2024 DUBLIN

2 - 4 October, 2024 / Dublin, Ireland

REVIEWING THE 2022 KA-SAT INCIDENT & IMPLICATIONS FOR DISTRIBUTED COMMUNICATION ENVIRONMENTS

Joe Slowik

The MITRE Corporation, USA

JSLOWIK@mitre.org

www.virusbulletin.com

INTRODUCTION

Critical infrastructure assets, from electric utility operations to military communication networks, are increasingly moving towards distributed models incorporating (or dependent upon) space-based segments. While expanding communication coverage quickly and efficiently, such migration also expands the overall attack surface of these systems and provides opportunities for adversaries to disrupt them. Such developments are in parallel with overall migration towards distributed, wireless communication methodologies for efficiency and efficacy across critical infrastructure segments. Although the economic benefits of such migration are clear, they also come with risks in terms of security and availability that are often overlooked.

In this discussion, we will examine one notable incident impacting space-based distributed communication systems: the 2022 disruptive attack against the *ViaSat*-owned, *Eutelsat* and *Skylogic*-operated KA-SAT network at the start of Russia's full invasion of Ukraine. In addition to reviewing the event we will explore how our understanding of this incident has evolved through additional analysis and disclosures in the time since its initial discovery. Finally, we will conclude with a discussion of the broader implications of disruptive attacks on distributed communication environments, what this means for critical infrastructure entities, and what defensive options exist.

SATELLITE COMMUNICATION BACKGROUND

While currently expanding in scope and coverage, satellite communication in critical infrastructure environments is hardly 'new'. Technologies such as very small aperture terminals (VSATs) have provided communications for mines, offshore oil operations, and many other remote systems for years. Of interest at present is the extension of these models to become backup, or even primary, communication mechanisms for assets such as distributed energy resources (DERs) and renewable energy (principally wind and solar generation).

While DERs and renewable generation feature a variety of possible communication pathways, from existing cellular and wireless networks to systems such as power line communication (PLC), the flexibility and geographic reach of satellite-based communications offer a variety of benefits as bandwidth has improved [1]. For example, low earth orbit (LEO) constellations of relatively inexpensive communication satellites, such as the *Starlink* system, can provide significant coverage for distributed assets without costly physical infrastructure investment to ensure connectivity [2]. By incorporating a mix of legacy and emerging technologies, necessary control and connectivity to DER or renewable generation assets can be achieved without extensive investment in physical, wired connections.

Importantly, DER assets and especially renewable generation require near real-time, bidirectional connectivity for a variety of reasons ranging from operational management to process protection and safety. Attack (and defence) scenarios against DER management systems and control operations have already been documented in academic literature [3], and extending the possible attack surface through real-time communication dependencies 'over the air' allows for more scenarios to emerge. More importantly, such increased interaction and connectivity extends from operator management and overall operations within the larger energy management system to equipment vendors who typically offer preventative maintenance and monitoring services.

As control and monitoring extend outward from deployed assets into an increasingly distributed ecosystem, the same efficiency and convenience offered by satellite-enabled communications and control also extends the attack surface available to those seeking to disrupt such activity. The classic structure of a satellite communication system includes three primary components: the space segment of overhead systems (satellites, consisting of bus and payload); ground stations connected to the overhead network; and the up and downlink connections between ground stations and the overhead asset [4]. Each element of the overall system provides an opportunity to an adversary, via physical, electronic, or cyber mechanisms, to disrupt the functionality or efficacy of the system. Importantly, each end terminal, including those at the end-user or consumer stage, becomes a potential inject point into the system for malicious activity.

As shown in Figure 1, satellite-facilitated communication extends the overall attack surface available to adversaries by increasing the number of possible inject or touch points to the overall environment. As defined in frameworks such as the *Aerospace Corporation*'s Space Attack Research and Tactic Analysis (SPARTA) matrix, opportunities to influence or impact the environment (including, for example, end-user assets such as a remote renewable generating asset) extend from various types of ground terminal intrusions to a variety of exotic attack mechanisms, such as kinetic or electronic warfare anti-satellite technologies, against overhead assets [5].

While SPARTA highlights several attack vectors, including physical and electronic warfare mechanisms, this investigation is focused on information system attack scenarios. Particularly, this paper is concerned with those cyber-nexus capabilities that can influence, disrupt, or significantly degrade satellite-based communication networks with impacts on critical infrastructure. The number of (public) examples of such activity is quite small, but one recent event stands out from the beginning of Russia's full invasion of Ukraine in February 2022.

THE 2022 KA-SAT INCIDENT

Concurrent with Russia's full-scale invasion of Ukraine on 24 February 2022, *ViaSat*'s KA-SAT satellite broadband service, operated by *Eutelsat* subsidiary *Skylogic*, experienced several service interruptions. These impacts were largely felt

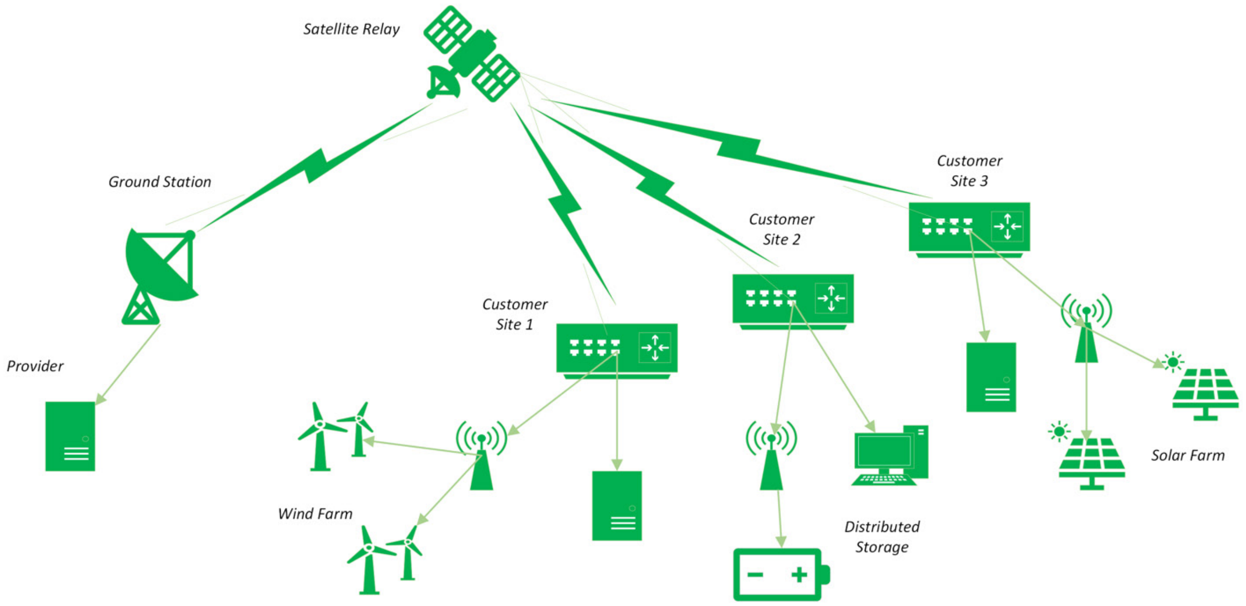

Figure 1: Satellite communication architecture.

in Ukraine, with additional disruptions among European customers [6]. Initially suspected to be the result of a distributed denial of service (DDoS) event [7], which would align with other disruptive cyber activity concurrently targeting Ukrainian networks, reports subsequently indicated that the KA-SAT disruption resulted in significant communication impacts for Ukrainian military elements at this critical moment in time [8] [9].

As is often the case with major cyber (or apparently cyber) events, technical information as to how the KA-SAT network was disrupted was initially scarce, leading to significant speculation. However, in late March both *ViaSat* and information security vendor *SentinelOne* published reports linked to the incident. Both reports agreed that novel malware, named 'AcidRain' by *SentinelOne*, was responsible for disrupting some KA-SAT customer modems [10] [11] [12]. However, an overview of events indicates that the execution of AcidRain was not the only disruptive event against the KA-SAT network on 24 February 2022. A post-incident review from *ViaSat* identifies DDoS activity emanating from *SurfBeam 2* and *SurfBeam 2+* modems within the KA-SAT network starting at approximately 03:02 UTC that day [11]. DDoS activity against the network continued until 04:15 UTC, at which time what had previously been a gradual decline of modems connected to the network shifted to a significant loss of consumer terminals over the next 45 minutes.

