An analysis of the cyberattack against ViaSat of February 2022

From technical details to the overall relevance for cybersecurity of critical infrastructures

Alessandro Mura*

**MA student at University of Bologna.* *alessandro.mura6@studio.unibo.it*

Abstract While the first Russian soldiers were putting their boots on Ukrainian soil, giving start to the Russo-Ukrainian conflict in 2022, the private company ViaSat, providing satellite services to the Ukrainian Army, suffered a severe cyberattack. The present work summarizes all publicly available information surrounding the malicious action and, in particular, it provides a detailed technical analysis of all phases and types of attack. Furthermore, the offensive action is put into the context of the recent developments in cyberwarfare and the most relevant Russian disruptive attacks in cyberspace against Ukrainian infrastructures. The paper will argue that the case under study is emblematic of most relevant developments in cybersecurity of the space sector and it therefore reconnects the dynamics of the event to the most recent literature on the topic. The analysis spurs into the elaboration of a number of lessons learned from the attack and highlights the need to better inquire all opportunities and criticalities coming from the increasing surge of private actors in the space sector.

1. Introduction

The aim of this paper is to analyze the cyberattack conducted against the US-based company ViaSat hours before the Russian invasion of Ukraine, on the 24th of February 2022. In particular, the offensive was directed towards the management network of the KA-SAT satellite of the aforementioned company, which provided internet access services mainly in Europe and in some part of the Middle East and, most importantly, counted among its clients the Ukrainian Army. Studying the incident is of uttermost importance for many reasons. Firstly, the act has been carried out in the context (or, it could be said, as the first bullet shot) of an interstate war and has had military consequences on the battlefield which severely deteriorated Ukraine capabilities. Hence, it is a case worth considering for studying the battlefield impact that attacks carried out on cyberspace can have. Secondly, the attack aimed at disrupting internet services offered by dual-use communications satellites operated by a private company: it is not since long that non-public enterprises are entering the space sector, and this brings along both risks and opportunities. The ViaSat case can be analyzed as an instance of the former. In general, the increasing fragmentation of strategic infrastructures' ownership translates into the need of expanding the scope of cybersecurity to corporate and private ownership dynamics, as this case will highlight. Thirdly and lastly, the present work reiterates what should be an obvious argument, namely that cybersecurity guidelines and best practices are of fundamental importance, especially when dealing with critical infrastructures providing security services to national armies. The hackers, indeed, most probably accessed the network of the KA-SAT satellite through a legitimate user account, that is through identity theft, which is a vulnerability mostly posed by the humans behind the screens, their behaviors and the effort an enterprise puts in establishing security guidelines which are both sufficiently effective and practical to follow even by non-expert users.

The paper will unfold as follows. After the current brief general introduction, section two will provide an additional overview of the company and its operations, its organizational structure and the acquisition process in which it was involved still at the time of the attack. Even if it could be possible to argue that these details are unrelated to the attack itself, this is not true; indeed, as said above, the surging presence of private actors in space infrastructures makes for an increase and variation in the sources of vulnerability that can be

exploited by attackers. Furthermore, a summary will be made of Russian offensive operations in cyberspace specifically aimed at Ukraine since 2014. Section three, the core of the paper, will delve deep into the technical details of the attack and all of its phases. It is important to note that some issues are still not completely clear, but numerous studies from solid analysts and a reconstruction of events from people directly involved in the response process inside the ViaSat team will allow for a faithful depiction of how the action was conducted. Sections four and five will deal, respectively, with the impact the attack had, and the lessons learned from the event. Finally, section six will sum up and conclude the paper.

2. Context and background

Understanding the context of the attack means primarily gathering information about the attacker and the victim. Following attribution of the attack to hacker groups related to the Russian army by the US government[1] and the European Union[2], this section shortly reconstructs Russian cyberattacks against Ukraine since 2014. Regarding the victim, a brief review of *ViaSat* operations in the business of satellites communication will serve as a paradigmatic case for understanding the issues, from a cybersecurity standpoint, which comes along with the surge of private ownership of space infrastructures.

2.1 ViaSat

ViaSat is a US enterprise founded in 1986 and headquartered at Carlsbad, California. The company provides satellites broadband services both for commercial and military uses. Since its early years, indeed, *ViaSat* worked on technological developments for the defense sector, making orders for military appliances account for two thirds of total orders in 2002 and making the company more defense oriented[3]. The company retains this orientation even today: recent examples of this are the 2018 *National Security Agency* (NSA) authorization for *ViaSat's* Battlefield Awareness and Targeting System

[1] See Blinken, 2022. https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/#:~:text=Today%2C%20in%20support%20of%20the,those%20actions%20had%20spillover%20impacts

[2] See the related press release of the Council of the EU. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[3] See "ViaSat shift focus". https://www.sdbj.com/imported/viasat-shifts-focus-from-commercial-to-defense/

Dismounted (BATS-D)[4], the 2020 award of a contract for providing NATO's Allied Rapid Reaction Corps with new technology in the field of cross-domain integration[5] and the provision of satellite communications to the British Royal Navy since the same year[6]. *ViaSat* launched its first satellite into space, *ViaSat1*, in 2011; however, already in 2009 it had acquired the company *WildBlue*, which owned the *WildBlue*-1 satellite launched in 2006 and was also operating Ka-band resources on *Telesat Canada* owned Anik-F2 satellite. In addition to this space fleet, *ViaSat* acquired in 2020 from *Eutelsat* control over *Euro Broadband Infrastructure Sàrl* (EBI), formerly owned together with *Eutelsat* as a joint venture; this acquisition included ownership of the KA-SAT satellite, launched in space in 2010, and all its related infrastructure[7]. The KA-SAT satellite is composed of infrastructure at the physical layer of cyberspace, both in space and on the ground, and at the logical layer, allowing the functioning of the service. The space segment consists of the satellite itself while on the ground there are 10 Gateway Earth Stations which cover eighty-two geographic cells, or spot beams, in which the total satellite coverage is partitioned. Each geographic cell has a diameter of 250km circa. The other component of the ground infrastructure is composed by the end-user terminal, a Spotbeam 2 modem which also includes a transceiver and an antenna. At the time of the attack, KA-SAT network counted with 110 to 120 thousand commercial modems active.[8] The Gateways were connected among them through a fiber ring to a Core Node providing for the control plane and the management plane. Specifically, the network was segmented into three Bandwidth Aggregation Points, mainly according to the geographical region of the modems. Two of these BAPs were managed by *Skylogic*, while another one, specifically tailored for aviation and government customers, was directly under the responsibility of ViaSat itself. This segmentation, which is the result of the acquisition agreement

[4] See "Viasat's AN/PRC-161 BATS-D". https://www.prnewswire.com/news-releases/viasats-anprc-161-bats-d-handheld-link-16-radio-receives-nsa-authorization-for-use-by-international-military-forces-300700755.html

[5] See "Viasat, CDW Awarded NATO Contract". https://markets.businessinsider.com/news/stocks/viasat-cdw-awarded-nato-contract-for-agile-command-control-and-communication-project-1029725407

[6] See "ViaSat to supply Britain". https://www.defensenews.com/industry/2020/11/03/viasat-to-supply-britains-future-frigate-with-satellite-communications-tech/

[7] See "ViaSat completes purchase". https://www.satellitetoday.com/connectivity/2021/04/30/viasat-completes-purchase-of-euro-broadband-infrastructure/ and https://investors.viasat.com/news-releases/news-release-details/viasat-completes-acquisition-remaining-stake-its-european

[8] Information from a ViaSat official presentation on the issue, "Lessons Learned from the KA-SAT Cyberattack: Response, Mitigation and Information Sharing" on the channel "BlackHat". See https://www.youtube.com/watch?v=RdjthhBylMk.

of KA-SAT between *Eutelsat* and *ViaSat*, was exploited by the attackers as we will see later. It is important to remind that, at the time of the attack, the Network Operating Center managing broadband traffic and communications between a portion of the gateways and the end-user terminals, were still in the hands of *Eutelsat's* subsidiary *Skylogic*[9].

