Satellite Jamming

A Technology Primer

BY PAVEL VELKOVSKY, JANANI MOHAN, AND MAXWELL SIMON

TYPE	CHARACTERISTICS	RISK FACTORS
Electronic Warfare	Precision, Persistance, Resiliency, Speed	Action-enabling, First-mover incentive
DOMAIN	**COUNTRY**	
Space, Land, Air, Sea	United States, Russia, China, Non-state actors	

> "The global threat of electronic warfare attacks against space systems will expand in the coming years in both number and types of weapons. Development will very likely focus on jamming capabilities."[1]
> – U.S. Director of National Intelligence Dan Coats, May 2017

Introduction

Satellite jamming is a form of electronic anti-satellite (ASAT) attack that interferes with communications traveling to and from a satellite by emitting noise of the same radio frequency (RF) within the field of view of the satellite's antennas.[2] Considered a growing threat by the U.S. intelligence community, jamming equipment operates across multiple domains.

All space capabilities are made up of a ground segment and a space segment, as well as the communication, or link, that ties them together. Satellite jammers threaten adversary capabilities via the communication segment and can be used from the ground, ocean surface, or air. In contrast to kinetic physical counterspace weapons, such as direct-ascent ASAT missiles, or non-kinetic physical weapons, such as lasers or high-powered microwaves (HPM), jamming does not physically damage satellites. It is an entirely reversible form of attack because once the jamming signal is turned off, adversary communications are restored.[3]

---

[1] U.S. Congress, Senate, Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community*, 115th Cong., 1st sess., (2017), 32.

[2] Brian Garino and Jane Gibson, "Space System Threats," AU-18 Space Primer (Maxwell Air Force Base: Air University Press, 2009), p. 274; Todd Harrison, *Future of MILSATCOM* (Washington, DC: Center for Strategic and Budgetary Assessments, 2013), p. 10; Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2019* (Washington, DC: CSIS, April 2019), 4.

[3] Ibid., 4.

There are two main types of satellite jamming. The first, uplink jamming, interferes with the signal going from a ground station or user terminal to the satellite. An RF signal of the same frequency as the targeted uplink signal is transmitted to the satellite, aiming to limit the satellite transponder from differentiating between the jamming signal and the actual signal.[4] The second type, downlink jamming, disrupts transmissions sent from the satellite to ground-based or airborne receivers using RF signals that mimic the frequency of the downlink signal. It aims to inhibit ground users from receiving transmissions from the satellite and only needs to be as strong as the signal being received on the ground.[5] Uplink jamming is considered more difficult because greater transmitter power is required to reach a given satellite's transponders. It could be more impactful, however, due to its ability to degrade the satellite's signal for all its users.[6] Because downlink jammers must be within the field of view of the receiving terminal's antenna, however, the effects of downlink jamming are more localized.

Jamming technology tends to be commercially available and relatively inexpensive. Satellite jamming systems are easy for states and non-state actors to develop given the relative low cost of their procurement and operation. There is a low threshold of technological competency required to perform jamming, and the technology is available to a plethora of actors across the globe. For example, interference with satellite signals has emanated from Indonesia, Cuba, Ethiopia, Libya, and Syria, among others.[7] Furthermore, simple terrestrial jamming systems are cheap and commercially available, despite being illegal under both U.S. FCC laws and rules of the International Telecommunications Union.[8] Recent improvements in such commercial jammers include reductions in size from jammers about the size of a Frisbee to those the size of a hockey puck.[9] As a consequence, there are few downsides to developing jamming capabilities.

Jamming can also occur accidentally: in 2015, U.S. military officials noted they were unintentionally jamming satellite communications an average of 23 times per month.[10] Purposeful jamming can be difficult to differentiate from accidental interference, making attribution more challenging. According to General John Hyten, then-commander of the Air Force Space Command, U.S. military personnel lack "awareness of what our own forces are doing in the spectrum, let alone of what an adversary might do."[11]

State of Play

Technology for satellite jamming has been in use for several decades. During World War II, states disrupted adversary radio broadcasts with the same principles used in satellite jamming. For example, in Germany, the

---

[4] Garino and Gibson, "Space System Threats," 275.

