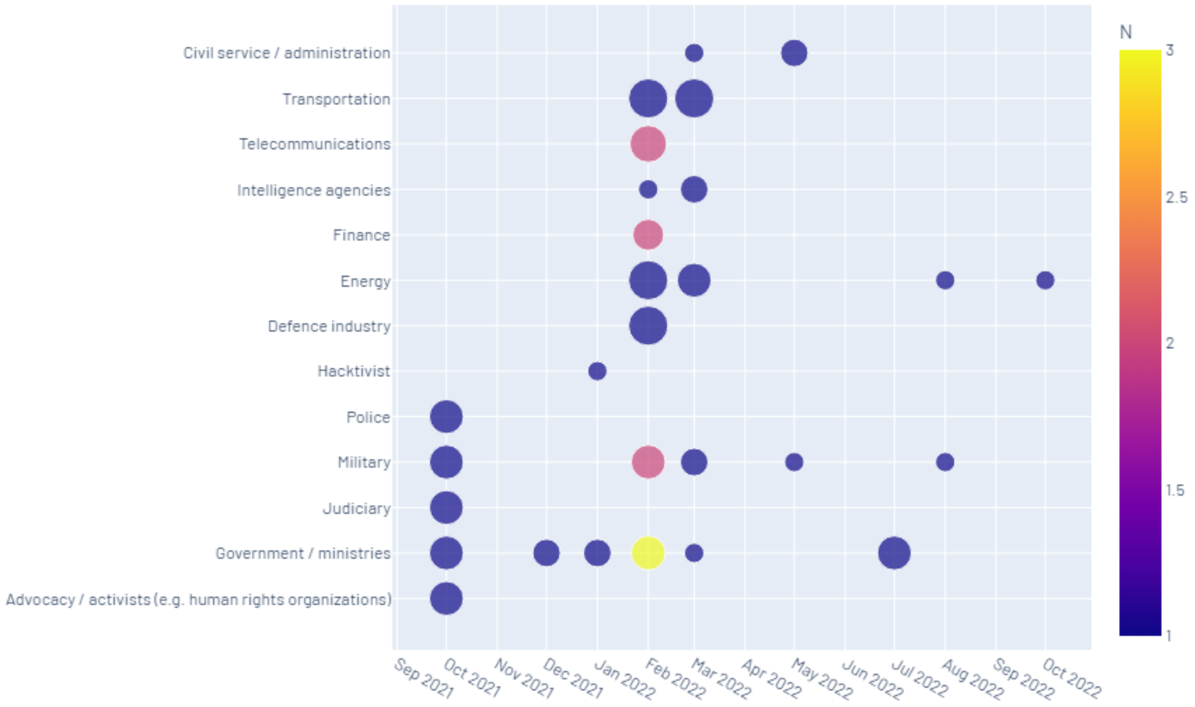
By Mika Kerttunen, Kim N. Schuck, and Jonas Hemmelskamp

Impact and significance

The KA-SAT hack mainly affected user modems belonging to the European satellite network EUTELSAT located on Ukrainian and Western European territory. In addition, the remote communications of around 5,800 wind turbines from German turbine manufacturer Enercon were also affected, with the connection being interrupted but the turbines continuing to function. [2] As a result, 30,000 new modems had to be shipped out to stabilise the Enercon system on a large scale, and replacements had to be made on-site. [3]

Notably, both the Ukrainian military and police used the affected modems. They were likely required for the normal functioning of smart weapons systems and in combined-arms manoeuvres of Ukrainian armed forces, which increasingly rely on internet connections. [4] Thus, although the attack on the KA-SAT satellite ground infrastructure of modems and routers was successful and has been assigned the highest intensity in the EuRepoC database (4 out of 15), we find, based on public reporting, that its military operational significance was limited.