This brief reconstruction of *ViaSat* business operations, apart from providing basic information and a sketched characterization of the cyber-attack victim, mainly serves to provide an idea of the dynamics underlying ownership changes of space infrastructures resulting from the increasing presence of private entrepreneurs in this sector. Privately owned satellites are subject to sales, acquisition and various types of corporate agreements. Key to this specific case, for example, is the fact that a transition agreement included in the 2020 acquisition of *EBI* between ViaSat and *Eutelsat* (which gave *ViaSat* ownership of the attacked KA-SAT satellite), provided that an Italy-based subsidiary of *Eutelsat*, called *Skylogic*, was in charge of operating a partition of the KA-SAT network, for the rest operated by ViaSat itself. The network management was therefore divided between two different entities, ViaSat and Skylogic, and most reconstructions of the incident established that the attackers entered the network by exploiting vulnerabilities in the *Skylogic* operated partition, moving laterally afterwards. This fragmentation in the management network hampered uniformity of cybersecurity measures and augmented the attack surface exploitable for malicious actions.

2.2 Russian cyberattacks against Ukraine.

The hacking of the KA-SAT satellite network happened in the context of increased offensive operations by Russia against Ukraine since the takeover of Crimea in 2014, and hours before an escalation of hostilities with the Kremlin's full-scale invasion and the ensuing "Battle of Kiev". Indeed, following the mass protests in Ukraine that came to be known as "Euromaidan" in 2013, succeeded by the "Revolution of Dignity" in 2014, Russian forces announced annexation by force of the Crimean Peninsula, and a military conflict started between the Ukrainian government and Russian-backed separatist forces in the Donbas region. Especially since 2014, cyberattacks aimed at Ukrainian governmental

[9] See Boschetti, Nicolò, Nathaniel G. Gordon, and Gregory Falco. "Space cybersecurity lessons learned from the viasat cyberattack." ASCEND 2022. 2022. 4380.

facilities or assets became more frequent, sophisticated and impactful, denoting the ability of Russian cybergroups. Relevant examples include the attack of the Ukrainian electrical power grid in 2015 and 2016, and various malware attacks such as the spread of the so-called "NotPetya", a false ransomware. The first attack involved the use of the "BlackEnergy 3" and "KillDisk" malwares[10] to take control of Supervisory Control and Data Acquisition (SCADA) systems of Ukrainian "oblenergos", which basically constitute the regional energy distribution substations, and put them out of service. The attack resulted in power outages affecting more than 200.000 customers[11]. One year later, a similar attack was performed using the "Industroyer" malware (also known as "crashoverride"), displaying limited effects but signaling, by its increased complexity, the willingness to develop new software specifically tailored to the functioning of the Ukrainian electric power grid[12]. The "NotPetya", instead, is a malware designed to basically destroy data and disks. It appears as a ransomware, asking for a payment in exchange for the encrypted data while these are actually not recoverable. This makes it more similar to a wiper[13]. Starting from June 2017, various government agencies, the central bank, several airports and even the Chernobyl nuclear plant and the Danish firm *Maersk* were infected, suffering grave damages[14]. *Maersk* estimated the losses resulting from the alt of activities in $1.3 billion, with the unprecedented harm caused by the malware resulting in a judicial controversy with its insurers about whether the attack could be considered as an act of war[15]. The total losses caused by "NotPetya" spread around the globe are estimated to be around $10 billion[16].

Finally, it must be highlighted that the *ViaSat* network hacking of February 2022 was not the first instance of an offense directed to space satellites' infrastructures in the region. Less than two months before, indeed, on the first

[10] See "2015 Ukraine Electric Power Attack". https://attack.mitre.org/campaigns/C0028/.
[11]See Case, Defense Use. "Analysis of the cyber-attack on the Ukrainian power grid." Electricity Information Sharing and Analysis Center (E-ISAC) 388.1-29 (2016): 3.
[12] See Slowik, Joe. "Anatomy of an attack: Detecting and defeating crashoverride." VB2018, October (2018).
[13] See "NotPetya". https://attack.mitre.org/software/S0368/.
[14] See Dearden, "Ukraine cyber attack". https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html.
[15] And therefore, outside of the insurance coverage. See https://www.bloomberg.com/news/features/2019-12-03/merck-cyberattack-s-1-3-billion-question-was-it-an-act-of-war?embedded-checkout=true.
[16] See Barichella, Arnault. "Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe.", Jacques Delors Institute, Policy Paper 281, September (2022).

days of January, approximately 1.350 kilometers of a submarine cable providing connection between Norway and the Svalbard Satellite Station were found cut and removed[17]. Involvement in the attack of Russian forces has been suggested but not proven[18]. Eirik Kristoffersen, Norwegian Chief of Defence, declared that "this could have happened by accident, but the Russians are capable of cutting cables"[19]. If demonstrated as a deliberate human action, the cable-cut would be a further example of an act of sabotage directed at a satellite infrastructure, specifically in the physical layer of cyberspace.

3. A detailed analysis of the attack

3.1 The incident in brief

On the early hours of February 24, 2022, the network of the KA-SAT satellite, owned by US-based satellite telecommunications company *ViaSat*, suffered a cyberattack. Indeed, hours before Russian ground forces started to physically invade Ukraine, marching towards its capital city, Kyiv, satellite communications provided from ViaSat to thousands of users among which the Ukrainian army, started to be severely disrupted. What follows is an attempt to reconstruct the technical details of the incident. This reconstruction draws heavily on two presentations that ViaSat officials made around the issue, one during the "BlackHat" USA cybersecurity event of 2023[20] and another one during the "Defcon31" conference[21]. Of course, other sources are cited in the analysis. As reported by *ViaSat* officials, the KA-SAT network actually suffered two different types of attack: the first one comprised the use of a wiper malware to knock out end-user modems; the other one was instead a Distributed Denial of Service (DDoS) attack aimed at flooding KA-SAT network so as to render it unresponsive to legitimate requests of connection. Both attacks are described in detail in the sections that follow.

[17] See Kolovos, 2022.
[18] See Schia, Rødningen and Gjesvik, 2023.
[19] See Gronholt-Pedersen and Fouche, 2022. https://www.reuters.com/graphics/ARCTIC-SECURITY/zgvobmblrpd/.
[20] See Colaluca and Walter, 2023. https://www.youtube.com/watch?v=RdjthhBylMk.
[21] See Colaluca and Sanders, 2023. https://www.youtube.com/watch?v=qI_ICtX3Gm8.

3.2 The Wiper Attack

The attack was realized through the logical layer of the KA-SAT infrastructure and damaged only a part of its physical components: the satellite itself and other physical infrastructures were not directly harmed, whereas the final targets of the malicious action were the "SurfBeam2" modems. The surface vector for the attack was the internet: *ViaSat* sources talked about a "misconfiguration in a VPN appliance"[22]. The hacker group must have first carried out a work of reconnaissance, to look for vulnerabilities and gather information about legitimate users, stealing their credentials, acquiring legitimate access and compromising accounts. As said, *Skylogic* was in charge of managing a partition of the overall KA-SAT network (in Figure 2 a schematization of the partition from the "Defcon31" presentation made by *ViaSat* officials). In particular, as explained, the network was divided into different "Bandwidth Aggregation Points" (BAPs), grouping users from different regions, with *Skylogic* in charge of the management of "BAP1" and "BAP2" (see Figure 2). *ViaSat* has made clear that according to their analysis, the exploited vulnerability to access the network was in the part managed by *Skylogic*. Security researcher Ruben Santamarta, which has extensively covered the attack and its analysis, reveals that *Skylogic* at the time counted on the company *Fortinet* for VPN services[23]. *Fortinet*'s VPN, called "Fortigate", disclosed in 2021 that it suffered a cyberattack from the Russian group "Groove", which led to the leak of almost half a million credentials of VPN appliances[24]. *Fortinet*, however, developed and released a patch to the uncovered vulnerability, but it is possible that *Skylogic* had not deployed it yet at the time of the attack. This provides the first idea of the initial attack vector of the hackers. The breach of the VPN happened in the Core Node of Turin[25]. *Skylogic*, indeed, operates and has one of its teleports in Turin (the other one being in Cagliari). The specific timeline of the attack, as reconstructed by *ViaSat*'s Chief Information Security Officer (CISO) Mark Colaluca, has been the following (see also Fig 3 for a graphic representation). The attackers, on the 23rd of February, hence the day before the attack, in the evening accessed *Tor* network. From there, they tried with different sets of credentials to login to the VPN appliance of Turin's Core Node, without success.