Further details emerged several months later, when *ViaSat* personnel presented more detailed incident findings at the Black Hat USA and Def Con 31 events. First, the presentations detailed precisely how events began: through a logon (potentially from captured, valid credentials) to the VPN concentrator for a Turin, IT based control centre for the impacted KA-SAT infrastructure [13] [14]. This activity progressed to accessing several critical systems managing the KA-SAT environment, including servers gathering modem telemetry (e.g. how many devices are active and device-specific information) and an FTP server that allowed for file transfer to networked modems. This activity took place around midnight on 24 February, in advance of the heightened DDoS activity, and led to subsequent deployment of the AcidRain payload over the next three to four hours [13].

Concurrently with the above, DDoS activity impacted the KA-SAT network. Starting around 03:00 UTC on 24 February, terminals legitimately authenticated to the KA-SAT network via AAA engaged in waves of DHCP-based DDoS attacks [14]. Some of these were simple volumetric attacks seeking to overload the network, but others leveraged specially crafted DHCP packets for more complex attack scenarios. For example, a user device connected to an authenticated terminal would send a malicious DHCP request that would propagate to the DHCP relay, which then communicated with the DHCP server. The DHCP server would REJECT the request as invalid, and in the process generate a DHCP negative acknowledgement (NAK) message that would result in the relaying terminal being removed from the KA-SAT network, along with any customer systems connected to that terminal [14] [15].

While particular elements of the above will be analysed in greater detail, placing these events in the wider context of Russia's invasion of Ukraine shows that the disruptive KA-SAT activity closely follows the initial physical assault. As shown in Figure 2, active KA-SAT disruption began approximately 10 minutes after Russian President Vladimir V. Putin announced a 'special military operation' at 02:50 UTC [16]. Furthermore, the KA-SAT disruption also took place within the wider context of more traditional DDoS activity against Ukrainian government and critical infrastructure entities [17].

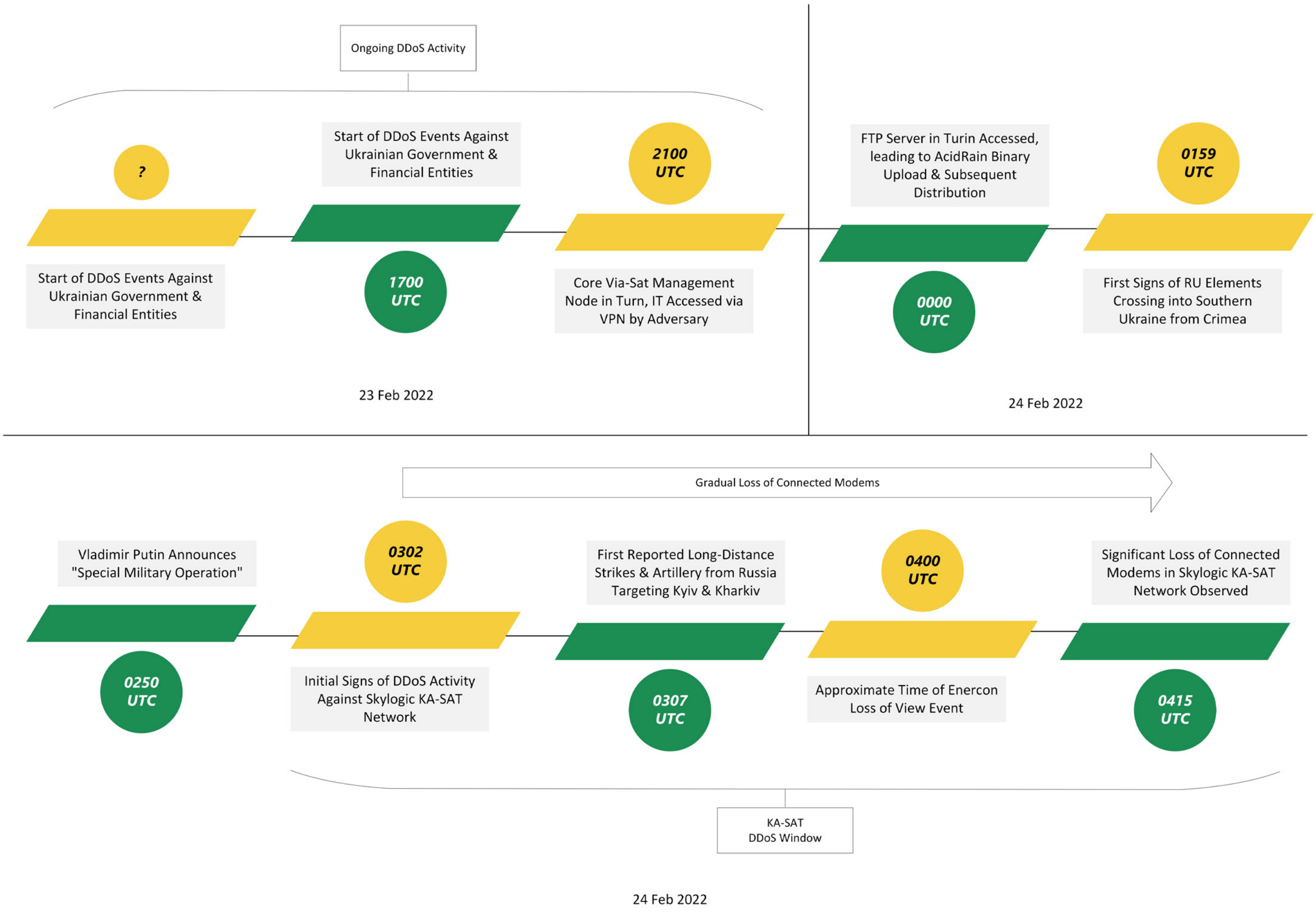
Ongoing DDoS Activity
?
Start of DDoS Events Against Ukrainian Government & Financial Entities
Start of DDoS Events Against Ukrainian Government & Financial Entities
1700 UTC
2100 UTC
Core Via-Sat Management Node in Turn, IT Accessed via VPN by Adversary
23 Feb 2022
FTP Server in Turin Accessed, leading to AcidRain Binary Upload & Subsequent Distribution
0000 UTC
0159 UTC
First Signs of RU Elements Crossing into Southern Ukraine from Crimea
24 Feb 2022
Gradual Loss of Connected Modems
Vladimir Putin Announces "Special Military Operation"
0250 UTC
0302 UTC
Initial Signs of DDoS Activity Against Skylogic KA-SAT Network
First Reported Long-Distance Strikes & Artillery from Russia Targeting Kyiv & Kharkiv
0307 UTC
0400 UTC
Approximate Time of Enercon Loss of View Event
Significant Loss of Connected Modems in Skylogic KA-SAT Network Observed
0415 UTC
KA-SAT DDoS Window
24 Feb 2022

Figure 2: Timeline of events around Russian invasion of Ukraine.

Oriented to satellite and satellite communication operations in general, the 24 February 2022 events reflect several distinct mechanisms for denying access to or degrading the performance of such systems [18]:

- Ground segment intrusion to distribute a malicious payload to client terminals.
- Trusted client abuse to enable user segment denial of service via DDoS.
- User segment disruption via AcidRain malware.
- Potential space system impacts due to abnormal traffic patterns from user segment terminals.

While the above was of potential critical importance to Ukrainian military command and control during the early stages of the invasion [9], the KA-SAT disruption impacted entities beyond Ukraine. While reporting indicates disruptions throughout Europe, the most notable impacts involved wind turbines from the German manufacturer *Enercon GmbH* in undisclosed locations in Central Europe [19]. According to reporting, over 5,000 *Enercon* turbines, representing approximately 11 gigawatts of generating capacity, experienced a loss of communications – effectively a denial and loss of view condition [20] [21] – due to the KA-SAT disruption [22].

Although *Enercon* representatives stressed that there was no operational loss, as the impacted turbines switched to automatic, independent operations, a loss of communication for an extended period of time represents a serious concern for a part of the interlinked electric system. Although almost certainly collateral effects in the overall KA-SAT incident, the denial and loss of view conditions imposed on the operator – which effectively also amounted to a loss of control for a period of time [23] – highlights an interesting and concerning element of satellite communication dependency and potential impact scenarios that will be reviewed in greater detail below.

