AN OVERVIEW OF SPACE ELECTRONIC WARFARE

White Paper | Version 02.00 | Tim Fountain and Leander Humbert

ROHDE&SCHWARZ
Make ideas real

CONTENTS

LIST OF FIGURES

ABSTRACT

This paper is intended to give the reader an overview of electronic/electromagnetic warfare (EW) in space, the space domain ecosystem, and offensive and defensive measures for space EW. The paper starts with a brief overview of the space domain, satellite orbits and the basics of satellite communications. Next, the paper discusses the satcom segments and the military uses of the electromagnetic spectrum. The paper reviews the basics of offensive, defensive and cyber operations as it relates to space EW and gives examples of operational systems. In the solutions section, the paper discusses useful technologies that can be applied to space EW, including link budgeting, communications monitoring, signal analysis, carrier-under-carrier detection, interference hunting, capturing short-duration events, handheld interference hunting, and high bandwidth recording to capture long-term events.

All information presented in this paper was acquired from publicly available sources.

FAIR USE STATEMENT

"All armies prefer high ground to low, and sunny places to dark. With regard to precipitous heights, if you are beforehand with your adversary, you should occupy the raised and sunny spots, and there wait for him to come up." [Sun Tzu, The Art of War]

1 OVERVIEW

Space is globally recognized as being critical to economic success, national security and societal well-being. It is also a warfighting domain recognized by most nation state military forces. For instance, the establishment of the US Space Force in 2019 highlighted the importance of space as a domain to the US Department of Defense (DoD) alongside the more traditional branches of the DoD.

EW is a vital and proven capability for operating successfully in complex, contested environments. In the space domain, EW has the potential to be a game changer due to its non-kinetic force protection that avoids the generation of additional space debris, which is already an issue of major concern for safe space operations.

Space presents an expanded electromagnetic environment when compared to the terrestrial environment where atmospheric effects, terrain, flora and the curvature of the earth all conspire to constrain electromagnetic propagation. The lack of constraints in space opens up new sensing, communications, force protection and force projection capabilities. These new operational dimensions also present opportunities for technological and strategic surprise. Since space EW is most often associated with satellites and their communications links, it is important to note that the earth's atmosphere and physical distances also counterbalance the benefits of pure space transmission and play a critical role in determining what is possible with today's technology.

As nation states develop their space capabilities, spectrum superiority is just as important in space as it is for terrestrial operations. Space EW faces the significant challenge of operating throughout the entire electromagnetic spectrum under demanding environmental conditions. This in turn will drive the need for new EW techniques, technologies and systems that operate over a much wider spectrum and bandwidth.