[22] See Viasat Inc., 2022. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.
[23] See Santamarta, 2022. https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html.
[24] See Paganinni, 2021. https://securityaffairs.com/121985/cyber-crime/groove-gang-fortinet-leaks.html.
[25] See Valentino, 2022. https://aerospaceamerica.aiaa.org/features/why-the-viasat-hack-still-echoes/.

After approximately one hour, hackers finally gained remote access to the Core Node. In this way, they managed to escalate privileges and pass through the so-called “Demilitarized Zone”, or DMZ, of the network, aimed at working as a buffer zone between the external internet and the internal network of KA-SAT. They remained quiet, with the session active but doing nothing, for a couple of hours. At around 20:00 or 21:00 UTC, the attackers accessed a management server inside the Core Node, remarkably with a different set of credentials. In a matter of three or four hours, they accessed a network operations center which had the function of modem diagnostics. By accessing this network, it was possible to perform reconnaissance, connections discovery and information discovery. In particular, hackers had the possibility to check modem health, the number of modems connected and in general have access to all the modems online. At around midnight, after having accessed the management server and the network operations center, attackers moved again laterally to reach the “File Transfer Protocol” (FTP) server. FTP is a protocol which allows for transfer of files such as images, datasets, documents and other digital resources and it is also used to distribute software updates, patches, and so on[26]. Hence, the server was placed in a particular position of the network infrastructure, able to communicate with end-user modems. What the attacker did was to drop a ToolKit. This contained a set of scripts which had the function of enumerating and interrogating the network and to report back status after the execution of the code contained in the scripts. Other than these scripts, and crucially, the ToolKit also contained a wiper binary. This wiper binary was specifically aimed at the “MIPS” (Microprocessor without Interlocked Pipeline Stages) microprocessors of end-user’s modem devices and, in brief, were capable of overwrite and wiping the flash memory of SurfBeam2 hardware, rendering them unusable. At this point, it is important to note that not all modems were rendered unusable, but only those in Ukraine and in the nearby zone. This means that the hackers were able to select which of the geographic cells to target. The attackers proceeded, from the FTP server, to transfer the commands in the toolkit over the air, through the gateways to the satellite, reaching all of the modems belonging to the selected beam and finally rendering them inoperable.

[26] See “What is FTP”, Fortinet website. https://www.fortinet.com/resources/cyberglossary/file-transfer-protocol-ftp-meaning.

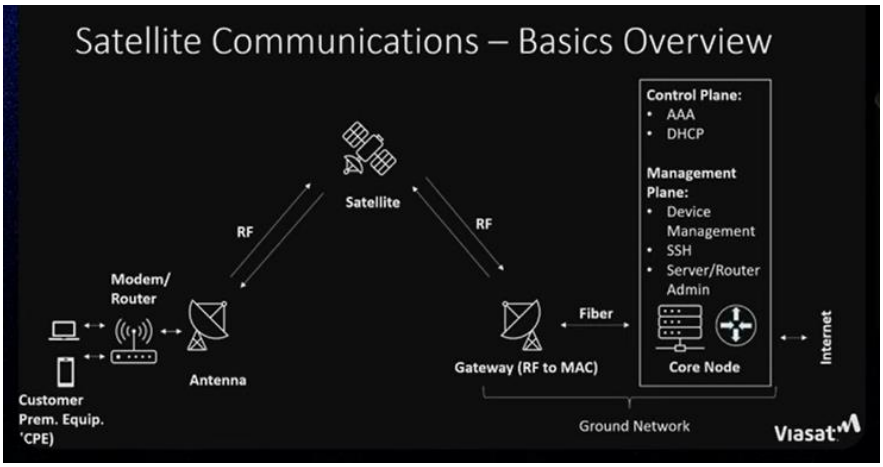

Figure 1 - An overview of how satellite communications work. Image from a presentation made by Mark Colaluca and Nick Saunders on the ViaSat cyber-attack.

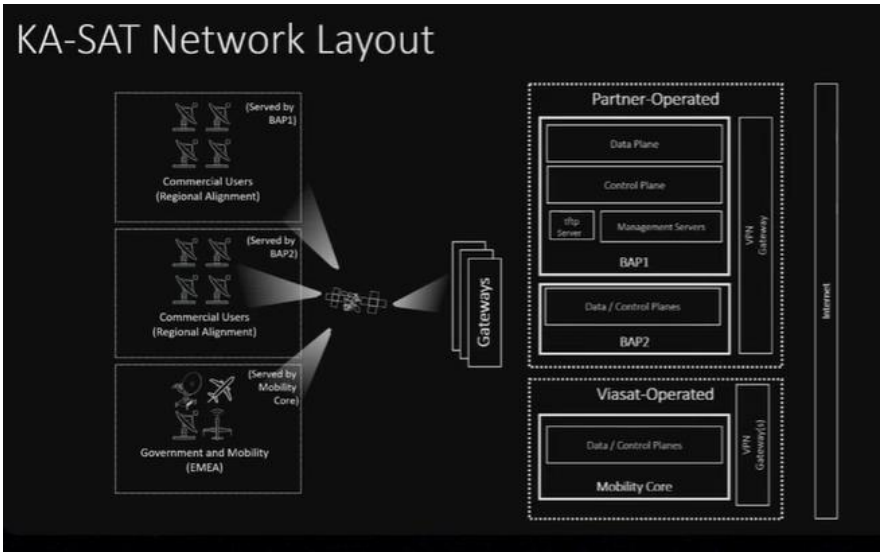

Figure 2 - Network layout of the KA-SAT. Image from a presentation made by Mark Colaluca and Nick Saunders on the ViaSat cyber-attack.

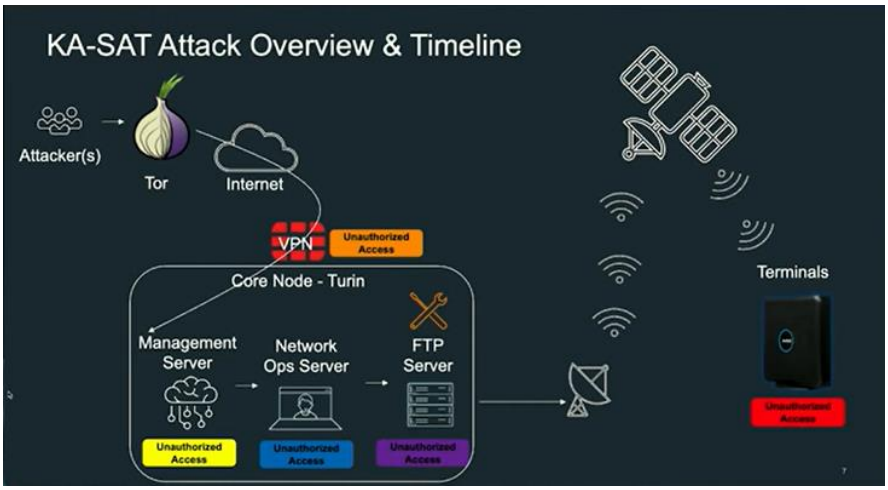

Figure 3 - A summary of the malware attack on ViaSat user terminals.

Before continuing with the analysis, it will be interesting to look in more detail at the wiper contained in the ToolKit.