Fig. 1: Cyber Incidents with coded receiver sector originating from Russia and targeting Ukraine since November 2021*, differentiated by targeted sector (N = 28)



Note: The size of the circles displays the mean intensity of incidents for each sector and month, while the colour indicates the number of incidents. The sample includes incidents in the EuRepoC database that originated in Russia and targeted Ukraine, with a sector coded for receivers. Incidents are displayed multiple times if they affected more than one target. | * according to incident start date.

According to reports, the hack may have been aimed solely at disrupting or even eliminating Ukrainian military communications during the Russian invasion. Further spill-over effects may have been unintentional. Initially, this attack was seen as a major disadvantage for the Ukrainian defence during the Russian offensive, especially when viewed against the background of the potential Ukrainian advantage gained through military coordination using intelligent satellite systems, and was thus widely reported in the media. Varying statements by Viktor Zhora, Deputy Chairman and Chief Digital Transformation Officer of the State Service of Special Communications and Information Protections of Ukraine, led to confusion; after stating at a press conference in early May that the Visat event had caused a "really huge loss in communications in the very beginning of war," he clarified this in an interview with the journalist Kim Zetter in September 2022, stating that it "did not" have a huge impact on Ukrainian military communications. [5]

In retrospect, one can see that the hack had limited impact on military and police forces' communications as they could primarily use analogue landlines, with digitally-based communications acting as an additional channel. [5] Therefore, Ukrainian political leadership, its military intelligence, and command-and-control communications were able to maintain functionality through terrestrial (landline and radio) communications. Ukrainian authorities were also able to restore satellite and internet connectivity within two days. [5]

Despite its limited military impact, following the attack, the Ukrainian Vice Prime Minister and Minister of Digital Transformation, Mykhailo Fedorov, requested assistance from Elon Musk via Twitter. This request was granted and resulted in Elon Musk's Starlink company providing satellite-based internet connectivity to Ukraine. [6] By providing seamless high-speed Internet coverage, Starlink ensured Ukraine not only stable civilian Internet access, but ultimately a crucial military gain. The precise drone strikes on Russian targets that followed, as well as the synchronisation of Ukrainian forces' speed and movements, were only made possible by Starlink LEO satellites providing a fast data flow. Even though Musk, meanwhile, has restricted the use of satellite Internet for Ukrainian military benefits, this nevertheless highlights the accompanying challenges of increasing commercial (space) involvement during times of high-intensity conflicts. Questions remain open about the militarisation of such commercial services without mandates from governments' defence departments, and thus whether they could be recognised as legitimate military targets. [35]

The Bigger Picture I: Militarisation of Space

Starting in the 1930s, the development of rocket systems by Nazi Germany foreshadowed military ambitions for space. [7] During the Cold War and the after the launch of the first satellite into orbit, military space systems were developed for the first time, which today are used by a steadily-increasing number of states to support terrestrial military operations. [8] In this context, the militarisation of space describes an intentional use of space technologies for military purposes. [9] With the development of new satellite systems for weather observation, reconnaissance, communication, and navigation, the support for their use in military contexts has progressed, thus increasing the significance of security policies. [8] [10] With digitisation speeding up, the previously-conventional kinetic militarisation of space has evolved into a non-kinetic and non-electronic means of interfering with satellites from Earth, primarily in order to disrupt downlink or uplink communications.

The Bigger Picture II: Weapons and Targets of Post-Modern Warfare

Attacking military and high-level civilian command-and-communication systems is a common feature of warfare. The explicit doctrinal foundations of command-and-control warfare (C2W) can be traced to the US' strategic thinking in the late 1980s and early 1990s, which focused on causing operational paralysis. [13] The ability to act independently or in a coordinated manner alongside fire and manoeuvre operations to cause such effects through cyberspace constitutes the anticipated core utility of military-cyber capabilities. [14]

