Space Cybersecurity Lessons Learned from The ViaSat Cyberattack

Nicolò Boschetti∗
Johns Hopkins University, Baltimore, MD, 21218, United States

Nathaniel G Gordon†
Johns Hopkins University, Baltimore, MD, 21218, United States

Gregory Falco‡
Johns Hopkins University, Baltimore, MD, 21211, United States

Just an hour prior to the Russian invasion of Ukraine, satellite communications provider ViaSat experienced an outage that dealt a critical blow to Ukrainian intelligence infrastructure. This cyberattack presents a landmark example of the vulnerabilities inherent to dual-use infrastructure in an active military environment. We present several technical- and organizational-level lessons demonstrated by the attack, as well as the significance of this cyberattack in the context of the conflict.

I. Nomenclature

\[
\begin{align*}
DDoS &= \text{ Distributed Denial of Service} \\
DMZ &= \text{ Demilitarized Zone} \\
ELF &= \text{ Executable and Linkable Format} \\
IDU &= \text{ Indoor Unit} \\
NOC &= \text{ Network Operations Center} \\
ODU &= \text{ Outdoor Unit} \\
POP &= \text{ Point Of Presence} \\
RFP &= \text{ Request For Proposals} \\
VPN &= \text{ Virtual Private Network} \\
ZTA &= \text{ Zero-Trust Architecture}
\end{align*}
\]

II. Introduction

ViaSat is a satellite communication service provider that experienced an outage of its KA-SAT Network on February 24, 2022[1]. Thousands of end-user terminals, through the use of a malware wiper, were disabled, preventing many users from connecting to the network without a subsequent replacement of the modem. This attack stands as a unique learning opportunity for several reasons, despite the mechanics of the attack itself being relatively standard. The outage is the most significant publicly disclosed attack against a space system in recent history, making it an ideal case study. Furthermore, the attack is the first instance of a cyberattack serving as a first digital strike in a military conflict, occurring just an hour before the Russian invasion of Ukraine in February 2022. Lastly, the added complexity of ViaSat’s dual-use paradigm of being leveraged as both a commercial and military asset is indicative of trends for future attacks as the space sector continues to commercialize.

III. The ViaSat KA-SAT Internet Network

Launched and owned by Eutelsat through the subsidiary Euro Broadband Infrastructure Sàrl (EBI), the KA-SAT network was acquired by ViaSat in 2020 (satellite and ground assets). During the acquisition transition period, the
management of the ground segment was still in the hands of the Eutelsat subsidiary Skylogic [2]. There are three aspects of the KA-SAT system - the space, link and ground segment, each of which is described below.

A. Space Segment

The space segment of the system consists of Eutelsat’s KA-SAT satellite. Based on the Eurostar E3000 bus and manufactured by EADS Astrium, it is designed to provide consumer-oriented broadband services operating in Ka-band. Ironically, it was launched into Geostationary orbit by a Russian Proton-M rocket from the cosmodrome of Baikonur in 2010 [3].

B. Link Segment

The satellite entirely operates in Ka-band through an 82 spotbeams configuration and ten Earth Gateway Centers connected to the internet [4]. At full capacity can provide a total throughput of 70 Gigabits per second. Each spotbeam serves a cell with a diameter of approximately 250 km.

C. Ground Segment

The ground segment consists of three main components. Ten Gateway Earth Stations, managed by the Eutelsat’s subsidiary Skylogic, manage the 82 spot beams in which is divided the satellite coverage. The ten Gateway Earth Stations are placed in Madrid (Spain), Cork (Ireland), Rambouillet (France), Turin, Udine, Scanzano (Italy), Berlin (Germany), Helsinki (Finland), Athens (Greece) and Cyprus. They are interconnected through a redundant fiber ring also through six additional POPs. The second component is the end-user terminal. The SurfBeam2 Terminal was initially produced and sold by Tooway but managed by the broadband provider Skylogic. The user terminal is composed of an IDU and an ODU. The IDU consists of a modem with wireless, LAN, and Ethernet capabilities, while the ODU comprises a transceiver and an antenna of variable diameter. The third component is the NOC that mainly manages the broadband traffic and the access of the end-users to the service.
IV. Attack Life Cycle

The ViaSat cyberattack involved an attacker that exploited weaknesses of the KA-SAT ground segment to disrupt its telecommunication network. While the attack’s signal was disseminated by the space segment, the space segment itself was not directly targeted. Further, unlike the jamming attacks on Starlink terminals deployed in Ukraine after the ViaSat attack, there were no intrusions or interference on the link segment. The attackers maximized their penetration capabilities across two components of the ground segment: the modems of individual users and the modem control servers. Through open-source intelligence, we have reconstructed the lifecycle of the attack. However, without first-hand knowledge of ViaSat’s systems, we cannot be certain about our hypothesis. The attack life cycle is depicted in Figure 1.