3.3 The "AcidRain" malware

First of all, what is a wiper? According to the IT encyclopedia of *Kaspersky Lab*, a wiper is "a type of malware, the purpose of which is to wipe (erase data from) the hard drive of the computer it infects."[27] We have seen how the binary code contained in the aforementioned ToolKit managed to reach the "SurfBeam2" modem: in brief, through the internet, more precisely by exploiting a security breach in the management network of the KA-SAT satellite. How did this wiper precisely work? Technical details of this type first came out as the result of a report made by a *SentinelOne* analyst one month after the attack[28]. What is important to know, is that *ViaSat* itself, later on, confirmed that the wiper analyzed in this report was the one actually used in the cyberattack. The discovered malware was named "AcidRain". We have already seen that the specific targets of the wiper were the MIPS microprocessors of the end-user

modems. Indeed, *SentinelLab* defines it as an "ELF MIPS malware", meaning that it was specifically designed for those microprocessors and that it was formatted as an "Executable and Linkable Format" (ELF) file. This is a common standard format file used in *Linux* and *Unix*-based systems[29]. When this file works as root, that is with the highest level of permissions and with unrestricted access to all commands and files, it starts to look for directories not named in standard ways in order to recursively delete all of the files within them. A directory is basically a file on a computer that organizes files by containing references that redirect to them or to other directories. Figure 4, from the *SentinelLab* report, displays the code used to perform this actionIt basically is a loop that looks for directories which are called with names different than ".", ". .", "bin", "boot", "dev", "lib", "proc", "sbin", "sys" and "usr", and then proceeds at recursively deleting all of the files within them. After this, the wiper is

[27] See "Wiper.". Kaspersky IT encyclopedia. https://encyclopedia.kaspersky.com/glossary/wiper/#:~:text=A%20type%20of%20malware%2C%20the,of%20the%20computer%20it%20infects.

[28] See Guerrero-Saade, "AcidRain | A Modem Wiper Rains Down on Europe", SentinelOne website, March 2022. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/.

[29] "What Is an ELF File?". Baeldung, Linux website. https://www.baeldung.com/linux/executable-and-linkable-format-file.

```
while( true ) {
                /* read the / directory */
  iVar2 = read_directory_maybe(iVar1);
                /* get the directory name string */
  directory = iVar2 + 0xb;
  if (iVar2 == 0) break;
                /* check for any standard directory names - skip them */
  iVar2 = strcmp(directory,".");
  if (iVar2 != 0) {
    iVar2 = strcmp(directory,"..");
    if (iVar2 != 0) {
      iVar2 = strcmp(directory,"bin");
      if (iVar2 != 0) {
        iVar2 = strcmp(directory,"boot");
        if (iVar2 != 0) {
          iVar2 = strcmp(directory,"dev");
          if (iVar2 != 0) {
            iVar2 = strncmp_maybe(directory,"lib",3);
            if (iVar2 != 0) {
              iVar2 = strcmp(directory,"proc");
              if (iVar2 != 0) {
                iVar2 = strcmp(directory,"sbin");
                if (iVar2 != 0) {
                  iVar2 = strcmp(directory,"sys");
                  if (iVar2 != 0) {
                    iVar2 = strcmp(directory,"usr");
                    if (iVar2 != 0) {
                      strncpy_maybe(copied_directory + 1,directory,0xfd);
                /* recursively delete the non-standard folder */
                      recursive_delete_files_in_dir(copied_directory);
                    }
```

Figure 4 - The portion of code within "AcidRain" that looks for non-standard directories and recursively deletes files within them. Source: SentinelLab report (Guerrero-Saade, 2022)

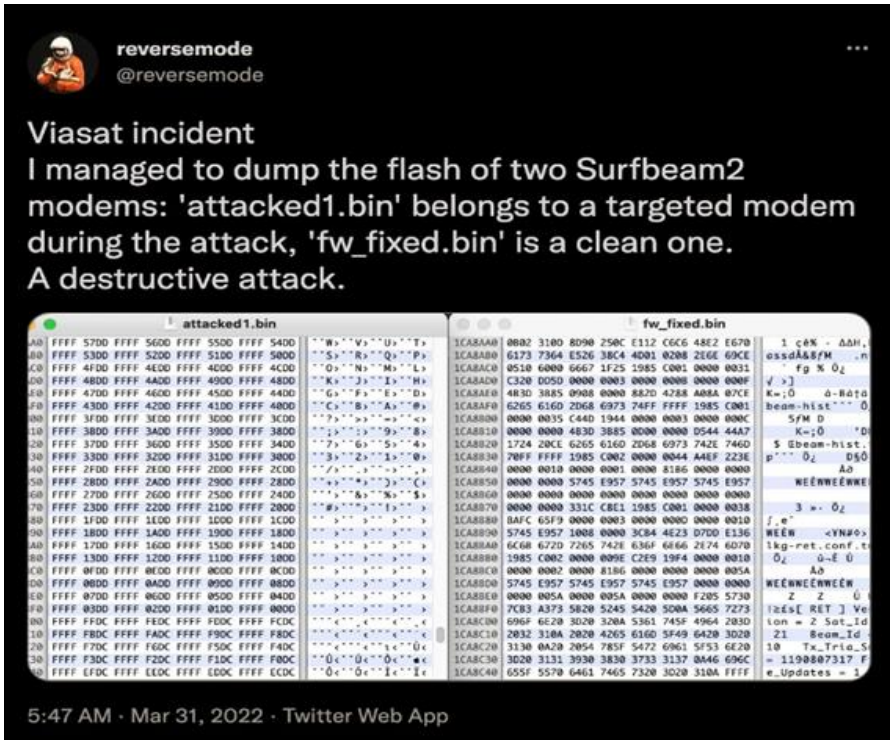

Figure 5 -A tweet on X that displays a comparison between data in the flash memory of an attacked modem (left) and a normal one (right). Source: image retrieved from Guerrero-Saade, 2022.

programmed to erase data in specific storage device files, such as the flash memory and the "Secure Digital" (SD) card or "MultiMediaCard" (MMC). The flash memory is usually in "Memory Technology Devices" (MTD) and are called "mtdblock", and the wiper is set to check for file identifiers from "mtdblock0" to "mtdblock99". To erase data in these devices, two methods are used by the wiper. In the first one, "Input Output Controls" (IOCTLs) calls are used to modify these files: "MEMGETINFO" to retrieve information about these devices, "MEMUNLOCK" to make the memory editable, "MEMERASE" to effectively delete the data contained in the device and "MEMWRITEOOB" to overwrite data on the out-of-band area (a small amount of extra storage used to store metadata) of the memory device. The other method used, instead, consists of simply overwriting the data by substituting them with a decrementing set of 4-byte integers starting at "0xffffffff". This detail is important, since it matches evidence collected on data found in the flash memory of attacked "SurfBeam2" modems (see Figure 5). After the data is wiped with either of the two methods, the modems are rebooted and rendered inoperable[30].

Having analyzed how the attackers managed to enter the network, reached modems operating in Ukraine and having sketched the basic working of the

"AcidRain" wiper, we can go on in the description of another channel of attack, namely a "Distributed Denial of Service" (DDoS).

3.4 The DDoS attack(s)

ViaSat reported that, during the very first phases of incident response regarding the wiper attack that was putting tens of thousand of modems out of order, they suffered a second cyber-offensive also aimed at end-user terminals, but not involving the spread of any malware. This was more precisely defined as a DDoS. *Kaspersky* defines it as a "type of attack [that] takes advantage of the specific capacity limits that apply to any network resources – such as the infrastructure that enables a company's website. The DDoS attack will send multiple requests to the attacked web resource – with the aim of exceeding the website's capacity

to handle multiple requests... and prevent the website from functioning correctly."[31]In this case, the attack was aimed at impairing the functioning of the "Dynamic Host Configuration Protocol" (DHCP) server. These servers have the

[30] See Guerrero-Saade, 2022.
[31] See "What is a DDoS attack?", Kaspersky. https://www.kaspersky.com/resource-center/threats/ddos-attacks.

function to assign, through the DHCP protocol, an IP address to external devices, or "hosts", wanting to connect to the network. Host devices need to have a unique IP address identifying them, hence, in general, IP addresses of devices are configurable, meaning that they are not permanently configured by manufacturers; indeed, if this would be the case, devices could only connect to one network, which structure should be known to the manufacturer when building the device. The DHCP server has the function of temporarily assigning, or leasing, IP addresses to host devices wanting to connect to the network. When a host device wants to connect to the network, it basically send a request to the server. This leases an IP address to the devices so that it can connect to the network[32]. As it can be appreciated from Figure 6, the actual working of the KA-SAT control plane is more sophisticated. In this case, indeed, requests from the terminal are first filtered by the Gateway, which decides whether requests go to the data plane or to the control plane. In the control plane, requests are managed by a virtualized "Access Service Network" (vASN), which acts as a DHCP relay agent. This basically means that it forwards messages between the client devices (in this case the terminals) and the appropriate DHCP server. After the requests reches the DHCP server, this returns an answer. Attackers used three different strategies to trick this process and flood the system with DHCP requests. All of these strategies made use of users' MAC addresses legitimately provided with active subscriptions. In the first one, depicted in Figure 7, an authenticated terminal issues a DHCPREQUEST, which gets forwarded to the Control Plane's vASN. From here is sent to the DHCP Server which finds it invalid and returns a "Negative Acknowledgement" (NAK) back to the vASN. This responds by issuing a command to disconnect the terminal, and the terminal gets out of the network. The other two strategies, summarized in Figure 8 and Figure 9 functions essentially in the same way, but use the requests "DHCPDECLINE" and "DHCPRELEAS"E to trick the vASN into disconnecting the routers from the network. These attacks flooded the system due to the number of terminals issuing these requests and therefore due to the huge volume of data reaching the server.