ADVERSARIES & EVENTS

The KA-SAT disruption was initially and widely viewed as a malware-driven event, but subsequent disclosure from *ViaSat* revealed a far more complex operation. Interestingly, the KA-SAT disruption appeared to combine two distinct mechanisms targeting Ukrainian infrastructure (or in this specific case, third-party infrastructure also used by Ukrainian entities) for many years between the Revolution of Dignity in Ukraine (also referred to as the Maidan Revolution or Euromaidan) in 2013-2014 and the full-scale Russian invasion of Ukraine in 2022 [24]:

- The use of wiper malware against information technology (IT) assets for disruptive purposes, particularly against government and critical infrastructure entities [25] [17] [26] [27].
- Extensive use of DDoS activity against targets and public portals relating to government and critical infrastructure services [28] [29].

While wiper and DDoS incidents certainly overlapped in the events leading to and following the 24 February 2022 invasion, the very close overlay between the KA-SAT events is strange, and stands out relative to other incidents impacting Ukrainian entities. As a result, multiple questions emerge into the nature of the event, who is responsible for it, and whether these entities remain active either in Ukrainian-targeted operations specifically, or in more widely targeted events.

How many adversaries and how many attacks?

The KA-SAT disruption event consists of two, distinct events that overlap in time:

1. DDoS activity consisting of both volumetric and targeted activity against KA-SAT infrastructure [14].
2. Deployment of wiper malware via company management systems to modems [11].

The core question surrounding these events is: was the same adversary responsible for both intrusions?

Specific attribution questions will be addressed separately, but in terms of attack sequencing and focus there are notable differences in each phase of operations. While the malware-focused attack sequence started with a compromise of KA-SAT management networks, the DDoS-focused attack sequence began with compromised user equipment connected to KA-SAT terminals, and started in advance of the compromise of the Turin-based management network. Although it is possible that both elements were executed by the same entity, the significant differences in tradecraft, timing, targeting, and the nature of disruptive effect in an overlapping time window strongly suggest different actors acting simultaneously as opposed to one unified intrusion.

Referring to the timeline in Figure 2, while sporadic DDoS activity continues before, during and (for two weeks) after the commencement of Russia's invasion, the AcidRain wiper deployment is limited to one point in time. Moreover, AcidRain's deployment was enabled through compromise of corporate management networks, while the DDoS activity originated with customer or customer-adjacent equipment. Based on available information, a minimum of two 'teams' of operators (potentially reporting to the same command authority) were involved in this event, and did not appear to collaborate or deconflict with one another during the KA-SAT disruption.

Review of DDoS activity

Recorded DDoS activity during the KA-SAT attack is interesting for several reasons. For one, the activity appears to have preceded and extended beyond the immediate event based on public comments from *ViaSat* personnel [14] [13]. Additionally, several varieties of DDoS took place during the relevant time period, indicating a mix of attack methodologies but all originating from legitimate modems or user equipment. The most direct of these events were volumetric DHCP-based DDoS attacks, which while impactful, are both relatively easy to understand and for which mitigations are quite clear.

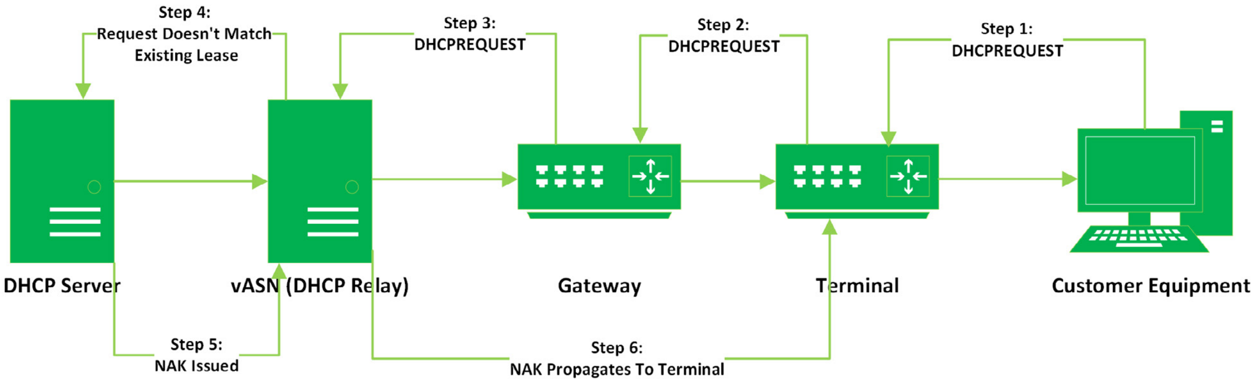

Figure 3: DHCP DDoS with NAK message.

More interesting were incidences of specially crafted DHCP-based traffic used to systematically knock systems off the KA-SAT network originating from end-user equipment connected to KA-SAT terminals. As noted previously, activity included a unique way of leveraging DHCP requests to deliver NAK messages to remove a specific, targeted terminal from the network, as shown in Figure 3. However, this is one of three variants of DHCP-based DDoS activity beyond the volumetric attacks observed during the KA-SAT event. Interestingly, target terminals were specified in the most interesting DHCP-based attacks, indicating a level of environment awareness and targeting for the DDoS activity as opposed to random endpoint selection. This could theoretically have been paired with the interactive intrusion into the Turin-based management network, but the timing of events (leaving only a few hours from initial access to survey of the landscape) suggests that these incidents (exfiltrating network information in preparation for AcidRain deployment and DDoS activity) are distinct.

Additional variants of the DHCP attack include one using DHCPDECLINE messages for a target terminal. This would result in the network disconnecting the referenced terminal as the message suggests the included address is already in use elsewhere within the network [15]. Another variant used DHCPRELEASE messages for essentially the same effect, where the DHCP server recognizes the address as not allocated and records the address as available for assignment [14] [15]. Notably, these variants emerged as responses to mitigations deployed by KA-SAT administrators and defenders, showing rapid adaptability on the part of the DDoS attacker – along with non-trivial knowledge of how to abuse the DHCP protocol that could be rapidly weaponized to continue disruptive acts.

Attribution & responsibility

The previous section highlights the strong possibility that more than one actor was involved in the KA-SAT incident. Multiple entities, including the US government, explicitly linked the KA-SAT event in its entirety to Russian government operations [30] [31]. Yet there are many Russian government-directed cyber teams, with at times different goals and certainly different methods of operation, while also exhibiting a lack of cooperation and coordination in many instances [32]. The differences in capability and impact focus documented previously may indicate that, while both intrusions originated with Russian strategic leadership, the events in question actually correspond to different entities within the Russian cyber and intelligence ecosystem.

The first and most obvious candidate for responsibility for the KA-SAT event is the Russian threat actor most associated with disruptive attacks in Ukraine: Sandworm, linked by multiple entities to Russia's Military Intelligence (GU, or more commonly GRU) Main Center for Special Technologies, field post 74455 [33]. Sandworm is directly linked to various flavours of wiper malware, from the 2017 NotPetya global incident to many wiper variants identified in Ukraine [25] [34], making its association with AcidRain reasonable, but lacking additional technical detail.

Binary analysis by *SentinelOne* revealed an interesting potential connection to Sandworm for the wiper attack. AcidRain features an odd overlap with functionality linked to another piece of malware, called VPNFilter, associated with Sandworm operations targeting network devices [35]. VPNFilter, and its replacement Cyclops Blink, were implants designed for small office-home office (SOHO) routers for incorporation into a Sandworm-controlled botnet [36]. These implants were modular in nature, with a particular VPNFilter module, 'dstr', used for wiping infected devices, having noticeable overlaps with AcidRain functionality [10]. Combined with other similarities, such as potentially sharing a compilation environment and similar use of input-output controls (IOCTLs) for wiping functionality, there appears to be a non-trivial link between VPNFilter's dstr module and AcidRain, but insufficient evidence at this level to definitively tie the two together.

Subsequent statements linked to the Ukrainian computer emergency response team (CERT-UA), in the context of a newer variant of AcidRain named 'AcidPour' (discussed further below), link the activity more firmly to a Sandworm-related entity, UAC-0165 [37]. This same Sandworm-linked entity was responsible for other wiper-based attacks on Ukrainian telecommunication infrastructure, making a link to the AcidRain and subsequent activity plausible [38]. Finally, the outline of the adversary attack path for AcidRain deployment highlights initial access using legitimate credentials to the Turin-based KA-SAT control centre VPN from a TOR network node [14]. While fragmentary and hardly unique, it is worth noting that historical Sandworm operations, such as the 2016 Industroyer event, have relied on abuse of the TOR network nodes (if not specifically the TOR protocol) to obfuscate last-hop traffic to victims [39].

