SSI ISSUE GUIDE

ELECTROMAGNETIC INTERFERENCE WITH SPACE SYSTEMS

NOVEMBER 2020

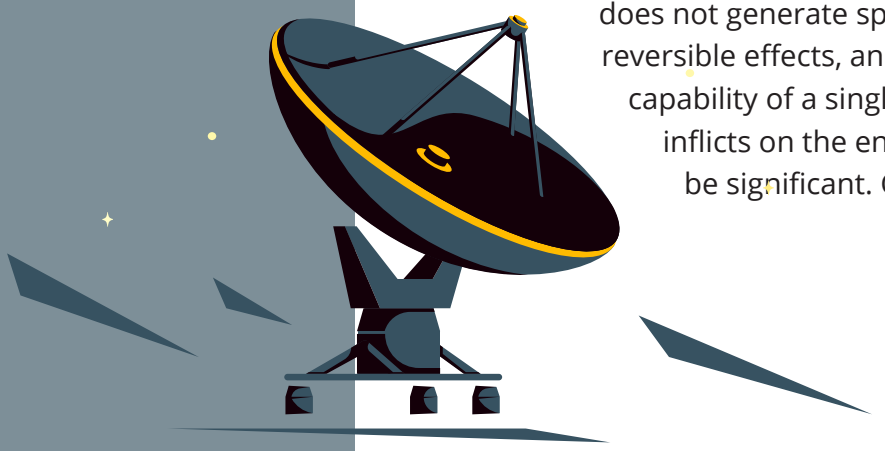
ABOUT

The core function of satellites is to collect and relay data in real time. To transmit data to ground stations and receive information from ground stations, satellites must access and use radio frequencies from the electromagnetic spectrum. These frequencies are vulnerable to a range of harmful interference techniques that are widely available and frequently employed in space negation efforts and electronic warfare (EW).

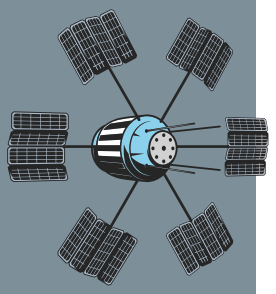
Electromagnetic interference can also occur naturally or accidentally; the focus of this Issue Guide is on intentional or harmful interference.

ELECTROMAGNETIC INTERFERENCE AND SPACE SECURITY

Such interference is not easily attributed to any particular actor and can be mistaken for natural interference from the space environment. Both factors increase the appeal of such attacks for hostile actors.



Unlike kinetic attacks on satellites, electronic interference does not generate space debris, often has temporary and reversible effects, and can narrowly target one specific capability of a single satellite. Nonetheless, the harm it inflicts on the end-users of space-based systems can be significant. Global Satellite Navigation Systems



(GNSS) such as GPS, which serve the military and are also essential in the operation of critical civilian infrastructures on Earth, are frequent targets of EW activity, as are commercial and civilian space systems.

Because such interference is rarely acknowledged publicly or countered, these attacks are perceived to be less escalatory and thus more acceptable. But such activities can lead to conflict escalation, particularly if they target strategically sensitive systems, such as those connected to nuclear command and control capabilities. The opaque nature of EW actions also breeds fear and uncertainty in victims, which can escalate conflict.

TYPES OF ELECTRONIC INTERFERENCE

Uplink signal attacks target the ground station computer systems. Down-link attackers target satellites.

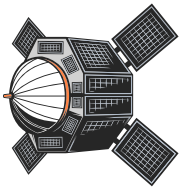


Figure 1: Types of electronic attacks against space systems

Common name	Description
Orbital jamming	A beam of contradictory signals directed toward a satellite, which then mixes, overriding legitimate signals and blocking their transmission.
Terrestrial jamming	Rogue frequencies directed to ground-based targets, such as consumer-level satellite dishes, distorting their transmission.
Hijacking	The unauthorized use of a satellite for transmission, or seizing control of a signal, such as a broadcast, and replacing it with another.
Spoofing	The creation of false GPS signals to fool receivers into thinking that they are at a different location and/or time.
Scanning	A process for identifying, attacking, and stealing information from a targeted host.

WHO HAS CAPABILITIES FOR ELECTRONIC INTERFERENCE?

