Policy Perspectives
Vol. 13/1, January 2025

CSS
ETH Zürich

Electronic and Cyber Operations Against Space Systems

Distinguishing between electronic and cyber operations is crucial for understanding threats to space systems. This Policy Perspective lays out the differences and suggests policy responses to mitigate these threats.

By Clémence Poirier

News reports and academic papers have frequently conflated electronic warfare operations with cyber operations. As the frequency of cyber and electronic attacks continues to rise, misunderstandings about the nature of attacks affecting satellite networks are likely to increase as well.

The attack on Walt Disney's BabyTV, whose signal is distributed by the French satellite operator Eutelsat, serves as a telling example. In March and April 2024, Russian propaganda was broadcast on BabyTV. Initial media reports mischaracterized the incident as a cyberattack, when in fact it was uplink jamming – a form of electronic attack.

Unlike cyberattacks on space systems, electronic operations against satellites fall strictly under the jurisdiction of the ITU, which does not address cyber operations. In fact, no regulatory body currently governs cyber threats against space systems. The BabyTV case, presented before the ITU, highlights the need to distinguish clearly between electronic and cyber operations targeting space systems.

The BabyTV Incident

BabyTV is an international television channel broadcast in over 100 countries and approximately 20 languages. Owned and operated by the Walt Disney Company, its programming consists primarily of cartoons tailored to children aged four and under. However, on 28 March 2024, BabyTV's usual cartoon lineup was unexpectedly replaced by content featuring Russian nationalist singer Oleg Gazmanov's music video "Go, Russia!". It depicted Soviet and Russian military parades and war

Key Points

- Electronic warfare operations target the radiofrequency (RF) spectrum. Cyber operations directly target data and computer networks.
- Terminological clarity is essential because incorrectly categorizing electronic attacks as cyberattacks can lead to technical misconceptions and jurisdictional misunderstandings.
- Satellite TV broadcasters should update their threat models – particularly when an armed conflict arises.
- Extending the International Telecommunications Union's (ITU) mandate to encompass cyber threats, or creating a new international organization to deal with cyber threats against satellites, is unlikely in the current geopolitical context.
- The ITU and the International Committee of the Red Cross (ICRC) should increase cooperation regarding aspects of International Humanitarian Law (IHL) that concern electronic and cyber warfare.

footage. On April 17, BabyTV's signal was hijacked again for 13 minutes. An investigation by Dutch news program NOS Nieuwsuur revealed that sound and images were broadcast in some countries while in others only images were displayed without any sound.

Subscribers in the Netherlands, Portugal, Belgium, and Sweden were reportedly affected, but other European countries were likely impacted as well. In early 2024, BabyTV was broadcast on the same frequency as four Ukrainian channels (Dlia Ciebie, Espresso TV, Freedom, and Dim). Some of these channels reported similar disruptions on the same day as the second BabyTV incident. Ukrainian channels such as 1+1 Ukraine, which rely on SES satellite Astra4a were also hijacked on the same day as the first BabyTV incident. It shows that satellite broadcasters can be accidentally targeted in the context of an armed conflict.

A satellite on a background of lines of code and electromagnetic waves. *Image generated with DALL-E OpenAI.*

In March, initial news reports mistakenly stated that a cyberattack was conducted against one of Eutelsat satellites. Dutch media NL Times first reported that the incident was a "sophisticated" cyberattack against Eutelsat. Dutch news outlet IAmExpat, Serbian media Politika, and the Moscow Times all referred to a cyber operation as well. In early April, Eutelsat clarified to Portuguese media outlet Observador that the BabyTV incident actually involved RF interference.

Hijacking Satellite Broadcasts

When a satellite broadcast operates normally, the content is encoded into a RF signal that contains video, audio, and data content, known as a modulated carrier signal. This signal is then transmitted from a ground station to a satellite, which receives the signal and broadcasts it back to Earth across a wide geographic area. Those signals are then picked up by satellite dishes, forwarding them to a receiver that decodes the signal and transforms it back into video, audio, and data content.

To inject its own broadcast, a malicious actor would need information about the system features and parameters of the target as well as offensive capabilities. First, the actor would need to have access to a satellite ground station or an antenna powerful enough to send a signal to the satellite that can override the legitimate one. The attacker would likely need to match the symbol rate, which defines the rate at which data travels from the ground station to the satellite, to ensure that the satellite is unable to distinguish between the legitimate and illegitimate signal. Additionally, the attacker would need to use the same modulation type as the legitimate broadcaster so that the satellite receivers can decode the signal properly and transmit digital data over radio frequencies.

Natural phenomena can disrupt RF signals and can thus affect the audio and image quality of satellite TV broadcasts. To address this, broadcasters use an algorithmic technique known as Forward Error Correction (FEC). FEC can detect and correct errors in the downlink stream to ensure that the signal does not have to be retransmitted. An attacker would likely have to match the FEC rate to avoid detection and ensure that the satellite receivers recognize the signal as valid. Finally, the actor would have to align the antenna of their ground station with the satellite's orbital position so that the signal can reach it. This requires Space Situational Awareness data, which tracks the location, speed, and trajectory of space objects.