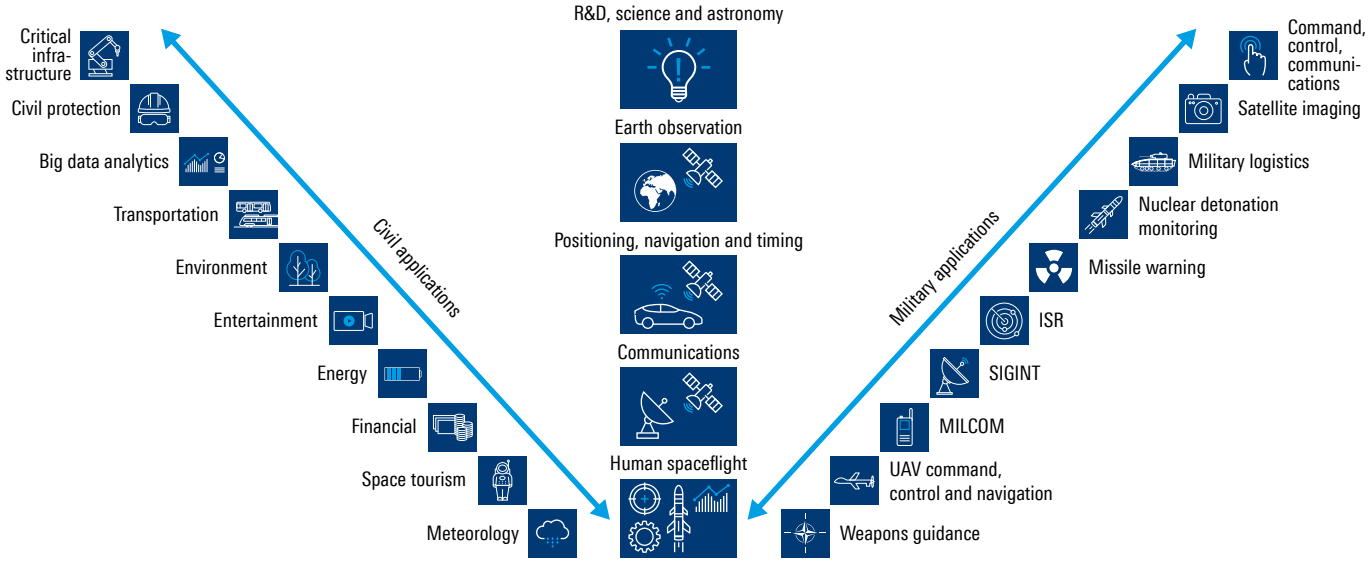
2 SPACE DOMAIN ECOSYSTEM

The space domain ecosystem is shown in Figure 1. In the middle, the endeavors that are most commonly associated with space are shown in square blocks, including:

- R&D, science and astronomy, such as the International Space Station (ISS)
- Earth observation, such as weather satellites
- Position, navigation and timing systems, such as GNSS
- Communications, such as Iridium, and satellite based TV, such as direct TV
- Human spaceflight

Figure 1: Space domain ecosystem

The left side shows civilian space applications while the right side shows military applications of space. This diagram demonstrates the complexity and demands placed on the space domain.



2.1 Orbits and segments

It is impossible to discuss satellites and space EW without a brief introduction to satellite-specific orbits and segments. Table 1 gives an overview of the different satellite orbits. As can be seen, they all have unique characteristics, advantages and disadvantages.

2.1.1 Low earth orbit (LEO) satellites

Low earth orbit (LEO) satellites are a growing area for commercial small satellite innovation. Most of these LEO large constellations are collectively referred to as "NEWSPACE" and/or "SMALLSAT", alluding to their small physical size. As the LEO name suggests, these satellite constellations are close in to the earth, at about 1200 miles, and therefore their footprint over the earth is small, requiring a large number of satellites to provide whole earth coverage. As an example, the SpaceX StarLink constellation will eventually number more than 10000 satellites. Due to their lower orbits, the satellites also need less transmit power for their intended coverage footprint and exhibit low latency when compared to higher orbit mid earth orbit (MEO) and geostationary orbit (GEO) satellites. LEO satellites will eventually fall back to earth (deorbit) due to atmospheric drag. Other challenges of LEO satellites include the need for crosslink data connections between satellites and a relatively short time window for connection to ground stations.

2.1.2 Mid earth orbit (MEO) satellites

Mid earth orbit (MEO) satellites occupy orbits between 1 200 miles and 22 000 miles. The MEO orbits include the two zones of energetically charged particles known as the Van Allen belts, which can damage satellite electronics. A satellite in the semi-synchronous orbit at an altitude of approximately 12 600 miles has an orbital period of 12 hours and passes over the same two spots on the equator every day. This reliably predictable orbit is used by the GNSS constellations, examples of which include GPS, GLONASS, Galileo and BeiDou, and provides consistent low latency communications links. A disadvantage of MEO satellites is the need for dual tracking antennas for continuous connectivity.

2.1.3 Highly elliptical orbit (HEO) satellites

Highly elliptical orbit (HEO) satellites utilize an elliptic orbit with high eccentricity and include the Molniya orbit, named after the Molniya Soviet communications satellites that utilize these orbits, and the Tundra orbit. Elongated HEO orbits have the advantage of a long dwell time over a specific point in the sky (as viewed from earth) during the approach to and descent from an apogee. The effect of a long apogee is the appearance that the space vehicle appears to move slowly and remain at high altitude over high-latitude ground sites for long periods of time. This apparent motion makes the HEO orbit useful for communications satellites. An example of a HEO satellite is the Sirius XM satellite radio system. It uses inclined HEO orbits, specifically the Tundra orbits, to keep two satellites positioned above North America, while a third satellite rapidly sweeps through the southern parts of North America during its 24-hour orbit.