The significance of the Viasat attack must be evaluated against the totality of Russian and Ukrainian dependencies, objectives, and activities in late February 2022. The attack can be considered successful in a technical sense if causing some form of disruption to the targeted systems was the goal. Similarly successful was the Ukrainian government's countermove to replace one satellite communication channel with another, enabling the government and military leadership to continue command and communications through satellites. On the other hand, instead of being perceived as the *main* Russian cyber-kinetic, C2W, or information warfare vector, the KA-SAT/Viasat attack could have been a supporting attack; an attempt to simply force the Ukrainian leadership to rely more on landline communications, which, according to Viktor Zhora, was already the case. These landline communications can be easily targeted and are vulnerable to conventional forces and tools. As long as the Russian operational thinking and strategy remains classified, contemporary assessments of the successfulness and significance of the Viasat attack can only be estimated.

Novelty of the Attack

The attack on the KA-SAT system and services demonstrates that cyberattacks against critical infrastructure are used and can be expected to continue to be used during armed conflicts. Commercial space systems can be seen as preferential targets in attacks meant to support terrestrial military operations since cybersecurity standards for commercial and governmental/military satellites differ, making commercial satellites potentially more vulnerable. [12] Moreover, the effects of such attacks are not limited to targeted (military) entities and systems. In the KA-SAT case, ripple effects occurred against numerous critical infrastructure systems far beyond the Ukrainian border.

Attribution

Viasat investigated the incident in cooperation with the IT security company Mandiant, as well as "law enforcement and U.S. and international government agencies." [14] On 30 March, the company released an initial statement confirming that the attacks focussed on Ukraine. [15] On 31 March, IT security company Sentinel Labs assessed "with medium confidence that there are developmental similarities between AcidRain and a VPNFilter stage 3 destructive Plugin." [16] As stated by the company, the FBI and US Department of Justice originally attributed the VPNFilter campaign to the Russian government and APT 28. The US National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) later attributed it specifically to the Sandworm group based on the attack behaviour, [16] which included previous sabotage operations against Ukrainian critical infrastructure that had physical effects (e.g., against the Ukrainian energy grid at the end of 2015 and 2016). Based on this circumstantial evidence, i.e., the timing alongside the onset of conventional warfare and the forensic similarities reported, the KA-SAT hack has been technically attributed to Russia.

On 10 May, the UK's National Cyber Security Centre (NCSC) was responsible for a political attribution for the attack. Based on US and UK intelligence, the NCSC assessed that Russia (specifically military intelligence, the GRU) was almost certainly responsible for the hack on Viasat. [17] The US [18], the UK [17], Canada [19], and Australia [20] attributed the incident to Russia in individual statements alongside the High Representative of the European Union. [21] Following this, North Macedonia, Montenegro, Serbia, Albania, Bosnia and Herzegovina, Iceland, Liechtenstein, Norway, Ukraine, Moldova, and Georgia aligned themselves with the European Union's statement. [21] Notably, these public attributions did not state which specific GRU-affiliated group was responsible for the attack, despite the reported evidence pointing towards the Sandworm group.

Operation Timeline and Attribution

24 February 2022	HermeticWiper on Ukrainian government computers; Attack on Windows machines
24 February 2022	Wiper AcidRain on KA-SAT 9A satellites Russia invades Ukraine
02:00 UTC	Russia starts missile strikes on Ukraine
03:02 UTC	Viasat detects malicious traffic on modems
04:15 UTC	Viasat detects modems exiting their networks
15 March	Viasat officially stabilised

Sources: [16][14][17]