ViaSat has shared that the initial attacker intrusion point was via the internet [1]. Skylogic’s control servers, the Gateway Earth Stations, and the Surfbeam2 modems rely on VPN appliances produced by the company Fortinet as indicated by the security researcher Ruben Santamarta [6]. In 2021, Fortinet disclosed an attack on their VPN “Fortigate” that exploited a vulnerability discovered in 2019 [7]. The allegedly Russian hacker group Groove stole and published credentials of almost 500,000 IP addresses in the same year [8]. It is known that Fortinet released a patch to address the vulnerability, but it is unclear if ViaSat’s operator, Skylogic, ever deployed the patch.

Therefore, we can surmise that the attacker used the unpatched VPN to access Skylogic’s Gateway Earth Stations or POP server from the open internet. This access, or privilege escalation, allowed the attacker to pass the DMZ and access the bent-pipe satellite intranet (the trusted management network) tunneling their way to the Surfbeam2 modem. This process is confirmed by ViaSat’s statement assessing that the “attacker moved laterally through [the] trusted management network to a specific network segment used to manage and operate the network” of modems [1]. Not all ViaSat modems were targeted. This can be explained by an operator’s capability at the Gateway Earth Stations to select which of KA-SAT’s 82 geographic cells receive signal [4]. This implies that the attacker specified which geographic cells (and their respective modems) would receive the signal with the malicious commands. Once at the modem, the attacker again escalated privilege using the unpatched VPN, enabling their manipulation of the modem’s management. The modem likely had limited or no firmware authentication requirements, therefore the attacker was able to provide a ‘valid’ firmware update, installing an ELF binary dubbed “AcidRain” which deleted data from the modem’s flash memory [9].

We hypothesize that the attack’s spillover effects in Germany and other European states are due to either an error when selecting the geographic cells that received the malicious signal, or simply the selection of cells that contained Ukrainian territory with overlap of other EU countries.
V. Lessons Learned

This serious and high-profile attack demonstrated that dual-use commercial space systems are a desirable cyber target. The space systems community can learn from these events, in terms of both technical and policy considerations.

A. Technical Lessons

Three technical insights can be gleaned from the attack. First, satellite providers must be concerned about their supply chains and vendor ecosystems. Second, aerospace companies should be cognizant of attacks occurring in non-adjacent industries. Finally, despite advancements in security technologies, maintaining a regular security update and patch management program is still critical for operations.

1. Monitor Supply Chain Concerns

   Carefully audit and manage the security of third-party provided ecosystem components and design technology ecosystems with Zero-Trust Architectures to avoid cascading cyber security failures.

   Supply chain attacks have been of principal concern to digital service providers and users, especially since the landmark Solar Winds cyberattack in 2020 [11]. Supply chain attacks are less documented for the aerospace sector, where ViaSat appears to be the first publicly documented incidence of a supply chain security impact on space systems. The ViaSat attack is yet another demonstration of the criticality of evaluating supplier products before integrating them as core components of a technology stack. Space system operators should engage in supply chain security best practices such as conducting extensive vendor cybersecurity evaluations. At its most basic, space system supplier selection should include a requirement during the RFP process that the vendor have a cyber risk management strategy and plan in place including an incident response program for a potential attack. Space system operators should also use third-party organizations such as Security Scorecard or Bitsight to evaluate suppliers’ cybersecurity posture through a simple rating system. Ideally, vendors should be penetration tested before engaging with their services to evaluate their cybersecurity first-hand. It is unclear if there were any such measures engaged by ViaSat before procuring their VPN provider’s services.

