CYBERDEFENSE REPORT

Hacking the Cosmos: Cyber operations against the space sector

A case study from the war in Ukraine

Clémence Poirier

Zürich, October 2024
Center for Security Studies (CSS), ETH Zürich

CSS
ETH Zürich

ETH zürich

Available online at: https://css.ethz.ch/en/publications/risk-and-resilience-reports.html

Author: Clémence Poirier

ETH-CSS project management: Stefan Soesanto, Project Lead Cyberdefense; Andreas Wenger, Director of the CSS.

Editor: Stefan Soesanto
Layout and Graphics: Clémence Poirier

DOI: 10.3929/ethz-b-000697348

Table of Content

Introduction

A few hours prior to the Russian invasion of Ukraine on February 24, 2022, Russia's military intelligence (GRU) launched a destructive cyberattack against ViaSat's KA-SAT satellite network. In specific, the GRU targeted thousands of ViaSat's SurfBeam 2 modems in Europe, which the Ukrainian Armed Forces depended upon for their internet satellite communications. First, the GRU carried out a Distributed Denial of Service (DDoS) attack against the modems and then exploited a vulnerability in a misconfigured Virtual Private Network (VPN) application. The vulnerability granted the GRU remote access to the KA-SAT management segment and allowed it to execute management commands on a large number of SurfBeam 2 modems simultaneously. The GRU used this ability to deploy a wiper malware (dubbed AcidRain) to overwrite the memory of thousands of SurfBeam 2 modems which rendered them unusable.

The timing of the ViaSat hack prevented the Ukrainian military from using its internet satellite communications to coordinate its response to the Russian invasion. Additionally, the cyberattack also affected military and civilian customers, as well as other infrastructure across Europe. The ViaSat hack is an important example of an offensive cyber operation that has been conducted to prepare the kinetic battlefield for a conventional military incursion.[1]

Following the ViaSat hack, many experts expected to see a significant increase of cyber activities against the space sector. Cyber security researcher Ruben Santamarta, who analyzed the Viasat hack, assessed that attackers would likely conduct additional operations.[2] Eytan Tepper, founding Director of the Space Governance Lab at Indiana University, even noted that *"a combined space-cyber warfare theatre is emerging to become the primary battlefield in the twenty-first century and the main mode of space warfare."*[3] And Joanna Rozpedowski, Adjunct Professor at George Mason University, argued that *"every terrestrial war is now simultaneously a space and cyber war requiring identification and active monitoring of threats from space assets."*[4] These assessments are a notably sea-change compared to the Russian annexation of Crimea in 2014. As far as open source goes, no cyber operation was conducted against any space infrastructure prior or amidst the annexation of Crimea.

Given the importance of the ViaSat hack, **this Cyber Defense Report investigates all other cyber operations that have occurred against the space sector during the war in Ukraine (February 2022 – September 2024). The report investigates the effects of these operations as well as their perpetrators and what it signifies in the larger context of the Russo-Ukrainian conflict.**

The exclusive focus of the report on the space sector stems from the reasoning that the ViaSat hack was a wake-up call for the global space sector, and it put cybersecurity in the spotlight in a sector that had long overlooked the topic. Cyber threats against space systems have also been increasingly acknowledged by government policies, explicitly citing ViaSat as a worrying example (e.g., EU Policy on Cyber Defence). To some extent, the ViaSat hack generated a sense of panic regarding the resilience of the sector to cyber threats, the lack of mitigation measures, and the overall cyber readiness of the space industry and government agencies. Furthermore, the importance of Starlink use in Ukraine and SpaceX's reallocation of resources towards cyber defense and anti-jamming measures at the expense of other major projects, might be an indication that other cyber activities might have or are expected to occur against satellites systems in the context of the Ukraine War and other future conflicts.[5]

Furthermore, although the ViaSat hack has led to various publications on space cybersecurity, there is currently no literature available that provides a comprehensive overview of all the cyber operations that have been conducted against the space sector in the context of the Russo-Ukrainian war. This report aims to fill this gap.

---

[1] Poirier, Clemence. "The War in Ukraine from a Space Cybersecurity Perspective." *ESPI*, October 2022, https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Report-84.pdf. Accessed 8 June 2024.

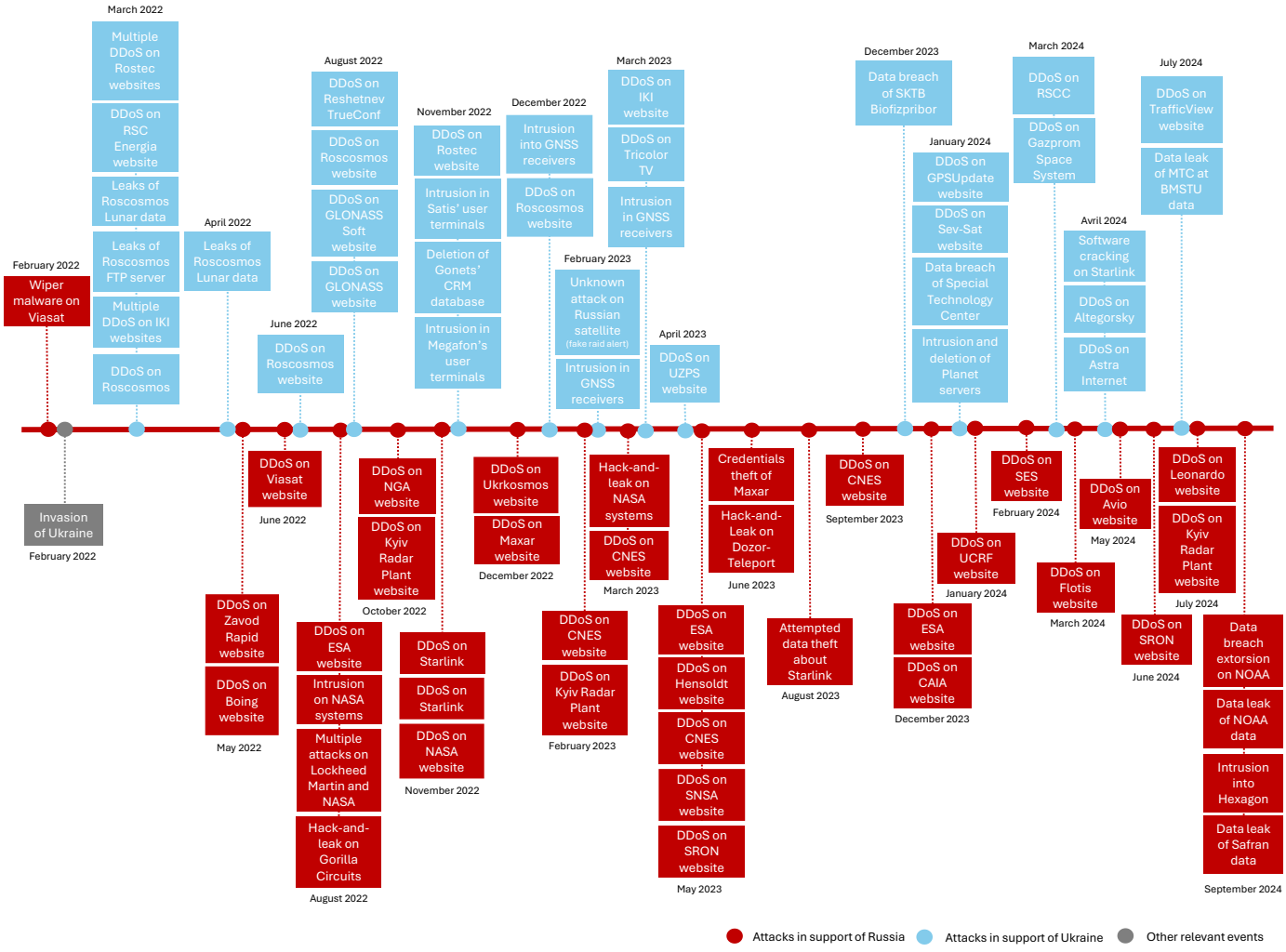
[2] Valentino, Andrea. "Why the Viasat Hack Still Echoes." Aerospace America, 1 Nov. 2022, https://aerospaceamerica.aiaa.org/features/why-the-viasat-hack-still-echoes/. Accessed 26 Sept. 2024.

[3] Tepper, Eytan. "The First Space-Cyber War and the Need for New Regimes and Policies, Policy Brief No. 173." *CIGI*, 2022, https://shorturl.at/KNWLN. Accessed 26 Sept. 2024.

[4] Rozpedowski, Joanna. "Every War Is a Space War Now." *Geopolitical Monitor*, 12 Mar. 2024, https://shorturl.at/OZKof. Accessed 8 June 2024.

[5] "Elon Musk." *X (Formerly Twitter)*, 5 Mar. 2022, https://rb.gy/fbaed8. Accessed 8 June 2024.

Figure 1: Cyber operations against the space sector as part of the war in Ukraine



Source: Compiled by Clémence Poirier

To reach these objectives, **this report has compiled a dataset of 124 publicly known cyber operations conducted against the space sector in the context of the Russo-Ukrainian war (see Figure 1).** The dataset only includes operations conducted against the space sector, which is understood as the broad set of systems, services, computers, companies, and organizations (including their data) involved in the design, production, operation, management, and use of space systems and services in both the upstream and downstream sectors as well as in the space supply chain.

The dataset only includes operations conducted against the space sector, which is understood as the broad set of systems, services, computers, companies, and organizations (including their data) involved in the design, production, operation, management, and use of space systems and services in both the upstream and downstream sectors as well as in the space supply chain.

The report demonstrates significant cyber activities against the space sector conducted by about 35 threat actors, including hacktivists and state actors, on both sides of the conflict. The report delves into the dynamics of pro-Russian and pro-Ukrainian hacktivist groups as well as the tempo of cyber operations against the space sector in relation to events linked to the conflict. Selected examples of attacks are provided in this Cyber Defense Report.

Chapter 1 addresses the various types of attacks that were carried out against the space sector, as well as the types of entities that were targeted.

Chapter 2 provides insights into the behavior of threat actors and their interests and motives.

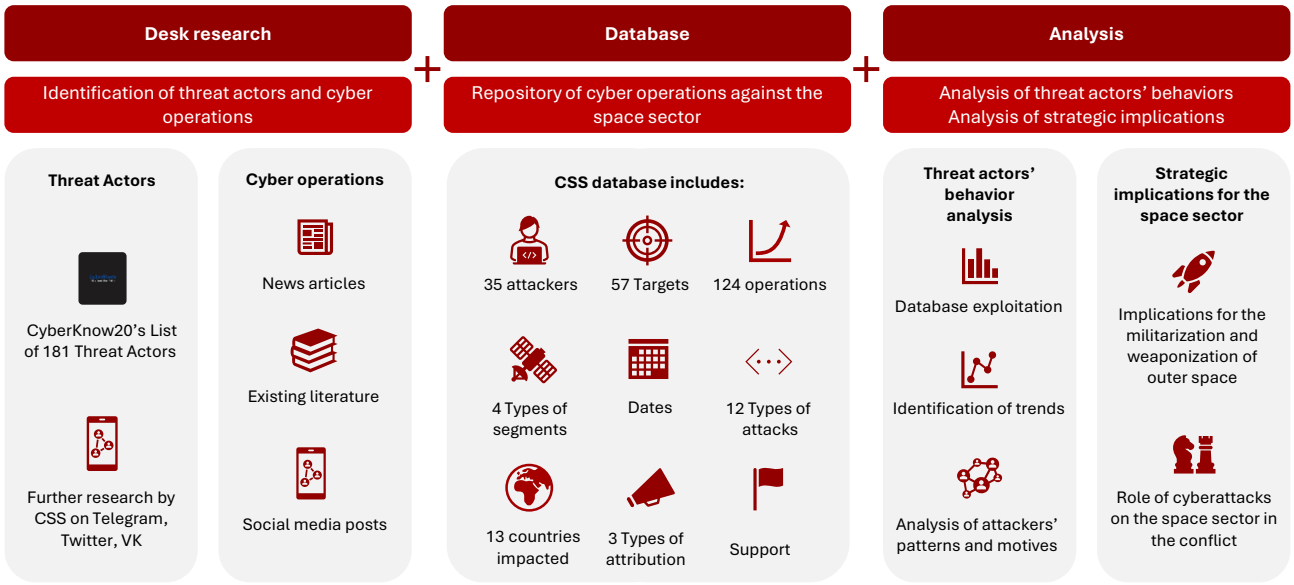
Chapter 3 looks into the political and strategic implications of cyber operations and their impact on the militarization and weaponization of outer space.

Figure 2: Main findings of the Cyber Defense Report

Source: Compiled by Clémence Poirier

Scope and Methodology

Figure 3: Methodology



Source: Compiled by Clémence Poirier

This report covers the period between February 24, 2022, to September 20, 2024. It includes most – if not all - publicly known cyber operations conducted against space systems by state and non-state actors on both sides of the conflict.

The research for this report was conducted in three steps. **First, the author used the map of threat actors created by Australian threat intelligence researcher CyberKnow20 as the basis for her desk research**. As of July 2024, CyberKnow20 identified 138 threat actors that are involved in the Russo-Ukrainian conflict, including 47 pro-Ukrainian groups and 91 pro-Russian groups. CyberKnow20 lists all types of threat actors, including hacktivists, state actors, state-sponsored groups, individual hackers, etc., that have taken sides in the conflict and have carried out cyber operations.

Taking CyberKnow20's threat actor list, **the author scraped – where available - the social media channels of hacking groups and individuals to identify whether they have claimed to have conducted any space-related cyber operations.** Overall, 183 Telegram channels and Twitter accounts were analyzed (61 pro-Ukrainian accounts and 124 pro-Russian accounts). The total number includes accounts on various platforms from the same threat actor, as well as channels and sub-groups from the same group. Inaccessible or deleted accounts were investigated where possible via snapshots on the Internet Archive's Wayback Machine or through TGStat, which is an online catalog and analytical platform for Telegram channels.

To narrow down the search of relevant social media posts, the author compiled a list of 77 keywords[6] related to Russian space systems, space operations, and space actors that were used to search each pro-Ukrainian channel. 108 Western and Ukrainian space sector relevant keywords[7] were searched on each pro-Russian channel. Relevant messages were then analyzed and contextualized with additional desk research.

The keyword search and analysis identified 12 pro-Ukrainian and 19 pro-Russian hacker groups that have claimed to have conducted operations against the space

[6] The full list of searched keywords is: Roscosmos, IKI, GLONASS, GPS, GNSS, Yuzhmash, космiч, Rogozin, NPO Energomash, Энергомаш, НПО, Gazprom, Gazprom Space, RKK Energiya, РКК Энергия, RSC Energia, космич, Полёт, Polyot, KBKhA, Khimavtomatika, химавтоматик, Chemical Automatics Design Bureau, CADB, Isayev, KhimMash, KBKhM, kbhmisaeva, Khrunichev, Конструкторское бюро, Kuznetsov Design Bureau, СНТК, Центр Келдыша, Keldysh Research Center, kerc.msk.ru, ОКВ Fakel, ОКБ Факел, EDB Fakel, NIIMash, Научно, Proton, Протон, Voronezh Mechanical Plant, Воронежский механический завод, Lavochkin, Лавочкин, Решетнёв, Reshetnev, Sputnix, aero, cosmos, kosmos, Starlink, Lin Industrial, Space, Satellite, spacex, Elon, orbit, rocket, gravity, navgeoexpert, Глонасс, РАН, Glavkosmos, супутник, rostec, Бюро 1440, 1440.space, ИКС Холдинг, x-holding.ru, gazpromkosmos, Gonets, Satis, sev-sat.

[7] The full list of searched keywords is: NASA, DLR, CNES, ASI, Starlink, telescope, Planet, ICEYE, radar, Maxar, ДКАУ, Starlink, Airbus, Thales, Lockheed, SSAU, Space, Satellite, Leonardo, Ariane, Safran, UKSA, L3Harris, ESA, cosmos, kosmos, Galileo, GPS, GNSS, Yuzhmash, Южмаш, Південмаш, Pivdenne Design Office, Airbus, Південне, Ivchenko-Progress, ZMKB, Прогрес, Хартрон, Khartron, Hartron, NPO Electropribor, Isar, НПО Электроприбор, Luch, Луч, Alcântara Cyclone Space, ACS, Мотор Січ, Motor Sich, НЦУВКЗ, NCUVKZ, Raytheon, космічн, NPO, НПО, космическ, спутник, aero, Spacex, Elon, Blue Origin, Astroscale, SES, Inmarsat, Intelsat, ULA, Preligens, orbit, Northrop, Boeing, rocket, Gravity, APCO, CSEM, Klepsydra, Viasat, Oneweb, Schurter, EO4UA, EUSPA, Copernicus, EOS, Yuzhmash, Capella, Satellogic, Eutelsat, Yuzhnoye, GEOSAT, OPT/NET, Umbra, MDA, sron, Norsk Romsenter, BELSPO, CSA, CCSDS, DTUSpace, JAXA, LSA, POLSA, nkau, Dniprokosmos, Makarov, aero-cosmic, ORIZON-NAVIGATION , Promin Aerospace, Kurs Orbital.

sector. On the Ukrainian side these are: Anonymous, Anonymous Italia, Cyber Resistance, CyberPalyanitsa, BO Team, GhostSec, HimarsDDoS, NB65, OneFist, the IT Army of Ukraine, Twelve, and V0g3lSec. On the Russian side the groups are: 62IXGROUP, Anonymous Russia, Bloodnet, Cyber Army of Russia, CyberDragon, Cyber Volk, Dark Strom Team, From Russia with Love, HDR0, Just Evil, Killnet, labs666, Legion Cyber Spetsnaz, LulzSec, NoName057(16), Pharanos Cyber Army (PCA), Phoenix, Richard W (Wagner), Sandworm, and User1. The Russian and Ukrainian governments can also be added to the list of identified threat actors.

Second, the author compiled a database of all identified cyberattacks against the space sector, including self-attributed, publicly attributed, and non-attributed attacks. It includes the date of occurrence of each operation, the type of target, the country that was targeted, the name of the target, the name of the attacker, the type of attack, the segment that was targeted, the type of system that was targeted, and the type of attribution. Information that was not available at the time of writing, has been marked as "unknown." Two types of cyber-related operations were excluded from the database: Electronic warfare such as jamming and spoofing, and disinformation campaigns that – for example use satellite data.

Third, the author analyzed the database and individual operations to identify potential trends affecting the space sector in and through cyberspace. The analysis provides insights into (a) the evolution of the threat landscape, (b) the behavior of threat actors, (c) the potential political and strategic implications of cyber operations against space systems, and (d) their effects on the weaponization and militarization of outer space.

The report is to a certain degree limited by the lack of visibility and lack of public reporting of space-related cyber incidents. The author did not have access to any information communicated or posted in private Telegram channels or invite-only hacker forums. Information degradation was a significant hurdle as well as several social media accounts and data leaks/dumps have been deleted or were taken down resulting in difficulties in accessing the raw data. This also affected the author's ability to provide functioning URLs for old tweets, Telegram channels etc.

Keywords

Distributed Denial of Service (DDoS): sending malicious traffic through multiple connected devices to overwhelm target and disconnect it.

Intrusion: unauthorized activity or access to a computer system, network, or digital device.

Hack and leak: unauthorized access to, and retrieval of data, which is followed by the public release of such data.

Data leak: data released in the public domain without authorization. This data may be obtained through various methods, including internal leaks, informants, malicious insiders, government actions, or other unauthorized means.

Malware: malicious software deployed to affect the confidentiality, integrity, or availability of a system or network.

Wiper Malware: type of malware to erase data of a system or network and render it unusable.

Software cracking: unauthorized modification of software to modify features to bypass restrictions.

Credential theft: unauthorized acquisition of a person's or organization's login information.

Data breach: sensitive or protected information is accessed, disclosed, or stolen without authorization.

Data breach extorsion: threat to publicly release stolen data unless the victim pays a ransom or meets specific demands.

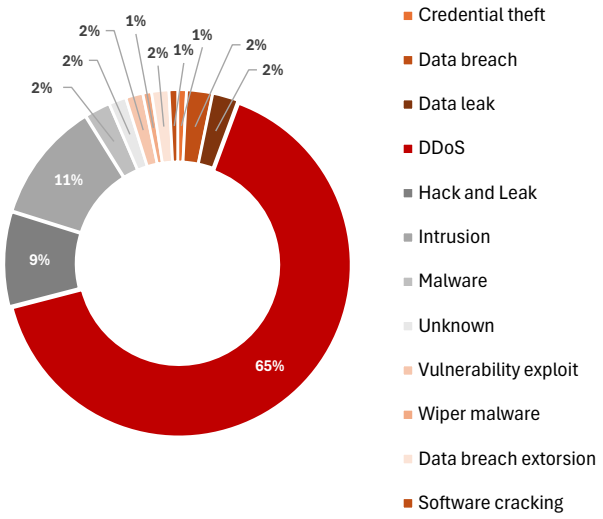
Vulnerability exploit: taking advantage of a flaw in a software or system to affect its confidentiality, integrity, or availability.

Disclaimer: At no point during the research did the author participate in any of the malicious or illegal activities mentioned in this report, nor did she join, post, or interact with users or channel administrators. The author did not contact or seek to contact any of the threat actors mentioned in this report.

1 Key targets in the space sector

This chapter addresses the types of cyber operations that were conducted against the space sector as well as the types of space entities that have been targeted by threat actors in the context of the war in Ukraine. Selected examples are provided to illustrate the report's research findings.

Figure 4: Types of attacks targeting the space sector as part of the war in Ukraine



Source: Compiled by Clémence Poirier

Out of the 124 identified cyber operations, 65% were Distributed Denial of Service (DDoS) attacks while 11% were intrusions into space systems and companies. 9% of attacks were hack and leak operations. 2% were data leaks or the result of malware or exploitation of vulnerabilities. The deployment of wiper malware, such as in the case of the ViaSat hack, is rather rare. It only represents 1% of cases identified.