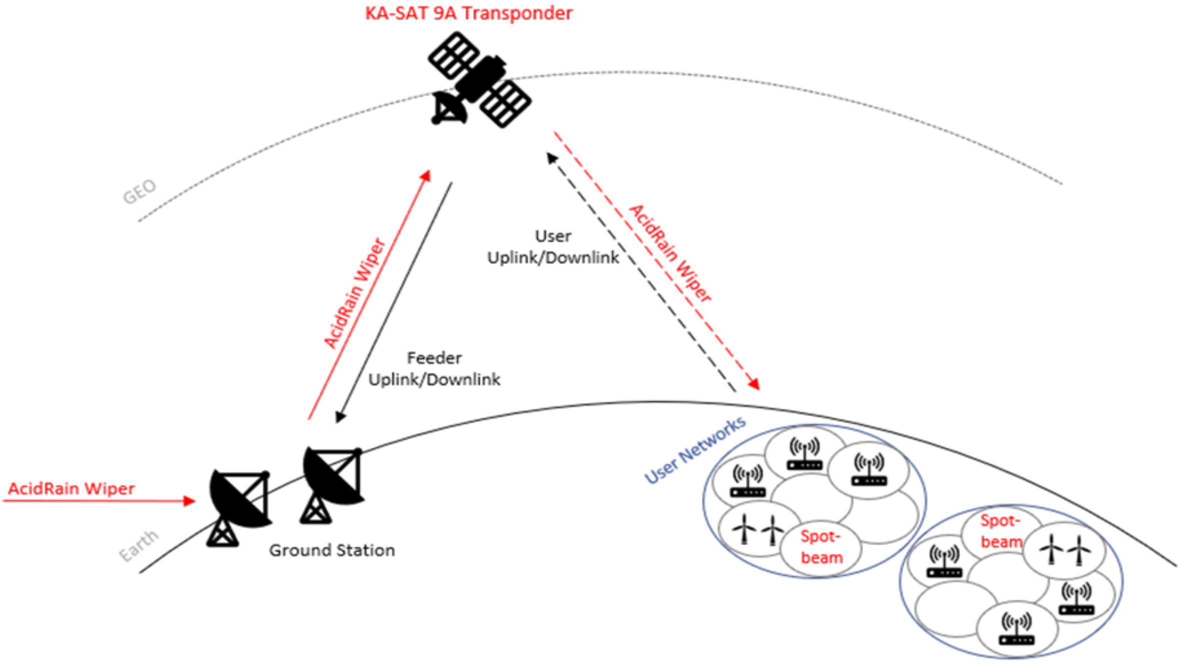
Technical Details

The attack did not affect the geostationary KA-SAT 9A broadband satellite itself, but rather the ground infrastructure of modems and routers. The operation included two phases: first, a distributed denial of service (DDoS) attack was detected by the operator, emerging from several SmurfBeam2 and SmurfBeam2+ modems and targeting other modems. After that, modems went permanently offline because their file system was wiped. [15] Most likely, the source of the initial access was a supply chain attack from the Internet. In the course of the attack, a poorly-configured VPN application probably gave the attackers access to a trusted management segment of the KA-SAT network. This enabled the use of management commands on a large number of residential modems simultaneously. [15] Analysis from the IT-security community suggests that available management commands of the system included the ability to run arbitrary codes on modems. The malicious binary code containing the wiper “AcidRain“ was probably executed this way. [22] It appears likely that those commands were also utilised to run other malicious codes, including the initial DDoS attacks, on the modems. “AcidRain“ instructed the modems to overwrite their flash memory, first erasing all non-standardised files on the system and then overwriting all storage. [16] In doing so, the wiper used a brute-force approach by iterating over all possible device identifiers. This made the malware appear less targeted than other wipers that would have known more about their target’s file system and would have deleted specific files rather than iterating over all possible names. It also differentiates “AcidRain“ from the highly-similar wiper modules of the malware “VPNFilter“ that has been associated with the Russian state-sponsored group “Sandworm.” SentinelOne hypothesised that this might have been a conscious choice to keep the tool “generic and reusable.” [16] Notably, SentinelOne further suggested that the code of “AcidRain“ was of lower quality than that of “VPNFilter.“ [16] The malware finally rebooted the terminals, which became unable to go back into service without the data from flash memory. This effectively made thousands of modems inoperable, which required either a fresh firmware flash or a complete replacement; while the modems were not physically destroyed by the malware, a factory reset would be necessary to recover their function. [15] The decision to confine the operation to reversible effects may be a sign of the threat actor's attempts to reduce the potential for escalation.