   It is entirely viable that proper supply chain security practices were engaged by ViaSat and the VPN provider’s vulnerabilities still went unnoticed, in which case ViaSat would have needed a ZTA to mitigate threats to its technology ecosystem. ZTAs hold the underlying assumption that some aspect of the technology ecosystem is compromised. An effective ZTA involves engineering systems so that if any individual component is compromised by an attack, the implications of the attack will be isolated and there will be no cascading consequences across all features of the system. Given the satellite terminal failures as a result of the compromised VPN, it is clear that ViaSat was not engaging a ZTA, which could have prevented the resulting denial of service across all terminals.

2. Track Precursor Indicators

   Continuously check to see if your devices have been part of attacks disclosed on darkweb forums and monitor the cyber threat landscape to anticipate impending threats.

   ViaSat’s modem vulnerability was not an isolated incident. There were several events preceding the attack which could have been critical to preemptively mitigating the attack’s impact. The first precursor was a set of attacks against the VPN provider and their devices. In 2021, an attack that effected 87,000 FortiGate SSL-VPN devices leveraged a vulnerability disclosed by Fortinet in 2019 [6,7]. Subsequently, the attacker, an operative from the Groove ransomware group, disclosed credentials for 498,908 VPN devices on the RAMP ransomware forum [8]. At the time of this disclosure by Fortinet, ViaSat could have done a crosscheck of their IP addresses and the compromised ones on credential dump. Such a practice should be a standard protocol for any organization after a substantial data breach of a service they use.

   The second warning of the attack included a series of wipers targeted at the Ukraine since the beginning of 2022. Specifically, there were six wiper malwares–WhisperKill, WhisperGate, HermeticWiper, IsaacWiper, CaddyWiper, and DoubleZero–detected in the year leading up to the AcidRain attack [9]. Microsoft asserted that more than 40% of the destructive wiper attacks in Ukraine were aimed at critical infrastructure, whereas 32% of destructive incidents affected Ukrainian government organizations [12]. Further, they posited that attackers were making small modifications to similar malware to evade signature detection. This pattern of attacks targeting critical infrastructure should have placed ViaSat on high alert given the critical nature of their satellite terminals for the Ukrainians. SentinelOne, who conducted a thorough investigation of the malware, also noticed that there was a 55% code overlap of the Acid Rain with VPNFilter which has plagued IoT devices and modems since 2018 [9].

4
While it is impossible to predict when an attack will occur, it is critical for aerospace organizations to carefully track relevant cybersecurity threats and anticipate how their technology relates to the current threat landscape. Noticing and acting on precursor indicators leading up the ViaSat attack could have helped ViaSat prepare for the incident.

3. Update Management

Develop and adhere to a regular patch management plan that pushes firmware updates to the technology ecosystem and enforce security authentication practices for system updates.

Persistently updating and maintaining software for security flaws should be standard practice for any technology ecosystem. A patch management program is critical to systematically address the ongoing discovery of vulnerabilities and implement remediation measures. Space system providers have no reason to avoid this common best practice. Security researcher Santamara, who had access to an infected Surfbeam2 modem conducted a firmware dump of the impacted device, revealed that the modem was running firmware version 3.7.3.10.9—which had not received an update since 2017 [6]. Upon further analysis, we discovered that there was at least one update to this firmware issued in 2018: firmware version 3.7.3.11.3. It is unclear if this update had any security patches contained therein; however the older, unpatched firmware version running on the Surfbeam2 terminals indicates there was a failure to push updates to devices by ViaSat. Given the compromised VPN credentials described previously, we would have expected that the terminals’ firmware be updated to engage the patched VPN.

It also appears that there was an inherent vulnerability described as a ‘lifeline’ features of the modem. An emergency firmware update capability allowed updates over a specific Multicast group [6]. Despite the presence of this feature, it was unusable after the AcidRain attack and could have likely been exploited to deploy this attack to the modems. It is unclear if there is any validation tied to this mode of pushing a firmware update.

Both concerns directly point to the need for robust and secure update management practices for technology ecosystems. Aerospace organizations should engage in regular patch management practices and carefully orchestrate how firmware updates and patches are allowed to be installed - ideally using validation and authentication techniques.

B. Management Lessons

The ViaSat cyberattack also illuminates operations management and policy lessons for the sector. First, dual-use space technology will increasingly be a cyberattack target. Second, space system failures have cascading consequences. Finally, agile responses are required for dual use technologies.