The high number of DDoS attacks in the dataset is likely part of a broader behavior trend in hacktivist groups. However, it is important to underline that DDoS are also fairly easily verifiable by researchers and are often self-attributed by threat actors. DDoS attacks are almost always temporary in nature and rarely impact the targeted actors' activities or space systems. Identified DDoS operations did not target satellites in orbit. In fact, most did not target any space system at all. An overwhelming majority (95%) of DDoS attacks targeted the user interface, that is to say the IT environment of the targeted space entity, in most cases its websites and online authentication portals. 5% of DDoS targeted the user segment, usually user modems or receivers.

State and state-sponsored actors have likely conducted the most sophisticated operations despite limited public reporting. Intrusions into a system can often only be seen by the victim. Hence, if the intrusions are not publicly disclosed, they are difficult to map with open-source methods. Our dataset illustrates this dynamic, as most operations that were not self-attributed were the most sophisticated and impactful.

Pro-Russian group Legion Cyber Spetsnaz targets ViaSat's website

On June 27, 2022, the Pro-Russian hacktivist group Legion Cyber Spetsnaz, which is a self-proclaimed project by the Pro-Russian hacking group Killnet, urged its members to conduct a DDoS attack against the US satellite internet provider ViaSat.[8]

The group listed ViaSat's URL among eight other designated targets in a Telegram post. It posted the link of ViaSat's website as well as one IP address.[9] Other targets in the post included mainly Latvian entities. ViaSat stood out as the only US company and the only space entity. Although ViaSat operates in Latvia, its inclusion in the post seems to have been rather random.

One hour after the post went live, the group listed another 11 URLs, including viasat[.]com. The group noted that these 11 targets were not yet defaced, and that the community should keep attacking them with DDoS before moving on to other targets. [10]

Unlike the destructive operation against ViaSat in February 2022, no space systems were affected by this DDoS attack. ViaSat's website was only rendered temporarily unavailable, and the company did not publicly react to the incident.

Legion Cyber Spetsnaz did not provide any specific reasons for targeting ViaSat.

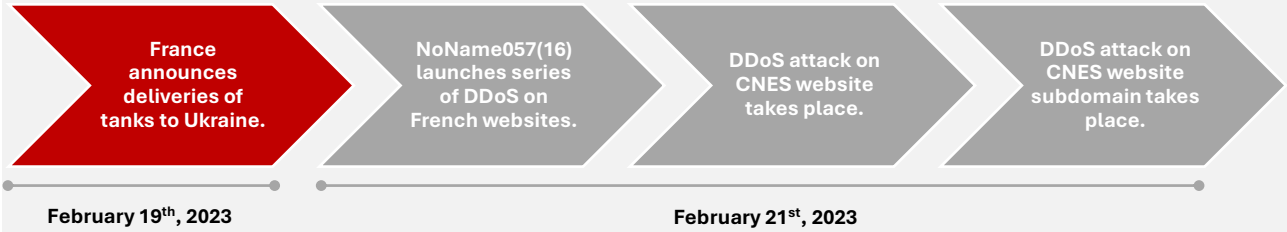
This type of DDoS campaign is typical for most DDoS attacks that have been conducted against space companies amidst the war in Ukraine.

[8] "WE ARE KILLNET." *Telegram*, https://t.me/s/killnet_reservs?q=viasat. Accessed 8 June 2024.

[9] "Post #604 — ЛЕГИОН🛡 - КИБЕР РАЗВЕДКА ⚔ (@Legion_Russia)." *TGStat.Ru*, https://tgstat.ru/en/channel/@Legion_Russia/604. Accessed 16 June 2024.

[10] "Post #608 — ЛЕГИОН🛡 - КИБЕР РАЗВЕДКА ⚔ (@Legion_Russia)." *TGStat.Ru*, https://tgstat.ru/en/channel/@Legion_Russia/608. Accessed 16 June 2024.

DDoS attacks against the French Space Agency's websites



On February 21, 2023, the pro-Russian hacktivist group NoName057(16) launched a series of DDoS attacks against French websites after French Defense Minister Sébastien Lecornu announced that France would provide Ukraine with AMX-10 armored fighting vehicles that would be delivered in the following week.[11] NoName057(16) explicitly referred to this announcement and declared that *"it's time to go on an exciting journey through the French Russophobic portals."*[12] Among the websites targeted was also the website of the French Space Agency (CNES).[13]

The National Centre for Space Studies (*Centre national d'études spatiales* - CNES*)* is the French national space agency, which is under supervision of the Ministry of Higher Education and Research; the Ministry of Economy and Finance; and the Ministry of Armed Forces. It proposes and implements France's space policy, represents France at the European Space Agency, develops and operates civilian satellites as well as military satellites in Low Earth Orbit (LEO), and operates the spaceport in Kourou, French Guiana, among other things.[14] CNES is not involved in any way in the design, development, or manufacturing of AMX-10 vehicles.

NoName057(16) shared a screenshot of the defaced CNES website and declared *"We put down the website of the National Centre for Space Studies."*[15] It also shared a link to check-host.net, which an online tool that checks the availability of websites, servers, hosts and IP addresses. Thes link was shared to prove that the DDoS attack was successful.

An hour later, NoName057(16) posted another message on Telegram, claiming another DDoS attack on another CNES website (*angels.cnes.fr/fr*). The group stated that *"following the main site of the French research center, we took down its subdomain"* along with a screenshot of the defaced website and a check-host.net link to prove the DDoS attack effectively happened.[16] The targeted web page is dedicated to ANGELS (Argos Neo on a Generic Economical and Light Satellite), which is a civilian demonstrator that collects, processes and disseminates environmental data. It does not have any links with defense-related activities or the war in Ukraine.

A few months later, on May 5, 2023, NoName057(16) claimed once again a DDoS attack on the website of the French Space Agency (CNES). The group declared that *"the National Centre for Space Studies was hit"* and provided a check-host link to prove its attack succeeded along with a screenshot of the defaced website.[17] This third attack was again part of a broader, albeit shorter, DDoS campaign against French websites. The same day, the group claimed DDoS operations on the websites of the Senate, defense company Naval Group, and DARES - a portal of the French Ministry of Labor. The group quickly moved to Swedish targets within the same day.

These operations did not directly target or affect French space systems. Only the websites of CNES were temporarily affected. Neither CNES nor its supervisory ministries publicly reacted to these attacks.

[11] Point.fr, Le. "La France s'apprête à Livrer Des Chars Légers à l'Ukraine." *Le Point*, 19 Feb. 2023, https://www.lepoint.fr/monde/la-france-s-apprete-a-livrer-des-chars-legers-a-l-ukraine-19-02-2023-2509175_24.php#11.

[12] "NoName057(16)." *Telegram*, https://t.me/noname05716/2005. Accessed 10 July. 2024.

[13] "NoName057(16)." *Telegram*, https://t.me/noname05716/2012. Accessed 5 July 2024.

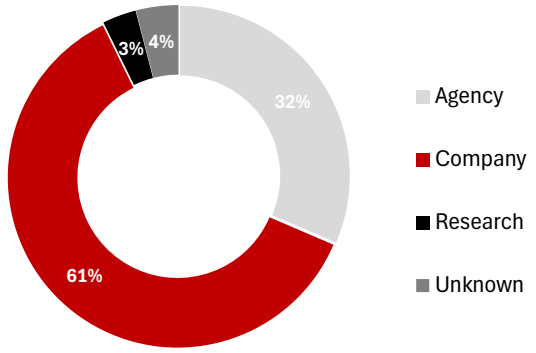
[14] Assemblée Nationale. "Rapport d'information Sur Le Secteur Spatial de Defense." *Assemblée Nationale*, 2019, https://www.assemblee-nationale.fr/dyn/15/rapports/cion_def/l15b1574_rapport-information.pdf.

[15] "NoName057(16)." *Telegram*, https://t.me/noname05716/2012. Accessed 10 July. 2024.

[16] "---." *Telegram*, https://t.me/noname05716/2014. Accessed 10 Sept. 2024.

[17] "---." *Telegram*, https://t.me/noname05716/311. Accessed 10 July. 2024.

Figure 5: Types of space entities targeted by cyber operations in the context of the war in Ukraine

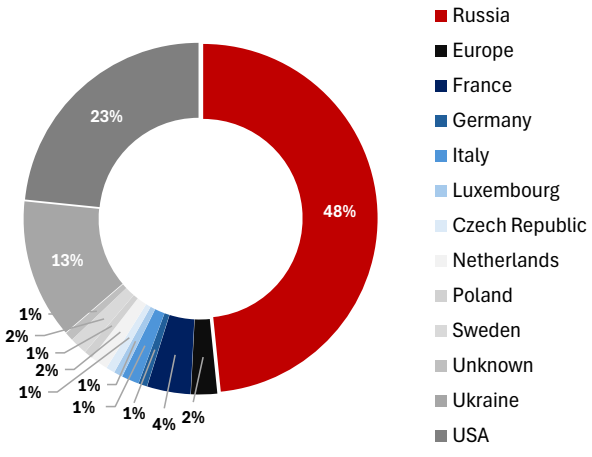


Source: Compiled by Clémence Poirier

Across 124 operations, the most targeted types of entities were space companies. 61% of identified operations targeted space companies, 32% were aimed at government space agencies, and 3% were targeting research institutes. The remaining 4% of operations were directed against space systems or entities whose identity was not revealed in public media reporting.

This result is not surprising. Ukraine does not have sovereign satellites, let alone military ones. As a result, many commercial space systems and services have been used in the conflict, which put space companies in the spotlight like never before and thus caught the attention of threat actors.

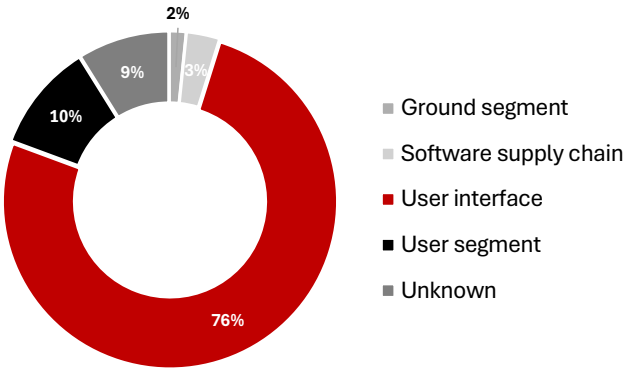
Figure 5: Countries targeted by cyber operations against the space sector



Source: Compiled by Clémence Poirier

48% of pro-Ukrainian operations were aimed at the Russia space sector, while 52% of pro-Russian operations were targeting the Ukrainian and Western space sector. Among these, 13% were Ukrainian entities, 23% were US-based entities, 4% were French, and 2% are the European Space Agency. Overall, **the volume of attacks conducted on both sides is almost balanced.**

Figure 7: Targeted segments in identified cyber operations against the space sector



Source: Compiled by Clémence Poirier

76% of identified cyber operations targeted the user interface. It is therefore the most common entry point. 10% of operations targeted the user segment. 3% of them impacted the software supply chain. And 2% of operations targeted the ground segment. For 9% of cases, the targeted segment was not publicly disclosed.

The space segment does not seem to have been targeted. It is likely that threat actors attempted to do so but no successful operation was publicly disclosed so far.

Keywords

Space segment: the spacecraft in orbit, including the structure and satellite bus, the payload, and the components on-board.

Ground segment: the ground-based systems of a space infrastructure such as the ground station, telescopes, radars, etc.

User segment: devices of end-users which enables to use satellite services such as internet modems, GPS receivers, satellite phones, satellite TV dish, etc.

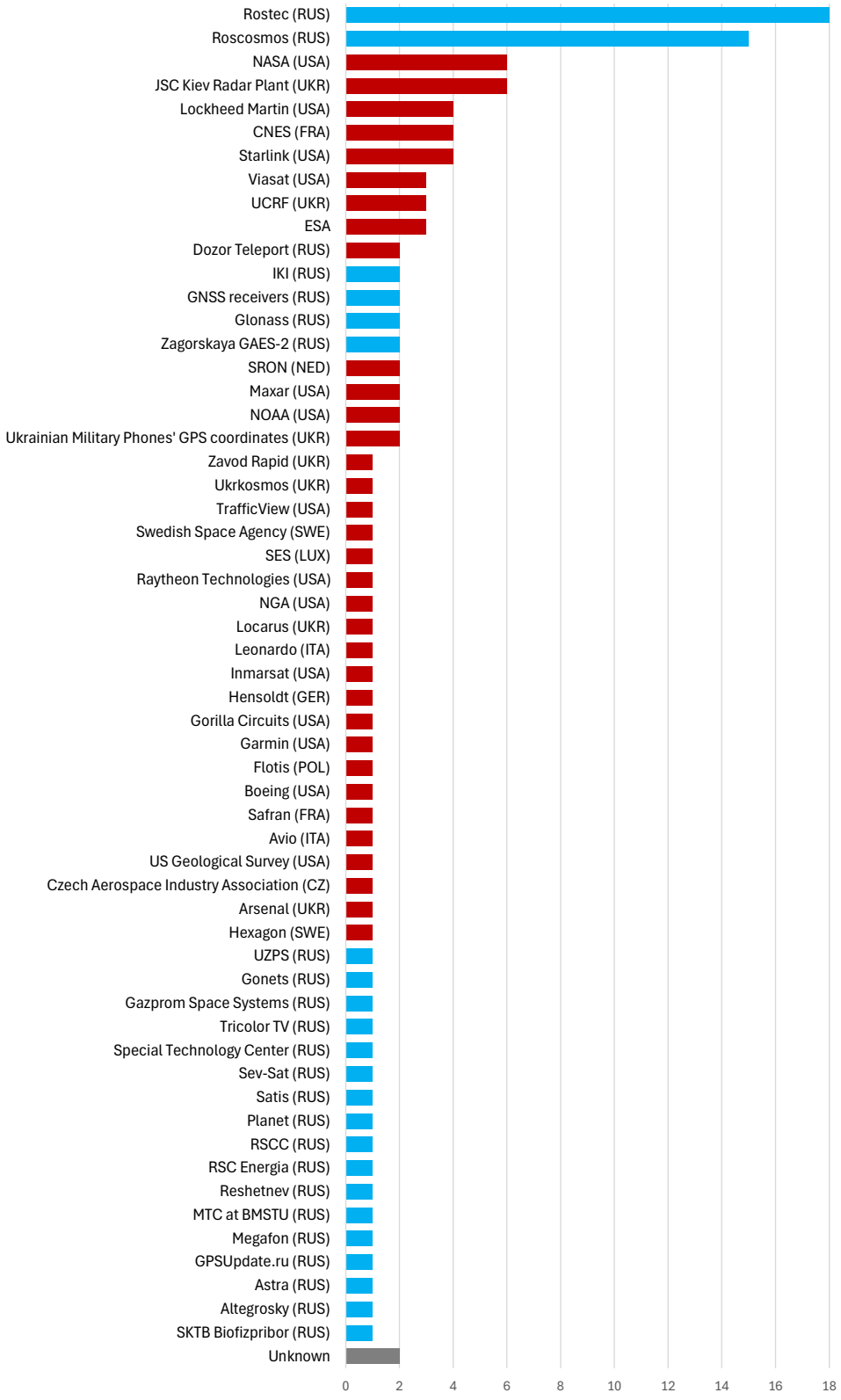
User interface: the IT environment of space organizations, including their websites, authentication portals, social media accounts, etc.

Software supply chain: the software services and companies upon which space companies and space systems rely for their functioning. It includes the tools used by sub-contractors in the manufacturing process of a satellite for instance. It can include Virtual Private Networks (VPN), multi-factor authentication tokens, project management software, etc.

The open-source mapping revealed that at least **57 different targets in the space sector were impacted by cyber operations** coming from both sides of the conflict. 60 operations (48%) targeted 23 organizations across the Russian space sector. 64 operations (52%) targeted 34 organizations across the Western and Ukrainian space sector. Among these, 16 operations specifically targeted the Ukrainian space sector.

Notably, pro-Russian attacks were more widespread across different Western and Ukrainian space targets, while pro-Ukrainian operations were concentrated on a few Russian targets – specifically Russian aerospace and defense company Rostec and Russia's space agency Roscosmos (see Figure 8)

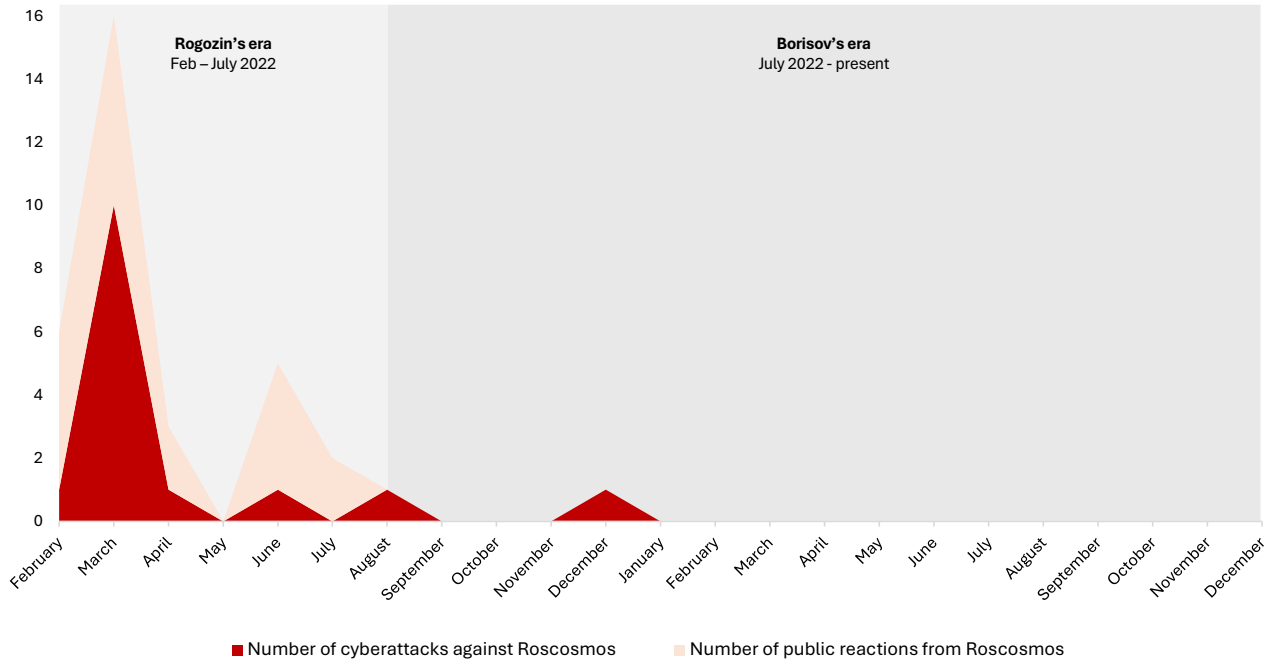
Figure 8: Victims of cyber operations in the space sector as part of the war in Ukraine



Source: Compiled by Clémence Poirier

1.1 Roscosmos: a symbolic target

Figure 9: Number of identified operations against Roscosmos and the number of official reactions from Roscosmos



Source: Compiled by Clémence Poirier

Roscosmos (Роскосмос) is Russia's national space agency. It is in charge of implementing Russia's space po licy and regulations, carrying out Russia's space program, and conducting international space cooperation and space research for both civilian and military purposes. It is often the main shareholder of Russian space companies.

Roscosmos has been a symbolic and recurring target for pro-Ukrainian groups, accounting for about 24.6% of all pro-Ukrainian attacks against Russia's space sector. Most of these attacks are DDoS campaigns conducted against different Roscosmos' websites, as well as the agency's online authentication portals.

When the Russian invasion of Ukraine commenced in February 2022, Dimitry Rogozin was the head of Roscosmos - and had been serving in that role since 2018. Rogozin's avid use of social media and controversial public statements significantly shaped the tone and perception of the agency as a polarizing actor. In July 2022, Rogozin was eventually dismissed and replaced by then Deputy Prime Minister Yuri Borisov. Rogozin currently serves as a senator for the Russian-occupied Zaporizhzhia Oblast.

Pro-Ukrainian groups view Roscosmos as a direct contributor to the Russian war effort. Roscosmos for example introduced a *"principle of mobilization"* to reorganize its production efforts for wartime.[18] In June 2023, the Financial Times revealed that Roscosmos was recruiting and training a battalion of its employees to be sent to the frontline.[19] Since May 2023, Roscosmos has been under Ukrainian sanctions.[20]

When it comes to cyber operations against Roscosmos we can distinguish between two distinct phases:

February 2022 to July 2022: out of 15 operations in total, 13 were conducted between February and July 2022. This period was marked by chaotic public relations and strong public rhetoric from Roscosmos and Dimitry Rogozin. Many DDoS attacks on the space agency's website were publicly acknowledged by the agency and generated strong and antagonistic reactions to the extent that Rogozin would even personally react to hacktivists' claims on Twitter. On the one hand, in March 2022, Rogozin declared to Russian news media outlet Interfax that cyberattacks against Russian satellites would be considered as casus belli.[21] On the other hand, Roscosmos underlined the uselessness of DDoS attacks on Roscosmos' websites and the lack of impact on Roscosmos' operations. These statements were widely disseminated in both Russian and Western media. Similarly, on March 1, 2022, pro-Ukrainian hacktivist

[18] Сидоркова, Инна. "Рогозин Ограничил Сотрудникам «Роскосмоса» Выезд За Рубеж и Отпуска." *РБК*, 9 Mar. 2022, https://rb.gy/0yn1pn.

[19] Berger, Eric. "It Appears That Roscosmos Really Is Recruiting Soldiers for the Ukraine War." *Ars Technica*, 20 June 2023, https://rb.gy/e2ch4s.