Enablers

This attack was enabled by a complex network of stakeholders within the KA-SAT network, a "misconfigured" VPN application, and insufficient security procedures in the protocols and software of modems. With various organisations having access to the networks, the risk of a weak link increased. According to the operator, a misconfigured VPN application was used for initial access, [15] and, deducing from reporting, there were likely not enough security measures for users inside the trusted networks behind the VPN (e.g., a "zero-trust policy"). Furthermore, there was insufficient security on the modems; the modems included an integrated option for remote code execution. Finally, it appears that countermeasures on behalf of the operator, despite noticing that something was going on within the networks, failed to stop the attack. [15]

Fig. 2: The Wiper "rains down" from the Satellite



Private Sector Engagement

Viasat [15]
Skylogic [analysis, mitigation, and recovery actions] [15]
SentinelOne [analysis] [16]
Eutelsat [15]
Mandiant [15]

Legal Assessment

Several countries and legal scholars have commented on the Viasat incident, which has been singled out as one of the largest formal attributions of a cyberattack to a nation-state in history. Nearly 20 countries accused Russia of being responsible for this hack, including a dozen EU member states and the Five Eyes countries. [25]

Most countries confirmed the disruptive spillover effects of the incident, highlighting that the original objective had been to disrupt Ukrainian command-and-control during the invasion. [17] [18] [21] The US and Canada condemned the attack, stating it undermined the rules-based international order and justifying steps by the United States and its allies to take "steps to defend against Russia's irresponsible actions." [18] [19] The UK's statement further clarified the nature and scope of damage: the "unprovoked aggression" affected personal and commercial internet users, as well as wind farms in central Europe. [17] The EU also qualified the Viasat intrusion as facilitating the military aggression against Ukraine while simultaneously causing indiscriminate communication outages and disruptions to several public authorities, businesses, and users in Ukraine, as well as affecting several EU member states. [21] However, the EU abstained from any legal assessments, noting simply that Russia's behaviour was "contrary to the expectations set by all UN Member States of responsible State behavior." [21]

Australia framed the incident as a threat to international peace and security. [20] The Nordic countries issued a joint statement, pointing out that "State actors carrying out cyber-attacks against critical infrastructure do so in clear violation of international law and fail to live up to the agreed voluntary non-binding norms, which all Member States have endorsed by consensus in General Assembly resolution 70/237." [26] Considering such behaviour unacceptable, the Nordic states called on the Security Council to cease all national cyber activity that conflicts with international law and to work towards a Council that can call out transgressions of international law in cyberspace that threaten international peace and security. [26] Estonia also qualified the Viasat incident as a violation of international law: "These cyberattacks run counter to international law and therefore, we are unequivocally condemning them." [27]

Several scholars have commented on the incident and its implications under the law of operations [28] [29] and international space law. [30] [31] [32] The incident has received commentary from the Cyber Peace Institute [33] and has been included in the CCD COE Cyber Law Toolkit. [34]

Sources

[1] Matthias Schulze and Mika Kerttunen (2023). *Cyber Operations in Russia's War against Ukraine. Uses, limitations, and lessons learned so far*. SWP Comment 2023/C 23 April 17. Available at: https://www.swp-berlin.org/publikation/cyber-operations-in-russias-war-against-ukraine [Archived on: 09.05.2023].

[2] Moritz Tremmel (2022). *Wiper legte Satelliten-Netzwerk lahm*, Golem. Available at: https://www.golem.de/news/viasat-wiper-legte-satelliten-netzwerk-lahm-2204-164366.html [Archived on: 09.05.2023].

[3] Martin Matishak (2022). *Western powers blame Russia for Ukraine satellite hack*, The Record. Available at: https://therecord.media/eu-uk-blame-russia-for-ukraine-satellite-hack [Archived on: 09.05.2023].