[5] Harrison, Johnson, and Roberts, *Space Threat Assessment 2019*, 4.

[6] Harrison, *Future of MILSATCOM*, 11.

[7] Ronald G. Wilgenbusch and Alan Heisig, "Command and Control Vulnerabilities to Communications Jamming," *Joint Force Quarterly* 69, no. 2 (2013): 58.

[8] **"**GPS, Wi-Fi, and Cell Phone Jammers Frequently Asked Questions," Federal Commerce Commission Enforcement Bureau, https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf; David Bosco, "When Can States Jam Radio Broadcasts?" *Foreign Policy*, October 5, 2012, https://foreignpolicy.com/2012/10/05/when-can-states-jam-radio-broadcasts/.

[9] Mike Gruss, "Companies See Market for Systems to Counter GPS Jamming Devices," SpaceNews.com, December 5, 2014, https://spacenews.com/37706companies-see-market-for-systems-to-counter-gps-jamming-devices/.

[10] Sydney J. Freedberg, Jr., "US Jammed Own Satellites 261 Times; What If Enemy Did?" Breaking Defense, December 2, 2015, http://breakingdefense.com/2015/12/us-jammed-own-satellites-261-times-in-2015-what-if-enemy-tried/.

[11] Ibid.

Nazis blocked radio signals from Western media outlets.[12] Since then, jamming has advanced to include disrupting the radio signals sent to and from civilian, commercial, and military satellites. The United States has developed its own electronic attack systems, such as the Counter Communications System (CCS).[13] The CCS is a land-based jammer development program operated by the U.S. Air Force to temporarily jam signals from adversaries' satellites. Originally operationalized in 2004, the CCS has undergone several advancements, most recently to upgrade its operating system to an updated block configuration.[14]

Several other countries have also developed satellite jamming capabilities, including China and Russia. These two countries own sophisticated satellite jamming vehicles, with stronger signals and more maneuverability than previous systems. In Russia, "electronic warfare systems"—such as the Krasukha-2, Zhitel, and Borisglobesk-2—have been deployed in battlefields in Syria to jam adversary communications.[15] These systems involve vehicles carrying satellite jamming devices originally developed in the 1980s with recent upgrades to increase maneuverability and reduce their vulnerability to heat-seeking missiles.[16] Although these developments have increased the military utility of Russian jamming, they are not a fundamental departure from previous jamming technology.[17] System vulnerabilities still remain, including that vehicles can only jam signals in one direction in a relatively narrow band of frequencies. Meanwhile, China also has formidable satellite jamming capabilities. Although it has focused resources on kinetic ASAT technologies, China originally bought jamming systems from Ukraine in the 1990s and used this technology to develop its own capabilities.[18] More recently, China deployed military-grade satellite jamming equipment on contested islands in the South China Sea, and U.S. intelligence suggests that they will have an operational ASAT weaponry system within the next few years.[19]

Militaries are becoming increasingly reliant on technology that is vulnerable to jamming due to the importance of constant coordination and communication in modern warfare, especially via satellites. As such, in addition to jamming capabilities, several states have developed countermeasures to reduce susceptibility to interference. One such method is frequency hopping spread spectrum (FHSS), which makes it more difficult for a jammer to match RF signals by using a pseudorandom sequence.[20] The sequence is known to the transmitter and receiver and is used to spread the signal across a wider frequency range, also making the signal harder for an adversary to detect.

---

[12] Serge Schmemann, "Soviet Union Ends Years of Jamming Radio Liberty," *New York Times*, December 1, 1988, https://www.nytimes.com/1988/12/01/world/soviet-union-ends-years-of-jamming-of-radio-liberty.html.

[13] "U.S. Satellite Jamming Systems," Spyflight, https://spyflight.co.uk/space/#Jamming.