[32] See Peterson, Larry L., and Bruce S. Davie. Computer networks: a systems approach. Morgan Kaufmann, 2021, especially Chapter 3 and subchapter 3.3.7.

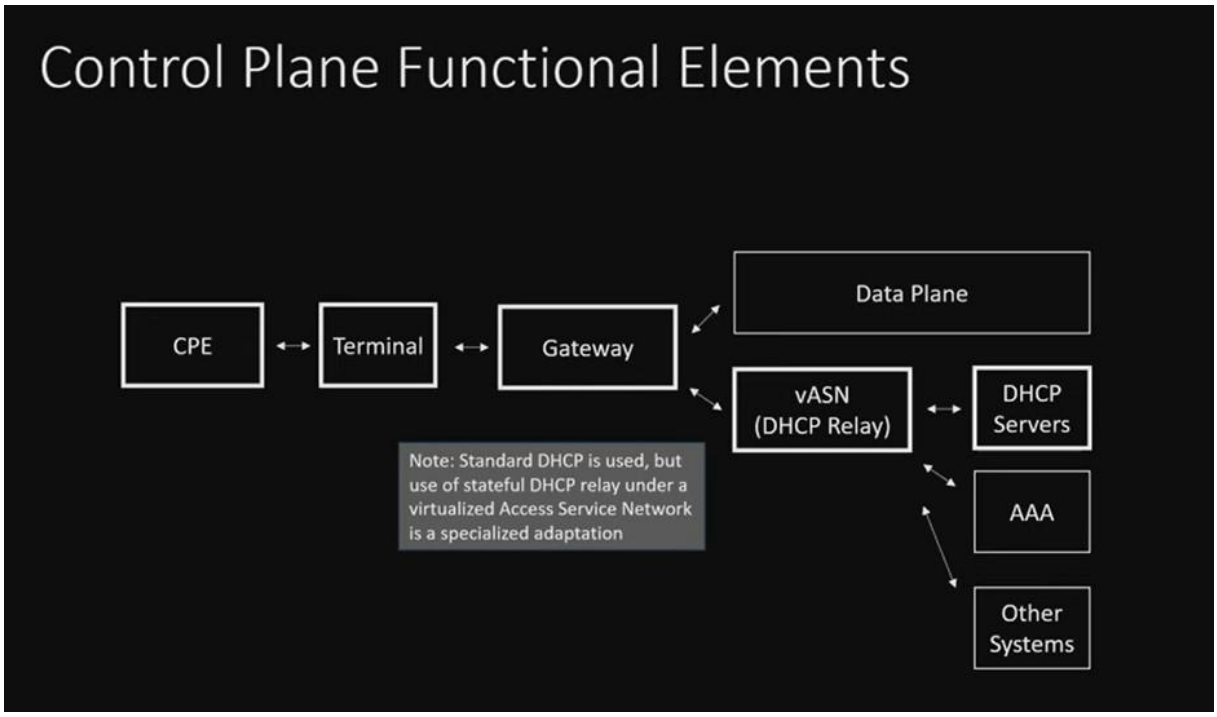

Figure 6 - A depiction of how the KA-SAT control plan is structured. Source: ViaSat officers Marc Colaluca and Nick Saunders' presentation at Defcon31.

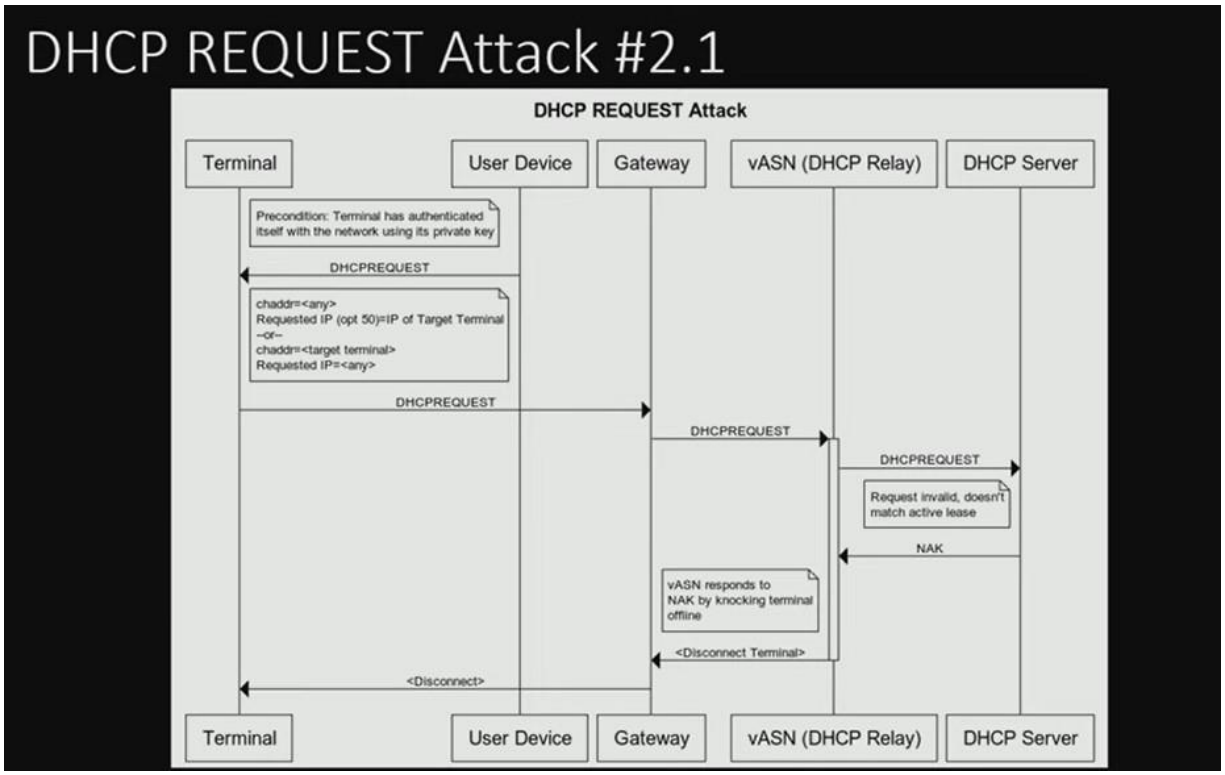

Figure 7 - A scheme of the first type of DDoS attack that affected KA-SAT's DHCP Server. Source: ViaSat officers Marc Colaluca and Nick Saunders' presentation at Defcon31.