While AcidRain links to Sandworm appear reasonable, no information has surfaced with respect to the concurrent DDoS activity. Furthermore, as noted in *ViaSat* discussions, this DDoS activity in various forms extended before and for some weeks after the 24 February 2022 events [14]. Ukrainian entities, including telecommunication providers, have experienced waves of DDoS activity prior to and since the beginning of the full-scale invasion in February 2022, but none of these events appear to have leveraged the same crafted and targeted DHCP-based activity as observed in the KA-SAT event.

While Sandworm is capable of DDoS activity, it is not the only Russian threat actor associated with such actions. More interestingly, the DHCP-based DDoS activity started with compromised customer equipment [14]. Depending on specific installation and use, terminal-connected equipment could be a single endpoint, or a consumer network appliance. If the latter, operations could relate this to SOHO network device compromises which are strongly linked to Sandworm operations such as VPNFilter and Cyclops Blink. Yet this link remains only one possibility as other Russian-linked entities, such as another GRU group, APT28, have also historically targeted consumer network appliances [40].

Given available evidence, it appears that AcidRain (and its enabling steps) is the responsibility of the Sandworm threat actor. Unfortunately, insufficient evidence exists to definitively tie the other, more technically interesting part of the

KA-SAT event – the DHCP DDoS activity – to Sandworm or any specific Russian-nexus threat actor. One possibility is that various elements within the broader 'Sandworm construct' were operating simultaneously to degrade the KA-SAT network at the beginning of the invasion: one using wiper malware, the other leveraging exploited customer or customer-facing equipment as part of a DDoS-focused botnet. GRU entities, such as Sandworm, are linked to the contracted development of automated scan and exploit frameworks, such as 'Scan-V', through the Vulkan Leaks, which may enable subsequent operations such as the DHCP DDoS via botnet commands [41] [42]. This is a tantalizing explanation that explains both concurrent timing and noticeable tradecraft differences, while unifying operations under GRU control, yet is one that remains within the realm of speculation in the absence of more convincing and direct evidence.

New wiper variant

In 2024, multiple analysts identified a variant of AcidRain, given the name AcidPour. As noted by analysts at *SentinelOne* and *Trellix*, AcidPour has significant overlaps with the original AcidRain, making its association clear, while also extending wiping capabilities to a larger number of systems and services [43] [44]. AcidPour shares many of the same characteristics in wiper function as AcidRain (and, by extension, the dstr module of VPNFilter), and appears to possess identical mechanisms for wiper functionality in terms of logic and program flow.

While the wiping functions are nearly identical, AcidPour extends targeting beyond the MIPS-based devices targeted by AcidRain in the KA-SAT event. Potential targets include any device running an *x86 Linux* distribution, meaning impacts could be felt on any number of embedded devices [43]. Furthermore, wiping is extended to additional interfaces and targets within or connected to the operating system, including mapped devices, allowing for impacts on logical volumes, network attached storage, and RAID implementations.

SentinelOne researchers noted an interesting programmatic overlap with an altogether different wiper, CaddyWiper. AcidPour, like CaddyWiper, relies on 'statically-compiled libraries or imports. Most functionality is implemented via direct syscalls, many called through the use of inline assembly and opcodes' [43]. This technical quirk is interesting given that CaddyWiper use is linked to Sandworm operations such as the attempted electric utility disruptive event deploying Industroyer2 malware [45]. Thus links to Sandworm, at least for the wiper portion of the KA-SAT incident, become stronger through technical analysis of associated samples.

More importantly, AcidPour indicates that the capability in AcidRain remains under apparent continuous development with a desire to extend this to additional platforms beyond the MIPS-based devices targeted in the KA-SAT event. For example, functionality in AcidPour enabling wipe of flash memory (MMC) cards could be extended to *Starlink* user terminals (although the software would need to be revised for an ARM environment) [46]. More concretely, samples of AcidPour appeared roughly concurrent with claims of Ukrainian telecommunication disruption by the SolntsepekZ persona on 13 March 2024 [47]. While the use of AcidPour in the wild cannot be confirmed, the continuing evolution of the codebase from AcidRain and the ongoing use of wipers targeting Ukrainian critical infrastructure indicate persistent interest by Russian entities, particularly Sandworm, in targeting network-related equipment.

LESSONS LEARNED AND IMPLICATIONS OF THE 2022 INCIDENT

That distributed communication networks for critical infrastructure control exist and are targeted for disruption is widely known. However, the dependencies that exist between critical infrastructure operations and commercial providers are less well understood, opening a potential attack vector for malicious entities to degrade these links at times of crisis. Either due to direct targeting or, as in the February 2022 events, due to collateral damage, an increasing number of critical infrastructure operations find themselves at risk from disruptions in satellite or related distributed communication networks.

The Enercon scenario

The *Enercon* outage from the KA-SAT disruption appears to have been both brief and unimpactful. The German Federal Office for Information Security (BSI) noted that there were no impacts from the outage 'due to the redundant communication capabilities of the responsible grid operators' [19]. Other reporting indicates the location of the impacted systems was in 'Central Europe' and not necessarily Germany alone [22], meaning the BSI assessment may not be complete.

Wind generation (and related renewable energy resources such as solar) will continue some degree of operation irrespective of positive control over the assets (i.e. turbines can still spin so long as there is wind, although physical emergency controls may also step in to stop such functionality). However, the nature of renewables compared to traditional thermal power sources makes for variable generating output and frequency issues that require control and balancing throughout the overall electric system [48]. While these are resolvable and manageable issues, they do require the ability to manage systems or the interconnection between generating assets and wider-scale transmission and distribution. Removing communication links to allow for free operation of a generating asset, while likely mitigated through other controls at transmission and distribution levels, reduces overall system resiliency and opens it to potential impacts as 'n+1' reliability is degraded, if not removed [49].

Furthermore, many renewable systems such as wind generation are increasingly dependent upon remote monitoring and communications for maintenance and related purposes [50]. *Enercon* itself advertises remote monitoring software for wind turbine maintenance [51], while other significant wind generation players such as *Vestas* and *Siemens Gamesa* offer managed remote monitoring solutions [52] [53]. Severing these links, such as through a DDoS scenario like that observed in the KA-SAT incident, might be an inconvenience, but far more worrying possibilities emerge when one views these links as bidirectional, allowing for possible adversary interaction with deployed assets via distributed communication systems. For example, instead of merely degrading these links, an adversary could utilize them to access deployed energy resources for manual interaction and capability deployment direct to the asset.

The increasing networked availability of these generating assets, including through various 'over-the-air' communications, has extended the attack surface of these entities to various alternative mechanisms. Whereas a traditional generating asset would face many potential layers of security, monitoring, and control between external facing services and critical OT systems, newer communication models in DER and renewable environments increase the number of touch points and avenues of ingress to sensitive systems.

Distributed energy resources and critical infrastructure operations

Modern electric generation and the DER landscape mandate flexible, scalable communications. While it is possible to run fibre or similar to remote or distributed assets, doing so is prohibitively expensive and is a single point of potential failure. Given cost and reliability pressures, leveraging existing wireless communication frameworks, from cellular modems to commercial satellite systems, becomes not just desirable but necessary. Yet precisely how these networks are managed and implemented, and the repercussions for hooking into these networks for critical assets, remain underexplored, and notably underdefended.

Use of systems such as the KA-SAT network or similar flexible, over-the-air systems is unavoidable in the current landscape, and in many respects, desirable given the flexibility and adaptability of modern wireless communication networks. Yet in migrating more communications to these pathways, despite greater systemic reliability and bandwidth, asset owners and operators must also realize the new dependencies and attack scenarios that emerge. For example, legacy telecommunication networks with hard-wired connections may provide only a few mechanisms for directly accessing service provider controls and capabilities, depending on logical networking underneath the physical layer. Yet in situations such as the KA-SAT network, direct access to control systems may be facilitated through operator immaturity (e.g. single-factor authentication to a VPN guarding access to the control centre), or immaterial as access to any node in the system may enable unique attack pathways to other system nodes such as the DHCP-based DDoS activity.

Within these environments adversaries face a menu of options for operating, ranging from target development and profiling through various active and passive mechanisms, to disruptive operations targeting either the network itself or specific nodes within it. While it may be an inconvenience for some types of customer, real-time systems operating on physical equipment face higher levels of reliability and requirements for operator intervention. Implementing distributed communication systems, whether for DER and renewables or pipelines and mines, thus requires close consideration of what dependencies and attack possibilities emerge through their use, and identifying ways to mitigate or reduce the risk of such actions resulting in system disruption.