2.1.4 Geostationary orbit (GEO) satellites

Geostationary or geosynchronous orbit (GEO) satellites are found in geostationary orbits around 22 000 miles from earth. Their location with respect to earth is constant and fixed. Since their location is fixed with respect to earth, the ground segment equipment does not need to track the satellite. Since the satellite is so far away from earth, a single GEO satellite can cover about 1/3 of the earth's surface area. The distance also creates large latencies and large signal loss. Since GEO satellites occupy a single ring above the equator, there are a limited number of orbital slots available, and consequentially high demand for those slots.

Table 1: Overview of different satellite orbits

Orbit	Distance (in miles)	Advantages	Disadvantages	Example
LEO	1 200	► Global coverage ► Low latency	► Traffic switching between satellites ► Large number of satellites needed for full coverage	StarLink, Iridium
MEO	1 200 to 22 000	► Global coverage ► Predicable locations	► Traffic switching between satellites	GPS, Galileo, SpaceLink
HEO	25 000 at apogee	► Polar coverage ► Lower number of satellites	► Traffic switching between satellites ► Variation in distance/coverage ► Radiation in Van Allen belt ► Variable latency	SirusXM, QZSS
GEO	22 000	► Stationary ground equipment ► Can cover 1/3 of the earth with a single satellite	► Limited polar coverage ► Large signal path loss ► Large latency	DirecTV, MUOS, AEHF

Figure 2: Pictorial representation of different satellite orbits

Courtesy of the US Defense Intelligence Agency [1]

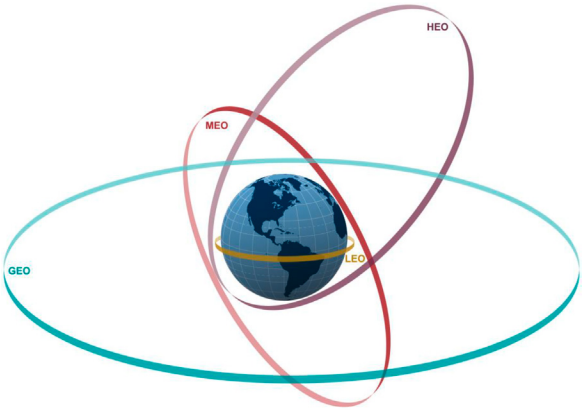
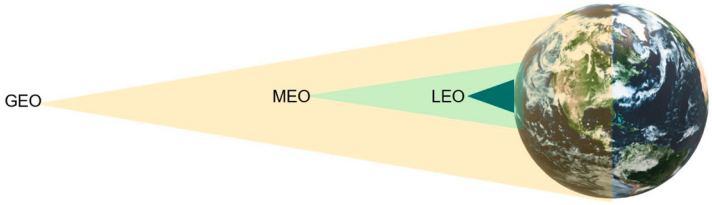


Figure 3: Earth coverage vs. satellite orbit



2.2 Satellite communications overview

As shown in Figure 4, the satellite ecosystem consists of two main segments: the space segment comprising launch and satellites, and the earth segment comprising the ground segment and user segment. These are described in more detail below.

2.2.1 Launch segment

The launch segment is concerned with launching the satellite into the correct orbit. Technologies included in the launch segment are the rocket and launch facilities. The location of the launch facilities is dependent on the desired orbit. For instance, most GEO satellites would be launched from locations along the equatorial plane such as Guiana Space Center in Kourou, French Guiana.