Open-source information collected in a report by the United Nations Institute for Disarmament Research (UNIDIR) suggests that all states with significant space programs have some EW capabilities. Technology that can interfere with satellite communication is mature and widely available and used, even at a consumer level by non-state actors. It is noteworthy that reports on global counterspace capabilities published by the Secure World Foundation and the Center for Strategic & International Studies indicate that major space programs are making significant investments in EW capabilities.

China: Information technology is central to China's military strategy. In 2015, China created a Strategic Support Force that integrated space, cyber, and electronic warfare missions. Capabilities that have reportedly been tested and deployed include jamming equipment that interferes with communications and radar systems, and with GNSS systems.

United States: The U.S. Counter Communications System, which became operational in 2004, uses radiofrequency interference to block a potential enemy's satellite communications. An upgraded Block 10.2 version was made available to the U.S. Space Force in 2020. Jamming capabilities have been the focus of various war-game exercises.

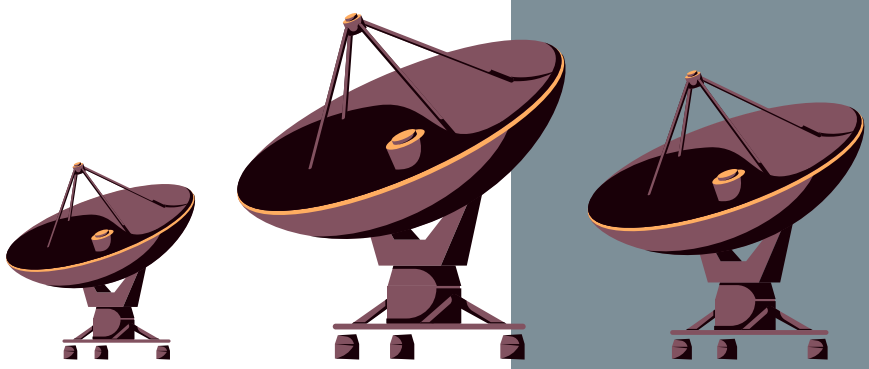
Russia: The Russian military operates some of the most advanced EW systems in the world. Known systems include:

- Tirada-2 and Bylina-MM, mobile systems that target communication satellites
- Krasukha-4, which targets radar reconnaissance satellites
- RB-301B "Borisoglebsk-2" and R-330Zh "Zhitel," which can jam GNSS signals.

Arms expert Bart Hendrickx reports that Russia is also developing a capability that deploys EW interference from orbiting satellites.

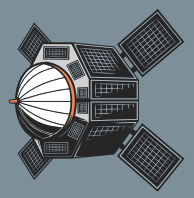
Japan: While the Japanese military has been authorized to develop satellite jamming capabilities, there is no evidence of deployment of such a system.

Other states known to have demon-



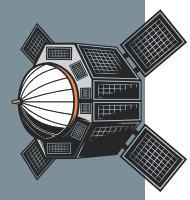
strated EW capabilities include:

- Turkey, which has a Radar Electronic Attack System similar to the Krasukha
- Iran, which frequently jams foreign communications satellites as a form of censorship
- North Korea, which is known to jam GNSS satellite signals.



HAS ELECTRONIC WARFARE BEEN USED IN CONFLICT?

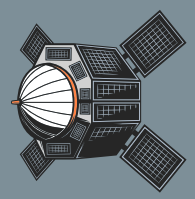
Electronic interference with satellite systems is currently used to target foreign satellites and is an active tool of conflict. It has been asserted that Russia deliberately jammed GPS signals in Norway and Finland during NATO exercises. Conflicts in Syria and Ukraine have featured electronic interference with both communications and reconnaissance satellites.



The 2020 U.S. military doctrine, published in the report Joint Electromagnetic Spectrum Operations, prioritizes protection measures, but includes activities to "exploit, attack, protect, and manage the electromagnetic operational environment" in the event of conflict.

WHAT MEASURES EXIST TO PROTECT AGAINST ELECTRONIC INTERFERENCE?

Protection requires specific electronic measures, which are not usually made public. However, available electronic protections against interference—intentional, natural, and accidental—include:



- data encryption
- error protection coding to increase the amount of interference that can be tolerated before communications are disrupted
- directional antennas that reduce interception or jamming vulnerabilities
- antennas that use natural or human-made barriers to protect from line-of-sight electronic attacks
- shielding and radio emission-control measures that reduce the radio energy that can be intercepted for surveillance or jamming purposes

- robust encryption onboard satellites.