Wider implications and concerns

First, the dual-use nature of significant communication components, whether satellite infrastructure, undersea cables, or traditional telecommunication environments, provides both opportunity and risk to operators and stakeholders. On the one hand, the availability of commercial, distributed communication channels presents operators of critical infrastructure the opportunity to leverage existing networks for greater efficiency and lower cost compared to the creation of dedicated, purpose-built communication systems. However, in leveraging these environments, such entities place themselves at the mercy of the commercial providers to maintain and secure such infrastructure against attack and disruption.

Second, the evolution of the current energy landscape, from increasingly remote and challenging oil and gas production and transportation to distributed generation through renewables like solar and wind, requires an increasingly flexible and distributed communication network. Given cost pressures and efficiencies, remote wind farms or pipeline compressor stations cannot and will not be manned any time soon. As a result, we should expect critical elements of the overall energy system to be tied together to centralized monitoring and control systems dependent upon increasingly remote and potentially fragile communication links. While a boon to economic possibility and efficiency, this increasingly distributed and remotely managed element of critical infrastructure also provides a significant opportunity to adversaries for a variety of disruptive scenarios.

Third, the KA-SAT events show that potential adversary ingress points into critical networks can take a variety of forms. While the AcidRain vector garners the most attention as a malicious payload pushed to KA-SAT terminals, the DDoS scenario arguably offers a more concerning vector. Through some still unspecified and undisclosed mechanism, the KA-SAT attackers leveraged legitimate equipment within the network to initiate traffic resulting in a cascading DDoS condition. This requires an ability either to compromise a few nodes of the network interactively, or to introduce a botnet-like functionality across

KA-SAT consumer terminals to then initiate the DHCP-based DDoS condition. In either case, observers will note that distributed communication networks by their nature feature a variety of possible touch points that adversaries can take advantage of for malicious purposes, leading to service degradation overall and outright loss for some.

CRITICAL INFRASTRUCTURE ATTACK SCENARIOS VIA SATELLITE COMMUNICATIONS

Various attack vectors exist in distributed communication systems with satellite components. Among other items, electronic warfare and kinetic effects can work to eliminate or severely degrade platforms or infrastructure, particularly in a time of conflict. However, in this discussion we will focus solely on cyber-nexus effects: those deny, degrade, disrupt, or destroy scenarios where a cyber component factors as a key contributor to events.

In this cyber-focused realm, we still observe several possibilities across impact scenarios. Using models such as the MITRE ATT&CK framework for cyber events and the *Aerospace Corporation*'s SPARTA framework for space system security, we can develop multiple plausible scenarios, using events such as the 2022 KA-SAT incident for inspiration, for communication disruption.

Command collection, replay and injection

In many cases, communication streams over satellite links are unencrypted. While the underlying protocol may be encrypted or secured in some fashion, the transport layer remains ‘in the clear’. Thus, if the underlying communication stream is not using an encrypted application protocol, such as SSH or some implementation of TLS, the communication takes place in a fashion that allows for collection, and potentially worse. This is an existing issue in OT-focused communication protocols, where they essentially exist in the clear and unencrypted [54] [55]. When applied to an accessible, over-the-air communication link that also features no security or hardening, significant concerns begin to emerge, largely defined via the SPARTA framework's Eavesdropping technique for reconnaissance [56].

From an adversary's perspective, opportunities exist to collect, examine, and potentially inject into communication streams through various mechanisms. On the physical side, capturing signal ‘bleed through’ by placing a collection asset adjacent to one communication node (either overhead or on the ground) is one potential avenue, but one requiring significant investment and physical presence to enable. Limiting ourselves to cyber mechanisms, traffic capture and replication through compromised systems at various stages across ground and potentially space systems can allow for visibility into uplink and downlink traffic.

Through the compromise of communication nodes such as user terminals, ground station infrastructure, or potentially even satellite payloads, adversaries can gain a viewpoint into communication links. Unless the underlying traffic is secured, opportunities then exist for capturing and replaying or modifying such communication for malicious purposes. Examples include injecting commands or other logic into downlink streams to critical infrastructure assets, such as increasing pressure at a pipeline compressor station, or sending back faulty telemetry to monitoring stations to obscure malicious activity in a Stuxnet-like replay scenario [49].

Although challenging to perform while avoiding operator (and defender) attention, adversaries may not care if their ultimate goal is delivering a cyber-physical impact via compromised communication pathways. Additionally, adversaries can lurk, undetected, while passively collecting information and building a profile of system telemetry to enable subsequent attacks without sophisticated (and expensive) monitoring of and active hunting within network infrastructure.

Ground-station focused intrusion and manipulation

Ground stations and related terrestrial infrastructure arguably represent the weakest and most accessible link across the entire satellite distributed communication model. Multiple techniques within SPARTA focus on ground station compromise, access, or interaction to facilitate subsequent operations against the entire space system [56]. Operator ground stations represent a ‘single point of access’ (and failure) for maintaining systems, while user terminals and modems can be subverted to gain access to the wider system. From a cyber perspective, various opportunities exist to leverage these items for malicious purposes, with the entire MITRE Enterprise ATT&CK framework in play to interact with (and potentially subvert) these systems.

Although not observed in 2022, access to ground station networks can be the precursor to a destructive cyber attack such as wiper deployment within ground station networks. While IT-focused, such an incident has the possibility of crippling operations by removing IT-based visibility and control over network operations and management. Given our understanding of the 2022 incident impacting Ukraine (and others), IT-based wiper malware is well within the capability of such entities and could be deployed to crippling effect to degrade communication links at a management level, impacting all participants within the victim network.

Stepping away from the KA-SAT event and Ukraine, commodity tools, such as IT-focused ransomware, may be equally impactful if deployed against distributed communication management infrastructure. For example, a ransomware event targeting the IT network of control centres can effectively produce a loss of view and loss of control scenario for the overhead assets and network operations. The ongoing ransomware epidemic, including widespread impacts to critical infrastructure environments from hospitals to pipelines, shows that such criminal capabilities could, even if inadvertently, impact critical communication networks through operational disruption [57].

In addition to operator ground station infrastructure and back-office IT infrastructure, user terminals represent an interesting and poorly defended touch point for adversary operations. One still unknown feature of the 2022 KA-SAT incident is how the DHCP-based DDoS took place, as initial activity appears to have originated with user equipment [58]. One plausible explanation is that multiple such endpoints were compromised by the adversary for inclusion in a botnet, which then allowed the adversary to issue malicious commands to the network. As noted previously, AcidRain bears some similarity to the botnet malware VPNFilter, linked to Sandworm. The Sandworm threat actor is notorious for building and maintaining botnets of compromised systems, particularly small office and home office network gear, through software such as VPNFilter, Cyclops Blink, and related capabilities [35] [59].

For the KA-SAT event then, it is plausible that the Sandworm adversary used a variant of existing infrastructure malware to create a botnet of KA-SAT end-user equipment to enable the subsequent DHCP DDoS activity. As observed throughout the Ukraine war (even prior to the current full-scale invasion phase), Russian-controlled botnets for DDoS activity featured prominently in a variety of disruptive events targeting government and civilian infrastructure [30] [17]. The ability to leverage capabilities for commodity, consumer hardware to inject into and create an impact in more complex (and potentially fragile) distributed communication networks thus represents a significant and concerning possibility. Unfortunately, direct evidence for such activity is not available at this time, leaving this botnet-focused approach in the realm of informed speculation.

Satellite-specific attacks and disruption

Initial breach of ground station assets and networks can facilitate follow-on connectivity to satellites, with implications for both bus and payload components. While unobserved to date, existing spacecraft command-and-control systems could be subverted via cyber means to deliver an impact both to the spacecraft itself and with follow-on effects for the overall system.

For example, in the AcidRain scenario the customer-focused update mechanism was compromised to push the malware to terminals, resulting in subsequent communication outages. Had different systems associated with space system control been compromised, as described in the SPARTA Compromise Ground System initial access technique, the possibility exists of leveraging legitimate control functionality to push malicious commands or updates to the space system [56].

Although notional, significant research and analysis has identified critical weaknesses in space system operations through cyber-nexus effects delivered via compromised ground station components [60] [61]. If successfully executed, loss of a space system asset would have enormous consequences on entire regions of activity. Even if not directly targeting critical infrastructure operations, such an action taken as part of wartime operations would have very clear and immediate impacts on critical functionality and visibility as a collateral effect.

