TYPES OF COUNTERSPACE WEAPONS

SPACE IS AN INCREASINGLY IMPORTANT ENABLER of economic and military power. The December 2017 United States National Security Strategy prioritizes maintaining U.S. leadership and freedom of action in this critical domain, but it notes that:

> *Many countries are purchasing satellites to support their own strategic military activities. Others believe that the ability to attack space assets offers an asymmetric advantage and as a result, are pursuing a range of anti-satellite (ASAT) weapons. The United States considers unfettered access to and freedom to operate in space to be a vital interest. Any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing.*[1]

Counterspace weapons vary in the types of effects they create, and the level of technological sophistication and resources required to develop and field them. They also differ in how they are employed and how difficult they are to detect and attribute. The effects of these weapons can be temporary or permanent, depending on the type of system and how it is used. The country-by-country assessments that follow this section group counterspace weapons into four broad categories: kinetic physical, non-kinetic physical, electronic, and cyber.

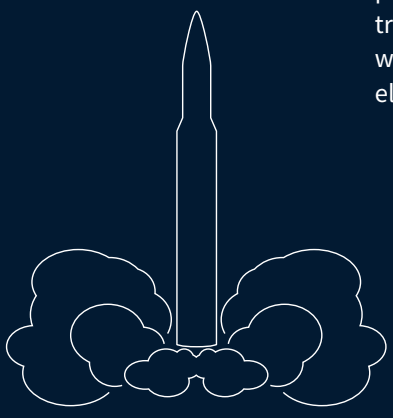

Illustration A ballistic missile can be used as a kinetic physical counterspace weapon.

KINETIC PHYSICAL

KINETIC PHYSICAL COUNTERSPACE weapons attempt to strike directly or detonate a warhead near a satellite or ground station. A direct-ascent ASAT weapon attempts to strike a satellite using a trajectory that intersects the target satellite without placing the interceptor into orbit. Ballistic missiles and missile defense interceptors can be modified to act as direct-ascent ASAT weapons provided they have sufficient energy to reach the target satellite's orbit. A co-orbital ASAT weapon differs from a direct-ascent weapon because it is first placed into orbit. When commanded, the satellite then maneuvers to strike its target. Co-orbital ASATs can remain dormant in orbit for days or even years before being activated. A key technology needed to make both direct-ascent and co-orbital ASAT weapons effective is the ability to detect, track, and guide the interceptor into a target satellite. An onboard guidance system requires a relatively high level of technological sophistication and significant resources to test and deploy.[2]

Ground stations are vulnerable to kinetic physical attacks by a variety of conventional military weapons, from guided missiles and rockets at longer ranges to small arms fire at shorter ranges. Because they are often highly visible, located outside of the United States, and are more accessible than objects in space, ground stations can be an easier target for adversaries seeking to disrupt or degrade space systems. Even if the ground stations themselves are difficult to attack directly, they can be disrupted indirectly by attacking the electrical power grid, water supply, and the high-capacity communications lines that support them.

Kinetic physical attacks generally have irreversible effects on the satellites and ground stations targeted. These counterspace weapons are likely to be attributable because the United States and others can identify the source of a direct-ascent ASAT launch or ground attack and can, in theory, trace a co-orbital ASAT's orbital data back to its initial deployment. In both cases, the attacker is likely to know whether its attack is successful almost immediately because the effects would be publicly visible through orbital debris or a damaged ground station.

NON-KINETIC PHYSICAL

NON-KINETIC COUNTERSPACE weapons, such as lasers, high-powered microwave (HPM) weapons, and electromagnetic pulse (EMP) weapons, can have physical effects on satellites and ground stations without making physical contact. These attacks operate at the speed of light and, in some cases, can be less visible to third-party observers and more difficult to attribute.

High-powered lasers can be used to damage or degrade sensitive satellite components, such as solar arrays. Lasers can also be used to temporarily dazzle or permanently blind mission-critical sensors on satellites. Targeting a satellite from Earth with a laser requires high beam quality, adaptive optics, and advanced pointing control to steer the laser beam as it is transmitted through the atmosphere—technology that is costly and requires a high degree of sophistication.[3] A laser can be effective against a sensor on a satellite if it is within the field of view of the sensor, making it possible to attribute the attack to its approximate geographical origin. The attacker, however, will have limited ability to know if the attack was successful because it would not likely produce debris or other visible indicators.