[20] "Державна Корпорація з Космічної Діяльності 'Роскосмос.'" *NSDC of Ukraine Office*, https://drs.nsdc.gov.ua/actions/personal.

[21] "Рогозин Назвал Попытки Взлома Хакерами Российских Спутников Casus Belli." *Интерфакс*, 2 Mar. 2022, https://www.interfax.ru/russia/825713.

group Network Battalion 65 (NB65) claimed on its Twitter account that it broke into the Vehicle Monitoring System of one of Roscosmos' Earth observation satellites. The following day, Dimitri Rogozin denied these allegations.[22] On March 18, 2022, NB65 directly responded to Rogozin's comments and leaked internal documents of Roscosmos to prove its point.[23] In addition, Rogozin was promptly reacting to sanctions against the Russian space sector and the termination of international cooperation in space missions. Rogozin threatened to disconnect the Russian segment of the International Space Station (ISS), warning that it is responsible for orbit correction and collision avoidance. Without it, the ISS would crash down to Earth.[24] Rogozin's comments likely added fuel to the fire.

July 2022 onwards: in July 2022, the Kremlin announced that Dimitri Rogozin was dismissed from Roscosmos and replaced by then Deputy Prime Minister Yuri Borisov.[25] With Borisov's onboarding, Roscosmos stopped publicly acknowledging DDoS attacks against its website. Overall, the agency's public relation's posture became blander and moved away from war-related topics. A few cyber operations against Roscosmos still occurred, but the overall quantity of attacks against Roscosmos significantly dropped.

Similarly, pro-Ukrainian threat actors were often mocking Rogozin on their Telegram channels in the first few months following the invasion, this behavior almost entirely stopped once Borisov took over. In the same vein, some pro-Ukrainian hacktivist group such as V0g3lSec claimed to have targeted Rogozin's cell phone.[26] It does not seem that Borisov was personally targeted at all. Although Roscosmos' contribution to the Russian war effort remains unchanged, Rogozin's posture may have further incentivized threat actors to continue their attacks on Roscosmos as it gave them significant visibility and media coverage regardless of the extent of the damage caused by each operation.

Surprisingly, while Russia's space agency is seen as a symbolic target, Ukraine's national space agency has neither been targeted nor mentioned in any pro-Russian hacktivist channels. Notably, Ukraine does not have sovereign satellites and thus heavily relies on foreign space systems. Thus, pro-Russian hackers often prefer to target Western space agencies such as NASA, CNES, ESA, or even the Swedish National Space Agency (SNSA).

The IT Army of Ukraine targets Roscosmos website

On June 28, 2022, the IT Army of Ukraine announced a DDoS attack against Roscosmos' website and posted a check-host.net screenshot. The group declared that the *"Space Agency website is down as result of pointless intimidation too."*[27] The intimidation likely refers to Roscosmos' reactions to other cyberattacks or to sanctions.

On June 29, 2022, Roscosmos' press service reacted to the incident on its Telegram channel. It stated that *"after Roscosmos published space images of 'decision-making centers', the state corporation's website was subjected to a DDoS attack. This time […] not from abroad, but from my native Yekaterinburg."* It is likely that the attacker used a VPN to mask its IP address to appear as if they were located in Yekaterinburg, Russia. The IT Army, as most hacker groups, is using VPNs to conduct its operations.[28] Roscosmos' press service further outlined that *"Roscosmos IT specialists successfully repelled a massive cyberattack on the state corporation's website. […] The site is stable. The DDoS attack had no result."* On the same day, the IT Army shared another message on its Telegram channel, ironically stating: *"Roscosmos […] still cannot find their website. Friendly fire suspected"* along with screenshots of Russian news articles from Lenta, RIA Novosti, and Izvestia that were reporting on the DDoS attack.[29]

On July 4, 2022, Roscosmos reported that its team traveled to Yekaterinburg for an exhibition and seized the opportunity to recall the DDoS attack that allegedly came from there: *"Roscosmos entered Yekaterinburg, from where DDoS attacks on the Roscosmos website were recently conducted. […] For hackers, I would like to inform you that your attacks on the State Corporation's website do not cause any damage to Roscosmos. The Roscosmos website is a purely informational platform that does not provide commercial services to partners or government services to the public and is in no way tied to the internal processes of the rocket and space industry. That is, the temporary disabling of the site only makes it difficult for readers to read the official messages of the State Corporation - no more."*[30]

---

[22] Rogozin. "X.Com." *X (Formerly Twitter)*, https://t.ly/9mCww. Accessed 10 July 2024.

[23] NB65. "X.Com." *X (Formerly Twitter)*, 18 Mar. 2022, https://rb.gy/rnupgf. Accessed 10 July 2024.

[24] Grush, Loren. "Russian Space Director's Wild Threats Could Have Real Implications for the ISS." *The Verge*, 25 Feb. 2022, https://shorturl.at/eidAe.

[25] TASS. "Putin Picks Former Deputy PM Borisov to Head Roscosmos." *TASS*, 15 July 2022, https://tass.com/politics/1480581.

[26] "v0g3lSec (@v0g3lSec)." *Twitter*, https://shorturl.at/ar86J. Accessed 10 July 2024.

[27] "IT ARMY of Ukraine." *Telegram*, https://shorturl.at/RM7O8. Accessed 12 July 2024.

[28] IT Army of Ukraine. *Інструкції Для VPN*. https://itarmy.com.ua/vpn/. Accessed 12 July. 2024.

[29] "---." *Telegram*, https://shorturl.at/eHnJQ. Accessed 12 July 2024.

[30] "Закрытый Космос." *Telegram*, https://t.ly/asALx. Accessed 12 July 2024.

1.2 Starlink: a prime target for Russian threat actors?

Two days after the invasion, Starlink services were activated in Ukraine to provide internet broadband to the Ukrainian population, the government, and the Ukrainian military.[31] On March 5, 2022, Elon Musk announced that SpaceX's resources were *"reprioritized to cyber defense & overcoming signal jamming",* suggesting a potential high number of cyberattacks.[32] Due to the intensity of Russian electronic attacks against Starlink, SpaceX also had to remotely update the software of its user terminals.[33] Pro-Ukrainian hacktivist group Cybersec announced they would retaliate to these attacks.[34] According to Musk, Starlink is often the only non-Russian communication system available in some parts of Ukraine, which naturally raises the probability of electronic signals being identified and modems eventually being shelled.[35] By May 2024, Starlink accounted for more than 3 million customers, with a significant share in Ukraine.[36]

The analysis of threat actors' social media accounts revealed that **Starlink is regularly mentioned by hacktivists.** Pro-Russian groups often share news related to Starlink, showcasing the ability of the Russian military to buy secondhand terminals for their own use; or to locate terminals used by the Ukrainian Armed Forces. Elon Musk is both praised and mocked by Russian and Ukrainian hackers alike, depending on his public statements and actions related to the conflict.

Considering the criticality of Starlink for Ukraine's military operations and the ability of its civilian population to connect to the Internet, one would assume that the number of cyber operations against Starlink would be very high. **Surprisingly, our dataset shows only a limited number of operations that have targeted Starlink.** The author identified four reported attacks against Starlink, three of which were conducted by the pro-Russian hacktivist group Killnet and Russian advanced persistent threat (APT) actor Sandworm (i.e. GRU's unit 74455). Killnet carried out two DDoS attacks against Starlink's official website and authentication portal. Sandworm infiltrated Ukrainian Android tablets, which were used by Ukrainian soldiers and were connected to Starlink in order to retrieve information about the satellite constellation.

Sandworm's interest in Starlink

On August 8, 2023, the Security Service of Ukraine (SBU) issued a press release and a technical report regarding Russian attempts to access Android devices used by Ukrainian soldiers through the deployment of 7 different malwares. The SBU attributed the attack to Russian military intelligence, specifically Sandworm.[37]

The attack did not directly target space assets. Yet, SBU believes that the operations primarily geared towards data gathering to gain insights on the *"configuration of connected Starlink satellite terminals."*

The SBU noted that Sandworm aimed to *"abuse the preconfigured access to local networks in some devices to take appropriate intelligence measures and discover the methods for securing and distributing malicious files to other devices."*

The SBU noticed open ports (Android Debug Bridge mode) on devices. ADB is a command-line tool that enables communication between a computer and an Android device. SBU outlined that Russia *"planned to install malicious files to gain a foothold in on the devices"* using the ADB mode. Several malwares were identified, which aimed at ensuring *"persistence in the systems and carry[ing] out internal intelligence"; "remote access to the device"; "exfiltrating data" and "gather data from Starlink satellite system"*.

SBU noted that the malware was *"developed to operate on systems with mobile ARM architecture. It contains a set of commands and internal terminal and router IP addresses to connect with Starlink via the internal network. While operating, a TCP connection is established by sending hex data in the HTTP request body via a POST request. The result is saved on the local device."* The SBU concluded that the malware is intended for intelligence purposes.

The SBU assessed that the preparation stage for the attack was long and thorough, and that the Tactics, Techniques, and Procedures (TTP) were typical for APT actors.[38] The SBU said that it managed to block these attacks. It remains unknown whether Sandworm managed to get any information at all about Starlink.[39]

---

[31] Fedorov, Mykhailo. "X.Com." *X (Formerly Twitter)*, https://t.ly/PeldH. Accessed 13 July. 2024.

[32] Musk, Elon. "X.Com." *X (Formerly Twitter)*, https://t.ly/qOOY0. Accessed 13 July. 2024.

[33] ---. "X.Com." *X (Formerly Twitter)*, https://t.ly/3SYnn. Accessed 13 July 2024.

[34] "CyberSec's UA." Telegram, 2022, https://t.ly/maJEl. Accessed 13 July 2024.

[35] Musk, Elon. "X.Com." *X (Formerly Twitter)*, https://t.ly/SEVot. Accessed 12 July 2024.

[36] "Starlink Celebrates New Milestone: 3 Million Customers in 99 Countries." *TESLARATI*, 21 May 2024, https://shorturl.at/0obcm. Accessed 12 July 2024.

[37] "SBU Exposes Russian Intelligence Attempts to Penetrate Armed Forces' Planning Operations System." *SBU*, https://shorturl.at/mUogP. Accessed 13 July 2024.

[38] "Cyber Operation of Russian Intelligence Services as a Component of Confrontation on the Battlefield, Technical Report." *SBU*, https://shorturl.at/axWI1. Accessed 14 July 2024.

[39] SBU, op cit

What stands out is that these three cases were highly mediatized compared to many other attacks on the space sector,[40] illustrating the high value of Starlink as a target for pro-Russian threat actors.

In fact, **hacktivist groups on both sides are interested in targeting Starlink with cyber operations due to its potential for significant effects on the frontline**. For instance, a spokesperson of the IT Army of Ukraine stated that Russia was using Starlink on the battlefield and that if the group was *"able to disrupt communications near the Russian administrative points, they won't be able to see their drone feed data from the front"*.[41] Yet, the IT Army never claimed any electronic or cyberattack on Starlink in its public communications. It may be assumed that the IT Army would ultimately see an attack on Starlink as a double-edged sword where both Ukraine and Russia would risk being affected.

Similarly, in April 2024, Dmitry Kuzyakin, Director General of the Russian Center for Integrated Unmanned Solutions (Центр Комплексных Беспилотных Решений – ЦКБР), which produces and trains operators of First Person View (FPV) military drones, accused the Ukrainian Armed Forces of hacking Starlink terminals to bypass territorial restrictions.[42] SpaceX blocked Ukrainian Armed Forces' access to Starlink over areas such as Crimea[43] or for specific operations such as drone strikes.[44] These accusations stem from claims that Russia managed to capture and dissect a "Baba Yaga" Ukrainian military drone, which was equipped with a Starlink antenna. It led them to discover that significant changes to the terminal and the software were made to remove territorial restrictions as well as paywalls and thus use Starlink as free riders. Kuzyakin stated that a Raspberry Pi (i.e., small single-board computer) was likely used to implement these changes. Kuzyakin asserted that such changes were impossible to carry out without insider information either 1) directly provided by SpaceX to tacitly support Ukrainian Armed Forces or 2) coming from a data leak that provided sensitive information about Starlink.[45] However, it remains impossible to verify Kuzyakin's claims.

The low number of operations identified by the report's open-source mapping can be explained in two ways:

First, open-source mapping depends on public disclosures, by either the attacker, the victim, or a third source who has insider knowledge about an incident. In the case of hacktivist groups, public self-attribution statements are common. Other operations against Starlink may have been discussed on invite-only hacker fora or invite-only Telegram channels that were inaccessible to the author. When it comes to state actors, self-attributions are rare. Instead, intelligence assessments are publicly shared weeks if not months or years after the fact by cybersecurity companies, government agencies, media outlets, or the victims themselves. Thus, while Killnet's operations were self-attributed, Sandworm's was officially attributed by Ukraine's Main Directorate of Intelligence (GUR). When we look at the role of Starlink in the war in Ukraine we can safely assume that it is a high priority target for Russian intelligence services. But as long as neither SpaceX itself or a third party with knowledge of a cyber operation against SpaceX is publicly coming forward, open-source efforts are unable to map state actors and will only capture hacktivist groups that openly communicate their conduct.

Second, most efforts to curtail Starlink services in Ukraine might be jamming and spoofing (i.e. electronic warfare) rather than cyber activities. For instance, in May 2024, the New York Times reported that Ukraine's 92nd Assault Brigade, which was using Starlink for communications, intelligence, and drone operations, suffered from Russian electronic interference. It prevented them to use satellite communications and forced them to use text messages.[46] Russia is also well-equipped and experienced in conducting electronic warfare. In 2020, MITRE released a report underlining that Russia considers electronic warfare to be a major aspect of military operations, especially against what is perceived as the West's weakness - the reliance on high-bandwidth networks and space systems. MITRE noted that Russia was expanding the use of electronic warfare as an independent branch and testing dedicated units to disorganize Western armies.[47] In addition, in April 2024, Col. Nicole Petrucci, Head of US Space Force's Space Delta 3, reported that the *"the Ukraine-Russia conflict is more EW than we have ever seen before"*[48]

---

[40] Lyngaas, Sean. "Russian Military Hackers Take Aim at Ukrainian Soldiers' Battle Plans, US and Allies Say." CNN, 31 Aug. 2023, https://t.ly/HmhT7; Система Starlink, Используемая ВСУ, Была Взломана Хакерами. 19 Nov. 2022, https://t.ly/fFxiD. Accessed 15 Aug. 2024.

[41] Kirichenko, David. "Ukraine's IT Army Now Aids Drone Strikes on Russian Oil Refineries." *Euromaidan Press*, 29 June 2024, https://shorturl.at/xc6jt. Accessed 15 Aug. 2024.

[42] "В ЦКБР Сообщили, Что ВСУ Взломали Терминалы Starlink Для Бесплатного Выхода в Интернет." *ТАСС*, https://t.ly/mxliF. Accessed 15 Aug. 2024.

[43] Jordan, By Dearbail. "Elon Musk Says He Withheld Starlink over Crimea to Avoid Escalation." *BBC News*, 8 Sept. 2023, https://shorturl.at/ZYLIt. Accessed 15 Aug. 2024.

[44] Brodkin, Jon. "Musk Refused Ukraine's Request to Enable Starlink for Drone Attack [Updated]." *Ars Technica*, 7 Sept. 2023, https://t.ly/_6N6q. Accessed 15 Aug. 2024.

[45] *TACC, op cit.*

[46] Mozur, Paul, and Satariano, Adam. "Russia Is Increasingly Blocking Ukraine's Starlink Service." *The New York Times*, 24 May 2024, https://t.ly/AJCAT. Accessed 15 Aug. 2024.

[47] Thomas, Timothy. "Russia's Electronic Warfare Force: Blending Concepts with Capabilities." *MITRE Center for Technology and National Security*, 2020.

[48] Gordon, Chris. "'More EW Than We Have Ever Seen Before' in Ukraine, Space Force Official Says." *Air & Space Forces Magazine*, 24 Apr. 2024.

Pro-Russian hacktivist group Killnet targets SpaceX's Starlink

On November 18, 2022, pro-Russian hacktivist group Killnet claimed on its Telegram channel that it launched a DDoS attack against Starlink. Killnet shared the following message: *"We have long been waiting for this, comrades!"*. The group subsequently shared the details and consequences of the attack, highlighting that the collective DDoS attack prevented users from logging into Starlink, blocked the main Application Programming Interface (API) by overloading Starlink's database with *"tons of gigabytes of digital shit."* Killnet also provided a link to check-host.net which is an online portal in which internet users can check for the availability of websites, servers, or IP addresses online. Killnet also credited its sub-groups and individual hackers that took part in the attack such as Killmilk (leader and founder of Killnet), Msidstress, Radis, Anonymous Russian, Mirai, and Halva.[49]

It seems that Starlink promptly reacted to the attack. Killnet shared another message 17 minutes later, outlining that Starlink was changing its authentication links.

Killnet subsequently asked its followers to go to Starlink's website and click on the login page, take screenshots, and share them online. Killnet then again noted that "Starlink's databases are offline." Two hours after the first claim of the attack, Killnet published a video of the targeted website to show the attack was successful along with the caption: *"we would like to point out that the personal accounts of millions of Starlink users still do not work!"* and a check-host.net link.[50] Killnet then shared a link and screenshot of downdetector.com, which is a website that enables users of online services to report problems and incidents. The screenshot illustrates a peak of reported incidents for Starlink. It is important to note that Down Detector only reports incidents when the number of problem reports is significantly higher than usual.[51]

On November 19, 2022, Killnet shared another message on its Telegram channel and announced that it was continuing to target Starlink's website. It once again provided a check-host.net link to prove the attack was still ongoing along with a screenshot of the defaced website.[52] The attack was also widely shared and publicized by Telegram channels covering news from the war[53], Russian media figures on Telegram channels[54] and news outlets.[55]

Interestingly, Valentin Gorshenin, special correspondent for Russia Today, posted a message on its Telegram channel to take credit for giving Killnet the idea to target Starlink. Indeed, on November 17th, 2022, he posted a call to action to hackers to target the Ukrainian mobile application eRaketa, which enables Ukrainians to share GPS coordinates with Ukrainian air defense when they see a Russian missile or drone fly above their heads. Although it did not mention Starlink, Gorshenin posted another message on November 19th, 2022, to recall that he called upon IT specialists to block websites and applications that work in the *"interests of the enemy"* and that his *"cry was picked up by the KILLNET team"*. He further noted that *"his team did more than just disable the Ukrainian military's instrument […] KILLNET hackers blocked the satellite communication system for more than 3 hours across the world".*[56] This message was reshared by Killnet on the group's channel.[57] It remains unclear whether Killnet's idea to target Starlink really came from Gorshenin.

The attack does not appear to have targeted the space, ground, or user segments in this case, but rather the user interface. It means that the space system itself was not targeted in this attack. Yet, it still prevented users from accessing satellite connectivity.

---

[49] "WE ARE KILLNET." *Telegram*, 18 Nov. 2022, https://t.me/killnet_reservs/3565. Accessed 16 Aug. 2024.

[50] "---." *Telegram*, 18 Nov. 2022, https://t.me/killnet_reservs/3582. Accessed 16 Aug. 2024.

[51] "---." *Telegram*, 18 Nov. 2022, https://t.me/killnet_reservs/3583?single. Accessed 16 Aug. 2024.

[52] "---." *Telegram*, 19 Nov. 2022, https://t.me/killnet_reservs/3596. Accessed 16 Aug. 2024.

[53] "---." *Telegram*, 18 Nov. 2022, https://t.me/killnet_reservs/3581. Accessed 16 Aug. 2024.

[54] "Soloviev Live." *Telegram*, 18 Nov. 2022, https://t.ly/qfAOi; "RT Russian." Telegram. 19 Nov 2022, https://t.me/rt_russian/137289. Accessed 16 Aug. 2024.

[55] Мартынова, Полина. "Хакеры Killnet Атаковали Сервисы Системы Starlink." *РБК*, 19 Nov. 2022, https://www.rbc.ru/technology_and_media/19/11/2022/6377edef9a7947d0be3f5e78. Accessed 16 Aug. 2024.

[56] "Работает Горшенин!" *Telegram*, 19 Nov. 2022, https://t.me/s/vgor999?q=starlink. Accessed 16 Aug. 2024.

[57] "WE ARE KILLNET." *Telegram*, 19 Nov. 2022, https://t.me/killnet_reservs/3605. Accessed 16 Aug. 2024.

1.3 Earth observation companies under attack

Following the invasion of Ukraine, Ukraine's Minister of Digital Transformation called upon commercial Earth observation (EO) companies to share satellite images with Ukraine.[58] Progressively, several companies such as Planet, Capella Space, Satellogic, ICEYE, or MDA Space publicly declared their support and agreed to directly or indirectly provide data to Ukraine.

In addition, satellites images made their way to the general press, providing better awareness about the capabilities of Earth observation satellites. For instance, Maxar Technologies signed partnerships to provide satellite images to several media outlets. As a result, many Maxar images are used to illustrate news reports on the war in Ukraine.[59] This strategy enabled EO companies to demonstrate their capabilities, but also put them in the crosshairs of cyber threat actors'.

In this context, and especially after the ViaSat hack, Earth observation companies started to realize that their threat model was evolving, calling for enhanced cybersecurity and cyberdefense capabilities. It created some panic within the EO industry, which saw the number of cyberattacks increase. EO industrial stakeholders declared that they had to improve cyber monitoring following the invasion of Ukraine and be more aware of espionage.[60] Some companies even expressed their concerns regarding the lack of identified process for reporting cyberattacks and coordinating incident response.[61] Some also underlined that most cyberattacks they faced targeted the IT environment of their companies rather than their space systems, which is consistent with the findings of the dataset.[62]

Throughout the report, identified threat actors' social media channels were searched for references to Earth observation companies, in particular the ones that publicly provide images to Ukraine. Hacktivist groups sometime use and discuss satellite images. Some use readily available satellite images for disinformation purposes. Others may modify such images for information warfare, but such operations are usually limited to groups that specialize in this domain and do not conduct other types of cyber operations, and therefore were not included in the scope of the report. Threat actors rarely mention specific EO companies as their main targets. It can be assumed that the dataset only represents a small part of all operations against the EO industry and that most attacks are probably not conducted by hacktivist groups. The dataset also illustrates that the EO industry rarely publicly communicates in case of cyber incidents.