While such scenarios may seem far-fetched at present, numerous programmes already exist testing and demonstrating the possibilities of interacting with and disrupting space systems through cyber operations. On the benign end of the spectrum, programmes such as the 'Hack-A-Sat' capture the flag event draw attention to the information security weaknesses of space systems once connectivity to them can be achieved [62]. More worryingly, significant interest appears to exist among many entities to develop counter-space cyber capabilities to augment more traditional mechanisms [63]. Thus policy makers, network owners, and asset operators should take the possibility of cyber-induced space system impacts as a serious, if not yet realized, concern.

Network-wide impacts

Opportunities for network-wide impact scenarios can include scenarios of direct access to internal systems, primarily via ground station assets, outlined above, but can also extend to manipulation of third-party systems to overwhelm communication networks. In this case, a more classic DDoS approach emerges where botnets of infected devices direct traffic to the environment to overwhelm its capacity.

One mechanism, similar to the 2022 Ukraine incident, is to leverage customer equipment within the targeted network to initiate traffic that overwhelms the environment. In the 2022 incident, this was achieved through malicious DHCP traffic resulting in terminals being removed from the network. However, more brute-force type attacks are possible with enough systems compromised in the environment to flood it with noise, overwhelming legitimate operations [64].

Opportunities to leverage either malformed traffic or traffic floods to achieve DDoS conditions abound from both in-network gear and out-of-network, third-party devices targeting the networks of interest. Mitigations are certainly possible, but the limited bandwidth already available for satellite communication links make them extremely susceptible to traffic flood or similar volume-based events [65]. The ability to overwhelm these environments essentially induces at minimum a loss of view and potentially a loss of control scenario for impacted critical infrastructure entities. While a DDoS event may appear to be relatively primitive in terms of sophistication and blunt targeting, it remains an effective mechanism to blind operators and induce potential system outages to avoid operations taking place in an uncontrolled, unmonitored state for various infrastructure types.

OPERATING IN A DISTRIBUTED LANDSCAPE

Operational, economic, and even environmental pressures all mean that critical infrastructure operators, from the electric sector and oil & gas to logistics, will increasingly rely on dispersed, over-the-air communication networks. Often, these will either exist primarily as space system communication networks, or feature these systems prominently as backup command-and-control mechanisms. As a result, asset owners and operators must identify mechanisms to operate in secure, integrity-preserving fashion within this environment.

Communication security

Over-the-air communication via wireless networks requires that signals be hardened against collection and interference. While there may be justifiable reasons to avoid encrypted communications for certain industrial processes when those networks are not directly exposed to outside scrutiny, space system communications require some measure of improved security in the face of potential threats [66].

Changing fundamental OT communication and monitoring protocols is out of scope for this discussion, but adding security at the transportation layer appears to be a minimum viable option given the threat landscape. Unfortunately, simply adding transportation layer security is a non-trivial issue for satellite-focused communication mechanisms. While advancements in commercial platforms have increased bandwidth in many instances, space-based communications remain limited in total available throughput. Adding overhead to existing communications by wrapping them in an encrypted or secure layer, combined with existing latency concerns for space-based communication, may be unsuitable in some applications requiring rapid transfer of significant amounts of data or quick communication of control commands.

While the problem is hard, this issue needs to be resolved as the opportunities for command interception and potential injection are significant across multiple potential vectors: ground interception, space interception, communication capture via compromised devices, and other opportunities. At minimum, system owners and operators should explore adding integrity checks and checksums to commands sent over insecure wireless communication networks to reduce (but not eliminate) the potential of command injection and replay.

Device and platform security

As seen in the 2022 Ukraine incident, customer equipment can be both a site for attacker impact as well as an ingress point to affect the overall network (such as in a DDoS situation). At present, significant resources and attention are focused on platform security in the form of satellite hardening and similar actions. While these efforts are certainly important and address a critical weakness in overall system operations, they also address a notional impact scenario that is yet to be publicly identified in terms of cyber risk.

Instead of the overhead assets in the KA-SAT network, the 2022 incident operated through compromised customer equipment and ground station access. While not as exotic or interesting as improving overhead platform security, the overall attack surface presented by these devices is significantly larger and easier to gain access to, allowing for follow-on actions impacting the network's overall functionality.

To address this need, service providers as well as end-users need to critically examine what equipment is used in these networks, and identify mechanisms to ensure equipment is hardened, patched and resilient in the face of adversary activity. Unfortunately, this is an extremely difficult problem given the sheer volume of equipment and challenges in maintaining an updated, secure posture for customer premise gear. Nonetheless, existing cases demonstrate clearly that adversaries recognize this route as a weak link within larger networks, and they will continue to leverage such environments until unable to do so.

Redundancy and fail-over

Finally, asset owners need to design and implement communication and control models that allow for redundancy and resilience in the face of disruption. That the *Enercon* turbines in the 2022 incident were no longer actively monitored by the vendor following the KA-SAT network disruption is simply unacceptable for critical infrastructure operations. Identifying and investing in redundant and fail-over mechanisms is not merely a 'nice to have', but as distributed, remote elements such as renewable generation become increasingly critical to grid operations this resiliency is necessary.

As with many items, this is neither easy nor cheap to execute. Building in greater resiliency features in various policy-maker recommendations and reporting, such as recent reporting from the US President's Council of Advisors on Science and Technology [67]. While understanding the need for greater system resilience is clear, allocating resources or a willingness to bear the cost of doing so appears lacking. Building redundant communication mechanisms to ensure continuous remote monitoring and control in critical environments means forgoing the cost savings and efficiency of a single over-the-air link, and those costs will need to be addressed by someone. Absent a clear mechanism to approach this issue and invest in greater communication resilience, this issue will be difficult to resolve, leaving increasingly vital elements of critical national infrastructure vulnerable to various types of disruption.

CONCLUSIONS

The 2022 KA-SAT incident highlights multiple items of concern with respect to distributed communication models, not just satellite-based systems. By understanding this incident, and particularly the novel DHCP-based DDoS activity that appears to be responsible for both the longest-lasting and greatest-impacting portions of the event, we can learn multiple lessons in terms of weaknesses in these systems and defensive and operational guidance to harden them against attackers.

Unfortunately, the rapid expansion of distributed critical infrastructure applications means that similar extension in remote communication dependency has taken place without significant security hardening or investigation. While the KA-SAT incident does not appear to have resulted in significant civilian critical infrastructure operational loss, it is quite easy to imagine similar scenarios resulting in outsized effects on DER and related renewable energy resources. By understanding how the KA-SAT event took place, including its various phases and impacts, we can begin modelling responses and security controls to limit the impacts of such actions.

Overall, the move toward greater distributed, over-the-air communication frameworks for critical infrastructure operations is both inevitable and, in many ways, desirable. But such a move, especially in an increasingly contested international environment, must take place aware of the new risks created. Through analysis of historical events, such as the 2022 KA-SAT incident, and modelling future potential incidents, critical infrastructure asset owners and operators can begin discerning specific threat and attack vectors for follow-on hardening, defence, and increased resilience.

REFERENCES

[1] Yu, F. R.; Zhang, P.; Xiao, W.; Choudhury, P. Communication systems for grid integration of renewable energy resources. IEEE Network, vol. 25, no. 5, pp. 22-29, 2011.

[2] Duan T.; Dinavahi, V. Starlink Space Network-Enhanced Cyber-Physical Power System. IEEE Transactions on Smart Grid, vol. 12, no. 4, pp. 3673-3675, 2021.

[3] Duan, N.; Yee, N.; Otis, A.; Joo, J.-Y.; Stewart, E.; Bayles, A.; Spiers, N.; Cortez, E. Mitigation Strategies Against Cyberattacks on Distributed Energy Resources. In 2021 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC USA, 2021.

[4] Elbert, B. Introduction to Satellite Communication, Norwood, MA: Artech House, 2008.

[5] The Aerospace Corporation. Understanding Space-Cyber Threats with the SPARTA Matrix. 18 October 2022. https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix. [Accessed 2 May 2024].

[6] Reuters. Satellite firm ViaSat probes suspected cyberattack in Ukraine and elsewhere. 28 February 2022. https://www.reuters.com/business/aerospace-defense/satellite-firm-viasat-probes-suspected-cyberattack-ukraine-elsewhere-2022-02-28/. [Accessed 2 May 2024].

[7] MITRE ATT&CK. Network Denial of Service. The MITRE Corporation. 25 March 2022. https://attack.mitre.org/techniques/T1498/. [Accessed 2 May 2024].

[8] O'Neill, P. H. Russia hacked an American satellite company one hour before the Ukraine invasion. 10 May 2022. https://www.technologyreview.com/2022/05/10/1051973/russia-hack-viasat-satellite-ukraine-invasion/. [Accessed 2 May 2024].