[14] "Harris Awarded Counter Communication System Contract," *SIGNAL Magazine*, November 4, 2016, https://www.afcea.org/content/Blog-harris-awarded-counter-communication-system-contract.

[15] Sergey Sukhankin, "Russian Electronic Warfare in Ukraine: Between Real and Imaginable," Eurasia Daily Monitor, May 24, 2014.

[16] Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Tallinn, Estonia: International Center for Defense and Security, September 2017).

[17] Ibid., 14.

[18] Todd Harrison, Kaitlyn Johnson, and Thomas G. Roberts, *Space Threat Assessment 2018* (Washington, DC: CSIS, April 2018), 10.

[19] Michael R. Gordon and Jeremy Page, "China Installed Military Jamming Equipment on Spratly Islands, U.S. Says," *Wall Street Journal*, April 9, 2018, https://www.wsj.com/articles/china-installed-military-jamming-equipment-on-spratly-islands-u-s-says-1523266320; Sandra Erwin, "U.S. Intelligence: Russia and China Will Have 'operational' Anti-satellite Weapons in a Few Years," Space News, September 14, 2018, https://spacenews.com/u-s-intelligence-russia-and-china-will-have-operational-anti-satellite-weapons-in-a-few-years/.

[20] Harrison, *Future of MILSATCOM*, 25.

Within the space segment of the information transmission process, antenna notching and nulling can be used to improve resistance to jamming. Antenna notching blocks signals of certain frequencies from being received, while antenna nulling blocks signals transmitted from a specific geographical location, such as the location of a suspected uplink jammer.[21]

To avoid proliferating transmission errors that arise from uplink jamming back to receivers via the downlink, systems can decode information on a satellite before retransmitting it to another user in a process called on-board processing.[22] Finally, since RF interference tends to occur in bursts rather than in a steady and predictable stream, successful jamming leads to errors in contiguous parts of a transmission of data. As such, interleaving describes the process whereby data is shuffled before transmission and then reconfigured after it is received. This strategy improves resistance by lowering the likelihood that a burst of interference would create multiple errors within a single data packet.[23] As a result of the shuffling and reshuffling process, however, interleaving slows data transmission speed. When used together, these defenses can significantly improve resilience to jamming.

In the United States, recent research and development has focused on building protection into satellite communications. The Trump administration's FY 2020 budget requested $174 million to accelerate development of a Protected Tactical Satellite Communications (PTS) system and proposed another $105 million for development of the PTS ground system known as the Protected Tactical Enterprise Service (PTES).[24] The Air Force plans to eventually complete a family of PTS systems, with space, ground, and gateway segments all connected.[25] It has also already developed Advanced Extremely High Frequency satellites that incorporate the previously mentioned jamming technology to achieve "a high degree of protection."[26]

Effects on Situational Awareness

Satellite jamming capabilities are often intended to disrupt the sensor-shooter kill chain by lowering an opponent's level of situational awareness—their ability to characterize the operating environment and detect attacks. Jamming can disrupt missile warning systems, impede access to GPS, and decrease *precision* and *persistence*.[27] Interference with transmissions could interrupt one's ability to continuously collect and transmit data, thereby decreasing the data's reliability and accuracy.

Jamming capabilities would also, by definition, degrade an opponent's *resiliency***.** In a contested environment, jamming could make it harder to effectively rely on missile warning satellites, perform reconnaissance, collect intelligence on the battlefield, and maintain communication. Opponent forces would have lower situational awareness as they would acquire less intelligence about the battlefield and would have more trouble communicating among themselves.

---

[21] Harrison, *Future of MILSATCOM*, 26.

[22] Ibid.

[23] Ibid.

[24] Sandra Erwin, "Military Space Gets Big Boost in Pentagon's $750 Billion Budget Plan," Space News, April 1, 2019, https://spacenews.com/militaryspace-gets-big-boost-in-pentagons-750-billio/.

[25] Ibid.

[26] Harrison, Johnson, and Roberts, *Space Threat Assessment 2018*, 1.