2.2.2 Space segment

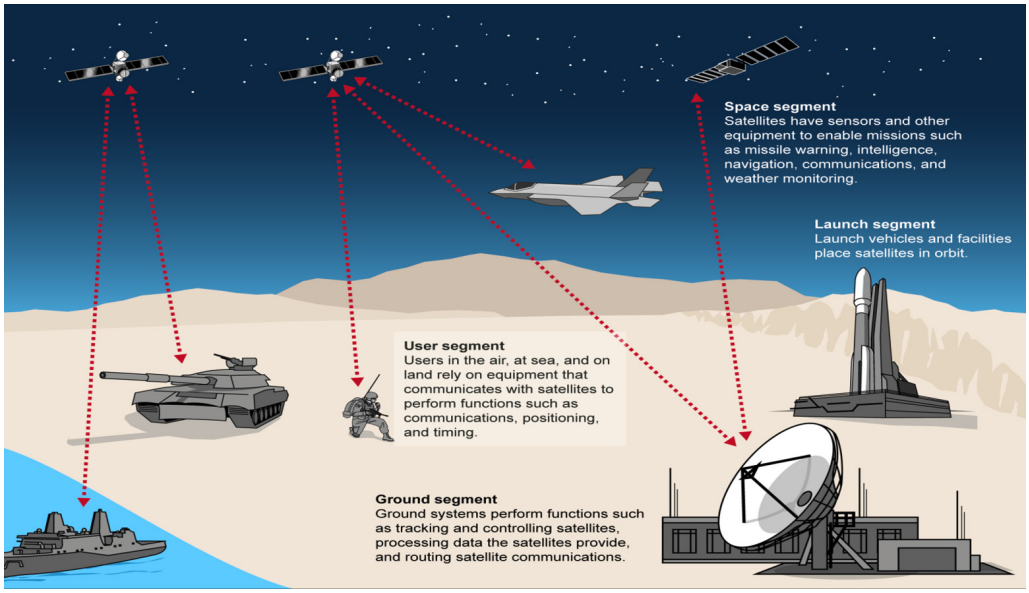
The space segment comprises the satellite or satellite constellations. This segment includes the equipment associated with the satellite, such as the antennas/transponders, attitude positioning systems, thermal management systems, tracking, telemetry and control (TT&C) systems, power/solar arrays, payload and buses.

2.2.3 User segment

The user segment consists of the end users/consumers of the satellite provided service and can be land, sea or air based. The user equipment communicates with the satellite(s) to perform functions such as communications, imaging, positioning and timing.

Figure 4: The various segments of a satellite ecosystem

Source: [2]

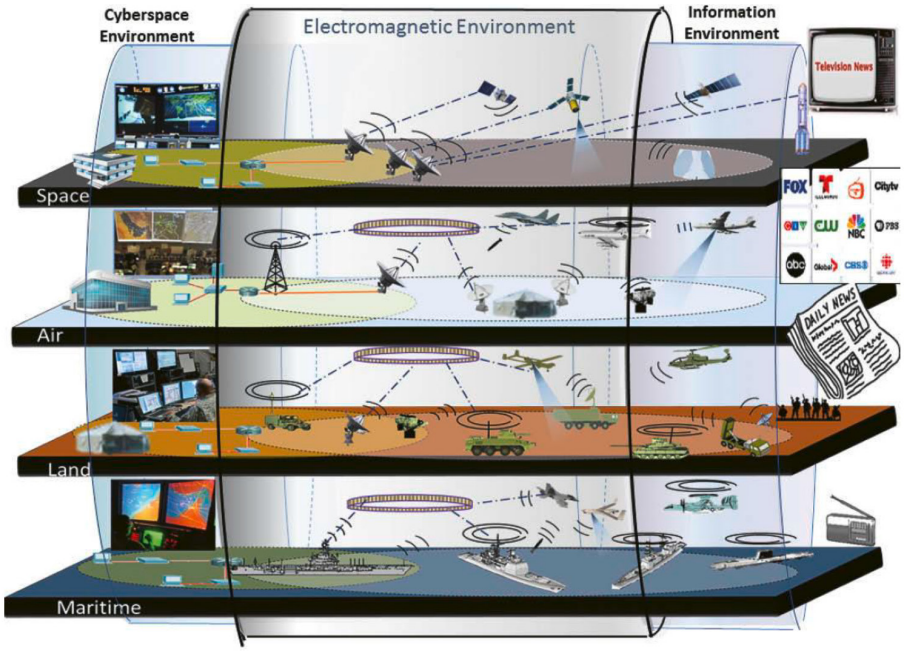


3 DEFINITION OF SPACE ELECTRONIC WARFARE

NATO defines electronic/electromagnetic warfare (EW) as "a military action that exploits electromagnetic energy, both actively and passively, to provide situational awareness and create offensive and defensive effects". It is warfare within the electromagnetic spectrum (EMS) and involves the military use of electromagnetic energy to prevent or reduce an enemy's effective use of the EMS while protecting its use for friendly forces.