[9] Satter, R. Satellite outage caused 'huge loss in communications' at war's outset – Ukrainian official. Reuters. 15 March 2022. https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/. [Accessed 6 May 2024].

[10] Guerrero-Saade, J. A.; van Amerongen, M. AcidRain | A Modem Wiper Rains Down on Europe. 31 March 2022. https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/. [Accessed 2 May 2024].

[11] ViaSat, Inc. KA-SAT Network cyber attack overview. 30 March 2022. https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. [Accessed 2 May 2024].

[12] MITRE ATT&CK. AcidRain. 12 April 2024. https://attack.mitre.org/software/S1125/. [Accessed 2 May 2024].

[13] Colaluca, M.; Walter, K. Lessons Learned from the KA-SAT Cyberattack: Response, Mitigation, and Information Sharing. Black Hat USA. 1 March 2024. https://www.youtube.com/watch?v=RdjthhBylMk. [Accessed 2 May 2024].

[14] Colaluca, M.; Saunders, N. Defending KA-SAT. DEFCON Conference. 15 September 2023. https://www.youtube.com/watch?v=qI_ICtX3Gm8. [Accessed 2 May 2024].

[15] Droms, R. Dynamic Host Configuration Protocol. IETF, March 1997. https://datatracker.ietf.org/doc/html/rfc2131. [Accessed 2 May 2024].

[16] Lister, T.; John, T.; Murphy, P. P. Here's what we know about how Russia's invasion of Ukraine unfolded. CNN. 24 February 2022. https://www.cnn.com/2022/02/24/europe/ukraine-russia-attack-timeline-intl/index.html. [Accessed 2 May 2024].

[17] ESET Research. A year of wiper attacks in Ukraine. ESET. 24 February 2023. https://www.welivesecurity.com/2023/02/24/year-wiper-attacks-ukraine/. [Accessed 2 May 2024].

[18] National Air and Space Intelligence Center. Competing in Space. December 2018. https://www.nasic.af.mil/Portals/19/documents/Space_Glossy_FINAL--15Jan_Single_Page.pdf?ver=2019-01-23-150035-697. [Accessed 2 May 2024].

[19] Reuters. Satellite outage knocks out thousands of Enercon's wind turbines. Reuters. 28 February 2022. https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/. [Accessed 2 May 2024].

[20] MITRE ATT&CK. Denial of view. MITRE. 13 October 2023. https://attack.mitre.org/techniques/T0815/. [Accessed 2 May 2024].

[21] MITRE ATT&CK. Loss of View. MITRE. 13 October 2023. https://attack.mitre.org/techniques/T0829/. [Accessed 2 May 2024].

[22] Holzki, L.; Nagel, L.-M.; Verfürden, M.; Witsch, K. Massive Störung der Satellitenverbindung: Enercon meldet fast 6000 betroffene Windanlagen. Handelsblatt. 28 February 2022. https://www.handelsblatt.com/unternehmen/energie/erneuerbare-energien-massive-stoerung-der-satellitenverbindung-enercon-meldet-fast-6000-betroffene-windanlagen/28114360.html?ticket=ST-5593272-HeAL9WNhaZP9e9EKQYsK-ap3. [Accessed 2 May 2024].

[23] MITRE ATT&CK. Loss of Control. MITRE. 13 October 2023. https://attack.mitre.org/techniques/T0827/. [Accessed 2 May 2024].

[24] Diuk, N. EUROMAIDAN: Ukraine's Self-Organizing Revolution. World Affairs, vol. 176, no. 6, pp. 9-16, 2014.

[25] Microsoft Digital Security Unit. Destructive malware targeting Ukrainian organizations. Microsoft. 15 January 2022. https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/. [Accessed 2 May 2024].

[26] Greenberg, A. Russia's New Cyberwarfare in Ukraine Is Fast, Dirty, and Relentless. Wired. 10 November 2022. https://www.wired.com/story/russia-ukraine-cyberattacks-mandiant/. [Accessed 2 May 2024].

[27] ESET Research. IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine. ESET. 1 March 2022. https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/. [Accessed 2 May 2024].

[28] UK National Cyber Security Centre. UK government assess Russian involvement in DDoS attacks on Ukraine. UK NCSC. 18 February 2022. https://www.ncsc.gov.uk/news/russia-ddos-involvement-in-ukraine. [Accessed 2 May 2024].

[29] ASERT Team. DDoS Threat Landscape - Ukraine. Netscout. 21 March 2022. https://www.netscout.com/blog/asert/ddos-threat-landscape-ukraine. [Accessed 2 May 2024].

[30] Blinken, A. J. Attribution of Russia's Malicious Cyber Activity Against Ukraine. US Department of State. 10 May 2022. https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/. [Accessed 2 May 2024].

[31] Truss, E. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. UK Foreign, Commonwealth, & Development Office. 10 May 2022. https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion. [Accessed 2 May 2024].

[32] Galeotti, M. Putin's Hydra: Inside Russia's Intelligence Services. 11 May 2016. https://ecfr.eu/wp-content/uploads/ECFR_169_-_PUTINS_HYDRA_INSIDE_THE_RUSSIAN_INTELLIGENCE_SERVICES_1513.pdf. [Accessed 2 May 2024].

[33] US National Security Agency. Sandworm actors exploiting vulnerability in Exim mail transfer agent. 28 May 2020. https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf. [Accessed 2 May 2024].

[34] US Department of Justice. Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace. US Department of Justice. 19 October 2020. https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and. [Accessed 2 May 2024].

[35] Largent, W. New VPNFilter malware targets at least 500k networking devices worldwide. Cisco Talos. 23 May 2018. https://blog.talosintelligence.com/vpnfilter/. [Accessed 2 May 2024].

[36] US Cybersecurity and Infrastructure Security Agency. New Sandworm malware Cyclops Blink replaces VPNFilter. 23 February 2022. https://www.cisa.gov/sites/default/files/publications/AA22-054A%20New%20Sandworm%20Malware%20Cyclops%20Blink%20Replaces%20VPN%20Filter.pdf. [Accessed 3 May 2024].

[37] Antoniuk, D. Sandworm linked group likely knocked down Ukrainian internet providers. The Record. 22 March 2024. https://therecord.media/ukraine-isps-attacks-solntsepek-sandworm-gru. [Accessed 3 May 2024].

[38] Computer Emergency Response Team of Ukraine. Особливості деструктивних кібератак Sandworm у відношенні українських провайдерів (CERT-UA#7627). CERT-UA, 15 October 2023. https://cert.gov.ua/article/6123309. [Accessed 3 May 2024].

[39] Cherepanov, A.; Lipovsky, R. Industroyer: Biggest threat to industrial control systems since Stuxnet. ESET. 12 June 2017. https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/. [Accessed 11 May 2024].

[40] US Federal Bureau of Investigation. Russian Cyber Actors Use Compromised Routers to Facilitate Cyber Operations. 27 February 2024. https://www.ic3.gov/Media/News/2024/240227.pdf. [Accessed 3 May 2024].

[41] Wahlstrom, A.; Roncone, G.; Lunden, K.; Zafra, D. K. Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan. Google Cloud. 30 March 2023. https://cloud.google.com/blog/topics/threat-intelligence/cyber-operations-russian-vulkan. [Accessed 14 May 2024].

[42] Slowik, J. Burrowing Through the Network: Contextualizing the Vulkan Leaks & State Sponsored Offensive Ops. Def Con 31. 16 September 2023. https://www.youtube.com/watch?v=H7bV_99I7O4. [Accessed 14 May 2024].

[43] Guerrero-Saade, J. A.; Hegel, T. AcidPoud | New Embedded Wiper Variant of AcidRain Appears in Ukraine. SentinelOne. 21 March 2024. https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/. [Accessed 2 May 2024].

[44] Kersten, M. Pouring Acid Rain. Trellix. 30 April 2024. https://www.trellix.com/blogs/research/pouring-acid-rain/. [Accessed 2 May 2024].

[45] ESET Research. Industroyer2: Industroyer reloaded. ESET. 12 April 2022. https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/. [Accessed 3 May 2024].

[46] Research group COSIC, KU Leuven. Dumping and extracting the SpaceX Starlink User Terminal firmware. KU Leuven. 6 July 2021. https://www.esat.kuleuven.be/cosic/blog/dumping-and-extracting-the-spacex-starlink-user-terminal-firmware/. [Accessed 3 May 2024].