1. Dual-Use Technology

Commercial technology that is engaged for both civilian and military purposes should be prepared to be treated as if they are military targets.

ViaSat provides satellite communications services to a wide selection of entities across Europe that range from governments to small businesses. One such customer is the Ukrainian military. Despite ViaSat being a US-headquartered commercial entity, it was clearly a military target in the context of Russia’s invasion of Ukraine. The US Department of State issued a comment regarding the attack that Russia’s intention was to “disrupt Ukrainian command and control during the invasion” [13]. This conclusion is consistent with the timing of the event that occurred one hour before its invasion of Ukraine.

While space systems historically have been developed, owned, and operated by civilian government and military agencies, the commercial space sector is thriving and providing a myriad of dual-use services to commercial and government organizations. Aerospace enterprises should assume that sales to government entities will cause their assets to be treated by adversaries as if they were owned and operated by the government in the cyber realm. Therefore, commercial space companies should evaluate their risk profile and their risk appetite when selling services to governments that may be the target of an adversary. It is unlikely for governments to come to the defense of companies targeted in the cyber domain, therefore, space companies selling to government agencies should be prepared to defend their assets should they become a cyber target.

2. Cascading Effects

Consider engaging a heterogeneous ecosystem of technology across end user sectors to mitigate cascading sectoral failures.

While Russia targeted ViaSat in order to hamper Ukraine’s military command and control, there were consequences
well outside of Ukrainian territory. ViaSat is a global company with hundreds of thousands of modems deployed. Of these hundreds of thousands of satellite modems, 40,000 were destroyed beyond repair [14]. Some of these 40,000 compromised modems were engaged for command and control of Enercon’s wind turbines throughout Germany, rendering nearly one fifth of the Germany (5800 turbines) wind energy production system inaccessible for control intervention[15]. While many believe that the impact on Enercon’s wind turbines was an unintended consequence of the attack, the impact on Enercon was nevertheless present.

This ancillary effect is notable because space system cybersecurity is typically the soft, white underbelly of a wide variety of critical infrastructure. It is rarely considered when assessing the security of various sectors; however, space systems are the linchpin to many operations [16]. When a space system is compromised, it could become a single point of failure across a variety of assets. This creates the potential for cascading failures of critical infrastructure prompting the need for heterogeneous ecosystems of space systems. Aerospace organizations should consider implementing software diversity into their configurations and deployments to limit potential fallout from the compromise of a single system.

3. Organizational Complexity

Streamline operational control, security practices and incident response policies across an organization, regardless of geographic dispersion.

The KA-SAT infrastructure ecosystem is organized across several subsidiaries that manage different components of the operation. Such a complex organizational structure risks fragmenting security control processes as was the case here, evidenced by the apparent lack of coordination of ViaSat, Eutelsat, and Skylogic when responding to the attack. Given each subsidiary is responsible for different elements of the KA-SAT infrastructure, it becomes challenging to keep track of the security controls that each are responsible for and has actually executed. Further, the geographic dispersion of the organizations and their integration through corporate acquisition did not help with the managerial coordination of the attack response. A highly fragmented command structure across the subsidiaries and the geographies further weakens an infrastructure’s security profile[17].

The attack occurred during an ownership transition period, which likely further complicated incident coordination[2]. During a merger or acquisition, aerospace organizations should clarify their cyber risk incident response plans and the responsibility of constituent parties. Should an aerospace company be highly distributed and fragmented among subsidiaries, it is critical to maintain and execute consistent cyber risk management processes that are well-understood by all entities.

4. Incident Response Agility

Systems engaged for mission-critical functions should have agile, software-enabled response strategies, rather that slow hardware replacement requirements.

The AcidRain wiper malware resulted in the development of 40,000 inoperable modems [14]. ViaSat’s response included pushing over-the-air updates to some of the modems, while replacing the modems altogether for other users [1]. It is unclear why some modems were able to continue working after an over-the-air firmware update, whereas others needed replacements. Based on details about the AcidRain malware, it is surprising that a compromised modem would be able to receive an over-the-air update given the system that would be accepting the update is non-functional. Further ViaSat cites the shipment of “tens of thousands of replacement modems” [1] to its distributors, which implies a significant number of the compromised modems were entirely replaced. It is unclear how long it took to furnish end users with the replacement modems and what communication capabilities were made available to them in the interim.