Figure 5: Electromagnetic operations in the EMS

Courtesy japcc.org [3]



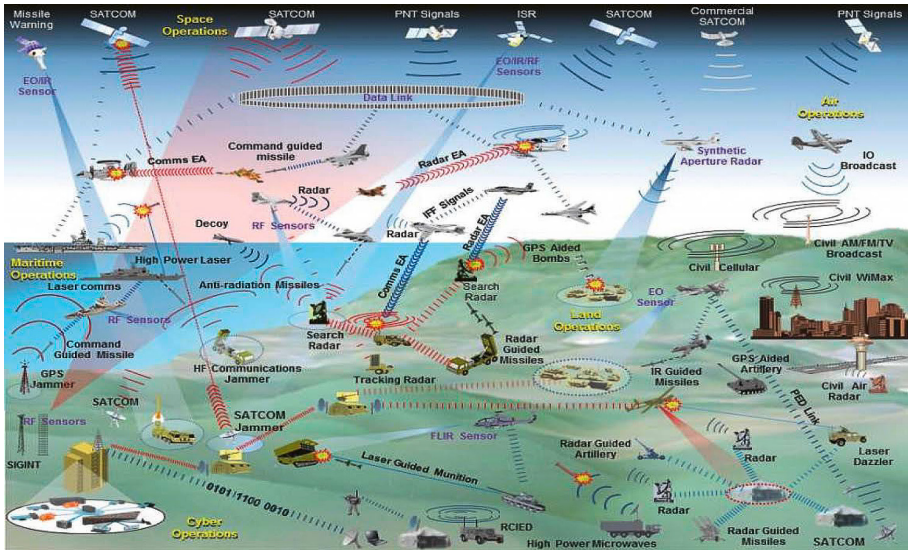
EW is conducted across four domains

- Maritime
- Land
- Air
- Space

These domains are shown in Figure 5. Another view of the military EW domain is shown in Figure 6. It intentionally demonstrates the complexity of today's electromagnetic spectrum operations (EMSO). Dominance through EMSO is a critical factor in determining a positive outcome to military operations.

Figure 6: EW in today's military environment

Courtesy japcc.org [3]



EW comprises three main areas

- Electronic attack
- Electronic protect
- Electronic support

3.1 Electronic attack

Electronic attack (EA) is the strategic use of electromagnetic or directed energy weapons to assault enemy forces' electronic infrastructure with the intent to disrupt, deny, degrade, destroy or deceive communications. This includes threat analysis and response, as well as countermeasures such as signal jamming, spoofing, directed energy, lasers and RF weapons.

3.2 Electronic protect

Electronic protect (EP) involves safeguarding a country's personnel, facilities and equipment against the effects of EA. This threat suppression is achieved using cyber and multispectral radio frequency/infrared (RF/IR) tools to detect, analyze and initiate a response to those effects.

3.3 Electronic support

Electronic support (ES) uses RF sensors and systems to detect, intercept, identify and track electromagnetic energy sources to categorize threats, collect targeting and signals intelligence data, and disseminate that information to warfighting planners.

As mentioned, space is just another EW domain with a few notable differences that will be discussed in the remainder of this paper. Space EW is most commonly associated with satellites and their communications links – collectively known as satcom.

4 OFFENSIVE SPACE ELECTRONIC WARFARE

Offensive space EW is the act of electronic attack on an adversary in the space domain. The attack can be divided into the five D's:

- Disrupt
- Deny
- Degrade
- Deceive
- Destroy

Countermeasures include signal jamming, spoofing, directed energy, lasers and RF weapons.

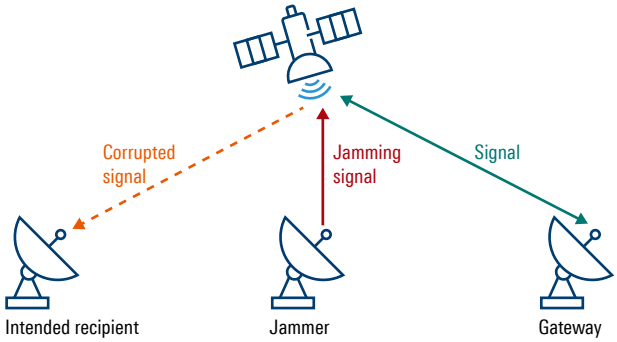
Jamming is a form of electronic attack that interferes with RF communications by transmitting interference signals in the same frequency band and within the field of view of the antenna of the satellite or receiver it is targeting, thus disrupting communications. Jamming is temporary and non-destructive – once the jammer is turned off, normal communications will resume.