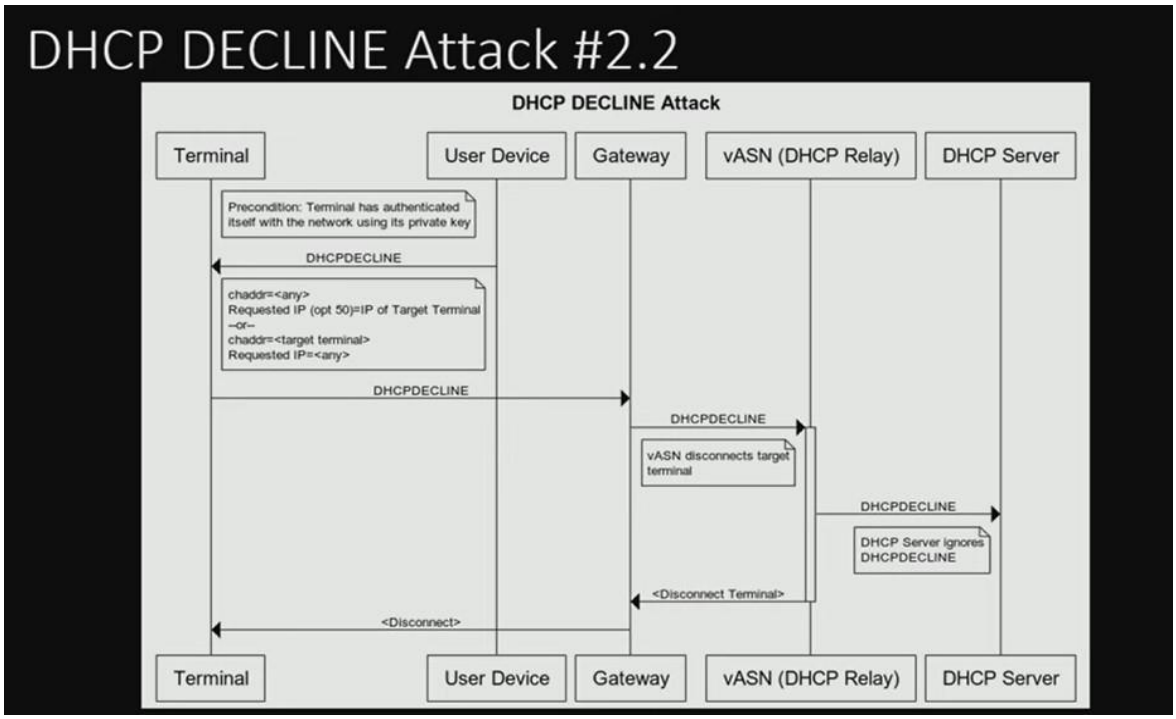

Figure 8 - A scheme of the second type of DDoS attack that affected KA-SAT's DHCP Server. Source: ViaSat officers Marc Colaluca and Nick Saunders' presentation at Defcon31.

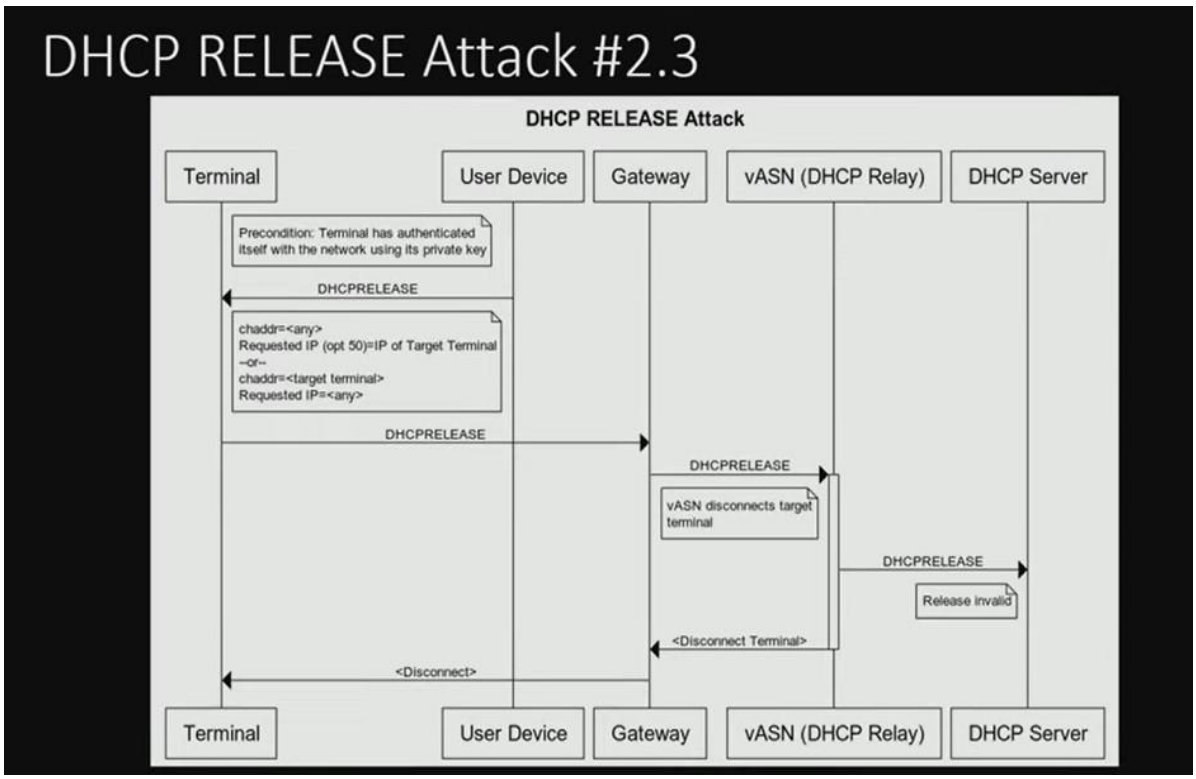

Figure 9 - A scheme of the third type of DDoS attack that affected KA-SAT's DHCP Server. Source: ViaSat officers Marc Colaluca and Nick Saunders' presentation at Defcon31.

Mark Colaluca, CISO of ViaSat, spoke of over 100.000 requests in a 5 minutes time span. These type of attacks were also making that a lot of modems were kicked off the network and that legitimate subscribers trying to get back in or issuing legitimate requests to the server couldn't reach it, precisely because of the flooding of requests.

In sum, the cyberattack against the KA-SAT network involved two distinct offensives: one made use of a wiper malware, subsequently named "AcidRain", to wipe out the flash memory of modems making them unusable; the other one was essentially a sophisticated DDoS attack which exploited privileged access to the network to flood with requests the DHCP server and to making it push modems out of the network. The consequences of the attack are discussed in the following section.

4. Impact of the attack

The combined effect of the two attacks meant that modems in the order of tens of thousands were disconnected from the network and rendered unable to reconnect without direct intervention from a technician or a software update. The "European Union Agency for Cybersecurity", ENISA, spoke of at least 27 thousand modems hit from the cyberattack[33]. However, the actual number was probably much higher, given that ViaSat itself, while avoiding providing the exact number of hit devices, has declared that more than 30 thousand new devices were sent to customers in an effort to restore connectivity[34]. As already mentioned, apart from providing commercial services to private users, ViaSat is also a contractor of the US government and army, NATO, the UK marine and the Ukrainian army. The attack was clearly aimed at disrupting the Ukrainian defenses in the face of the Russian invasion and subsequent "Battle of Kiev". With regards to the battlefield impact of the cyberattack Victor Zhora, a Ukrainian senior cybersecurity official spoke of a "huge loss of communications in the very beginning of war"[35].

[33] See Zorloni, 2022. https://www.wired.it/article/ucraina-europa-spillover-attacchi-informatici-enisa/.
[34] See Bing and Satter, 20222. https://www.reuters.com/business/media-telecom/exclusive-hackers-who-crippled-viasat-modems-ukraine-are-still-active-company-2022-03-30/.
[35] See Satter, Raphael (2022). https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/.

Furthermore, the KA-SAT network was still heavily impacted from the attack at least after 18 days from the incident[36]. To make up for the huge defense loss for the Ukrainian forces, already 48 hours after the Russian invasion had started, Minister of Digital Information of Ukraine, Mykhailo Fedorov, requested to Elon Musk the provision of the Starlink service in order to restore connectivity from space[37]. This marked a sensible turning point in the war, since *Starlink* satellites proved to be a reliable and resilient satellite service provider. Already as of April 2022, the director of electronic warfare at the Office of the Secretary of Defense Dave Tremper had the possibility to witness the speed with which Elon Musk' founded enterprise was able to respond to signal-jamming attacks in a matter of hours and declared himself impressed[38].