Critical military systems often have more robust protections. The United States is developing a new, more secure, military 'M-code' signal as part of the next-generation GPS III system that will include new receivers with improved capabilities against jamming and spoofing. New military communications systems such as the Advanced Extremely High Frequency (AEHF) communications satellites and the Wideband Global SATCOM satellites are said to be highly secure. As well, the United States and NATO reportedly have access to countermeasures to defend against electronic attacks.

Nascent capabilities include laser-based communications, which face technical challenges from cloud cover and the degradation of signals as they travel through the atmosphere. Encryption capabilities based on quantum computing are being pursued in Canada, China, Japan, the EU, and the United States. In 2016, China became the first state to launch a quantum key entanglement experiment; in 2020, it conducted the first security communication demonstration.

For now, however, reliance on electronic systems and the electromagnetic spectrum means that satellite systems remain vulnerable to interference.

GOVERNANCE

The only legal prohibition on the non-peaceful uses of outer space in the Outer Space Treat is a restriction on the use, orbiting, or placement of weapons of mass destruction in space or on celestial bodies.

Article 45 of the International Telecommunications Union's constitution, which regulates the use and coordination of radio telecommunications, requires states "not to cause harmful interference" to communications in space. However, the constitution's Article 48 states that military communications are exempt. In recent years, this exception has been widely exploited to avoid registration of spectrum use with the ITU, but it also opens the door to greater use of EW tactics against such satellites.

For now, the ITU has a limited ability to respond to complaints. While there is movement to create an ITU database on interference, it is unlikely that states will report incidents of interference with military systems.

RESOURCES AND FURTHER READING

Chairman, Joint Chiefs of Staff (U.S.), Joint Electromagnetic Spectrum Operations, May22, 2020, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_85.pdf.

Todd Harrison et al., Space Threat Assessment 2020, CSIS, March 30, 2020, https://www.csis.org/analysis/space-threat-assessment-2020.

Bart Hendrickx, "Russia Gears Up for Electronic Warfare in Space (Part 1)," *The Space Review*, October 26, 2020, https://thespacereview.com/article/4056/1.

-----, "Russia Gears Up for Electronic Warfare in Space (Part 2)," *The Space Review*, November 2, 2020, https://www.thespacereview.com/article/4060/1.

Japan, *National Defense Program Guidelines for FY 2019 and Beyond*, December 18, 2018, http://www.cas.go.jp/jp/siryou/pdf/2019boueikeikaku_e.pdf.

James Johnson, "China's Vision of the Future Networked Battlefield," *The Diplomat*, April 26, 2017, https://thediplomat.com/2017/04/chinas-vision-of-the-future-networked-battlefield.

Dylan Malyasov, "OSCE Release Image of Modern Russian Jamming Systems in Eastern Ukraine," *Defence Blog*, April 3, 2019, https://defence-blog.com/news/army/osce-release-image-of-modern-russian-jamming-systems-in-eastern-ukraine.html.

Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, Republic of Estonia, Ministry of Defence, September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

Office of the Secretary of Defense (U.S.), *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2017*, May 15, 2017, https://www.defense.gov/Portals/1/Documents/pubs/2017_China_Military_Power_Report.PDF.

Rajeswari Pillai Rajagopalan, *Electronic and Cyber Warfare in Outer Space*, UNIDIR, May 2019, http://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf.

The State Council, People's Republic of China, *China's Military Strategy*,

White Paper, May 27, 2015, http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm.

Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," RealClearDefense.com, May 26, 2017, https://www.realcleardefense.com/articles/2017/05/26/russian_electronic_warfare_in_ukraine_111460.html.

The Today Press, "Japan to Discover Satellite-jamming Expertise," December 12, 2018, https://www.thetodaypress.com/2018/12/12/japan-to-explore-satellite-jamming-technology.

Brian Weeden & Victoria Samson, eds., *Global Counterspace Capabilities: An Open Source Assessment*, Secure World Foundation, April 2020, https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf.

Anatoly Zak, "Russian Anti-satellite Systems," RussianSpaceWeb, November 30, 2017, http://www.russianspaceweb.com/naryad.html.

Research contributed by William Campbell, University of Adelaide

www.spacesecurityindex.org