Spoofing is another form of electronic attack where a fake signal is produced by the attacker. In this case, if the spoofing attack targets the downlink data from a satellite to the ground, it could end up feeding false or corrupt data into the ground receiver system. Hijacking a satellite telemetry, tracking and control (TT&C) link and feeding it such data is another well-known means of disruption. Upon successful spoofing of the TT&C link of a satellite, the attacker theoretically has control of the satellite. The most common countermeasure against spoofing is the use of encryption to detect false data injection.

4.1 Uplink jamming

Uplink jamming, as shown in Figure 7, interferes with the signal from a ground station or user terminal to the satellite. An RF signal, commonly either wideband noise or a frequency modulated continuous wave (FM-CW) at the same center frequency as the targeted uplink signal and occupying the same bandwidth, is transmitted to the satellite. The aim is to limit or confuse the satellite transponder from differentiating between the jamming signal and the actual signal. The result is usually a corrupted downlink signal. Uplink jamming requires significant RF power to reach the satellite transponder at a sufficient amplitude to confuse the transponder on the satellite, commonly known as the jammer to signal ratio, or J/S. Uplink jamming degrades the signal for all recipients, which may or may not be a desirable outcome. An additional consideration common to all jamming techniques is that the jammer has high visibility (in the RF spectrum) to the adversary and that in turn can lead to geolocation and kinetic counter effects.

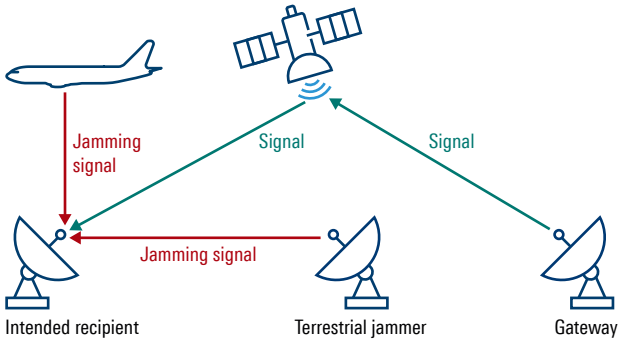
Figure 7: Uplink jamming



4.2 Downlink jamming

Downlink jamming, as shown in Figure 8, disrupts transmissions sent from the satellite to ground based or airborne receivers using RF signals (commonly the same types as discussed in uplink jamming) that mimic the frequency of the downlink signal. This inhibits ground users from receiving transmissions from the satellite. The RF jamming power can be relatively low when compared to uplink jamming. The downlink jammer may be terrestrial or airborne, depending on the intended target. One consideration is that the downlink jammer needs line of sight (LOS) to the intended receiver, which could be problematic in a conflict zone. An additional consideration common to all jamming techniques is that the jammer has high visibility (in the RF spectrum) to the adversary, and that in turn can lead to geolocation and kinetic counter effects.

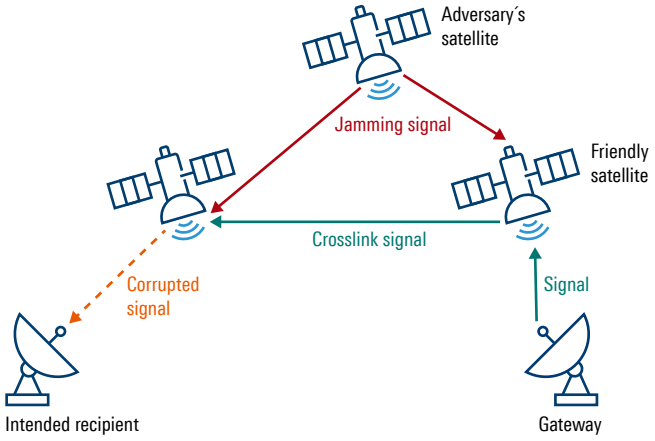
Figure 8: Downlink jamming



4.3 Crosslink jamming

Crosslink satellite communications is the exchange of data between two satellites. The crosslink can be either RF or optical. As an example, the SpaceX StarLink satellites use optical crosslink communications. In crosslink jamming, shown in Figure 9, an adversary's satellite is positioned such that it can jam the crosslink signal between two friendly satellites. All satellites need to have LOS to each other. Directional antennas and phased array antennas can limit the effectiveness of an adversary's jamming signal. Jamming of optical links is considered more challenging as the adversary's satellite optical jammer needs to be closely aligned (physically) to the crosslink optical beam. The beam is very directional and narrow in bore, making effective jamming challenging. Finally, positioning of the adversary's satellite can be difficult to achieve in a timely manner, depending on how far the satellite has to be moved to be "on station".