[27] Todd Harrison, "The Risks a War in Space Poses for Nuclear Stability on Earth," in Caroline Dorminey and Eric Gomez eds., *America's Nuclear Crossroads* (Washington, DC: Cato Institute, 2019), 30.

By disrupting communication reliability and interfering with access to radar technology, satellite jamming could also degrade the *speed* at which an opponent could collect and act on information.

Risk Factors for Strategic Stability

Jamming can be action-enabling due to its ability to heighten situational awareness relative to an adversary. By disrupting an opponent's ability to monitor, communicate, and coordinate forces across a conflict theater by jamming communications and GPS satellites, for example, satellite jamming would reduce the opponent's understanding of the battlefield and ability to react.

As such, jamming capabilities pose a short-term risk to crisis stability due to their ability to provide a first-mover advantage. By disabling the communications and GPS capabilities that allow a state to project force in response to another's military action, they could sufficiently weaken an adversary's short-term ability to effectively respond. With less reliable information about the actions of the first-mover and fewer conventional capabilities to counter those actions, escalation could be more likely.

In this sense, jamming capabilities present a risk to strategic stability in that they could embolden an offensively-minded state to act more aggressively. For example, the U.S. Army reports that the maneuver brigades of the Russian Ground Forces (RGF) maintain large electronic warfare companies that are capable of jamming and disrupting communications, GPS, and ground, airborne, and maritime radars at a range of up to 300 kilometers.[28] In a hypothetical invasion, such capabilities could be used to impede an opposing state's communications and lower their sensors' ability to detect aircraft or missile launches, offering significant advantages. More concretely, after losing multiple aircraft to Georgian air defense systems in the first phases of Russia's 2008 invasion of Georgia, the RGF deployed ground-based jamming platforms that significantly tilted the balance in their favor.[29]

Outside of open military conflict, jamming capabilities offer additional advantages relative to other ASAT weapons. Kinetic ASAT weapons are highly destructive, with irreversible effects on their targeted satellite or ground station. They tend to be easily attributable because many states can identify the source of kinetic ASAT attacks; the launch of direct-ascent weapons is traceable, and the orbital data of a co-orbital weapon can usually be tracked back to its initial deployment.[30] A successful attack would be known to both parties immediately as well because it would produce debris and other physical damage.[31]

However, unintentional satellite interference is very common. Even in cases of deliberate satellite interference, jammers can be hard to pinpoint because they can be highly mobile and intermittent in operation.[32] They can also blend in with commercial systems such as uplink news vehicles, appearing harmless.[33] Even if found, due to the size of less sophisticated jamming equipment, the technology can be placed in a population center or in a third country where an adversary might be unwilling to target it. There is a large offense-defense cost differential

---

[28] Maj. Gen. Morgan J. Spring-Glace, "Return of Ground-Based Electronic Warfare Platforms and Force Structure," *Military Review* (July/August 2019): 42, https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JA-19/Spring-Glace-Electronic-Warfare.pdf.

[29] Ibid., 43.

[30] Harrison, Johnson, and Roberts, *Space Threat Assessment 2019*, 3.

[31] Ibid.

[32] Wilgenbusch and Heisig, "Command and Control Vulnerabilities to Communications Jamming," 61.

[33] Ibid.

in favor of satellite jammers, as they are much easier to procure, deploy, and operate than they are to locate and destroy.

Due to the attribution and detection challenges associated with jamming, it is reasonable to assume that the likelihood of jamming-related vulnerabilities being exploited is higher than that of kinetic ASAT weapons.[34] Insofar as jamming is reversible and neither kinetic nor publicly visible, it operates somewhere below open warfare, constituting a "gray zone" tactic that can be used in peacetime without a high likelihood of escalation. Most simply, if an attack cannot be conclusively attributed in a timely fashion, retaliation is less likely. For example, Iran has frequently jammed satellite communication broadcasts like the British Broadcasting Corporation and Voice of America at times of heightened international pressure without major repercussions.[35] North Korea regularly jams GPS signals transmitting into South Korea, and Russia has jammed GPS signals during NATO military exercises.[36] In each instance, actors hostile to the United States and its allies have avoided significant retaliatory action.