Identified operations in the dataset targeted a few EO companies such as Maxar with both DDoS and credential theft.

Maxar's credentials for sale online

In June 2023, an offer was published on a Russian-speaking forum to sell access to a satellite operated by the US Earth observation company Maxar Technologies for 15.000 USD. The post originated from a user named "labs666," who claims to have no affiliation with any hacker group. The post specifically notes that this access would enable the buyer to "see military and strategical positions." Labs666 offered prospective buyers to pay through escrow accounts.[63]

It is unknown whether labs666 had gained access to actual Maxar credentials or whether anyone took up the offer and paid 15.000 USD.

Maxar's credentials may have been obtained through various ways such as phishing, social engineering, keylogging, brute force attacks, credential stuffing, or insider threats.

Interestingly, two operations from pro-Russian hacktivist group Cyber Army of Russia, which are described below, aimed at targeting ICEYE but ended up affecting ESA, which demonstrates how actors that are not involved in the conflict can end up being targeted, which calls for a larger threat model for space actors. Companies involved in various verticals, including Earth observation, also got targeted by DDoS (e.g., Leonardo). However, they are rarely targeted for their specific remote sensing activities. Other operations were targeted at EO entities, including the National Geospatial Intelligence Agency (NGA), NASA's online climate portals, the US National Oceanic and Atmospheric Administration (NOAA) databases, the US Geological Survey's database, ESA's climate portals, CNES' ANGELS website, or the Russian Far Eastern Scientific Research Center of Space Hydrometeorology "Planet".

[58] ---. "X.Com." *X (Formerly Twitter)*, 1 Mar. 2022, https://t.ly/bZww6.

[59] "News Bureau." *Maxar*, 2024, https://maxar.com/news-bureau.

[60] "Security Officer in a New space company – dream job or mission impossible"? *Cysat 2024*, Conference, Paris, April 2024

[61] Albon, Courtney. "How Commercial Space Systems Are Changing the Conflict in Ukraine." *C4ISRNet*, 25 Apr. 2022, https://t.ly/vI6vh. Accessed 18 Aug. 2024.

[62] "Switzerland in Space: Navigating between Security Threats and Opportunities" ETH-Arbeitstagung, Zurich, July 2024

[63] Waqas. "Military Satellite Access Sold on Russian Hacker Forum for $15,000." *Hack Read*, 21 June 2023, https://t.ly/j0Lfw. Accessed 18 Aug. 2024.

Cyber Army of Russia attempts to target ICEYE and eventually attacks ESA

On August 18, 2022, ICEYE issued a press release to announce it signed a contract to provide images to Ukraine. On the same day, the hacker group Cyber Army of Russia called upon its Telegram members to DDoS the Finnish space company ICEYE.

Cyber Army of Russia declared: *"Our new important goal. The Finnish company ICEYE and the foundation of Ukrainian businessman Serhiy Prytula, who entered into an agreement to provide the Ukrainian Armed Forces with full access to satellite images of one of the ICEYE satellites for [a period of] more than a year ahead."*[64]

Indeed, ICEYE signed a contract with the Serhiy Prytula Charity Foundation, which is a Ukrainian NGO *"focused on strengthening the Defence Forces of Ukraine and providing assistance to the civilians affected by Russian aggression."*[65] It purchases various systems that can support the army such as UAVs, thermal binoculars, digital VHF radios, digital mobile radios, Starlink terminals, etc.[66] The agreement with ICEYE comprises the leasing of the full capacity of one of ICEYE's Synthetic Aperture Radar (SAR) satellite, which remains operated by the company. It means that it grants Ukraine with access to satellite images, which can be captured through cloud covers and at night. The agreement also enables Ukraine to have access to other satellites of the ICEYE constellation.[67]

What is surprising is that the Cyber Army of Russia shared a URL and IP address to attack with its community. However, it did not share a URL owned or related to ICEYE, but a URL of the European Space Agency's Earth Online portal.[68] As a result, the target of the attack ended up being ESA rather than ICEYE. Along with its message, Cyber Army of Russia published a screenshot of ESA's website, which lists its mission programs, including Earth explorer, Heritage missions, and Third-party missions.[69]

ESA is not involved in defense-related activities and does not provide any images to Ukraine. However, ICEYE and ESA have been cooperating via the Third Party Missions Program (TPM) since 2020. TPMs are Earth observation missions that are owned and operated by commercial companies or public agencies, whose data is distributed free of charge under ESA's Earthnet Programme.[70] It is unclear whether the DDoS against ESA was in relation to ICEYE's participation in the Earthnet Programme or whether the Cyber Army of Russia misunderstood the relationship between ICEYE and ESA.

On May 5, 2023, the exact same message was posted by the Cyber Army of Russia on its Telegram channel with the same ESA website URL, IP address, and screenshot.[71] Notably, on the same day, the Ukrainian military intelligence service (GUR) released an article titled *"People's satellite sees everything!"* which praised the relevance of ICEYE's satellite imagery for Ukrainian military operations.[72]

In these attempted attacks, space systems themselves were not targeted, but only the websites of ESA. It is unclear whether the attack was successful. Neither ESA nor ICEYE reacted to the activities of Cyber Army of Russia.

---

[64] "Народная CyberАрмия." *Telegram*, 18 Aug. 2022, https://t.me/CyberArmyofRussia_Reborn/972. Accessed 20 Aug. 2024.

[65] *"About Ukrainian Charity: Serhiy Prytula Charity Foundation." Prytula Foundation, 2024, https://prytulafoundation.org/en/about.* Accessed 20 Aug. 2024.

[66] "Help Ukrainian Defence Forces." *Prytula Foundation*, 2024, https://prytulafoundation.org/en/help-army. Accessed 20 Aug. 2024.

[67] "ICEYE Provides Ukraine with Access to Its SAR Satellite Constellation." *ICEYE*, 2022, https://www.iceye.com/press/press-releases/iceye-signs-contract-to-provide-government-of-ukraine-with-access-to-its-sar-satellite-constellation. Accessed 20 Aug. 2024.

[68] "Народная CyberАрмия." *Telegram*, op cit.

[69] Ibid

[70] "Third Party Missions." *ESA Earth Online*, 2024, https://earth.esa.int/eogateway/missions/third-party-missions. Accessed 20 Aug. 2024.

[71] "Народная CyberАрмия." *Telegram*, 2022, https://t.me/s/CyberArmyofRussia_Reborn?q=ESA. Accessed 20 Aug. 2024.

[72] "'Народний Супутник' Бачить Все!" *ГУР МО*, 5 May 2023, https://gur.gov.ua/content/narodnyi-suputnyk-bachyt-vse.html. Accessed 20 Aug. 2024.

1.4 Guidance Gambit: cyber threats against GNSS

Today, all modern armed forces are dependent on Position Navigation and Timing (PNT) and almost all operations rely on Global Navigation Satellite Systems (GNSS), including for missile guidance, strikes, location and situational awareness, etc. In Ukraine, GNSS signals are subject to electronic warfare on a daily basis affecting both civilian and military systems. [73] These jamming and spoofing efforts also affect neighboring countries.[74] But are GNSS systems a high value target for hacktivists as well?

Among the 124 identified cyber operations in our dataset, 12 were conducted by hacktivist groups against satellite navigation. In terms of types of attacks, 64% were DDoS against GNSS(-based) systems or companies. 36% were intrusions. 51% of them were conducted in support of Russia. They targeted GPS-based business such as Polish company Flotis, Ukrainian company Locarus, or US-based companies Garmin and TrafficView. 47% of operations were carried out in support of Ukraine. They targeted GNSS receivers around the Kremlin, GNSS receivers around a Russian hydroelectric power plant, the websites of Russia's global navigation satellite system (GNSS) GLONASS, and Russian website GPSUpdate.ru. This sample, albeit small, can provide some insights. First, no attack successfully targeted GNSS satellites in orbit. Most attacks targeted the ground segment, the user segment, or the user interface. Second, these operations illustrate how downstream applications and companies, which rely on GNSS to function, can be targeted by cyber operations (e.g., Locarus, Flotis). Third, while GNSS systems are dual use, the majority of these targets were civilian ones, which are not related in any way to the conflict in Ukraine.

Looking at threat actors' communications, the IT Army of Ukraine mentioned GNSS systems. Its first ever post called upon volunteers to target Russia through DDoS attacks by providing a list of 21 Russian top priority targets, including banks, businesses, and government websites. The IT Army of Ukraine included GLONASS.[75] However, it never publicly claimed any attack on that system. Moreover, among threat actors, who effectively conducted operations against GNSS(-based) targets, they often shared screenshots of user interfaces of GNSS receivers to prove their intrusions were successful. Yet, it remains difficult to find additional proof that these operations really took place.

As a result, GNSS systems are perceived as important assets in the conflict, which caught the attention of hacktivists. No operation conducted by a state-sponsored actor was identified, although they probably happened. They are simply not publicly reported.

NoName057(16) targets Polish company Flotis

In February 2024, Polish farmers took part in a series of protests against the European Green Deal and the continued grain imports from Ukraine, which they perceive as an economic threat to their business. These protests led to an agreement between the Polish Minister of Agriculture and various farmers' trade unions to suspend imports of agricultural products from Ukraine.[76]

This event was used as an opportunity by pro-Russian group NoName057(16) to target Polish websites, including Flotis' website.[77] Flotis is a GPS car and fleet monitoring service developed by the Polish software company Neptis S.A.[78]

NoName057(16) announced on its Telegram channel that it *"decided to support Polish farmers who went to extreme measures against the pro-Ukrainian policy of their country's authorities and hold protests."*[79] It subsequently shared a list of Polish websites to target such as the Polish National Roads and Highways Directorate General, the National Hotspot Service, the Gdańsk Transport Company or the Autobahn A4 and A2. Among them, Flotis was listed. All targets pertained to the transportation sector. NoName057(16) shared a link to check-host.net to prove its attack was successful.

Space systems were not targeted. Only the website of the company was temporarily unavailable. Flotis and Neptis did not publicly react to the incident.

Even though the farmer protests had nothing to do with the space sector or Flotis in specific, hacktivist still targeted Neptis.

[73] "Daily Fight for Ukraine Spectrum Superiority Puts Electronic Warfare Front, Center." *National Defense Magazine*, 8 Mar. 2023, https://t.ly/wtNiQ. Accessed 21 Aug. 2024.

[74] "Live GPS Spoofing and Jamming Tracker Map." *Skai Data Services*, 2024, https://spoofing.skai-data-services.com/. Accessed 22 Aug. 2024.

[75] "IT ARMY of Ukraine."*Telegram*, https://t.ly/kU51p. Accessed 22 Aug. 2024.

[76] "Polish Farmers End Protest as Government Agrees to Suspend Ukrainian Agricultural Product Imports." *AA*, 20 Mar. 2024, https://t.ly/RtSBz. Accessed 21 Aug. 2024.

[77] "NoName057(16)." *Telegram*, 4 May 2023, https://t.me/s/noname05716?q=flotis. Accessed 22 Aug. 2024.

[78] "O Nas." *Flotis*, 2024, https://flotis.pl/o-nas. Accessed 22 Aug. 2024.

[79] "NoName057(16)." *Telegram*, 4 May 2023, op cit.

1.5 Aerospace and defense companies: space as collateral damage

Out of the 124 identified operations, 35 were targeted at aerospace and defense conglomerates, which manufacture space systems or components. It represents a significant number of operations against the space sector, which is therefore important to analyze.

18 pro-Ukrainian operations targeted Russian aerospace and defense companies. These only include unsophisticated DDoS operations carried out by the IT Army of Ukraine and CyberPalyanitsa against the website of Russian defense company Rostec. 17 pro-Russian operations were targeted at Western aerospace and defense companies. These include more sophisticated operations such as hack-and-leak operations as well as exploitations of vulnerabilities against Lockheed Martin, which were conducted by From Russia With Love, Killnet, and its sub-group Legion Cyber Spetsnaz; or data leaks from French company Safran released by Just Evil. Other operations were unsophisticated DDoS against the websites of Boeing, Leonardo, Raytheon Technologies, Hensoldt, and JSC Kiev Radar Plant. Other operations likely took place but were simply not publicly reported.

Aerospace and defense companies are primarily targeted because they manufacture defense equipment and not because of their space activities. Hacktivist groups usually mention the specific equipment that these companies are manufacturing and how they are used on the battlefield. A few of these operations may be correlated with announcements related to weapons deliveries to Ukraine although this is not the majority.

Threat actors may not even be aware that these companies are involved in space activities. In some cases, hackers were even surprised to find information about space when targeting defense companies. This was the case of Killnet in its operation against Lockheed Martin, which mostly unveiled information about its cooperation with NASA (see Figure 10). As a result, the space sector can be seen as collateral damage in some cyber operations against defense companies.

Cyber Army of Russia targets Hensoldt

On May 18, 2023, hacktivist group Cyber Army of Russia called upon its community to target the German defense and space company Hensoldt.[80]

Hensoldt's space activities focus on the design and manufacturing of space optronics and electronics solutions.[81]

Cyber Army of Russia shared a quote from Russian military correspondent Evgeniy Poddubny stating *"New German TRML-4D radars may enter enemy service. HENSOLDT will deliver six radars in the second half of this year. Now, according to company representatives, Ukrainian operators are being trained. According to the performance characteristics, TRML-4D radars are capable of early detection, tracking and classification of various types of air targets: airplanes, helicopters and cruise missiles."*[82] along with a link to a post of Poddubny's Telegram channel depicting a TRML-4D radar.[83]

Cyber Army of Russia therefore called its members to attack the website of Hensoldt, providing a screenshot and the URL of the website and an IP address: *"We are attacking the HENSOLDT website! HENSOLDT's core business areas are intelligence sensors, electromagnetic spectrum management solutions and mission avionics systems. Our broadly diversified product portfolio caters to defense and security customers and covers the full range of air, sea and land mission applications. HENSOLDT solutions are used on a variety of platforms, including helicopters, fixed wing aircraft, unmanned aerial vehicles, ships and submarines, armored vehicles and satellites."*[84]

Hensoldt was not targeted due to its space activities but because of its defense activities, in particular the manufacturing of the TRML-4D radar. Yet, it still affected a space company.

As part of this attack, space systems themselves were not targeted, but only the websites of Hensoldt. Hensoldt did not react to the incident.

[80] "Народная CyberАрмия." *Telegram*, 18 May 2023, https://t.me/s/CyberArmyofRussia_Reborn?q=HENSOLDT. Accessed 22 Aug. 2024.

[81] "Space." *HENSOLDT*, 2024, https://www.hensoldt.net/what-we-do/space/. Accessed 22 Aug. 2024.

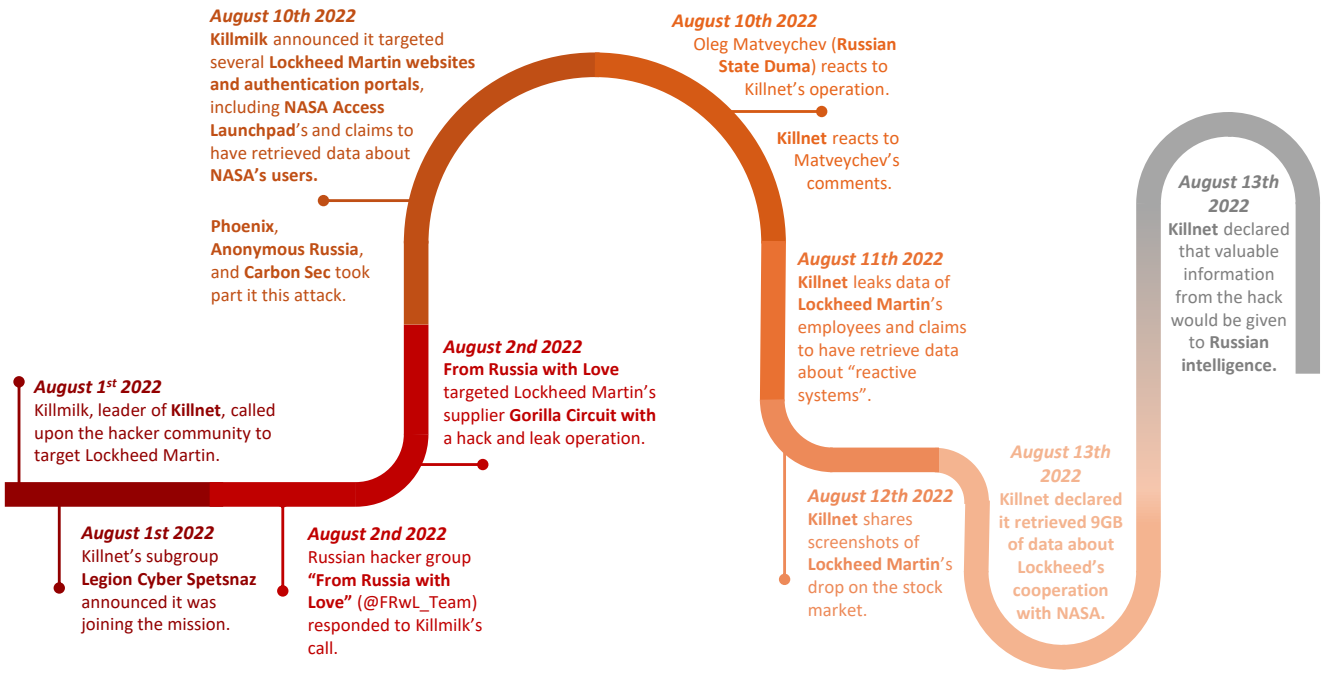
[82] Народная CyberАрмия." Telegram, 18 May 2023, op cit.

[83] "Поддубный." *Telegram*, 16 May 2023, https://t.me/epoddubny/15969. Accessed 22 Aug. 2024.

[84] "Народная CyberАрмия." Telegram, 18 May 2023, op cit.

Pro-Russian group Killnet's attack against Lockheed Martin: a tale of space as collateral damage

Figure 10: Timeline of Killnet's operations against Lockheed Martin



Source: Compiled by Clémence Poirier

On August 1, 2022, pro-Russian group **Killnet called upon the hacker community on its Telegram channel to target US aerospace and defense giant Lockheed Martin**.[85] In the context of the war in Ukraine, Lockheed Martin is probably most well-known for supplying the High Mobility Artillery Rocket System (HIMARS)[86] and the Army Tactical Missile Systems (ATACMS).[87]

Killmilk, Killnet's leader, declared: *"From this day forward, the defense corporation Lockheed Martin will be subject to my cyber attacks. The production control system of the Lockheed Martin industrial complexes will be paralyzed! All data of employees of this terrorist company will be published publicly. All Lockheed Martin employees will be persecuted and killed around the world! I am against weapons! I am against the trade in death! I call on all hacker groups to create escalation in the production cycles of Lockheed Martin around the world, as well as to disseminate personal information about the terrorists of this company. #BurnLockheedMartin #FUCKNATO #KillMilk #Killnet #ZOV."*[88]

Killnet's subgroup Legion Cyber Spetsnaz announced it was joining the mission on August 1, 2022. It called its members, in particular pentesters, to try to break into Lockheed Martin's network.[89] It remains unknown whether they were successful in their attempts.

On August 2, 2022, the Russian hacker group **"From Russia with Love"** (@FRwL_Team) responded to Killmilk's call with a blog post on telegra.ph.[90] **The group revealed that it targeted a US company named Gorilla Circuits** which is a manufacturer of printed circuit boards. Gorilla Circuits is one of Lockheed Martin's 16.000 suppliers worldwide. It is involved with the PAC-3 missile program, which was highlighted by From Russia with Love.[91]

From Russia with Love released the name and employee ID of dozens of Gorilla Circuit's employees as well as a list of customers, which explicitly included space actors such as Astronics, Boeing, NASA's Ames Research Center, Telespan Data, ViaSat Inc., etc. The blog further highlighted: *"we gained full access to the entire infrastructure of Gorilla Circuits and stole all data including backups from 2016 to the present, technical*

[85] "KillMilk." *Telegram*, 1 Aug. 2022, https://t.ly/qaat1. Accessed 22 Aug. 2024.

[86] Webmaster, OUSD A&S. "Advanced Rocket Launcher System Heads to Ukraine." *Office of the Under Secretary of Defense*, https://t.ly/fvVDC. Accessed 22 Aug. 2024.

[87] Holland, Steve, and Idrees Ali. "The US Quietly Shipped Long-Range ATACMS Missiles to Ukraine." *Reuters*, 24 Apr. 2024, https://t.ly/vAD26. Accessed 24 Aug. 2024.

[88] "KillMilk." *Telegram*, op cit.

[89] "Telegram Channel 'ЛЕГИОН🛡 - КИБЕР РАЗВЕДКА⚔' — @Legion_Russia ." *TGStat*, https://tgstat.ru/en/channel/@Legion_Russia. Accessed 1 Sept. 2024. Accessed 24 Aug. 2024.

[90] @FRwL_Team. "Возмездие!" *Telegraph*, FRwL_Team, 1 Aug. 2022, https://telegra.ph/Vozmezdie-08-01. Accessed 24 Aug. 2024.

[91] "USA PCB Manufacturer: Turn Key PCB Services." *Gorilla Circuits*, 21 Sept. 2020, https://www.gorillacircuits.com/. Accessed 24 Aug. 2024.

documentation of your confidential developments (which we will publish as necessary), data on supplies and consumers. What does this mean?! Let's just say one thing – '0-day'! All companies, organizations that use your products are now at risk or compromised, their data, like yours, is no longer safe. By the time we finish our business with you, they will no longer be safe. Even terrorist organizations work for fear of their privacy!"[92] It illustrates how space companies can be exposed through attacks against other companies in the supply chain.