Cyber vs. Electronic Warfare

Drawing a clear distinction between an electronic attack and a cyberattack is not always straightforward. UNIDIR's 2019 report "Electronic and Cyber Warfare in Outer Space" provides one of the clearest definitions, noting that electronic operations use the RF spectrum to interfere with satellites while cyber operations use software and network techniques to interfere or control space systems.

However, both terms are used interchangeably to refer to common electronic attacks such as jamming (blocking RF signals) and spoofing (generating false signals to replace valid ones). In 2019, the US Defense Intelligence Agency noted in its report "Challenges to Security in Space" that electronic warfare uses "jamming and spoofing techniques to control the electromagnetic spectrum."

By contrast, in 2016, a Chatham House report titled "Space, the Final Frontier to Cybersecurity?" included jamming and spoofing as cyberattacks against space-based systems. In 2020, a publication of the Joint Air Power Competence Centre noted that jamming and spoofing are considered cyber threats. In 2022, an article in the Space Policy journal also categorized jamming as a cyber threat.

The Source of Confusion

According to former US Army Intelligence Officer Jeffrey Bardin, the confusion has persisted because of fundamental technical misunderstandings surrounding the term "hacking." Electronic interference, unlike hacking, does not necessarily involve an intrusion into a computer system; it simply intercepts the signal emitted by a satellite. No internet connection or code modification is required.

The confusion also partly derives from historical language use since the term "electronic warfare" was used long before the invention of the computer. When the first cyberattacks were detected, they were classified as "electronic" because that was the existing category that most closely resembled the observed phenomenon.

The issue may stem from the digitalization of space systems, which has enabled the jamming and spoofing of satellites through cyber means. This can be described as "cyber-electronic convergence", an overlap between cyberspace and the electromagnetic spectrum. Cyber operations can also affect the electromagnetic spectrum because electronic and radio systems increasingly rely on computer systems.

Theoretically, in the BabyTV case, a similar effect could have been achieved with a pure cyber operation. The malicious actor could have exploited a vulnerability in one of Eutelsat's ground stations, in order to access that station's network. Then, the attacker could have attempted to access the satellite control systems to replace the original signal feed with an alternative one, transmitting it to the satellite in orbit. Although the outcome of the operation would have been the same, its nature would have been entirely different.

Electronic attacks may also require reconnaissance to gather key data such as the RF band, transmission power, ground station location, and similar. Although BabyTV's incident remains an electronic warfare operation, the reconnaissance phase could have involved a cyber component (or at least open-source intelligence).

The ITU's Mandate

Unlike cyber threats, electronic operations against satellites fall under ITU's mandate. ITU's Radio Regulations use the term "harmful interference" to describe operations that disrupt the functioning of radio frequencies and radionavigation services. Radio Regulations forbid jamming and spoofing by prohibiting the emission of unnecessary, false, misleading, or unidentified signals. In case of interference, member states can resolve the issue bilaterally. Member states can also directly report the situation to the ITU and request assistance from the Radiocommunication Bureau. This body facilitates technical evidence gathering to locate the source of interference and ensures cooperation between administrations. Following this, the ITU provides recommendations to its members.

In June 2024, on behalf of Eutelsat, France filed a complaint with the ITU for harmful interference. The French complaint confirmed that the attack against BabyTV was likely an electronic operation as the ITU does not deal with cyberattacks. In August 2024, the 96th meeting of the ITU Radio Regulations Board (RBB) addressed the French complaint. It revealed that the interference was identified as coming from large ground stations in Moscow, Kaliningrad, and Pavlovka in Russia.

Prior to the RBB meeting, Paris reached out to Moscow for clarification. France received four delivery receipts of its letters and one reply, stating that Russia did not find any emissions from their territory that could have interfered with Eutelsat's satellite. Since the interference persisted, France turned to the ITU.

(In)Effective Multilateralism

Like other intergovernmental organizations, the ITU is not immune to the influence of geopolitics on its internal deliberations, with procedural rules often serving as tools to promote diverse interests. When France submitted its complaint in June 2024, Luxembourg, Sweden, the Netherlands, and Ukraine also filed interference complaints, several of which were linked to the war in Ukraine. The Ukrainian government reported 11 cases of interference, affecting 37 Ukrainian media programs from February to May 2024.

Notably, one business day prior to the August RBB meeting, Russia submitted a delayed complaint covering 22 cases of harmful interference against Russian satellites between February 2022 and 2024. However, the ITU did not receive any technical information on this interference and Russia did not report the cases through the ITU's Satellite Interference Reporting and Resolution System (SIRRS). During the meeting, RBB Member for the Africa region, Hassan Talib, stated that Russia likely only submitted this complaint after the other countries provided technical data that geolocated the source of the interference in Russia, substantiating their complaints.