[47] Goodin, D. Never-before-seen data wiper may have been used by Russia against Ukraine. ArsTechnica. 21 March 2024. https://arstechnica.com/security/2024/03/never-before-seen-data-wiper-may-have-been-used-by-russia-against-ukraine/. [Accessed 3 May 2024].

[48] Schmietendorf, K.; Peinke, J.; Kamps, O. The impact of turbulent renewable energy production on grid stability and quality. The European Physical Journal B, vol. 90, no. 222, pp. 1-6, 2017.

[49] Slowik, J. Stuxnet to CRASHOVERRIDE to TRISIS: Evaluating the History and Future of Integrity-Based Attacks on ICS Environments. Dragos. https://www.dragos.com/wp-content/uploads/Past-and-Future-of-Integrity-Based-ICS-Attacks.pdf. [Accessed 14 May 2024].

[50] Staggs, J.; Ferlemann, D.; Shenoi, S. Wind Farms Security: Attack Surface, Targets, Scenarios and Mitigations. International Journal of Critical Infrastructure Protection, no. 17, pp. 3-14, 2017.

[51] Enercon. SCADA Remote. Enercon. https://www.enercon.de/en/service/scada-remote. [Accessed 3 May 2024].

[52] Vestas. Vestas Online. https://www.vestas.com/en/services/vestas-online. [Accessed 2 May 2024].

[53] Siemens Gamesa. Remote Services for wind farms. https://www.siemensgamesa.com/en-int/products-and-services/service-wind/diagnostics. [Accessed 3 May 2024].

[54] European Union Agency for Network and Information Security. Communication network dependencies for ICS/SCADA Systems. December 2016. https://www.enisa.europa.eu/publications/ics-scada-dependencies. [Accessed 12 March 2024].

[55] Fauri, D.; de Wijs, B.; den Hartog, J.; Costante, E.; Zambon, E.; Etalle, S. Encryption in ICS networks: A blessing or a curse? In 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 2017.

[56] The Aerospace Corporation. SPARTA: Space Attack Research & Tactic Analysis. 2022. https://sparta.aerospace.org/. [Accessed 12 March 2024].

[57] US Federal Bureau of Investigation. Federal Bureau of Investigation Internet Crime Report 2022. 2023. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. [Accessed 12 March 2024].

[58] Colaluca, M.; Saunders, N. DEF CON 31 – Defending KA-SAT – Mark Colaluca and Nick Saunders. YouTube, August 2023. https://www.youtube.com/watch?v=qI_ICtX3Gm8. [Accessed 27 February 2024].

[59] UK National Cyber Security Centre. New Sandworm malware Cyclops Blink replaces VPNFilter. 23 February 2022. https://www.ncsc.gov.uk/news/joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter. [Accessed 12 March 2024].

[60] The Aerospace Corporation. Protecting Space Systems from Cyber Attack. Medum. 21 March 2022. https://medium.com/the-aerospace-corporation/protecting-space-systems-from-cyber-attack-3db773aff368. [Accessed 12 March 2024].

[61] Bichler, S. F. Mitigating Cyber Security Risk in Satellite Ground Systems. April 2015. https://apps.dtic.mil/sti/pdfs/AD1012754.pdf. [Accessed 12 March 2024].

[62] Air Force Research Laboratory. Hack-A-Sat. 2023. https://afresearchlab.com/technology/hack-a-sat/. [Accessed 12 March 2024].

[63] Samson, V. The Cyber Counterspace Threat: Coming Out of the Shadows. 29 January 2023. https://www.cigionline.org/articles/the-cyber-counterspace-threat-coming-out-of-the-shadows/. [Accessed 12 March 2024].

[64] Kumar, R.; Arnon, S. Random Routing Algorithm for Enhancing the Cybersecurity of LEO Satellite Networks. Electronics, vol. 12, no. 3, p. 518, 2023.

[65] Usman, M.; Qaraqe, M.; Asghar, M. R.; Ansari, I. S. Mitigating Distributed Denial of Service Attacks in Satellite Networks. Transactions on Emerging Telecommunications Technologies, vol. 31, no. 6, 2020.

[66] Slowik, J. Assessing The Balance Between Visibility And Confidentiality In OT. S4 Events. 4 January 2023. https://youtu.be/3zqPY8ftrq8?si=z8OX4wHgHz8LdBxv. [Accessed 13 March 2024].

[67] President's Council of Advisors on Science and Technology. Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World. February 2024. https://www.fdd.org/wp-content/uploads/2024/03/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf. [Accessed 13 March 2024].

[68] US Cybersecurity & Infrastructure Security Agency. New Sandworm Malware Cyclops Blink Replaces VPNFilter. 23 February 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-054a. [Accessed 12 March 2024].

APPENDIX: KA-SAT EVENT ATT&CK AND SPARTA MAPPING

To facilitate understanding of the KA-SAT incident, the following mappings to the MITRE ATT&CK and *Aerospace Corporation* SPARTA frameworks are provided.

MITRE Enterprise ATT&CK mapping

ATT&CK ID	Technique name	Description
T1587.001	Develop Capabilities: Malware	One portion of the KA-SAT event involved developing malware targeting SurfBeam 2-type modems.
T1583	Acquire Infrastructure	The DDoS actor gained access to unspecified KA-SAT customer devices to serve as the launch point for subsequent DHCP-based DDoS activity.
T1133	External Remote Services	Prior to deployment of the AcidRain malware, the threat actor gained access to the victim network operations centre via a VPN appliance, likely through captured, legitimate credentials.
T1078	Valid Accounts	VPN access likely via captured, legitimate credentials was followed by lateral movement in the environment via credential re-use.
T1059.004	Command & Scripting Interpreter: Unix Shell	A toolkit was identified in the management network containing various scripts as well as suspicious binary files.
T1553	Subvert Trust Controls	The threat actor gained access to an FTP instance used to stage updates for customer modems in order to push AcidRain malware to victims.
T1049	System Network Connections Discovery	The threat actor used access to the control system network to pull information about connected customer nodes in the KA-SAT environment.
T1570	Lateral Tool Transfer	The threat actor deployed a toolkit in the management network containing various scripts and malicious binary files.
T1021	Remote Services	The threat actor moved laterally from VPN access through unspecified remote services within the environment.

ATT&CK ID	Technique name	Description
T1213	Data from Information Repositories	The threat actor used access to the management to pull information on system status and connected endpoints.
T1071	Application Layer Protocol	The threat actor used TOR nodes as final-hop connection points to the KA-SAT management network, but it is unclear if TOR protocol was used for this communication.
T1498	Network Denial of Service	For the DHCP DDoS portion of the activity, specially crafted DHCP packets were sent that would result in KA-SAT terminals being removed from the network.
T1561	Disk Wipe	The AcidRain malware wiped victim terminals following execution.
T1529	System Shutdown/Reboot	The final stage of AcidRain execution was to restart the victim terminals to complete wipe activity.

Aerospace Corporation SPARTA mapping

SPARTA ID	SPARTA name	Description
RD-0003	Obtain Cyber Capabilities	The threat actor developed a payload, AcidRain, to target end-user terminals in the KA-SAT network.
RD-0004.02	Stage Capabilities: Upload Exploit/Payload	The threat actor staged the wiper payload, AcidRain, along with support tools and scripts in KA-SAT management infrastructure.
IA-0007	Compromise Ground System	The threat actor compromised the management network for the KA-SAT system to deploy the AcidRain payload.
IA-0009.03	Trusted Relationship: User Segment	The DDoS threat actor used compromised user equipment as the source for crafted DHCP packets to knock terminals off the KA-SAT network.
EX-0010.02	Malicious Code: Wiper Malware	The threat actor deployed the AcidRain wiper malware against customer terminals in the KA-SAT network.
EX-0013.01	Flooding: Valid Commands	The DDoS threat actor used valid DHCP traffic to disconnect end-user terminals from the KA-SAT network.
LM-0007	Valid Credentials	The threat actor used valid credentials to gain access to and move laterally within the victim management environment prior to deploying the AcidRain wiper malware.
EXF-0007	Compromised Ground System	The threat actor used access to the ground station management network to gather and exfiltrate information related to KA-SAT network status and operations.
IMP-0002	Disruption	Deployment of both AcidRain malware and the DDoS campaign resulted in disruption in KA-SAT operations.
IMP-0003	Denial	DHCP-based DDoS activity prevented users from using the KA-SAT environment for communication purposes, including Ukrainian military communications and some renewable energy system management users.
IMP-0004	Degradation	Weeks-long DDoS activity (preceding and after 22 February 2022) impacted KA-SAT network functionality as the threat actor adapted DDoS activity to defender countermeasures.