The attack also had spillovers effects on other European countries. Most notably, the outage of KA-SAT network affected the functioning of a wind farm, in Germany, owned by *Enercon*. Specifically, the remote monitoring and control of approximately 5.800 wind turbines, which summed up to a total capacity production of 11 Gigawatt, were put out of service[39]. This event is a paradigmatic instance of the ways in which cyber interconnectedness, especially among both civilian and military use technology, can lead to unforeseeable consequences and damages. However, it is also important to highlight that the wind turbines themselves were not impaired and they were still able to function on automatic mode or with in-place monitoring and control: this shows how building up alternatives to internet-relaying functions to be used in case of emergencies can enhance the resilience of those systems that are exposed to attacks in the cyber domain; and this is especially true whenever, as in this case, the exploited vulnerabilities used for the attack where located outside of the scope of action of the firm, *Enercon*.

[36] Ibid. note 24.
[37] See "How Elon Musk", 2023. https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare
[38] See Kan, 2022. https://www.pcmag.com/news/pentagon-impressed-by-starlinks-fast-signal-jamming-workaround-in-ukraine.
[39] See Sheahan, 2022. https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/.

5. Lessons learned

Many aspects of the cyberattack deserve attention in light of current developments in cybersecurity of strategic infrastructures, in particular space infrastructures, and cyberwarfare. Given the size, the sophistication and the impact the attack had, one can analyze dozens of lessons that can be learned, for ViaSat itself and many other private actors in the space sector, for firms not in the space sector but relying on services provide by space telecommunications providers, and for sovereign states and governments in general. These lessons concern, for example, good practices for maintaining a satisfactory level of network hygiene, practices of information sharing and how to empower incident response teams. However, for reasons of space, it seems all the most relevant to emphasize here three lessons in particular which are both specific to this case and of uttermost importance for cybersecurity in general. Hence, the three lessons analyzed here concern (i) dual-use technologies, (ii) organizational complexity and "responsibility gaps" and finally (iii) cascading effects.

First of all, the attacked infrastructure was dual-use technology, and it was serving both civilian and military purposes but was owned by a private firm. This raises the issue of privately owned enterprises being considered as a military target in times of war. Whether right or wrong, this should be acknowledged as a reality already, and it translates into the fact that a scale-up in cybersecurity measures for these infrastructures is needed. In fact, being the target of a sovereign State, in this case a great power, means that the level of the threat to which one is exposed becomes much higher. Hacker groups sponsored by sovereign governments can of course count on way more resources than private criminal groups, for example, and they can enjoy protection against retaliations from other sovereign States. There is certainly an overlapping between cybersecurity practices that can be considered sound and effective against economically motivated cybercriminal groups and those instead deemed appropriate for defending strategic and military infrastructures against the threat of State-sponsored cybergroups, but the two cannot be confused. As an example, a systematic method to make preventive intelligence on potential threats, in the cyber realm, is Threat Modelling: this semi-formal technique requires, as a preliminary step, to focus i) on what it is to be protected and ii) against whom it is to be protected. We can already see from here the radical

differences existing among the two situations sketched above: to defend a valuable civilian asset from generic malicious actors on the internet and to defend a critical or strategic infrastructure from state-sponsored groups with political objectives. The problem with dual-use technologies is that this distinction is not always neat and clear. What it is to be learned from this case is that, since the scale of the threat these infrastructures face is of a different level than the type of menace put by the cyber realm to "normal" firms, they require a level of security in network architectures and good practices followed by workers and users which is closer to a military infrastructure than to a civilian one.

This brings us to the second lesson learned, that of the interrelated problems of organizational complexity and "responsibility gaps"[40]. The two phenomena are distinct but connected by the fact that they are both a consequence of the entry of private actors in the space sectors. The latter refers to the fact that governments or public actors in general have interests in providing a level of security appropriate to these strategic infrastructures, but they lack ownership rights, while private actors, which are in charge of them, have no incentives to provide more security than the amount which is efficient to provide according to a logic of profitability. In a nutshell, *ViaSat* had no economic incentives to incur in the costs necessary to implement cybersecurity policy which could render the KA-SAT infrastructure "war-proof", and this had consequences for the overall security level of the Ukrainian State and, virtually, for US interests and policies in the region. Organizational complexity refers to the fact that, since the services afforded, in this case those of satellite communications, are managed by privately owned firms, both assets and services are subject to market dynamics which include sales, acquisition, split in ownership and so on. This brings about institutional fragmentation[41], and in the *ViaSat* case we have seen how the split in the management of the Satellite's network increased the perimeter of the attack for the hackers and provided for the main vulnerabilities exploited by them. During the incident response phase, this has also brought about delays, coordination issues and all of the difficulties related to geographic dispersion,

[40] The term comes from Palm, Jenny. "Emergency management in the Swedish electricity market". Energy Policy 36.2 (2008): 843-849.
[41] See Eriksson, Johan, and Giampiero Giacomello. "Cyberspace in space." Cyber Security Politics. Routledge, 2022. 95-108.

since the incident happened in eastern Europe and the management was headquartered in the US.

A third lesson that can be learned from this case regards so-called cascading effects. As the case of the *Enercon* wind turbines suggests, a number of different infrastructures relied on the services provided by the KA-SAT satellite, such as the SCADA systems of *Enercon* wind farms. This interconnection among several infrastructures can become a transmission belt for a single failure in one of them to transmit to all others. The affected wind turbines continued to function in auto-mode, but it is clear that in case of a power outage the effects on an attack on *ViaSat* could have propagated also to all of those infrastructures depending on the energy produced by *Enercon* to function. The interconnectedness of different infrastructures means that a single vulnerability can result, indeed, in a cascade effect. Again, from the perspective of this third lesson, it is clear how a significant mismatch exists between the incentives each single actor faces in the level of security to be provided and the level necessary to guarantee a satisfactory level of protection against cascading effects from a "systemic" or societal perspective. Each private firm can learn from this case that it has to protect itself against possible disruptions in the working of third-party service providers, but none of them has the capability to provide system-wide security. This is what neo-Keynesian economics would consider as a market failure. But, analyzing the roots of the current situation, it can also be considered as the failure of State-led privatization policies and the inadequacy of the consequent model of public-private partnerships to address the issue[42]. Hence, apart from the lessons for private actors, a lesson for policymakers can also be extracted from this case, which, again, is of paramount importance since its consequences put in danger the security of a sovereign State and, according to many perspectives, of European States in general and of US interests in the region. This lesson regards the urgency of addressing system-wide security issues for critical or strategic infrastructure as a public-sector problem, for which governments have to invest more and more.

[42] See Giacomello, Giampiero. "A perfect storm: privatization, public–private partnership and the security of critical infrastructure." Technology and International Relations. Edward Elgar Publishing, 2021. 173-192.

6. Conclusions

The present article had the purpose of presenting a specific case study on the cyberattack suffered by *ViaSat* in February 2022. The introductory chapter served as an explanation for the relevance of such an effort. The second section illustrated the context in which the attack happened: both with respect to the ongoing Russo-Ukrainian conflict (and its cyberspace dimension) and to the corporate dynamics of *ViaSat* and the ownership status of the KA-SAT satellite. The core of the paper is to be found in section three, where a detailed and technical reconstruction of the attack is carried out. The significance of this analysis also resides in the fact that it has unified and homogenized the various open-access sources regarding the event. Four subsections deal with, respectively, a summary of the incident, the wiper attack, a focus on the functioning of the malware, "AcidRain", and finally a reconstruction of the DDoS attack. After this, a fourth section exposes the impact the attack had both in the Ukrainian military theater and outside, while the fifth section discusses the lessons learned from the event.

What are the conclusions to be taken from the present work? As an intensive study, it is outside its ambitions to derive from it general propositions which can be valid from the general field of cybersecurity. However, the literature analyzed in the course of analysis has been of help in identifying those issues which are specific of this circumstance, but also symptomatic of general current problems related to the security of cyberspace and in particular of space infrastructures: as an example, (i) the necessity to look more in depth into the vulnerabilities brought by the entry of the private sector in space infrastructures, (ii) the relevance for sovereign States to intervene in fixing market failures and addressing security externalities and "responsibility gaps" in cyberspace, and (iii) the urgence to build up critical infrastructures which are reliable, resilient and redundant.