[4] James Pearon, Raphael Satter, Christopher Bing, and Joel Chectman (2022). *Exclusive: U.S. spy agency probes sabotage of satellite internet during Russian invasion, sources say*, Reuters. Available at: https://www.reuters.com/world/europe/exclusive-us-spy-agency-probes-sabotage-satellite-internet-during-russian-2022-03-11/ [Archived on: 09.05.2023].

[5] Kim Zetter (2022). *Viasat Hack "Did Not" Have Huge Impact on Ukrainian Military Communications, Official Says*. Available at: https://zetter.substack.com/p/viasat-hack-did-not-have-huge-impact [Archived on: 25.05.2023].

[6] Mykhailo Fedorov (2022). Statement on Twitter. Available at: https://twitter.com/FedorovMykhailo/status/1497543633293266944 [Archived on: 09.05.2023].

[7] Jürgen Scheffran (2020). *Militarisierung des Weltraums und Möglichkeiten der Rüstungskontrolle: Eine zivilgesellschaftliche Perspektive*, BBE-Newsletter für Engagement und Partizipation in Deutschland. Berlin: Bundesnetzwerk Bürgerschaftliches Engagement.

[8] SSI 2019.

[9] Kai-Uwe Schrogl, ed. (2020). *Handbook of Space Security. Policies, Applications and Programs*, 2nd edition. Basel: Springer International Publishing.

[10] Peter Malanczuk (1991). "Erdfernerkundung," in: Karl-Heinz Böckstiegel (ed.), *Handbuch des Weltraumrechts*. Köln/Berlin/Bonn/München: Carl Heymanns Verlag KG: 307-347.

[11] Stephan Hobe (2019). *Space Law*. Baden-Baden: Nomos.

[12] Clémence Poirier (2022). *The War in Ukraine from a Space Cybersecurity Perspective*, ESPI Short Report. Available at: https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf [Archived on: 09.05.2023].

[13] Joint Chiefs of Staff (1996). *Joint Doctrine for Command and Control Warfare (C2W)*, JP 3-13.1. Available at: https://www.bits.de/NRANEU/others/jp-doctrine/jp3_13_1.pdf [Archived on: 09.05.2023].

[14] Information Office of the State Council of the People's Republic of China (2011). *China's National Defense in 2010*. Available at: http://www.china.org.cn/government/whitepaper/node_7114675.htm [Archived on: 09.05.2023].

[15] Viasat (2022). *KA-SAT Network cyber attack overview*. Available at: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview [Archived on: 09.05.2023].

[16] Juan Andrés Guerro-Saade (2022). *AcidRain | A Modem Wiper Rains Down on Europe*, SentinelOne. Available at: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ [Archived on: 09.05.2023].

[17] Foreign, Commonwealth & Development Office of the UK (2022). *Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion*. Available at: https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion [Archived on: 09.05.2023].

[18] Anthony J. Blinken (2022). *Attribution of Russia's Malicious Cyber Activity Against Ukraine*, United States Department of State. Available at: https://web.archive.org/web/20231004140606/https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/ [Archived on: 09.05.2023]

[19] Global Affairs Canada (2022). *Statement on Russia's malicious cyber activity affecting Europe and Ukraine*. Available at: https://www.canada.ca/en/global-affairs/news/2022/05/statement-on-russias-malicious-cyber-activity-affecting-europe-and-ukraine.html [Archived on: 09.05.2023].

[20] Marise Payne, Peter Dutton, and Karen Andrews (2022). *Attribution to Russia for malicious cyber activity against European networks*, Australian Minister for Foreign Affairs. Available at: https://www.foreignminister.gov.au/minister/marise-payne/media-release/attribution-russia-malicious-cyber-activity-against-european-networks [Archived on: 09.05.2023].