An HPM weapon can be used to disrupt a satellite's electronics, corrupt data stored in memory, cause processors to restart, and, at higher

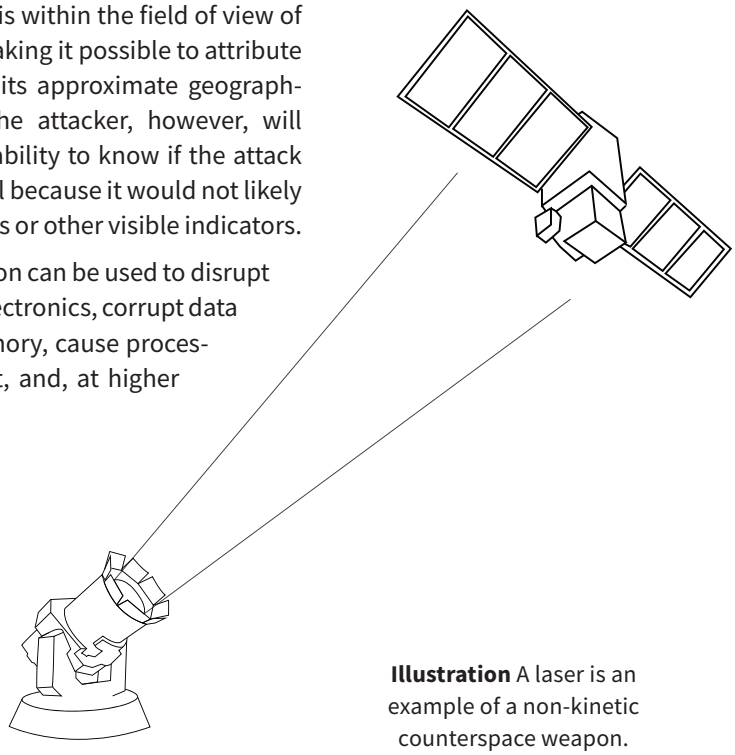

Illustration A laser is an example of a non-kinetic counterspace weapon.

power levels, cause permanent damage to electrical circuits and processors. A front-door HPM attack uses a satellite's own antennas as an entry path, while a backdoor HPM attack attempts to enter through small seams or gaps around electrical connections and shielding.[4] Because electromagnetic waves disperse and weaken over distance and the atmosphere can interfere with transmission at high power levels, an HPM attack against a satellite is best carried out from another satellite in a similar orbit. Both front-door and back-door HPM attacks can be difficult to attribute to an attacker, and as with a laser weapon, the attacker may not know if the attack has been successful.

The use of a nuclear weapon in space can be an indiscriminate form of non-kinetic physical attack. While a nuclear detonation would have immediate effects for satellites within range of its EMP, it also creates a high radiation environment that accelerates the degradation of satellite components over the long term for unshielded satellites in the affected orbital regime.[5]

ELECTRONIC

ELECTRONIC ATTACKS TARGET the means through which space systems transmit and receive data by jamming or spoofing radio frequency (RF) signals. Jamming is a form of electronic attack that interferes with RF communications by generating noise in the same frequency band and within the field of view of the antenna on the targeted satellite or receiver. An uplink jammer interferes with the signal going from the Earth to a satellite, such as the command and control uplink. Downlink jammers target the signal from a satellite as it propagates down to users on the Earth. User terminals with omnidirectional antennas, such as many GPS receivers and satellite phones, have a wider field of view and thus are susceptible to downlink jamming from a wider range of angles on the ground.[6]

The technology needed to jam many types of satellite signals is commercially available and relatively inexpensive. Jamming is a reversible form of attack because once a jammer is turned off, communications return to normal. Jamming can also be difficult to detect or distinguish from accidental interference, making attribution and awareness more difficult. In 2015, General John Hyten, then-commander of Air Force Space Command, noted that the U.S. military was unintentionally jamming its own communications satellites an average of 23 times per month.[7]

Spoofing is a form of electronic attack where the attacker tricks a receiver into believing a fake signal, produced by the attacker, is the real signal it is trying to receive. Spoofing the downlink from a satellite can be used to inject false or corrupted data into an adversary's communications systems. If an attacker successfully spoofs the command and control uplink signal to a satellite, it could take control of the satellite for nefarious purposes.

Through a type of spoofing called "meaconing," even the encrypted military GPS signals can be spoofed. Meaconing does not require cracking the GPS encryption because it merely rebroadcasts a time-delayed copy of the original signal without decrypting it or altering the data.[8] Like jammers, once a spoofer is developed, it is relatively inexpensive to produce and deploy in large numbers and can be proliferated to other state and non-state actors.

CYBER

UNLIKE ELECTRONIC ATTACKS, which interfere with the transmission of RF signals, cyberattacks target the data itself and the systems that use this data. The antennas on satellites and ground stations, the landlines that connect ground stations to terrestrial networks, and the

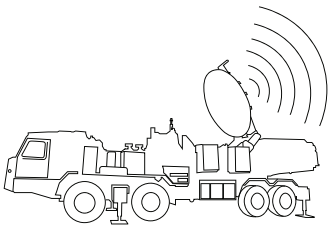

Illustration A truck-mounted jammer is a type of electronic counterspace weapon.