However, looking at FRwL's operation, it is unclear whether the leaked data was new or came from an old leak. Gorilla Circuits is a US company based in California. It is therefore subject to the California Consumer Privacy Act (CCPA), which requires companies to send a sample copy of a breach notice to the California Attorney General whenever a breach concerns over 500 Californian residents. Looking at reported breach notices, the only one submitted by Gorilla Circuits dates from August 2021.[93] While the documents shared by FRwL does not seem to exceed 500 people, and therefore would not trigger a new submission of a sample notice, it may be assumed that FRwL might have used some or all data from the leak of 2021. Indeed, the documents of Gorilla Circuits contain dates that are all prior to August 2021, hinting towards the possibility of a reused leak.

On August 10, 2022, **Killmilk announced it targeted several Lockheed Martin authentication websites, including NASA Access Launchpad's authentication portal**. NASA Access Launchpad is NASA's single sign-on service, which enables employees and contractors to log into numerous NASA online portals and services such as SATERN, the Jet Propulsion Lab's standards and patents portal, etc. To connect through NASA's Access Launchpad, users either use a NASA Smartcard or an RSA SecurID token, which are physical methods of Multi-Factor Authentication (MFA). RSA SecurID are used by both NASA and Lockheed Martin.

Killmilk claimed that "*the authorization system using the "NASA" smart card + RSA authorization token + agency user indicator has been killed!"* and that **he retrieved the usernames of NASA's users**.[94] Killnet acknowledged that other groups such as Phoenix, Anonymous Russia, and Carbon Sec took part it this attack. Killnet then shared several screenshots of defaced Lockheed Martin websites. However, he did not share screenshots of defaced NASA websites.

Interestingly, **Killnet's operations against Lockheed Martin caught the attention Oleg Matveychev, Deputy Chairman of the Russian State Duma's Committee for Information Policy, Information Technologies, and Communications.** Speaking to Life.ru, Matveychev called upon Killnet to focus their attention on HIMARS-related information and directly provide data to the Russian government. He said "*All kinds of databases, intelligence information that helps to find out the plans of opponents, the movement of the same HIMARS across the territory of Ukraine are interesting. If you want to bring real benefit, open some chats, communications means of the Ukrainian special services or military to find out where and how the same HIMARS are deployed, where they are now and what their coordinates are in order to inform our military."*[95] Killnet shared the article on its Telegram channel noting "*Well, sorry, you could have called bro."*[96]

On August 11, 2022, Killnet released two Excel files, which contained the data of Lockheed Martin's employees. Killnet called its community to target these individuals: *"If you have nothing better to do, you can email the Terrorists from Lockheed Martin - photos and videos of the consequences of their weapons! Let them realize what they are creating and what they are contributing to."*[97] Killmilk then shared a post to claim that what he did with Lockheed Martin was *"only 0.1%"* of what they managed to get out of this operation. He claimed "*Next you will see the latest technologies of this corporation. Of course, I don't understand reactive systems, but it will probably be useful to someone."* [98] In this context, *"reactive systems"* may refer to various systems, including space technologies, that might be able to respond rapidly to environmental or operational changes such as navigation systems, gyroscopes, star trackers, radars, etc. However no further information was provided by Killnet. One can only speculate whether it refers to space or defense technologies. Killnet further highlighted that it gathered data of *"more than 100 thousand Lockheed Martin employees"* and that the value of Lockheed Martin on the stock market will be affected. He further noted that he will show more about Lockheed Martin in the near future.[99] On August 12, 2022, he clarified that *"everything that was published in our channel about Lockheed Martin has no value. Everything valuable will be given to the*

[92] @FRwL_Team. "Возмездие!" op cit.

[93] "Search Data Security Breaches." *State of California - Department of Justice - Office of the Attorney General*, 2024, https://t.ly/KL4MQ. Accessed 24 Aug. 2024.

[94] "DARKNET." *Telegram*, 10 Aug. 2022, https://t.me/killmilk_rus/20. Accessed 24 Aug. 2024

[95] Симоненко, Анатолий, and Юлия Архипова. "Депутат Матвейчев Дал Killnet Наводку Для Новых DDoS-Атак После Взлома Сайта Lockheed Martin." *LIFE*, 10 Aug. 2022, https://life.ru/p/1515435. Accessed 25 Aug. 2024.

[96] "WE ARE KILLNET."*Telegram*, 10 Aug. 2022, https://t.me/killnet_reservs/2296. Accessed 25 Aug. 2024.

[97] "---." *Telegram*, 11 Aug. 2022, https://t.me/killnet_reservs/2305?single. Accessed 25 Aug. 2024.

[98] "DARKNET." *Telegram*, 11 Aug. 2022, https://t.me/killmilk_rus/35.

[99] Ibid

whole world after our processing!!!"[100] Killnet has not publicly shared further information on this operation to this day. It is unknown whether Killnet truly managed to get additional data or whether the group was trying to impress the government's officials with such claims.

On August 13, 2022, Killnet gave an interview to Russia Today and declared ***"the most important thing we got was cooperation with NASA.*** *Lockheed Martin has been working closely with NASA's satellite system for more than a decade. We received more than 9 GB of various information."* Killnet's representative also underlined that valuable documents that were extracted would be given to Russian intelligence services: ***"If you are wondering where the valuable documents will go, then I can boldly tell you: they will go as a gift to our intelligence services."***[101]

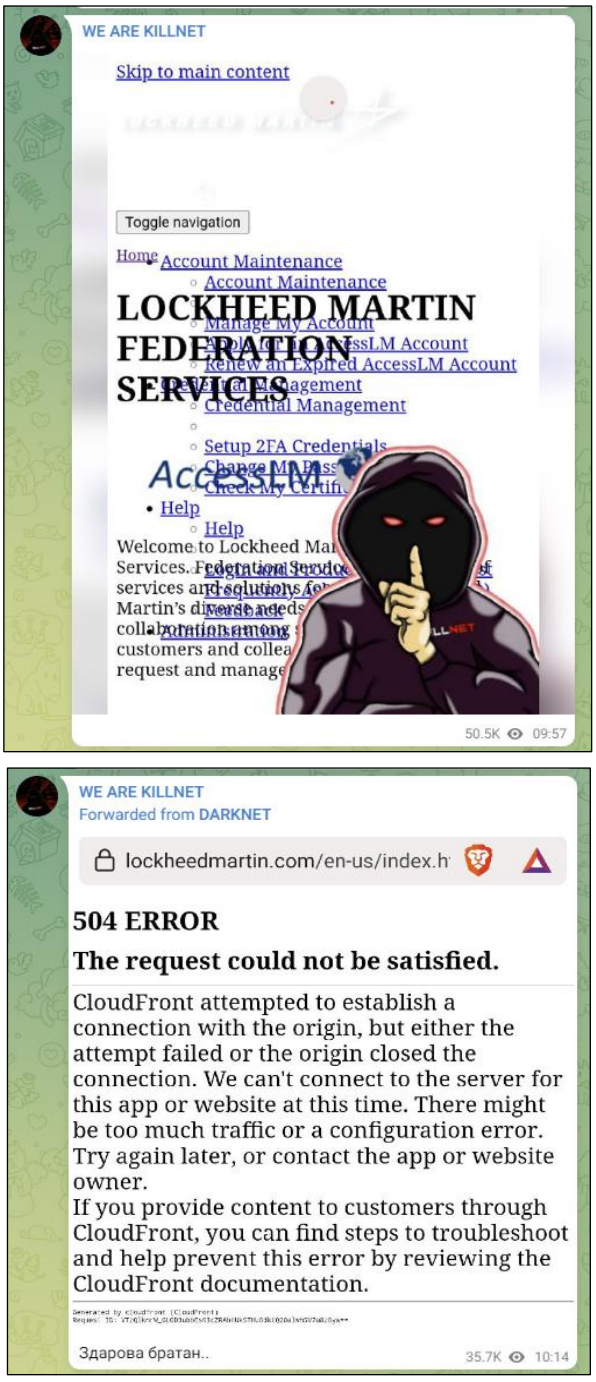
Similarly to other attacks, space systems do not seem to have been directly targeted, only the websites and authentication portals were. Yet, in this process, Killnet seems to have managed to retrieve information about Lockheed Martin's with NASA.

Lockheed Martin did not issue a press release, but a spokesperson told Newsweek that the company is *"aware of the reports and have policies and procedures in place to mitigate cyber threats to our business,"* and that it *"remain confident in the integrity of our robust, multi-layered information systems and data security."*[102] However, the company did not explicitly confirm the attack.

Overall, this operation against Lockheed Martin provides some insights regarding the state of cybersecurity in the space sector and the nature of organizations that are targeted:

- Lockheed Martin was targeted mostly because it manufactures defense equipment that is used in Ukraine and unlikely because of its space activities.
- NASA seems to almost constitute collateral damage in this operation. Killmilk even declared *"NASA-Nothing personal, you're just helping terrorists...."*, emphasizing that space actors might still be seen as civilian and scientific stakeholders by threat actors.[103]
- Hackers appear almost surprised that they found information about space instead of defense equipment.
- Hackers did not seem to have retrieved specific information about the defense equipment they looked for, but found information about Lockheed Martin's cooperation with NASA, suggesting this might have been less protected than defense-related data.
- It is not just space systems and space companies that are at risk, but also the employees of space organizations and their data.

Figure 11: Screenshots of Killnet's telegram channel



[100] Ibid

[101] "RT Russian." *Telegram*, 2022, https://t.me/rt_russian/123685. Accessed 28 July 2024.

[102] Carbonaro, Giulia. "HIMARS-Maker Lockheed Martin 'Confident' Against Russian Hackers." *Newsweek*, 10 Aug. 2022, https://shorturl.at/PdFs7. Accessed 28 July 2024.

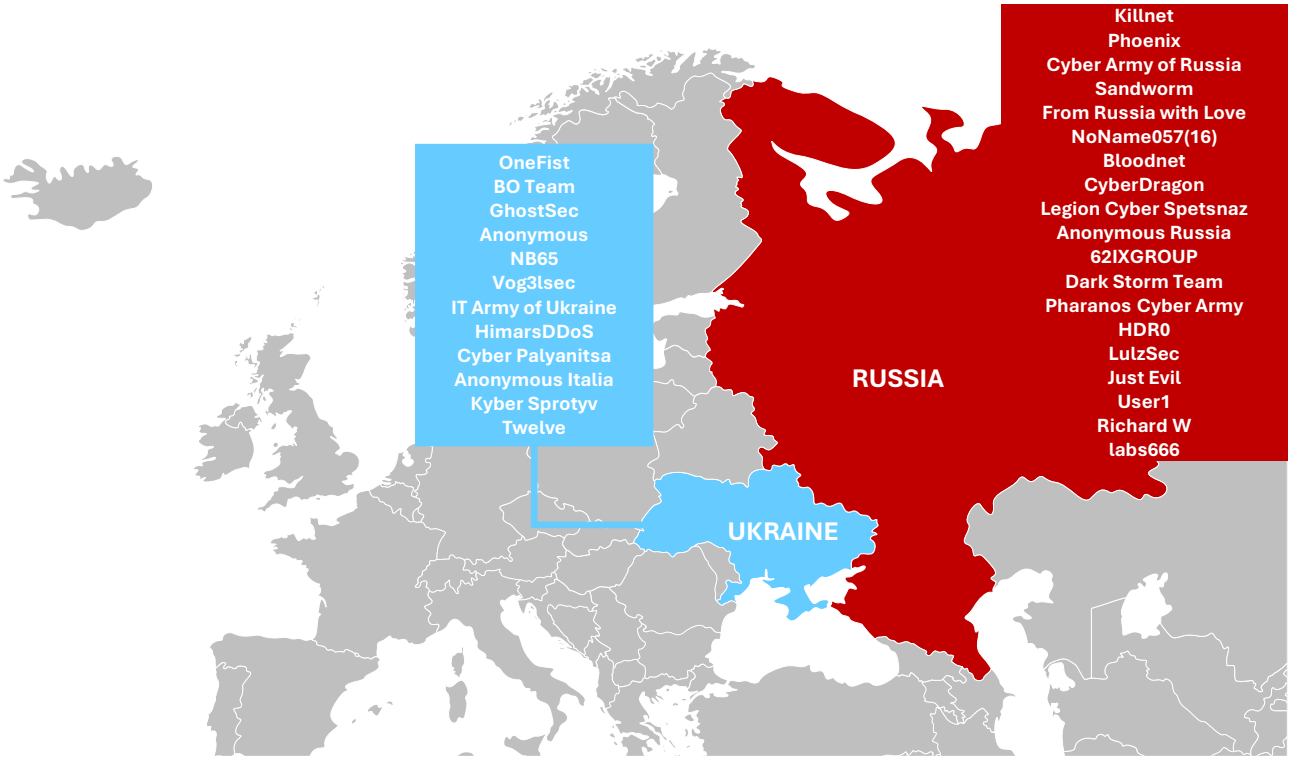
[103] "DARKNET." *Telegram*, 2022, https://t.me/s/killmilk_rus?q=nasa. Accessed 28 July 2024.

2 Understanding threat actors' behaviors

This chapter provides an overview of the various hacker groups that target the space sector as part of the Russo-Ukrainian war, how they behave, how it impacts activities on the battlefield, and how they are linked to their governments.

2.1 Hacktivist groups are into space

Figure 12: Hacker groups involved in cyberattacks against the space sector



Source: Compiled by Clémence Poirier

While the cyberattack against ViaSat was conducted by a state actor, the attacks that followed mostly came from hacktivist groups. **Out of 124 operations, 116 were conducted by hacktivist groups.**

Looking at the big picture of cyber operations in this conflict, CyberKnow20's threat actors list and cyber threat intelligence work illustrate that pro-Russian hacktivist groups are more numerous than pro-Ukrainian ones. He assessed that pro-Ukrainian groups are smaller in number and are concentrated among few very large groups such as the IT Army of Ukraine, which is well-organized and concentrates most operations. CyberKnow20 also assessed that Anonymous-related groups are usually pro-Ukrainian and conducting operations against Russia while also continuing attacks on other targets for other motives.

This assessment is also true regarding threat actors and cyber operations against the space sector. **The mapping identified 12 pro-Ukrainian hacker groups for 19 pro-Russian hacker groups that have targeted the space sector. The Russian and Ukrainian governments were also identified as threat actors.** The majority of pro-Ukrainian attacks was conducted by the IT Army of Ukraine and V0g3lSec. The most active pro-Russian groups targeting the space sector are NoName(057)16 and Killnet. Anonymous-related groups have conducted various attacks against the space sector, some which were motivated by the Russo-Ukrainian war while others were driven by other causes such as the Israel/Palestine conflict, gender-related issues, etc. Some groups are talking about hacking satellites without ever claiming attacks (e.g., AndraxRU joking about hacking NASA satellites).

Some hacktivist groups do not solely comprise members that are citizens of either Ukraine or Russia. Some groups are led by Western citizens such as OneFist or V0gl3Sec. Many groups bring together individuals from various countries and actively recruit candidates on their Telegram channels.

Most pro-Russian groups communicate in Russian while pro-Ukrainian groups often communicate in Ukrainian or English. Almost all Russian threat actors communicate on Telegram while pro-Ukrainian groups communicate either on Telegram or Twitter. Their means of communications is highly unstable. Many groups are regularly getting their accounts shut down or create new ones in case of internal feud, change of leadership, or other reorganization such as the creation of sub-groups. Some of the identified threat actors are no longer active at the time of writing (e.g., V0g3lSec).

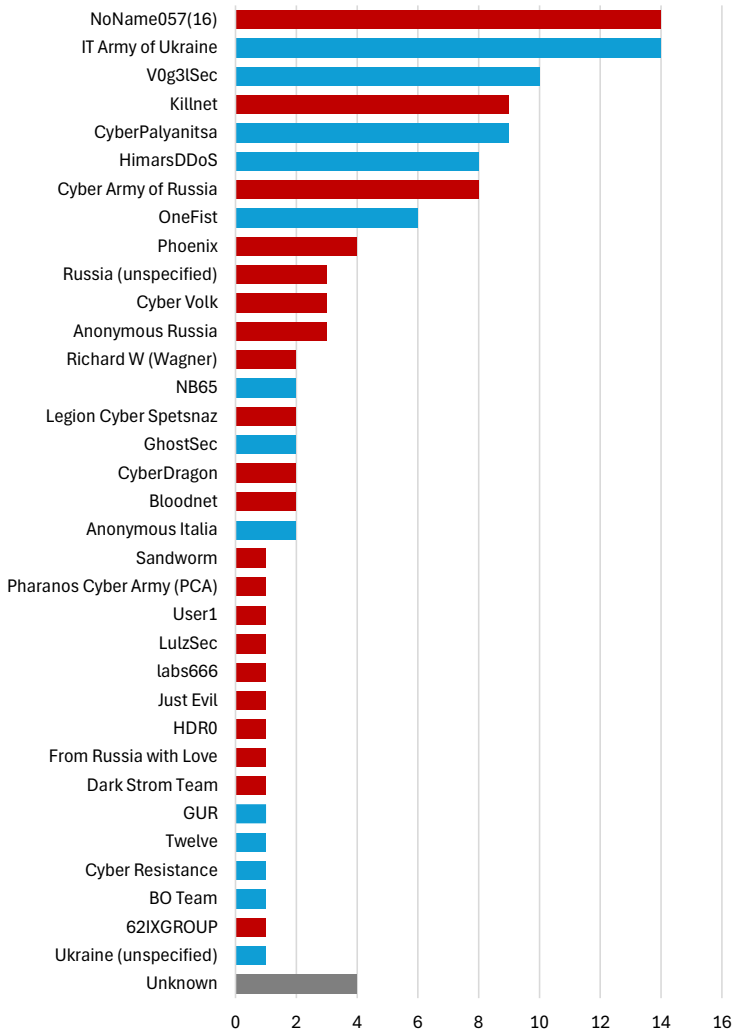
These findings enable to further analyze the evolution of the threat landscape. In 2022, James Pavur and Ivan Martinovic identified five periods in the space cyber threat landscape:

- 1957–1979: Early days (electronic threats between Soviet and US systems)
- 1980–1989: Piracy and spoofing (electronic threats and the interception of satellite data by pirates and amateur hackers as well as interference with satellite broadcast in the context of the Cold War)
- 1990–1999: Broadcast and flight control systems (satellite TV piracy)
- 2000–2009: Organized attackers (spoofing from non-state actors as well as state-sponsored attacks mostly targeting the ground segment)
- 2010–2022: Evolving threats (heterogeneous targets and threat actors)[104]

This report enables to define an additional period:

- 2022-present: Hacktivism and DDoS (interest in space from hacktivists, in particular in the context of armed conflicts such as the war in Ukraine, the Israel/Palestine conflict, Bangladesh/India/Pakistan disputes, etc.)

Figure 13: Threats actors targeting the space sector as part of the war in Ukraine

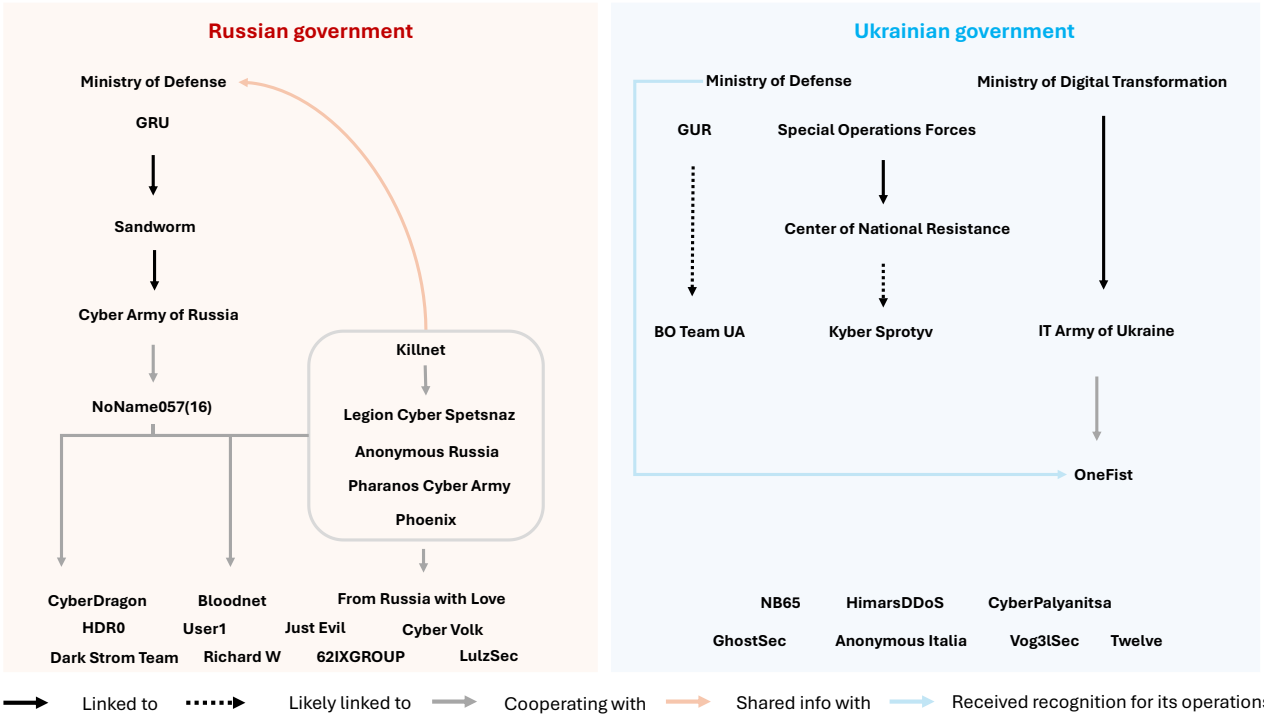


Source: Compiled by Clémence Poirier

[104] Pavur, James, and Ivan Martinovic. "Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 Years of Spaceflight." *Journal of Cybersecurity*, vol. 8, no. 1, Jan. 2022.