Jamming operates somewhere below open warfare, constituting a "gray zone" tactic that can be used in peacetime without a high likelihood of escalation.

Until the 1990s, policymakers had long assumed that adversaries would be deterred from attacking satellites involved with nuclear command and control. Because space-systems first evolved during the Cold War to primarily support nuclear systems, nuclear deterrence on Earth was closely connected with deterrence in space. Nonetheless, today it is conceivable that an adversary may unintentionally interfere with satellites involved in nuclear systems when seeking only to disrupt conventional capabilities. Space systems have become heavily integrated with conventional combat missions, and many satellites that were once solely used to support nuclear forces are now used in conventional missions as well.[37] In nonnuclear conflict, then, an adversary could seek to jam satellites that are being used to support conventional operations, even if those systems are also used in nuclear command and control.[38] Given the dual-use nature of U.S. space systems, the intentions of an adversary seeking to disrupt conventional capabilities, but inadvertently interfering with nuclear systems as well, could be misunderstood and lead to escalation through miscalculation.[39]

Conclusion

Satellite jamming capabilities decrease certainty surrounding adversary force posture and by consequence have the capacity to decrease strategic stability. During conflicts, these capabilities may also serve as an "equalizer." States with advanced militaries, like the United States, Russia, and China, have much more robust space systems and rely upon them for command and control. While they provide immense military advantages, they are also very expensive to develop and operate. Satellite jammers, however, are relatively inexpensive and require a low technological competency, allowing a wide range of states to disrupt superpower operations.

---

[34] Harrison, *Future of MILSATCOM*, 14.

[35] Kathleen H. Hicks et al., *By Other Means: Campaigning in the Gray Zone* (Washington, DC: CSIS, July 2019), 11.

[36] Harrison, Johnson, and Roberts, *Space Threat Assessment 2019*, 33; Hicks et al., *By Other Means*, p. 9.

[37] Harrison, "The Risks a War in Space Poses for Nuclear Stability on Earth," 32.

[38] Ibid., 34.

[39] Ibid.

Furthermore, given that satellite jamming does not cause permanent physical damage and that timely attribution can be difficult, the escalatory potential is relatively low.

Nonetheless, if these capabilities were used pre-emptively and were highly effective at rendering large parts of U.S. space systems inoperable, they would ultimately leave the United States with fewer conventional options to respond. And since many satellites now assist with nuclear command and control as well as conventional missions, it is possible that nuclear capabilities could be inadvertently degraded by adversaries seeking only to disrupt conventional missions. Miscommunication and escalation could then become more likely, especially in a crisis scenario.

Still, advanced militaries are developing multiple techniques to ensure satellites are highly resistant to jamming technology. Jamming capabilities could be highly disruptive, but more often, they constitute another "gray zone" tactic operating somewhere below the threshold of open war.

ABOUT CSIS

Established in Washington, D.C. over 50 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to providing strategic in-sights and policy solutions to help decisionmakers chart a course toward a better world.

In late 2015, Thomas J. Pritzker was named chairman of the CSIS Board of Trustees. Mr. Pritzker succeeded former U.S. senator Sam Nunn (D-GA), who chaired the CSIS Board of Trustees from 1999 to 2015. CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

Founded in 1962 by David M. Abshire and Admiral Arleigh Burke, CSIS is one of the world's preeminent international policy institutions focused on defense and security; regional study; and transnational challenges ranging from energy and trade to global development and economic integration. For eight consecutive years, CSIS has been named the world's number one think tank for defense and national security by the University of Pennsylvania's "Go To Think Tank Index."

The Center's over 220 full-time staff and large network of affiliated scholars conduct research and analysis and develop policy initiatives that look to the future and anticipate change. CSIS is regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer bipartisan recommendations to improve U.S. strategy.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).