Bibliography

"2015 Ukraine Electric Power Attack". MITRE ATT&CK website. https://attack.mitre.org/campaigns/C0028/

"How Elon Musk's satellites have saved Ukraine and changed warfare". The Economist. January 15, 2023. https://www.economist.com/briefing/2023/01/05/how-elon-musks-satellites-have-saved-ukraine-and-changed-warfare.

"NotPetya". MITRE ATT&CK website. https://attack.mitre.org/software/S0368/

"ViaSat Shifts Focus From Commercial To Defense Work". San Diego Business Journal. November 24, 2002. https://www.sdbj.com/imported/viasat-shifts-focus-from-commercial-to-defense/

"Viasat, CDW Awarded NATO Contract for Agile Command, Control and Communication Project." Press release, Business Insider website. October 27, 2021. https://markets.businessinsider.com/news/stocks/viasat-cdw-awarded-nato-contract-for-agile-command-control-and-communication-project-1029725407

"What is a DDoS Attack? - DDoS Meaning". Kaspersky website. https://www.kaspersky.com/resource-center/threats/ddos-attacks

"What Is an ELF File?". Baeldung, Linux website. https://www.baeldung.com/linux/executable-and-linkable-format-file.

"What is FTP (File Transfer Protocol)?". Cyberglossary, Fortinet website. https://www.fortinet.com/resources/cyberglossary/file-transfer-protocol-ftp-meaning.

"Wiper". Glossary, Kasperky IT Encyclopedia. Kaspersky website. https://encyclopedia.kaspersky.com/glossary/wiper/#:~:text=A%20type%20of%20malware%2C%20the,of%20the%20computer%20it%20infects.

Barichella, Arnault. "Cyberattacks in Russia's hybrid war against Ukraine and its ramifications for Europe.", Jacques Delors Institute, Policy Paper 281, September (2022).

Bing, Cristopher and Satter, Raphael. "EXCLUSIVE hackers who crippled ViaSat modems in Ukraine are still active – company official". Reuters, March 20, 2022.

Blinken, Anthony J. “Attribution of Russia’s Malicious Cyber Activity Against Ukraine”. US Secretary of State Press Statement of May 10, 2022. https://www.state.gov/attribution-of-russiasmalicious-cyber-activity-against-ukraine/.

Boschetti, Nicolò, Nathaniel G. Gordon, and Gregory Falco. "Space cybersecurity lessons learned from the viasat cyberattack." ASCEND 2022. 2022. 4380.

Case, Defense Use. "Analysis of the cyber-attack on the Ukrainian power grid." Electricity Information Sharing and Analysis Center (E-ISAC) 388.1-29 (2016): 3

Chuter, Andrew. “Viasat to supply Britain’s future frigate with satellite communications tech”. DefenseNews. November 3, 2020. https://www.defensenews.com/industry/2020/11/03/viasat-to-supply-britains-future-frigate-with-satellite-communications-tech/

Colaluca, Marc and Saunders, Nick. “Defending KA-SAT”. Defcon31 Conference, July 2023. https://www.youtube.com/watch?v=qI_ICtX3Gm8.

Colaluca, Marc and Walter, Kristina. “Lessons Learned from the KA-SAT Cyberattack: Response, Mitigation and Information Sharing”. BlackHat forum, March, 2023. https://www.youtube.com/watch?v=RdjthhBylMk.

Council of the EU. “Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union”. Press release. May 10, 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

Dearden, Lizzie. “Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers”. Indipendent. June 27, 2017. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html

Eriksson, Johan, and Giampiero Giacomello. "Cyberspace in space: fragmentation, vulnerability, and uncertainty." Cyber Security Politics. Routledge, 2022. 95-108.

Giacomello, Giampiero. "A perfect storm: privatization, public–private partnership and the security of critical infrastructure." Technology and International Relations. Edward Elgar Publishing, 2021. 173-192.

Gronholt-Pedersen, Jacob and Fouche, Gwladys. “Dark Arctic. NATO allies wake up to Russian supremacy in the region”. Reuters, November 16, 2022.

Guerrero-Saade, “AcidRain | A Modem Wiper Rains Down on Europe”, SentinelOne website, March (2022). https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

Jewett, Rachel. “Viasat Completes Purchase of Euro Broadband Infrastructure”. ViaSatellite. April 30, 2021. https://www.satellitetoday.com/connectivity/2021/04/30/viasat-completes-purchase-of-euro-broadband-infrastructure/

Kan, Michael. “Pentagon Impressed by Starlink's Fast Signal-Jamming Workaround in Ukraine”. PC Mag. April 21, 2022. https://www.pcmag.com/news/pentagon-impressed-by-starlinks-fast-signal-jamming-workaround-in-ukraine.

Kolovos, Alexandros. "Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict." Air & Space Management and Control Laboratory, OCCASIONAL PAPER 3 (2022).

Paganini, Pierluigi. “Groove gang leaks list of 500k credentials of compromised Fortinet appliances”. Security Affairs. September 8, 2021. https://securityaffairs.com/121985/cyber-crime/groove-gang-fortinet-leaks.html

Palm, Jenny. "Emergency management in the Swedish electricity market: The need to challenge the responsibility gap." Energy Policy 36.2 (2008): 843-849.

Peterson, Larry L., and Bruce S. Davie. Computer networks: a systems approach. Morgan Kaufmann, 2021.

Santamarta, Ruben. “VIASAT incident: from speculation to technical details.” REVERSEMODE. March 31, 2022. https://www.reversemode.com/2022/03/viasat-incident-from-speculation-to.html.

Satter, Raphael. “Satellite outage caused ‘huge loss in communications’ at war’s outset – Ukrainian official”. Reuters, March 15, 2022. https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/

Schia, Niels Nagelhus, Rødningen, Ida and Gjesvik, Lars. “The subsea cable cut at Svalbard January 2022: What happened, what were the consequences, and how were they managed?”. NUPI Policy Brief, Norwegian Institute of International Affairs, January, 2023.

Sheahan, Maria. “Satellite outage knocks out control of Enercon wind turbines”. Reuters, February 28, 2022. https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/.

Slowik, Joe. "Anatomy of an attack: Detecting and defeating crashoverride." VB2018, October (2018).

Valentino, Andrea. “Why the ViaSat attack still echoes”. Aerospace America, November (2022). https://aerospaceamerica.aiaa.org/features/why-the-viasat-hack-still-echoes/

ViaSat Inc. “Viasat's AN/PRC-161 BATS-D Handheld Link 16 Radio Receives NSA Authorization for Use by International Military Forces”. PR Newswire. August 22, 2018. https://www.prnewswire.com/news-releases/viasats-anprc-161-bats-d-handheld-link-16-radio-receives-nsa-authorization-for-use-by-international-military-forces-300700755.html

ViaSat Inc., “KA-SAT Network cyber attack overview”. ViaSat official website. March 30, 2022. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview

ViaSat Inc., “Viasat Completes Acquisition of Remaining Stake in its European Broadband Joint Venture, Inclusive of the KA-SAT Satellite and Ground Assets”. ViaSat official website. April 30, 2021. https://investors.viasat.com/news-releases/news-release-details/viasat-completes-acquisition-remaining-stake-its-european

Voreacos, David, Chiglinsky, Katherine and Griffin, Riley. “Merck Cyberattack’s $1.3 Billion Question: Was It an Act of War?”. Markets, Bloomberg. December 3, 2019. https://www.bloomberg.com/news/features/2019-12-03/merck-

cyberattack-s-1-3-billion-question-was-it-an-act-of-war?embedded-checkout=true

Zorloni, Luca. “L'Europa prova a bloccare lo “spillover” di attacchi informatici dalla guerra in Ucraina”. WIRED Italia. March 18, 2022. https://www.wired.it/article/ucraina-europa-spillover-attacchi-informatici-enisa/