Further Reading

Rajeswari Pillai Rajagopalan, **Electronic and Cyber Warfare in Outer Space,** Space Dossier 3, *UNIDIR,* 2019.
This report provides an analysis of emerging technologies and capabilities in the field of electronic and cyber warfare against space systems.

Tim Fountain / Leander Humbert, **An Overview of Space Electronic Warfare,** White Paper, *Rhode & Schwarz,* 2023.
This report provides an overview of offensive and defensive electronic warfare on space systems.

Despite its limitations, the ITU remains relatively effective due to its technical focus, allowing for mediation between geopolitical adversaries – a capability increasingly absent in many other fora. However, the ITU lacks enforcement powers; it cannot revoke frequency allocations, impose fines, or sanction countries.

The likely coordination of complaints by several European countries amplified this diplomatic pressure on Russia and attracted greater media attention than individual filings would have. Nonetheless, the interference persisted in several instances.

Moving Forward

Several recommendations are vital for mitigating future cyber and electronic threats. First, journalists and researchers should exercise greater caution and precision when discussing electronic attacks and cyberattacks. These terms describe distinct phenomena. By adopting more specific terminology, stakeholders can foster a clearer understanding of these threats and their implications.

Second, accurate labeling of electronic and cyber operations is essential to enhance the protection of space systems. Operators must monitor distinct parameters to detect and mitigate malicious activities. RF emissions must be monitored to detect electronic attacks while networks and data must be monitored to detect cyberattacks. For electronic operations, mitigation measures include directional antennas, phased array antennas, software-defined satellites, component hardening, etc. For cyber threats, it includes encryption, the implementation of the Space Data Link Security protocol, Zero Trust architecture, etc. By understanding the nature of the attack operators can deploy the most effective detection and mitigation strategies.

Third, beyond the semantic debate, properly categorizing electronic operations allows state actors to register, attribute, publicly highlight international violations, and potentially resolve issues through the ITU. However, states may explore alternative options if multilateralism through the ITU does not prove effective. For instance, the BabyTV case could be labeled both as an electronic attack and information warfare since it broadcast propaganda. This label could allow states to activate various mechanisms at both the EU and national levels to identify, document, and publicly attribute information operations. Examples at the EU level include the EU Disinfo Lab, the East StratCom Task Force, and the European Cyber and Information Warfare Toolbox. At the national level, mechanisms like VIGINUM in France could be used. Alternatively, the BabyTV case could be considered a hybrid operation, which would allow EU member states to use the EU Hybrid Toolbox. This may mobilize EU Hybrid Rapid Response Teams to help rebuild affected systems or circumvent persistent interference, and enable the imposition of sanctions against entities involved.

Fourth, addressing the overlap between electronic and cyber threats could involve extending the ITU's mandate to cover cyber threats against space systems or creating a new international organization for this purpose. Both options are unlikely due to technical challenges and the crisis of multilateralism. Electronic operations, confined to the RF spectrum, allow victims to disclose interference data to the ITU and confidently attribute attacks without exposing sensitive information. This is rarely the case for cyber operations. Additionally, cyber operations rely more heavily on deception, further complicating attribution and reducing confidence.

Fifth, operators and broadcasters need to be more proactive in implementing mitigations. If feasible, they should update their threat models (i.e., identification and prioritization of threats and implementation of mitigations) and switch technical parameters whenever a conflict arises to avoid collateral damage. The BabyTV incident was likely collateral damage, as confirmed by the Dutch National Cyber Center. Today, BabyTV's signal no longer overlaps with Russian or Ukrainian channels. It broadcasts on a different frequency, symbol rate, and FEC.

Sixth, enhanced collaboration between the ITU and the ICRC could facilitate the adaptation of the Radio Regulations to address new challenges arising in warfare. While the regulations include special provisions against interference on distress and safety frequencies, they currently fail to account for the potential collateral damage to civilian space systems in the context of armed conflict.

In conclusion, understanding the differences between electronic and cyber threats is key for effective technical, military, political, and diplomatic responses. As adversaries combine cyber and electronic tactics to disrupt space systems, comprehensive mitigation and response strategies are essential.

Clémence Poirier is a Senior Cyber Defense Researcher at the Center for Security Studies at ETH Zürich.

Policy Perspectives is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy.

Series Editor: Daniel Möckli
Issue Editor: Gorana Grgić
Layout: Miriam Dahinden-Ganzoni

Feedback welcome: css.info@sipo.gess.ethz.ch
More issues and free online subscription:
css.ethz.ch/en/publications/css-policy-perspectives

Most recent editions:
Cyber Defense in Space: Quo Vadis? (12/3)
Prospects of a Transatlantic Arsenal of Democracy (12/2)
Time to Make 'Peace' with the Bandits (12/1)
Unequal Access to UN Human Rights Bodies (11/6)
Making Cyber Attribution More Transparent (11/5)
Satellite Imagery for Disaster Resilience (11/4)

ISSN: 2296-6471; DOI: 10.3929/ethz-b-000717330