2.2 Hacktivism unmasked: multifaceted government ties

Figure 14: Various links between governments and hacker groups that conduct operations against the space sector



Source: Compiled by Clémence Poirier

The activities of threat actors illustrate that one should go beyond the binary distinction between hacktivist groups operating on their own and state actors. **Identified threat actors showcased the degrees of links that hacker groups may have with their government:**

- Most hacktivist groups do not seem to have any links with the government they support.
- Some groups are coordinating and exchanging with their government for some operations (e.g., IT Army of Ukraine; Kyber Sprotyv).
- Some groups do not directly cooperate with governments but receive official certificates of recognition for their actions (e.g., OneFist).
- Some groups are craving links and support from their governments without necessarily benefiting from it (e.g., Killnet).
- Some groups present themselves as independent but might be personas or aliases for State actors (e.g., Cyber Army of Russia; BO Team UA).

State actors are also targeting the space sector (e.g. Sandworm targeting Starlink). Only five (likely six) operations conducted by state actors were mapped by the report. Their operations are harder to track unless they are publicly disclosed by victims or their governments. It explains the prevalence of hacktivist groups in the dataset as they often self-attribute attacks.

It is likely that identified state actors' activities represent only the tip of the iceberg. State actors likely conduct a greater share of all cyber operations against the space sector than mapped in the report. For example, in September 2024, the FBI, CISA, and the NSA revealed that actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) had been in charge of cyber operations with aims of *"espionage, sabotage, and reputational harm"* since at least 2020 through, among other things, the deployment of the WhisperGate malware.[105] In an attempt to gain information in exchange for financial rewards, the US Department of State released the name of five officers of Unit 29155, who targeted US critical infrastructure, in particular in the aerospace sector. However, the US State Department did not provide any details on their operations.[106] This example illustrates: 1) the interest of state actors in targeting the space sector; 2) the lack of publicly reported cyber operations conducted by state actors against the space sector; 3) the number of attacks against the space sector is underestimated.

[105] "Russian Military Cyber Actors Target US and Global Critical Infrastructure." *Cybersecurity and Infrastructure Security Agency CISA*, Sept. 2024, https://t.ly/ZDmPw. Accessed 3 Sept. 2024.

[106] "GRU Officers – Unit 29155 – Rewards For Justice." *Department of State*, Aug. 2024, https://t.ly/d-F5M. Accessed 3 Sept. 2024.

Pro-Ukrainian group BO Team targets Russian Far Eastern Scientific Research Center of Space Hydrometeorology

On January 24, 2024, the Main Directorate of Intelligence (GUR) of the Ministry of Defense of Ukraine officially reported an attack on the Russian Far Eastern Scientific Research Center of Space Hydrometeorology "Planet".

Planet is a Russian national institution under the Federal Service for Hydrometeorology and Environmental Monitoring (Roshydromet) under the jurisdiction of the Ministry of Natural Resources and Ecology. It operates and develops EO systems for environment monitoring. It processes and uses data from 11 Russian satellites in GEO and HEO, and 23 foreign satellites. This adds up to processing more than 1.5 terabytes of data per day. Planet is divided in three centers: a European Center in Moscow, a Siberian Center in Novosibirsk, and a Far Eastern Center in Khabarovsk. Its partners are numerous and include both civilian and military actors.[107]

GUR credited and attributed the attack to the Ukrainian group "BO Team", which was unknown prior to GUR's press release. The group's Telegram channel was actually created on January 26, 2024, two days after the press release. The BO Team's first message on Telegram was posted on January 29, 2024.

GUR explained that the group targeted and entered the database of the Far Eastern branch of the Center. It destroyed its 280 servers, resulting in the deletion of about 200 million gigabytes of meteorological and satellite data. GUR explained that the attack impacted the Center's supercomputer, which will likely not be able to be fully restored. The attack also affected the computers, air conditioning, power supply, and humidification systems of the Center's building. In addition, the attack reached the Center's station on Bolshevik Island in the Arctic, which GUR said contributed to activities of the Russian Ministry of Defense. GUR explained that the data of the Center was used by about 50 public entities, including the Russian Ministry of Defense, the General Staff of the Armed Forces, the Ministry of Emergency Situations, and Roscosmos.[108] GUR shared two screenshots of what appears to be the user interface of the targeted servers. The two images show the dashboard of Dell's EMC Unisphere storage management platform before the attack, depicting a pie chart of the used and free storage; and after the attack, depicting a pie chart where storage capacities are fully free, illustrating that all data was deleted.

It is only on March 18, 2024, that BO Team started to address the Planet operations it allegedly conducted. It declared *"by the way, you've probably already heard about the Far Eastern Center of the Federal State Budgetary Institution Scientific Research Center for Space Hydrometeorology Planet? Yes yes, it was us too. 280 servers were disabled. And 2 million gigabytes of scientific data went through… were carefully downloaded and destroyed by us on the company's servers. Station on the Bolshevik island completely left the chat."*[109] It subsequently shared the photo of the servers, which was shared by GUR with the caption *"these are the monsters that stored millions of gigabytes of data."* BO Team also shared pictures previously shared by GUR.[110]

Satellites in orbit do not seem to have been targeted directly, only the servers of Planet were targeted. No user reported on the consequence of the attack and neither Roshydromet nor the Center publicly acknowledged the attack. It is therefore difficult to assess whether all the claims of GUR and BO Team are factual.

It remains unclear to this day whether the attack on Planet was one of the first operations of the BO Team and why they did not publicize this operation on Telegram earlier. Several hypotheses may be drawn: 1) Planet was one of its first operations prior to the establishment of its Telegram channel and BO Team simply moved on to other attacks; 2) BO Team is a hacktivist group, which coordinates several of its operations with GUR, and allows the government to publicly attribute and communicate their attacks, including the one on Planet; 3) the BO Team may be a state-sponsored actor, who created an alias to appear as a hacktivist group and publicize GUR's cyber offensive operations and to easily leak data obtained by GUR. The latter may be more likely. Indeed, what stands out in BO Team's operations and communications is how they systematically underline the direct or indirect military nature of their targets, thereby emphasizing the legality to target them vis-à-vis international humanitarian law, which seems more consistent with the behavior of a state actor rather than a hacktivist group.

---

[107] НИЦ «Планета». 2024, http://planet.rssi.ru/index.php?page_type=main&page=partners&lang=ru. Accessed 29 Aug. 2024.

[108] "Головна." Знищили ворожу "планєту" — деталі кібератаки проти центру космічної гідрометеорології рф. Власність Головного управління розвідки Міністерства оборони України, 2024. https://gur.gov.ua/content/znyshchyly-vorozhu-planietu-detali-kiberataky-proty-tsentru-kosmichnoi-hidrometeorolohii-rf.html. Accessed 29 Aug. 2024.

[109] "BO Team UA." Telegram, 2024, https://t.me/BO_Team_UA. Accessed 29 Aug. 2024.

[110] Ibid

2.3 No hacktivist group is specialized in targeting space systems

Cyberattacks against space systems as part of the war in Ukraine demonstrate that **threat actors are not necessarily specialized in targeting space systems and no group has emerged to only target space systems.** On the contrary, most of them appear rather new to the space sector.

This is illustrated in the self-attribution statements of threat actors, which are now common practice. For instance, OneFist in Operation Polaris stated the attack was the group's first attempt to hack into a satellite network, which made *"the environment unique for [them]."* OneFist underlined that *"satellites are very complex, and it was not simple to get into them."*[116] Moreover, hacker groups sometimes claim that they hack a specific system (e.g., ground station) when they actually targeted another (e.g., user modems), which shows that they are not necessarily familiar with the space sector.

In addition, OpenAI and Microsoft reported that Russian hacker group FancyBear (also known as Forest Blizzard or APT28), which is linked to GRU Special Service Center's Unit 26165, was using their large language models to research *"various satellite and radar technologies that may pertain to conventional military operations in Ukraine, as well as generic research aimed at supporting their cyber operations, […] suggest[ing] an attempt to acquire in-depth knowledge of satellite capabilities."*[117] However, Microsoft did not manage to link such research to actual attacks. This further confirms the findings of the report: 1) there is an interest from state actors in attacking satellites; 2) it is hard to detect state actors' attacks against satellites; and 3) threat actors lack knowledge about space systems.

This suggests that there may be a certain difference between cybersecurity on Earth and in space. Nevertheless, it does not mean that their potential for disruption and destruction is not substantial.

Once threat actors better understand space systems, the threat landscape might evolve, and the space sector may become more vulnerable to cyber operations.

Pro-Ukrainian group OneFist targeted the Satis satellite network

In November 2022, OneFist recounted on its website what it called "Operation Polaris", which targeted the Russian Satis satellite network.[111]

The Satis satellite network provides connectivity services across Russia.[112] The attack targeted 12 user terminals, which relied on the Russian Yamal 401 (operated by Gazprom Space Systems)[113] and Ekspress-AM6 (operated by RSCC) satellites. The attack only targeted the user segment and did not directly affect satellites in orbit.

OneFist explained that one of its hackers called Mefisto broke into the network at UNIX level, which provided access to the operating system. This method is not surprising since the expertise of OneFist's founder has been in the security management of UNIX systems. OneFist did not explain how it got access to it. Plausible options may include the exploitation of vulnerabilities. Once it was within the network, OneFist modified the settings of the modems. It apparently remained within the network for a long period of time and hid *"like a Trojan Horse"* while waiting for the operators of Satis to notice and counter the attack and repair the system. OneFist explained that it enabled them to study the operators' methods to take back control of the network. Once the repair work was halfway done, OneFist triggered another attack. This method was apparently repeated several times. Satis' operators were closely monitoring the network. They fought back and forth to destroy and maintain the network. It seems that attackers modified the settings of the system to prevent connectivity. It is unclear whether they also used malware as part of the attack.

OneFist underlined that *"the mission was a complete success, as the duration of the outage means there is no easy fix."*[114] OneFist claimed that 12 user terminals were rendered inactive for several hours. OneFist explained that the user modems were manufactured in Belgium, which would make it difficult for Satis to have them replaced rapidly due to sanctions.[115]

OneFist provided several screenshots of what appears to be the user interface of the targeted user modems, providing some evidence the attack took place. Nonetheless, it remains difficult to find external proof of the attack. Neither Satis nor Russian authorities reacted to the attack.

[111] "Operation Polaris." *Team Onefist*, 5 Nov. 2022, https://www.onefist.org/post/operation-polaris. Accessed 1 Sept. 2024.

[112] "Решения ." *Satis*, https://www.satis-tl.ru/solutions/. Accessed 1 Sept. 2024.

[113] "Yamal 401." *Gunter's Space Page*, 2022, https://space.skyrocket.de/doc_sdat/yamal-401-2.htm. Accessed 1 Sept. 2024.

[114] "Operation Polaris." *Team Onefist*, op cit.

[115] Ibid

[116] Ibid

[117] "Staying Ahead of Threat Actors in the Age of AI." *Microsoft Security Blog*, 14 Feb. 2024, https://shorturl.at/kC4IY. Accessed 1 Sept. 2024.

2.4 Hacktivists' claims are hard to prove

When conducting cyber threat intelligence with open-source information, there are two outstanding issues: 1) the difficulty to assess whether an attack actually happened and had the consequences described by threat actors; and 2) the struggle to fully understand the steps of each attack.

Indeed, threat actors may claim an attack that did not actually happen or exaggerate its impact. According to Mandiant, hacktivists' claims targeting operational systems are often exaggerated or unsubstantiated, to the point of making them challenging to debunk.[118] According to CyberScoop, hacker groups such as OneFist and GhostSec were caught lying or exaggerating about some attacks as part of the war in Ukraine.[119] While this was not demonstrated for attacks on space systems, there is also no proof on whether some of the identified attacks against the space sector actually took place. Anyone can take screenshots of a user interface and claim it maliciously got into a network. In the same vein, threat actors may use old data leaks and present them as new operations (e.g., leaks of Gorilla Circuits or Safran). However, this is not specific to the space sector and applies to cyber threat intelligence in general.

One should always keep in mind the risk of disinformation in self-attributions and the potential for their negative consequences. Even when an attack did not happen, false claims may affect the reputation of a space company, undermine trust in satellite services, or create fear and panic among end-users and governments, which might simply be the end-goal of these threat actors.

While threat actors sometimes describe their operations in detail, self-attributions are often made on Twitter, Telegram channels, or hacker forums, using "memes", jokes, idioms, insults, various languages (often a mix of English, Ukrainian, and Russian) along with photo montages, screenshots of their targets, which may create misunderstandings about the attack and the sequence of events.

Overall, about 20% of identified operations in the dataset were not fully verifiable. It primarily concerns the most sophisticated operations. Furthermore, media coverage is often limited due to the overall volume of hacktivists' campaigns and information often gets lost between the primary source, the technical press, and the general press. Further investigations are limited due to the lack of access to information and limited technical knowledge on space cybersecurity.

2.5 Generating effects may not be so important

Most of the identified operations did not actually target the space system itself but only the website (e.g., Killnet's attack of Starlink and Phoenix's attack of SES) of a satellite service, network, or company. These operations do not affect satellites in orbit, do not impact users, or the operations or the targeted organizations. Therefore, one may wonder what purpose these attacks serve.

Many questions remain unanswered:

- Are user interfaces a lower hanging fruit for hackers because actual space systems themselves are too complex and require specific knowledge to be hacked?
- Are user interfaces targeted because these operations are not specific to space? In other words, they are simply another attack on a computer and easy to launch
- Are user interfaces targeted because actual space systems are well protected?
- Do DDoS attacks enable hackers to easily make a claim and show support for a cause regardless of the damage?

In fact, beyond space-related targets, most attacks conducted by identified threat actors are DDoS against websites. It seems that DDoS attacks are sufficient to gather media attention and indicate hostility and reaction towards specific actors. As described by Mandiant, hacktivism leverages cyber operations to convey political or social narratives.[120] Threat actors move from one target to another on a daily basis. Very few focus on the same actor for extended periods of time.

On another note, the impact of some operations may appear months or years later. For instance, several attacks against Russian targets allegedly rendered some components unusable (e.g., OneFist's operations against Zagorskaya GAES-2 and Satis' satellite network) and would need to be replaced. However, since many of these

[118] "We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems." *Google Cloud*, 22 Mar. 2023, https://t.ly/y9N0m. Accessed 1 Sept. 2024.

[119] Vasquez, Christian. "Fact or Fiction, Hacktivists' Claims of Industrial Sabotage in Russia or Ukraine Get Attention Online." *CyberScoop*, 22 Mar. 2023, https://t.ly/IdxmR. Accessed 1 Sept. 2024.

[120] Ribeiro, Anna. "Mandiant Reveals Hacktivists Increasingly Targeting OT Systems, Raising Likelihood of Actual and Even Substantial OT Incidents." *Industrial Cyber*, 23 Mar. 2023, https://t.ly/6PT9-. Accessed 1 Sept. 2024.

components are from Western companies, sanctions may prevent Russia to repair some systems. In the same vein, the data leak of Russian company Special Technology Center (STC) enabled to showcase how the company and its subsidiaries where circumventing sanctions to procure components for their equipment, which eventually led the involved entities to be sanctioned.[121]

2.6 Hacker group behaviors may conflict with the government they support

On social media, hackers are often reacting to the words and actions of space companies in relation to the conflict. For example, when Elon Musk gives his opinion on the conflict or cuts Starlink for drone attacks in Ukraine[122], pro-Ukrainian hackers may take sides and call upon their communities to hack him (his companies, his personal accounts, etc.) in retaliation. Although these hackers support Ukraine, their calls and actions are not always aligned with broader government goals and may create unintended interference on Ukrainian military operations. In case Ukrainian groups target Starlink in reaction to Elon Musk's actions or opinions, the Ukrainian government cannot afford that Starlink is interrupted as it is essential for military operations and civilian activities.

Coordination between governments and hacker groups is rarely organized, linear, and hierarchical in cyber conflict. Hacker groups that support the same party to the conflict are regularly fighting each other (e.g., Killnet vs. Phoenix, Killnet vs. Raty, etc.).

Furthermore, government officials may consider the operations of hacktivist groups as useless to attain their objectives. This is illustrated in some of the attacks against the space sector. For instance, when Killnet targeted Lockheed Martin, and eventually NASA, the Russian government underlined that these operations were not very useful and that hackers should focus their attention towards finding the location of military equipment on the frontlines instead. Killnet responded that the government could have asked them in the first place, highlighting disorganized coordination between authorities and hacktivist groups. Overall, state-tolerated attacks are very common but state-sponsored ones are rarer.

2.7 Space as an object of fascination for hackers

Both pro-Ukrainian and pro-Russian hacktivist groups are regularly talking about space on their Telegram channels or Twitter accounts. **Space seems to be one of many tools of hacktivist groups to sustain online engagement with their community beyond the cyber operations they collectively conduct.**

On the Ukrainian side, the IT Army sometimes shares messages and information related to space on its Telegram channel. The IT Army sometimes shares fun facts about space such as the date when the first coffee was brewed on board the International Space Station (ISS). They also regularly share articles regarding the use of space in the conflict or make comments about the lack of satellite internet capabilities on the Russian side of the frontline. References to the ViaSat hack are also common on the channel.

On the Russian side, several pro-Russian hacktivist groups regularly talk about space. Groups such as NoName057(16), Killnet, and Cyber Army of Russia made posts for the day of cosmonautics on April 12, which celebrates the first human spaceflight of Yuri Gagarin in 1961. NoName057(16) has a recuring "IT news Digest", which includes Russian news in the digital sector. News on the Russian space sector is regularly included in it. Cyber Army of Russia also shares news related to space such as the use of American EO satellites over Crimea[123], or the launch of the Russian lunar lander Luna-25.[124] Killnet sometime shares news and photo montages related to Elon Musk and Starlink, or Chinese's plans to develop counterspace weapons,[125] jokes about Roscosmos.[126]

Pro-Russian groups sometime joke about the possibility of hacking a satellite or debate whether this is feasible without necessarily taking any actions (e.g., AndraxRU). It further underlines the fascination for space. It is seen by hacktivists as an ultimate challenge.

---

[121] "Кібер Спротив." *Telegram*, 26 Aug. 2024, https://t.me/cyberResistanceUA/462?single. Accessed 1 Sept. 2024.

[122] Davenport, Christian, and Joseph Menn. "Musk Refused to Allow Ukraine's Military to Use Starlink to Attack Russian Fleet." *The Washington Post*, 7 Sept. 2023, https://www.washingtonpost.com/technology/2023/09/07/ukraine-starlink-musk-biography/. Accessed 1 Sept. 2024.

[123] "Народная СуberАрмия." *Telegram*, Apr. 2023, https://t.me/CyberArmyofRussia_Reborn/3333. Accessed 1 Sept. 2024.

[124] "---." *Telegram*, 31 July 2023, https://t.me/CyberArmyofRussia_Reborn/4384. Accessed 1 Sept. 2024.

[125] "WE ARE KILLNET." *Telegram*, 29 May 2022, https://t.me/killnet_reservs/1595. Accessed 1 Sept. 2024.

[126] "---." *Telegram*, 13 May , https://t.me/killnet_reservs/5682. Accessed 1 Sept. 2024.

3 Understanding the political and strategic implications of cyber conflict in space

This chapter addresses the political and strategic stakes of cyber operations against the space sector as part of the war in Ukraine, providing an overview of the role of the conflict in the evolution of the threat landscape as well as its implications for the militarization and weaponization of outer space.

3.1 Cyberattacks on space systems are becoming more prevalent in armed conflicts

According to market intelligence company CyberInFlight, only 337 cyberattacks[127] have been publicly recorded since the 1970s, 90 of which took place in 2023, and 30 in the month of January 2024 alone.[128] This is likely a low estimate as most attacks are not publicly disclosed. **If considered as a ballpark basis, the 124 operations related to the war in Ukraine, which were identified by CSS, would constitute a significant part of all attacks ever carried out against the space sector.**

Cyberattacks on satellites used to be rather rare, and attacks as part of armed conflicts even rarer. They mostly consisted of jamming and spoofing (electronic warfare) rather than intrusions, denials of service, data interceptions, data corruption, or seizures of control (cyber warfare). For instance, in 2009, insurgents in Iraq managed to access live video feeds from US military drones by intercepting unencrypted links between UAVs and telecommunications satellites by using the commercial software SkyGrabber.[129] In 2011, Iran shut down a US. RQ-170 military drone by overriding the drone's commands and control system and spoofing GPS coordinates to fool the UAV into thinking it was landing on a US air base in Afghanistan when it was actually flying over Iranian airspace.[130]

The war in Ukraine constitutes a shift in the exposure of satellites to cyberattacks during wartime for four reasons:

1) The conflict has been a widely publicly documented case study of the role played by satellites in armed conflicts. Threat actors, in particular hacktivist groups, were not necessarily aware of the extent of their use by armed forces. It therefore shed light on new attractive targets to attack.

2) The conflict has led to a surge in hacktivism coupled with an increasing trend and appraisal toward self-attribution.

3) Space is regularly mentioned by threat actors and seems to be both a topic of fascination and a new challenging and high value target.

4) All of which in a context of rising digitalization of space systems as well as democratization of space technologies and offensive cyber tools, thereby extending the attack surface on satellites and lowering the barrier of entry for threat actors.

It can be expected that cyberattacks against satellite networks will become more prevalent during future conflicts and that hacktivist groups will maintain their interest in space systems.