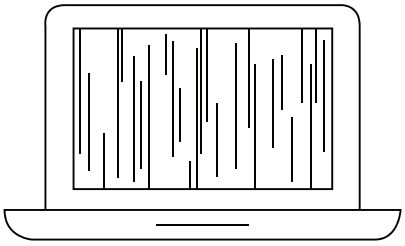

Illustration
Cyberattacks can be used to take control of a satellite and damage or destroy it.

user terminals that connect to satellites are all potential intrusion points for cyberattacks. Cyberattacks can be used to monitor data traffic patterns (i.e., which users are communicating), to monitor the data itself, or to insert false or corrupted data in the system. While cyberattacks require a high degree of understanding of the systems being targeted, they do not necessarily require significant resources to conduct. Cyberattacks can be contracted out to private groups or individuals, which means that a state or non-state actor that lacks internal cyber capabilities may still pose a cyber threat.[9]

A cyberattack on space systems can result in data loss, widespread disruptions, and even permanent loss of a satellite. For example, if an adversary can seize control of a satellite through a cyberattack on its command and control system, the attack could shut down all communications and permanently damage the satellite by expending its propellant supply or damaging its electronics and sensors. Accurate and timely attribution of a cyberattack can be difficult, if not impossible, because attackers can use a variety of methods to conceal their identity, such as using hijacked servers to launch an attack.

THREAT CHARACTERISTICS

The types of counterspace threats described above have distinctly different characteristics that make them more suitable for use in some scenarios than others. As shown in Table 1, some types of counterspace threats are difficult to attribute or have fully reversible effects, such as mobile jammers. High-powered lasers, for example, are “silent” and can carry out an attack with little public awareness that anything has happened. Other types of counterspace weapons produce effects that make it difficult for the attacker to know if the attack was successful, and some produce collateral damage that can affect space systems other than the one being targeted.

Counterspace weapons that are reversible, difficult to attribute, and have limited public awareness are ideally suited for situations in which an opponent may want to signal resolve, create uncertainty in the mind of its opponent, or achieve a fait accompli without triggering an escalatory response. For example, an adversary that wants to deter the United States from intervening in a situation may believe that such attacks will stay below the threshold for escalation (i.e., not trigger the very thing it is trying to prevent) while creating significant operational challenges for the United States that make the prospect of intervention more costly and protracted. Conversely, counterspace weapons that have limited battle damage assessment or that risk collateral damage may be less useful to adversaries in many situations. Without reliable battle damage assessment, for example, an adversary cannot plan operations with the confidence that its counterspace actions have been successful. Furthermore, weapons that produce collateral damage in space, such as large amounts of space debris, run the risk of escalating a conflict and turning other nations against the attacker.

Table 1

TYPES OF COUNTERSPACE WEAPONS

	Kinetic Physical			Non-Kinetic Physical			
Types of Attack	**Ground Station Attack**	**Direct-Ascent ASAT**	**Co-Orbital ASAT**	**High Altitude Nuclear Detonation**	**High-Powered Laser**	**Laser Dazzling or Blinding**	**High-Powered Microwave**
Attribution	Variable attribution, depending on mode of attack	Launch site can be attributed	Can be attributed by tracking previously known oribt	Launch site can be attributed	Limited attribution	Clear attribution of the laser's location at the time of attack	Limited attribution
Reversibility	Irreversible	Irreversible	Irreversible or reversible depending on capabilities	Irreversible	Irreversible	Reversible or irreversible; attacker may or may not be able to control	Reversible or irreversible; attacker may or may not be able to control
Awareness	May or may not be publicly known	Publicly known depending on trajectory	May or may not be publicly known	Publicly known	Only satellite operator will be aware	Only satellite operator will be aware	Only satellite operator will be aware
Attacker Damage Assessment	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Near real-time confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled	No confirmation of success	Limited confirmation of success if satellite begins to drift uncontrolled
Collateral Damage	Station may control multiple satellites; potential for loss of life	Orbital debris could affect other satellites in similar orbits	May or may not produce orbital debris	Higher radiation levels in orbit would persist for months or years	Could leave target satellite disabled and uncontrollable	None	Could leave target satellite disabled and uncontrollable

	Electronic			Cyber		
Types of Attack	**Uplink Jamming**	**Downlink Jamming**	**Spoofing**	**Data Interccept or Monitoring**	**Data Corruption**	**Seizure of Control**
Attribution	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Modest attribution depending on mode of attack	Limited or uncertain attribution	Limited or uncertain attribution	Limited or uncertain attribution
Reversibility	Reversible	Reversible	Reversible	Reversible	Reversible	Irreversible or reversible, depending on mode of attack
Awareness	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	May or may not be known to the public	May or may not be known to the public	Satellite operator will be aware; may or may not be known to the public	Satellite operator will be aware; may or may not be known to the public
Attacker Damage Assessment	No confirmation of success	Limited confirmation of success if monitoring of the local RF environment is possible	Limited confirmation of success if effects are visible	Near-real time confirmation of success	Near-real time confirmation of success	Near-real time confirmation of success
Collateral Damage	Only dirupts the signals targeted and possible adjacent frequencies	Only disrupts the signals targeted and possible adjacent frequencies	Only corrupts the specific RF signals targeted	None	None	Could leave target satellite disabled and uncontrollable