[21] Council of the European Union (2022). *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union*, European Council. Available at: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/ [Archived on: 09.05.2023].

[22] Ruben Santamarta (2022). *VIASAT incident: from speculation to technical details*, Reversemode. Available at: https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html [Archived on: 09.05.2023].

[23] Michael N. Schmitt (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

[24] United Nations General Assembly (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report A 68/98* (24 June); United Nations General Assembly (2015). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Report A 70/174* (22 July); United Nations General Assembly (2021). *Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Report A 76/135* (14 July).

[25] Kevin Poireault (2023). *Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites*, InfoSecurity Magazine. Available at: *https://web.archive.org/web/20231004121828/https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack/* [Archived on: 04.10.2023].

[26] Marie-Louise Koch Wegter (2023). *Nordic Statement at Arria Meeting on the Responsibility of States to Cyberattacks*, Ministry of Foreign Affairs of Denmark. Available at: https://web.archive.org/web/20231004122045/https://fnnewyork.um.dk/en/statements/nordic-statement-at-arria-formula-meeting-on-the-responsibility-of-states-to-cyberattacks [Archived on: 04.10.2023].

[27] Republic of Estonia Ministry of Foreign Affairs (2023). *Estonia joins the statement of attribution on cyberattacks against Ukraine*. Available at: https://web.archive.org/web/20231004135244/https://vm.ee/en/news/estonia-joins-statement-attribution-cyberattacks-against-ukraine [Archived on: 04.10.2023].

[28] Aurel Sari (2023). *International Law and Cyber Operations: Current Trends and Developments*, Council of Europe Committee of Legal Advisers on Public International Law. Available at: https://web.archive.org/web/20231004135653/https://rm.coe.int/64th-cahdi-pr-aurel-sari-presentation/1680aaaf48 [Archived on: 04.10.2023].

[29] Kristen E. Eichensehr (2023). *Ukraine, Cyberattacks, and the Lessons for International Law*. In the *American Journal of International Law.* Available at: https://web.archive.org/web/20231004135739/https://www.cambridge.org/core/journals/american-journal-of-international-law/article/ukraine-cyberattacks-and-the-lessons-for-international-law/69B36016B06998BCE1EC67C757CDF34D [Archived on: 04.10.2023].

[30] Jennifer A. Cannon (2023*). Targeting Dual-Use Satellites. Lessons Learned from Terrestrial Warfare*. In the *Air and Space Operations Review*, Vol. 2(2). Available at https://web.archive.org/web/20231004135841/https://www.airuniversity.af.edu/Portals/10/ASOR/Journals/Volume-2_Number-2/Cannon.pdf [Archived on: 04.10.2023].

[31] European Space Policy Institute (2022). *The war in Ukraine from a space cybersecurity perspective*, ESPI Short Report 1. Available at: https://web.archive.org/web/20231004121842/https://www.espi.or.at/wp-

content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf [Archived on: 04.10.2023].

[32] Tara Brown (2022). *The Risk of Commercial Actors in Outer Space Drawing States into Armed Conflict*, West Point Ukraine Symposium. Available at: https://web.archive.org/web/20231004140215/https://lieber.westpoint.edu/commercial-actors-outer-space-armed-conflict/ [Archived on: 04.10.2023].

[33] Cyber Peace Institute (2022). *Case Study Viasat*. Available at: https://web.archive.org/web/20231004140448/https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat [Archived on: 04.10.2023].

[34] Cooperative Cyber Defence Centre of Excellence (2022). *Viasat KA-SAT Attack (2022)*. Available at: https://web.archive.org/web/20231004140714/https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_%282022%29 [Archived on: 04.10.2023].

[35] Sandra Erwin (2023). *Limits on Ukraine's use of Starlink for war operations is a lesson for U.S. military.* Available at: https://spacenews.com/limits-on-ukraines-use-of-starlink-for-war-operations-is-a-lesson-for-u-s-military/

Last updated: 04.10.2023