This trend goes beyond the war in Ukraine. In 2023, the Israel/Palestine conflict showcased similar patterns with hacktivists positioning themselves, and self-attributing attacks on space systems or space companies. For instance, GhostSec claimed a cyberattack against 11 GNSS receivers in Israel to protest the action of Israel Defense Forces.[131] Similarly, Anonymous Sudan claimed it attacked GNSS systems in Israel following October 7.[132]

---

[127] "2023 highlights of space security market" Cyberinflight - Florent Rizzo. *CYSAT* 2024, Conference, Paris, 2024

[128] "Cyber Resilience in Space Workshop: Mapping Challenges, Forging Resilience" Workshop. *Belgian Presidency of the Council of the EU*, 8 Feb 2024.

[129] MacAskill, Ewen. "US Drones Hacked by Iraqi Insurgents." *The Guardian*, 17 Dec. 2009, https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked. Accessed 1 Sept. 2024.

[130] Vijayan, Jaikumar. "Iran Tricked U.S. Spy Drone into Landing in Country, Report Says." *Computerworld*, 16 Dec. 2011, https://www.computerworld.com/article/1541099/iran-tricked-u-s-spy-drone-into-landing-in-country-report-says.html. Accessed 1 Sept. 2024.

[131] "Israel Satellite and Water Pumps HACKED ~GhostSec." *Telegraph*, GhostSec, 6 Apr. 2023, https://telegra.ph/Israel-Satellite-and-water-pumps-HACKED-GhostSec-04-06.

[132] "Anonymous Sudan - @InfraShutdown." *Telegram*, Oct. 2023, https://t.me/s/xAnonymousSudan?q=Israeli+industrial+control+systems+have+been+attacked+by. Accessed 1 Sept. 2024.

3.2 The weaponization of outer space remains an emerging phenomenon

It does not seem that any identified attack directly targeted the space segment at the time of writing. Co-orbital cyberattacks launched from one satellite to another do not appear to have occurred either. No identified cyber operations rendered a satellite in orbit unusable or turned it into a piece of space debris. A significant majority of operations targeted the user interface (76%) and the user segment (10%). These findings are also consistent with interviews conducted with stakeholders in the space industry, who reported that most cyberattacks targeted the IT environment of their companies rather than their satellites.

The cyber conflict therefore extended to space systems but remained confined to systems on Earth (e.g., user terminals, user interface, ground stations) and has not yet spread to objects in the orbital environment. Yet, it was sufficient in numerous cases to disturb the confidentiality, integrity or availability of space services. Some operations such as the IT Army of Ukraine's attack against Russian internet service providers Astra and Altegrosky prevented users from using internet broadband for several hours. Killnet's attack against Starlink prevented users from connecting to the internet.

The fact that operations only targeted space systems on Earth tends to confirm that the weaponization of space, which is defined by the placement of weapons in outer space, remains an emerging phenomenon. Beyond the Russian-Ukrainian conflict, cyberattacks on the space segment do exist but they remain considerably less numerous than on other segments.

If the weaponization of outer space is not there yet, it is nonetheless slowly but surely increasing as states are steadily developing counterspace capabilities and observing hostile behaviors in space. These include anti-satellite tests (e.g., China in 2007, India in 2019, Russia in 2021) unannounced maneuvers and inspection missions with attempts to eavesdrop on other satellites (e.g. LuchOlymp), the release of projectiles (e.g., Kosmos-2523, Kosmos-2543), the development of robotic arms (e.g., SY-7), and the deployment of highly maneuverable space planes (e.g., X37-B).

3.3 Most cyberattacks are not part of joint operations

In February 2022, the cyberattack on ViaSat was an example of a joint coordinated operation in complement of the invasion on the ground. The reason for this pertains to the fact that the cyberattack on ViaSat was attributed to a state actor, which directly or indirectly worked for the Russian government, thereby enabling potential coordination between space cyber operations and land operations. However, most cyberattacks that affected space systems after the ViaSat incident were carried out by hacktivists groups that have little to no links with governments.

Some attacks were correlated to minor events on the ground or announcements that were related to the war in Ukraine such as deliveries of weapons (e.g., Cyber Army of Russia targeting Hensoldt), provisions of satellite images to Ukraine (e.g., Cyber Army of Russia trying to target ICEYE) or the hosting of conferences related to the war (e.g., NoName targeting the Swedish Space Agency). Yet, such examples are limited, and **no identified attack seems to be in coordination with land, sea, or air operations.**

Pro-Russian group NoName057(16)'s attack on the Swedish Space Agency

On May 4, 2023, NoName057(16) claimed a DDoS attack on the website of the Swedish National Space Agency.[133] This attack was part of a broader campaign against European targets, in particular Nordic countries following the Nordic-Ukrainian Summit in Helsinki, Finland, which took place on May 3, 2023.

NoName057(16) declared *"we put down the website of the Swedish National Space Agency"* and provided a check-host link to prove its attack succeeded along with a screenshot of the defaced website.[134]

The Swedish National Space Agency (Rymdstyrelsen), under the Swedish Ministry of Education and Science, only deals with civilian space activities.

The Swedish Space Agency was only one target among other Swedish governmental websites. It is unlikely that SNSA was targeted due to its space activities. The Agency did not publicly react to the attack.

[133] "NoName057(16)." *Telegram*, 4 May 2023, https://t.me/noname05716/3099. Accessed 1 Sept. 2024.

[134] Ibid

However, some cyber operations were conducted independently from land, sea, or air operations but related to them. For instance, Russia's capture of Baba Yaga drones to identify Ukraine's software cracking of Starlink or Russia's capture of Ukrainian soldiers' Android tablet to infect them with malware in order to obtain data about Starlink are examples of **cyber operations that are related to battlefield actions but conducted separately**. Likewise, Pro-Ukrainian group OneFist's operations against Zagorskaya GAES-2, which is described below, was a cyber operation conducted in retaliation to Russian kinetic attacks against Ukraine's energy infrastructure.

This lack of direct coordination tends to confirm the difficulty of conducting truly joint operations for both Ukrainian and Russian armed forces. Entering a satellite network and triggering the attack at the right moment requires sophisticated cyber offensive capabilities and coordination abilities with other branches of the armed forces. In addition, the integration of various commercial systems into broader military networks and weapons systems on land, sea, and air are likely significant challenges for armed forces.

3.4 Cyber operations shape the use of space in the battlefield

Although most cyber operations were conducted independently from land operations and led to minimal consequences, some of them contributed to shape how space was used on the frontlines, in particular on Russia's side.

Throughout the conflict, Russia demonstrated a lower-than-expected use of satellite communications (SATCOM) despite significant sovereign capabilities. **At the beginning of the war, SATCOM were supposed to be used as default by Russian troops** but were quickly abandoned due to malfunctions and a lack of efficient capabilities. For instance, they used encrypted satellite phones such as the Era cryptophone, which somehow needs 3G/4G to function. However, in some areas, Russia destroyed 3G/4G towers, disabling their own SATCOM capabilities.[135] Russian troops were thus forced to rely on unsecure devices such as unencrypted walkie talkies and private cell phones.[136] Data leaks also revealed that soldiers complained about the lack of SATCOM capabilities and the ability of Ukraine to eavesdrop on their communications.[137] However, **as the conflict is prolonging, terrestrial systems and networks have been progressively used by default instead.** For instance, after the Ukrainian incursion in Kursk, DDoS against internet service providers forced Russian armed forces to rely on SATCOM, thereby limiting their ability to communicate.[138]

3.5 Some operations are directed at civilian targets

Numerous operations were directed at purely civilian websites. This is the case of NoName057(16)'s DDoS operations against the websites of the Swedish Space Agency or Bloodnet's operation against Netherlands Institute for Space Research. Some operations targeted civilian infrastructures or organizations. This is the case of OneFist's operation against GNSS receivers at Russian hydroelectric plant Zagorskaya GAES-2, which is described below.

Some groups, usually pro-Ukrainian ones, are taking care of explaining the military or dual nature of their targets, thereby underlining their legitimacy to attack them. This was the case of BO Team's attack against Planet for instance. However, this is not the case for a majority of pro-Russian operations.

The targeting of civilian targets raises questions regarding the legality of such operations and the application of international humanitarian law in both space and cyberspace. Additionally, it raises questions regarding the tolerance of states for activities that are essentially illegal in most countries and whether they would react if a specific threshold was reached, such as an attack on the space segment of a satellite.

So far, there has been no example of a hacktivist group based in the West that targeted the Ukrainian space sector. It is unknown whether such a group would be tolerated by authorities should it appear in the threat landscape. Western groups targeting the Russian space sector were tolerated so far (e.g., V0g3lsec). Similarly, the Russian government is well-known to tolerate hacktivist groups' activities as long as they do not target Russian entities. Should a Russian group targeting the Russian space sector emerge, it is likely that authorities would attempt to dismantle it.

[135] Moss, Sebastian. "Ukraine: Russian Military's Own Encrypted Phones Impacted after Destroying 3G/4G Towers, Allowing Comms to Be Intercepted." *DCD*, https://t.ly/B44DK. Accessed 8 Sept. 2024.

[136] Horton, Alex, and Shane Harris. "Russian Troops' Tendency to Talk on Unsecured Lines Is Proving Costly." *The Washington Post*, 27 Mar. 2022, https://t.ly/4WP5r. Accessed 8 Sept. 2024.

[137] "ВЧК-ОГПУ." Telegram, 16 Aug. 2023, https://t.me/vchkogpu/40888?single. Accessed 8 Sept. 2024.

[138] "В Курской Области Наблюдаются Перебои с Мобильной Связью и Интернетом." *Ведомости*, 9 Aug. 2024, https://www.vedomosti.ru/technology/news/2024/08/09/1054950-nablyudayutsya-pereboi. Accessed 8 Sept. 2024.

Pro-Ukrainian group OneFist targeted a Russian hydroelectric plant

On December 11, 2022, OneFist, and more specifically the hacker "Thraxman", claimed to have conducted a cyberattack, coined "Operation Gradient", on Russian hydroelectric plant Zagorskaya GAES-2.[139]

Zagorskaya GAES-2 (Заторская ГАЭС-2) is a hydroelectric power station located near Sergiev Posad in the Moscow region, Russia. Zagorskaya GAES-2 is still under construction. A hydroelectric power station is nothing close to a satellite. However, its functioning relies on Supervisory Control and Data Acquisition (SCADA) systems, which are control systems that enable to monitor and control industrial systems and processes such as power plants, pipelines, wind turbines, oil rigs. These SCADA systems rely on various sensors, including GNSS receivers. OneFist explained that the *"power plant's SCADA system was run by Leica HID and Moxa PLC SCADA controllers"* and that the *"system was tied into GLONASS and GPS satellite networks",*[140] which it claimed to have compromised.

OneFist attached two screenshots of the user interface of Leica Geosystems' GNSS receivers. One screenshot displays the status of the Leica AR20 GNSS antenna.[141] Another one displays the Skyplot of the GNSS receiver in the user interface, which visually represents the various GNSS satellites that the receiver is able to track and potentially receive data from. Mostly GPS and GLONASS signals were available to the receivers.[142] OneFist claimed it *"successfully penetrated their SCADA sensor network as well as the corresponding GNSS base station that monitored the stability of the foundation. Over the course of a week, I gradually introduced circular error into the GNSS readings, reducing their accuracy to interfere with the construction work."* [143] OneFist likely deliberately introduced errors into the GNSS data, which eventually became less precise. However, it remains unclear how OneFist entered the SCADA network. OneFist stated that the *"antenna parameters were changed, and network SCADA connection disabled"*. [144]

OneFist then moved on to explain its attack against the MOXA SCADA controllers and declared that they *"had their configurations demolished, knocking them out until re-programmed by hand".* OneFist attached a screenshot of MOXA's user interface, displaying that settings were saved, and that the system was indeed restarting.[145] OneFist explained that it planned to *"email the staff a love letter from us, misconfigure (and knock-out) the satellite connection to the sensor arrays, and brick the SCADA system to disable as much of the construction site monitoring systems as possible."*[146] OneFist likely sent a phishing email to the staff of the power station, which may have enabled it to access the network, modify settings of GNSS controllers, and disable the SCADA system of the power station.

OneFist declared that *"if Putler*[147] *wants to knock our power plants out to kill is in the cold, we must respond. Note this kills no civilians, it causes economic and logistical damage only."*[148] This comes in a context in which Russia targeted the energy infrastructures of Ukraine in the fall of 2022. Ukraine's Office of the Prosecutor General reported that Russia conducted 92 attacks on Ukraine's energy infrastructure in October and November 2022.[149] This attack against Zagorskaya GAES-2 is seen by OneFist as a retaliation. OneFist further underlined that *"unlike the Moskali,*[150]*our attacks do not harm people - that is the difference between us. It should also be noted that this plant has been damaged from soil erosion before, so the loss of their Western-made devices should have a significant effect on their construction progress."*[151] OneFist also conducted this operation due to Russian action in Syria. It outlined "*Vladimir! Remember Syria? You are paying for it right now and will keep paying for it until Russia quits."*[152] As a result, there is a sort of convergence of hacktivisms as part of OneFist's operations.

OneFist claims that *"the loss of their western devices should have a significant impact on the progress of their construction."* However, it is difficult to confirm OneFist's claims.

---

[139] "Team OneFist." Telegram, 11 Dec. 2022, https://t.me/onefistua/765?single. Accessed 3 Sept. 2024.

[140] "Team OneFist – Operation Gradient." *The Cyber Shafarat* , 11 Dec. 2022, https://t.ly/9FHoe. Accessed 3 Sept. 2024.

[141] "Team OneFist." Telegram, 11 Dec. 2022, https://t.me/onefistua/765?single. Accessed 3 Sept. 2024.

[142] "---." *Telegram*, 11 Dec., https://t.me/onefistua/768?single. Accessed 3 Sept. 2024.

[143] "Team OneFist – Operation Gradient." *The Cyber Shafarat* , op cit

[144] "Team OneFist." *Telegram*, 11 Dec. 2022, https://t.me/onefistua/770?single. Accessed 3 Sept. 2024.

[145] "---." *Telegram*, 11 Dec., https://t.me/onefistua/771?single. Accessed 3 Sept. 2024.

[146] "Team OneFist – Operation Gradient." The Cyber Shafarat , op cit

[147] Slur that mixes the names of Adolf Hitler and Vladimir Putin.

[148] "Team OneFist." *Telegram*, 11 Dec. 2022, https://t.me/onefistua/770?single. Accessed 3 Sept. 2024.

[149] "Офіс Генерального Прокурора." *Telegram*, 16 Nov. 2022, https://t.me/pgo_gov_ua/7363. Accessed 3 Sept. 2024.

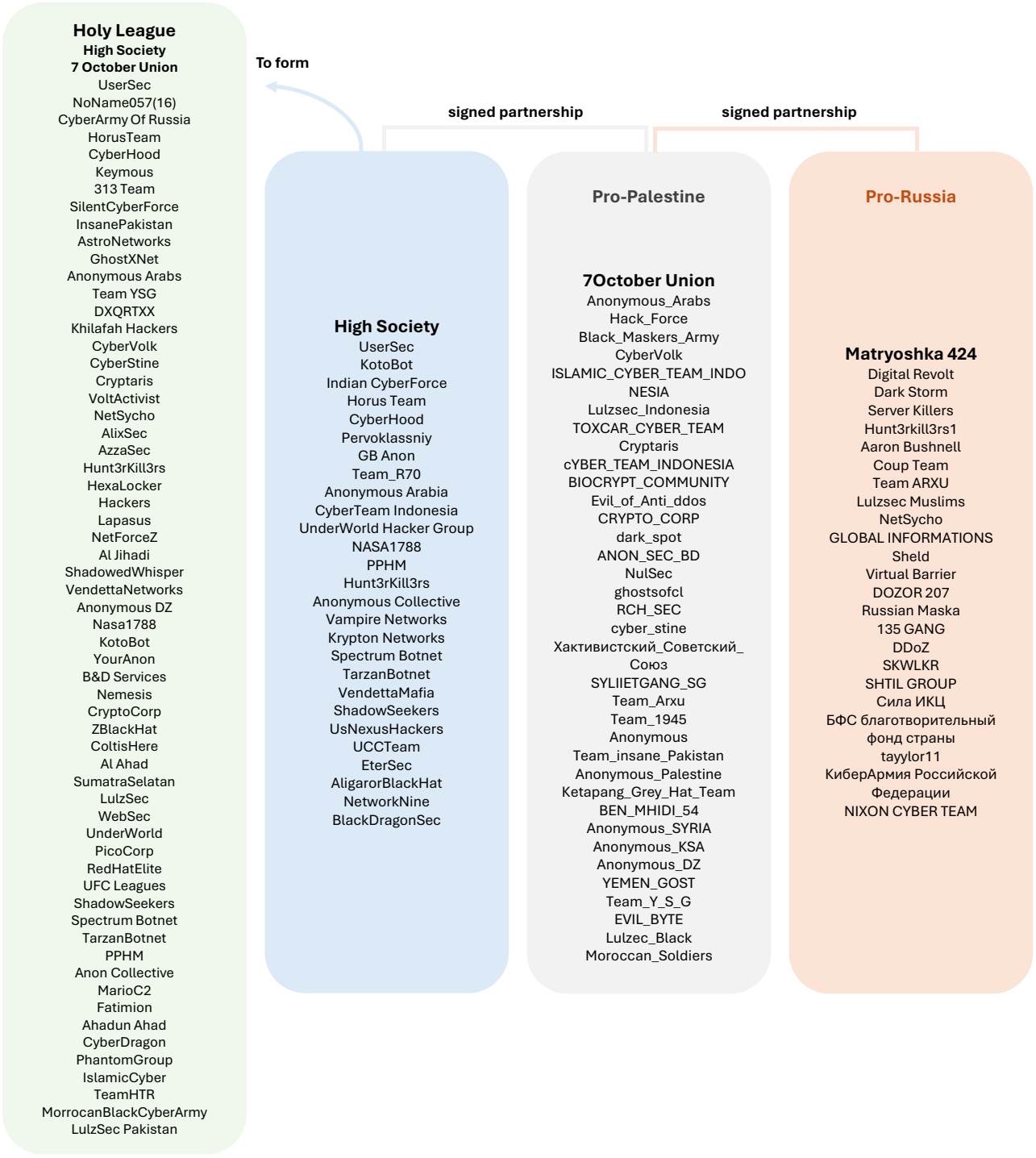
[150] Moskali is a slur that designates the residents of Moscow.

[151] "Team OneFist." *Telegram*, https://t.me/s/onefistua. Accessed 3 Sept. 2024.

[152] "---." *Telegram*, 11 Dec. 2022, https://t.me/onefistua/774?single. Accessed 3 Sept. 2024.

3.6 Pro-Russian and pro-Palestine groups are teaming up

Figure 15: Structure of alliances between pro-Russian and pro-Palestine group



Source: Compiled by Clémence Poirier

More broadly, a new trend has emerged among hacktivist groups. First, several pro-Russian groups created partnerships with one another and started to more regularly cooperate and coordinate their actions. Then, following October 7, 2023, several pro-Russian hacker groups took sides with pro-Palestine groups in the Israel-Palestine conflict. They have started to coordinate a few operations or reshare each other's content against pro-Israel or pro-Ukraine targets. Eventually, these groups decided to join forces to augment their capabilities and extend the impact of their operations. For instance, in April 2024, the pro-Russian collective Matryoshka 424 was established to *"unite as many forces and people from different spheres of activity as possibles to protect the*

interests of Russia as well as Russia's allies."[153] It gathers 22 Russian threat actors. In the same vein, in June 2024, the pro-Palestine collective 7 October Union was established to bring 36 hacktivist groups together to target Israel. In July 2024, Matryoshka 424 and 7 October Union announced the *"unification of their forces"* to combine *"efforts to achieve common goals."*[154] The same month, the two collectives High Society and 7 October Union announced that they *"decided to combine our teams and form one new one"* called the Holy League to target NATO, Europe, and Ukraine as well as Israel, bringing over 70 hacker groups together.[155]

Both pro-Russians and pro-Palestine hacker groups have independently targeted the space sector, the former focusing on Western and Ukrainian space targets and the latter focusing on the Israeli space sector. So far, they have not conducted joint cyber operations against space targets. It remains to be seen whether pro-Palestine groups will ever take part in pro-Russian groups' operations against space targets. Only time will tell how these hacktivist alliances will impact cyber operations against space systems and organizations related to the war in Ukraine.

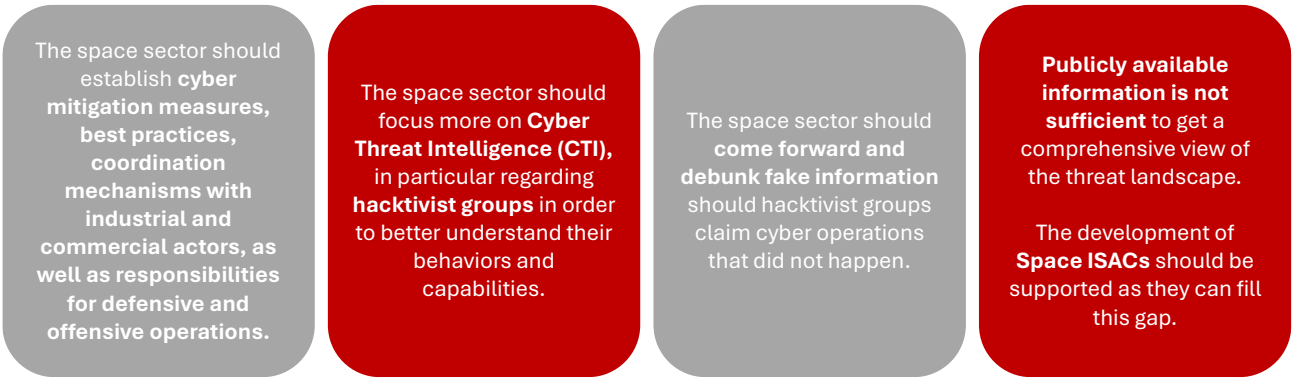
[153] Matryoshka424. "Кто Мы Такие? Что Такое Матрёшка 424?" *Telegraph*, 30 Apr. 2024, https://telegra.ph/Who-are-we-What-is-Matryoshka-424-04-30. Accessed 3 Sept. 2024.