Shipping tens of thousands of modems is undoubtedly time-intensive and costly. Given the critical nature of the satellite communication system, it is unacceptable for such a delay. Space system providers must plan for such attacks to occur against their system and establish mechanisms to engage with their devices despite their compromised nature and reduced functionality. Alternatively, redundant systems should be made available to users without requiring extensive logistical operations.

An example of an agile response to attack includes how SpaceX’s Starlink handled a jamming attack against its terminals that were subsequently delivered to Ukraine after the ViaSat attack. While under attack Starlink operators pushed a software update that was developed to restore access for users. Granted, Starlink was experiencing a different type of attack that impacted the radio signal, not the terminals themselves which allowed for opportunities such as dynamic spectrum switching to remedy the issue; however, Starlink was praised for their rapid response by the director of electronic warfare at the US Office of the Secretary of Defense, Dave Tremper[18]. Such agile, software-enabled
VI. Cyberattack in Context

The attack on Viasat’s KA-SAT infrastructure is part of the early stages of the Russian invasion of Ukraine that began on February 22, 2022. To contextualize the cyber attack, it is important to briefly describe the phases of what Moscow has called its Special Military Operation. What is not formally a war between Ukraine and Russia is still ongoing; therefore, some information may change after the publication of this research.

From a cyber point of view, the first weeks of war did not demonstrate the full extent of attacks that would be expected given Russian capabilities. Despite the reported large amount of wipers delivered to Ukrainian systems, the Russian Army has not been able (or willing) to attack Ukrainian critical infrastructure widely. In the time between the 2014 annexation of Crimea and the 2022 military operation, Ukrainian power grids suffered heavy cyber attacks. However, apart from the attack at the center of this research and several other aforementioned wipers, Russia has primarily focused on DDoS attacks and website hijacking [19].

It is confirmed that the Viasat’s service disabled by the attack had the Ukrainian armed forces and other government agencies among its clients [20]. The Russian interest in disabling Ukrainian communications and C2 links before the invasion is evident. This is especially in view of lightning war, isolation and overthrow of the government, and rapid penetration into enemy territory. The affected modems, however, were not only located on Ukrainian territory but also among other users, such as different operators of wind turbines in Germany or the satellite communication service provider EuroSkyPark [21].

From a strategic point of view, assuming that the Russian plan did not foresee the second phase of the war, it is clear that such spill effects would seriously affect the stability of the conflict. Moreover, in 2014, with the annexation of Crimea, despite heavy Western sanctions, the military and technological involvement of NATO nations was somewhat limited. Therefore, it seems logical that Russia was interested in making the international scenario follow the 2014 scenario rather than irritating or threatening European nations by pushing them to the intervention that occurred. We can therefore interpret spillover effects across the Ukrainian border as collateral damage that, on the one hand, highlight the imprecision of the attack and, on the other, could highlight one of the reasons for the reduced Russian cyber activity during the war.

VII. Discussion

The ViaSat cyberattack has brought the importance of space system cybersecurity into public view, despite it not being the first or most severe space system cyberattack. While the attack was not highly sophisticated compared with other statecraft cyber campaigns, space companies have an opportunity to learn from this attack and apply the lessons learned to their risk management practices. The technical and policy lessons gleaned from the ViaSat attack are not all unique to space systems nor do they require substantial cost to consider; hence should be manageable to implement.

VIII. Conclusion

This paper describes seven lessons learned from the ViaSat cyberattack experienced at the dawn of the Russia/Ukraine war in 2022. These lessons include both technical and policy considerations that should be heeded by space companies to improve their cybersecurity posture. Technical lessons involve, being mindful of supply chain cybersecurity, track precursor indicators to anticipate threats, and develop a robust update management process for the technology ecosystem. Policy lessons include that dual-use commercial space companies must be aware and prepared to be a military target in times of conflict, heterogeneous software practices could help reduce the single point of failure across diverse users, and the need for an agile and software-enabled strategy to quickly respond to attacks. We expect that the ViaSat cyberattack case study will become a common reference point for advocates of space cybersecurity in decades to come.

References


[2] Inc., V., Viasat Completes Acquisition of Remaining Stake in its European Broadband Joint Venture, Inclusive of the KA-SAT


[5] “Illustrations has been partially designed using graphic resources from Flaticom.,”, 2022.