[154] "Matryoshka 424." *Telegram*, 14 July 2024, https://t.me/Matryoshka424/66. Accessed 3 Sept. 2024.

[155] "@HACKERFORSE." *Telegram*, https://t.me/hackerforse/107. Accessed 3 Sept. 2024.

Conclusion

Figure 16: Recommendations



Source: Compiled by Clémence Poirier

This report identified 124 cyber operations that have targeted the space sector in the context of the war in Ukraine. The report also identified a set of diverse threat actors and laid out their behavioral patterns and motives.

The report similarly provided evidence of the sustained interest of state actors in targeting space infrastructure despite a small number of identified operations. Operations conducted by state actors are particularly challenging to detect and map as they are carried out covertly and rarely publicly attributed. As a result, **the 124 cyber operations identified likely represent only a fraction of the overall cyber activities targeting the space sector.** It is highly probable that numerous other operations have been conducted that remain unreported and undetected. Publicly available information is not sufficient for space operators to get a comprehensive view of the threat landscape. Thus, information sharing initiatives such as Space Information Sharing and Analysis Centers (Space ISACs), which pool together space companies and government agencies, should be supported as they can fill this gap (see Figure 9).

The implications for the space sector are high. The cyber threat against the space sector is unprecedented. **The number of cyber operations conducted in the context of the war in Ukraine represents a significant share of all cyberattacks that have ever been conducted against the space sector.** The report also puts things into perspective and emphasizes that most cyberattacks are far from being as damaging and sophisticated as the one against ViaSat.

More broadly, the report has explored how space is an object of fascination and a prime target for some cyber threat actors participating in the Russo-Ukraine war, in particular hacktivist groups. This is significant because it provides an overview into the cyber threat landscape in a sector that has long overlooked cyber threats.

In general, little focus has been given to hacktivist groups in Space Cyber Threat Intelligence (CTI). As exhibited in the report, the surge in hacktivist groups targeting the space sector requires to better understand these threat actors, their motives, capabilities, and behaviors in order to protect space infrastructure (See Figure 9).

These actors also bring new forms of public communication into a sector that is very secretive and rarely publicly acknowledges attacks. The report identified a majority of self-attributions. However, many operations could not be verified with publicly available information. Some groups might also have exaggerated their claims or blatantly lied about them. The space sector should therefore come forward and debunk fake information should hacktivist groups claim cyber operations that did not happen. Otherwise, these fake operations may gather pointless media attention, generate unnecessary panic, and undermine trust in space services. At the same time, communications should remain balanced, calm, timely, and non-politicized in order to avoid escalation or attracting more malicious actors. Reacting disproportionately to each and every attack will prove counterproductive as demonstrated in Roscosmos' case (see Figure 9).

Furthermore, the intrusions into space systems identified by this report suggest that many organizations and systems were not well protected and therefore easily penetrated by unsophisticated operations. This underlines that **space companies need to be aware of their own significance in times of war and take their cybersecurity posture seriously.** One successful operation against a satellite network may quickly lead to cascading effects across sectors and users.

More broadly, **the report demonstrated that space is not yet weaponized through cyber means.** Most

cyberattacks against the space sector have targeted the IT environment of space organizations as well as the user or ground segment of space systems. Spacecraft in orbit were not directly targeted by cyberattacks. Targeting space systems on Earth was sufficient to prevent end-users from using space capabilities on multiple occasions. As a result, the **cyber conflict extended to space systems but remained confined to systems on Earth.**

It illustrates that **the weaponization of outer space remains an emerging phenomenon.** Yet, this is an increasing concern for states, which observe an increase in hostile approaches, eavesdropping attempts, counterspace capabilities developments, and offensive space and cyber capabilities. Cyber offensive tools are attractive counterspace weapons as they provide plausible deniability, environmental independence, and a low barrier of entry for threat actors.[156] States should therefore prepare for this eventuality by establishing cyber mitigation measures, best practices, coordination mechanisms with industrial and commercial actors, as well as responsibilities for defensive and offensive operations (See Figure 9).

Future CSS research in this area will explore how the war in Ukraine is a representative case of the cyber threat landscape in space by looking at other conflicts such as the Israel/Palestine conflict, which seems to share similar patterns of hacktivist activities against the space sector.

[156] Pavur, James, and Ivan Martinovic. "The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space." *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 1, IEEE, 2019, pp. 1–18.

Appendix A – Cyberattacks against the space sector

Date Month	Date Year	Type of target	Country targeted	Target	Attacker	Type of attack
February	2022	Company	USA	ViaSat	Russia (unspecified)	DDoS
February	2022	Company	USA	ViaSat	Russia (unspecified)	Wiper Malware
May	2022	Company	Ukraine	Zavod Rapid	NoName057(16)	DDoS
February	2023	Agency	France	CNES	NoName057(16)	DDoS
March	2023	Agency	France	CNES	NoName057(16)	DDoS
May	2023	Agency	France	CNES	NoName057(16)	DDoS
May	2023	Agency	Sweden	Swedish Space Agency	NoName057(16)	DDoS
November	2022	Company	USA	Starlink	Killnet	DDoS
November	2022	Company	USA	Starlink	Killnet	DDoS
August	2022	Company	USA	Gorilla Circuits	From Russia with Love	Hack and Leak
August	2022	Company	USA	Lockheed Martin	Killnet	Hack and Leak
August	2022	Company	USA	Lockheed Martin	Killnet	Hack and Leak
August	2022	Company	USA	Lockheed Martin	Killnet	Hack and Leak
August	2022	Company	USA	Lockheed Martin	Legion Cyber Spetsnaz	Vulnerability exploit
August	2022	Agency	USA	NASA	Killnet	Data breach
August	2022	Agency	USA	NASA	Killnet	DDoS
October	2022	Agency	USA	NGA	Killnet	DDoS
March	2023	Agency	USA	NASA	Phoenix	Intrusion
March	2023	Agency	USA	NASA	Phoenix	Hack and leak
March	2023	Agency	USA	NASA	Phoenix	DDoS
February	2024	Company	Luxembourg	SES	Phoenix	DDoS
August	2023	Company	USA	Starlink	Sandworm	Malware
August	2022	Agency	Europe	ESA	Cyber Army of Russia	DDoS
May	2023	Agency	Europe	ESA	Cyber Army of Russia	DDoS
December	2022	Company	Ukraine	Ukrkosmos	Cyber Army of Russia	DDoS
May	2023	Company	Germany	Hensoldt	Cyber Army of Russia	DDoS
April	2024	Company	Russia	Astra	IT Army of Ukraine	DDoS
April	2024	Company	Russia	Altegrosky	IT Army of Ukraine	DDoS
June	2022	Agency	Russia	Roscosmos	IT Army of Ukraine	DDoS
March	2023	Company	Russia	Tricolor TV	IT Army of Ukraine	DDoS
March	2024	Company	Russia	Gazprom Space Systems	IT Army of Ukraine	Intrusion
March	2024	Company	Russia	RSCC	IT Army of Ukraine	Intrusion
March	2022	Agency	Russia	Roscosmos	NB65	Hack and Leak
March	2022	Agency	Russia	Roscosmos	NB65	Intrusion
February	2023	Unknown	Russia	GNSS receivers	GhostSec	Intrusion
March	2023	Unknown	Russia	GNSS receivers	GhostSec	Intrusion
March	2022	Agency	Russia	IKI	V0g3lSec	DDoS
April	2022	Agency	Russia	Roscosmos	V0g3lSec	Hack and Leak
August	2022		Russia	Glonass	HimarsDDoS	DDoS
August	2022		Russia	Glonass	HimarsDDoS	DDoS

August	2022	Agency	Russia	Roscosmos	HimarsDDoS	DDoS
December	2022	Agency	Russia	Roscosmos	HimarsDDoS	DDoS
March	2023	Research	Russia	IKI	HimarsDDoS	DDoS
November	2022	Company	Russia	Gonets	OneFist	Intrusion
November	2022	Company	Russia	Satis	OneFist	Intrusion
November	2022	Company	Russia	Megafon	OneFist	Intrusion
February	2023	Unknown	Unknown	Unknown	OneFist	Unknown
January	2024	Agency	Russia	Far Eastern Scientific Research Center of Space Hydrometeorology “Planet”	BO Team	Intrusion
June	2023	Company	USA	Maxar	labs666	Credential theft
March	2022	Company	Russia	RSC Energia	Unknown	DDoS
December	2022	Company	Russia	Zagorskaya GAES-2	OneFist	Intrusion
December	2022	Company	Russia	Zagorskaya GAES-2	OneFist	Intrusion
March	2022	Agency	Russia	Roscosmos	V0g3lSec	Hack and Leak
March	2022	Agency	Russia	Roscosmos	V0g3lSec	Hack and Leak
March	2022	Agency	Russia	Roscosmos	V0g3lSec	Hack and Leak
March	2022	Agency	Russia	Roscosmos	V0g3lSec	DDoS
March	2022	Agency	Russia	Roscosmos	V0g3lSec	DDoS
March	2022	Agency	Russia	Roscosmos	V0g3lSec	DDoS
March	2022	Agency	Russia	Roscosmos	V0g3lSec	DDoS
March	2022	Agency	Russia	Roscosmos	V0g3lSec	Unknown
March	2024	Company	Poland	Flotis	NoName057(16)	DDoS
May	2022	Company	USA	Boeing	Killnet	DDoS
June	2022	Company	USA	ViaSat	Legion Cyber Spetsnaz	DDoS
August	2022	Company	Russia	Reshetnev	IT Army of Ukraine	DDoS
December	2023	Agency	Europe	ESA	Anonymous Russia	DDoS
July	2024	Company	Italy	Leonardo	CyberDragon	DDoS
June	2022	Company	USA	Raytheon Technologies	CyberDragon	DDoS
November	2022	Agency	USA	NASA	Anonymous Russia	DDoS
December	2022	Company	USA	Maxar	Anonymous Russia	DDoS
January	2024	Company	Russia	Special Technology Center	GUR	Data breach
June	2023	Company	Russia	Dozor Teleport	Richard W (Wagner)	DDoS
June	2023	Company	Russia	Dozor Teleport	Richard W (Wagner)	Hack and Leak
September	2023	Agency	France	CNES	Bloodnet	DDoS
May	2023	Research	Netherlands	SRON	Bloodnet	DDoS
Unknown	2022	Company	USA	Inmarsat	Russia (unspecified)	Vulnerability exploit
July	2024	Research	Russia	Military Training Center at BMSTU	Cyber Resistance	Data leak
June	2024	Research	Netherlands	SRON	62IXGROUP	DDoS
December	2023	Company	Ukraine	Locarus	Dark Strom Team	DDoS
November	2023	Company	USA	Garmin	HDR0	DDoS
March	2024	Company	Ukraine	Unknown	Pharanos Cyber Army	Intrusion
April	2023	Company	Russia	UZPS	Anonymous Italia	DDoS
January	2024	Company	Russia	GPSUpdate.ru	Anonymous Italia	DDoS

July	2024	Company	USA	TrafficView	LulzSec	DDoS
January	2024	Company	Russia	Sev-Sat	HimarsDDoS	DDoS
July	2022	Company	Russia	Rostec	HimarsDDoS	DDoS
November	2022	Company	Russia	Rostec	HimarsDDoS	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	CyberPalyanitsa	DDoS
March	2022	Company	Russia	Rostec	IT Army of Ukraine	DDoS
March	2022	Company	Russia	Rostec	IT Army of Ukraine	DDoS
March	2022	Company	Russia	Rostec	IT Army of Ukraine	DDoS
March	2022	Company	Russia	Rostec	IT Army of Ukraine	DDoS
March	2022	Company	Russia	Rostec	IT Army of Ukraine	DDoS
March	2022	Company	Russia	Rostec	IT Army of Ukraine	DDoS
March	2022	Company	Russia	Rostec	IT Army of Ukraine	DDoS
July	2024	Company	Ukraine	JSC Kiev Radar Plant	NoName057(16)	DDoS
June	2024	Company	Ukraine	JSC Kiev Radar Plant	NoName057(16)	DDoS
February	2023	Company	Ukraine	JSC Kiev Radar Plant	NoName057(16)	DDoS
October	2022	Company	Ukraine	JSC Kiev Radar Plant	NoName057(16)	DDoS
July	2024	Company	Ukraine	JSC Kiev Radar Plant	Cyber Army of Russia	DDoS
January	2024	Agency	Ukraine	UCRF	Cyber Army of Russia	DDoS
January	2024	Agency	Ukraine	UCRF	Cyber Army of Russia	DDoS
January	2024	Agency	Ukraine	UCRF	Cyber Army of Russia	DDoS
February	2022	Agency	Russia	Roscosmos	Unknown	DDoS
September	2024	Agency	USA	NOAA	CyberVolk	Data leak
September	2024	Agency	USA	NOAA	CyberVolk	Data breach extorsion
April	2024	Company	USA	Starlink	Ukraine (unspecified)	Software cracking
May	2024	Company	Italy	Avio	NoName057(16)	DDoS
December	2023	Agency	Czech	Czech Aerospace Industry Association	NoName057(16)	DDoS
September	2024	Company	France	Safran	JustEvil	Data leak
September	2024	Company	Ukraine	JSC Kiev Radar Plant	NoName057(16)	DDoS
September	2024	Company	Ukraine	JSC Kiev Radar Plant	NoName057(16)	DDoS
September	2024	Agency	USA	US Geological Survey	CyberVolk	Data breach extorsion
September	2024	Company	Ukraine	Arsenal	NoName057(16)	DDoS
September	2024	Company	Sweden	Hexagon	User1	Intrusion
December	2023	Company	Russia	SKTB Biofizpribor	Twelve	Data breach
September	2024	Unknown	Ukraine	Cell phones (GPS data)	Unknown	Malware
September	2024	Unknown	Ukraine	Cell phones (GPS data)	Unknown	Malware

Appendix B – Analyzed threat actors

Name of group	Support
Onefist	Ukraine
Cyber Army of Russia	Russia
Phoenix	Russia
Killnet	Russia
Ukrainian Cyber Alliance	Ukraine
RUH8	Ukraine
From Russia with Love	Russia
Ghostsec	Ukraine
Ghostsecmafia	Ukraine
Ddos_separ	Ukraine
Russian bird sec	Russia
Joker DNR	Russia
Belarussian Cyber Partisans	Ukraine
Haydamaki	Ukraine
Legion Cyber Spetznats	Russia
Infinity hackers	Russia
Dumpforums	Ukraine
Cyber palyanitsa	Ukraine
Cyber anarchy squad	Ukraine
Himarsddos	Ukraine
Ddosia project	Russia
Nbp hackers	Russia
Anonymous russia	Russia
Redhackersalliance	Russia
NB65	Ukraine
ZSNOSINT	Russia
Beregini	Russia
WE ARE DARKER DI AND LUNA	Russia
Cyber front z	Russia
Cyber army zov	Russia
Bear it army	Russia
Chaossec	Russia
Kvazar ddos	Russia
Bloodnet	Russia
Zarya legion	Russia
Usersec	Russia
Anonymous sudan	Russia
Santalapuss ddos	Russia
Netside group	Russia
Indian cyber force	Russia
Devils sec ddos	Russia
RSOTM xackteam.	Russia
Squad303	Ukraine
Killmilk	Russia
Xaknet	Russia
Noname057(16)	Russia
IT Army of Ukraine	Ukraine
Kalihunt/Russia	Russia
Cyber dragon	Russia
Phantomgroup	Russia
Cybervolk	Russia
Overflame	Russia
High Society	Russia
Hunt3r Kill3rs	Russia
Matryoshka 424	Russia
User1	Russia
Autodafe internet	Russia
Zarya	Russia
Russian hackers team	Russia
Chapaev	Russia
Ddos API MIRAI	Russia
BO Team UA	Ukraine
Digital revolt	Russia
Server killers	Russia
Public clowns	Russia
Anonymous Central Russia	Unclear
Blackjack	Ukraine
Alixsec (7 October Union)	Russia
Zulik Group RU	Russia
Mr. Raty	Russia
22C	Russia
Drug_svo (Fund Friend)	Russia
October 7 Union	Russia
Secjuice	Ukraine
Kelvinsecurity	Ukraine
Heckenclub	Ukraine
Studentcyberarmy	Ukraine
Cybercossacks	Ukraine
Anonsec Italia	Ukraine
Saint Javelin	Ukraine
Cyber legions	Ukraine
#shdwsec (@shdwpnda)	Ukraine
Frc army UA	Ukraine
Cyber resistance	Ukraine
Cybersecs	Ukraine

Cyberpolk	Ukraine
Hack your mom	Ukraine
International intelligence legion	Ukraine
Cyber-regiment	Ukraine
Youranonukrir	Ukraine
Windef	Ukraine
Altrox	Ukraine
Ghostclan	Ukraine
Anonghost	Ukraine
Kromsec	Ukraine
HDR0	Ukraine
Informnapalm	Ukraine
Anon koryos	Ukraine
Nebula	Ukraine
Prana network	Ukraine
Head mare	Ukraine
Cyb3r1c	Ukraine
Nightmare	Russia
Skofilms	Russia
Rubitteam	Russia
Azzasec	Russia
Dedsec	Russia
Hacknet	Russia
Drunken bears	Russia
Evil empire	Russia
Frozenhacker	Russia
Shadowseekers	Russia
Rutherapygroup	Russia
Virtual barrier	Russia
Tekl3l	Russia
Nation ardan	Russia
Horusevolution	Russia
Robin hood cyber	Russia
Wolframiumz	Russia
Cortadorz	Russia
Federal legion	Russia
Coupteam	Russia
Coupboss	Russia
Just evil	Russia
We are legion	Russia
Darkstorm	Russia
Onfpower group	Russia
Onfpower	Russia
Rubit	Russia
Darkseek	Russia
ANDRAX nethunters	Russia

62IX	Russia
Zov cyber army	Russia
Against the west	Ukraine
Raidforums2	Ukraine
Cyber ddos	Russia
APXUB NATO	Russia
Писарь из Штаба	Russia
Kib0rg	Ukraine
Siegedsec	Russia
Ancient dragon	Russia
Deadwawe (cyberdamage)	Russia
Ddozmus	Russia
International cyber alliance	Ukraine
Incognito	Ukraine
SAPPHIRE RUS	Russia
Pharanos Cyber Army	Russia
Anonymous Arabia	Russia
UA Cyber Shield	Ukraine
Threatsec	Russia
Stormous	Russia
Blackforums	Russia
Five Families	Russia
UA-846	Ukraine
Lulzsec	Russia
Deanon Club	Russia
Holy League	Russia
Team R70	Russia
RTF	Russia
Nemesis	Russia
Tesla bot	Russia
V0g3lsec	Ukraine
Netsycho	Russia
Shtil	Russia
Youn1v3rzity (135 Gang)	Russia
ARXU	Russia
Hunt3r Kill3rs	Russia
NIXON CYBER TEAM	Russia
Glorysec	Ukraine
Hivenet	Russia
Global Informations	Russia
Information Soldiers Russian	Russia
Netforcez	Russia
CyberSec	Ukraine
Twelve	Ukraine

List of Acronyms

ANGELS	Argos Neo on a Generic Economical and Light Satellite
API	Application Programming Interface
APT	Advanced Persistent Threat
ATACMS	Army TACtical Missile System
CISA	Cybersecurity and Infrastructure Security Agency
CNES	Centre National d'Etudes Spatiales
DDoS	Distributed Denial-of-Service
EO	Earth Observation
ESA	European Space Agency
EU	European Union
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FPV	First-person view
GEO	Geostationary Orbit
GLONASS	GLObalnaya NAvigatsionnaya Sputnikovaya Sistema
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GRU	Glavnoye Razvedyvatelnoye Upravlenie
GUR	Holovne upravlinnia rozvidky
HIMARS	High Mobility Artillery Rocket System
IP	Internet Protocol
IT	Information Technology
LEO	Low Earth orbit
MFA	Multi-factor authentication
NATO	North Atlantic Treaty Organization
NASA	National Aeronautics and Space Administration
NSA	National Security Agency
PNT	Positioning, Navigation, and Timing
SAR	Synthetic Aperture Radar
SBU	Sluzhba bezpeky Ukrainy (Security Service of Ukraine)
SES	Société Européenne des Satellites
SNSA	Swedish National Space Agency
TPM	Third Party Mission
TRML	Telefunken Radar Mobil Luftraumüberwachung
TTP	Tactics, Techniques and Procedures
UAV	Unmanned Aerial Vehicle
URL	Uniform Resource Locator
US	United States
VPN	Virtual Private Network

About the Author

Clémence Poirier is a Senior Researcher in the Cyberdefense Project within the Risk and Resilience Team at the Center for Security Studies (CSS) at ETH Zurich.

Prior to joining CSS, she was a Research Fellow at the European Space Policy Institute (ESPI) in Vienna, Austria where she conducted multidisciplinary research on space affairs. Clémence also worked as a Researcher for Flinders University in Adelaide, Australia where she carried out policy and legal research on the cybersecurity of the Australian space infrastructure.

She serves as the Space Generation Advocacy and Policy Platform's Lead on Responsible Space Behavior at the Space Generation Advisory Council (SGAC). She is affiliated with the Open Lunar Foundation and the Jeff Bleich Centre for Democracy and Disruptive Technologies (JBC).

Her research interests include space cybersecurity, electronic and cyber conflict in outer space as well as broader space security and defense issues.

Clémence holds a master's degree in international relations, International Security and Defense as well as a bachelor's degree in Foreign Applied Languages (English, Russian, Spanish) from University Jean Moulin Lyon III, France.

CSS
ETH Zürich

The **Center for Security Studies (CSS)** at ETH Zürich is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.