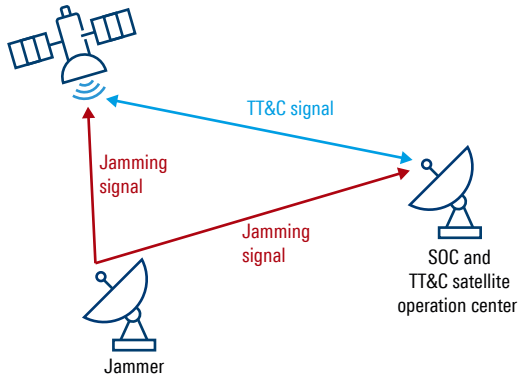
Figure 9: Crosslink jamming



4.4 Telemetry, tracking and command jamming

In telemetry, tracking and command (TT&C) jamming, as shown in Figure 10, the TT&C signal is jammed. Jamming can be against the ground operations center link, or against the TT&C receiver on the satellite. The TT&C signal is not part of the communications payload and is often on a completely separate frequency. TT&C signals are typically much narrower in occupied bandwidth when compared to the payload and therefore potentially easier to jam. The effects of jamming TT&C signals can be catastrophic, resulting in deorbiting of the satellite or movement from the intended orbit. TT&C jamming can also result in failure of the main payload signal due to loss of timing and control signals. Spoofing of TT&C is more challenging as the link is usually encrypted. Ground based jamming of the TT&C link needs LOS to the operations center and utilizes lower power. TT&C jamming on the ground based segment can be challenging due to the need to be LOS to the adversary's op center. Ground based jamming of the TT&C link on the satellite needs LOS to the satellite and higher power.

Figure 10: TT&C jamming



4.5 Other forms of offensive attacks in satellite operations

4.5.1 Optical attacks

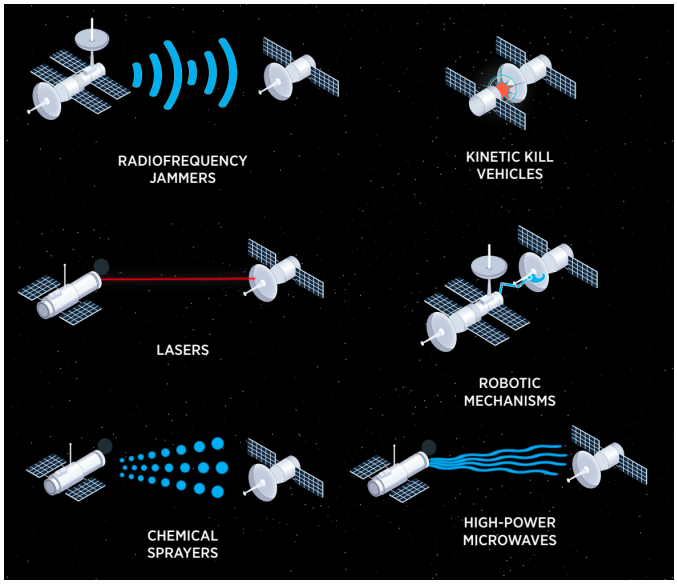
Optical attacks utilize high powered lasers to dazzle or damage the image sensor(s) on reconnaissance satellites. The laser may be either terrestrial or space based. The power of the laser and the distance to the target determine whether the attack causes temporary or permanent damage to the sensor. If the laser power is high enough, it can also cause permanent damage to the satellite's physical structure. Terrestrial attacks on satellites can be very challenging due to the required power, the accuracy of tracking a satellite moving at relatively high velocity, and atmospheric dispersion and aberrations.

4.5.2 Space based offensive attacks

Space based anti-satellite (A-SAT) operations can take many forms, as shown in Figure 11. Some examples in this context include high power microwaves that disable or destroy the satellite, RF jamming and lasers (discussed earlier in section 4.5.1), chemical sprays that disable the satellite, robotic kill vehicles that can damage the satellite through various kinetic methods, and robotic mechanisms that can capture and/or damage another satellite.

Figure 11: Space based A-SAT operations

Courtesy of the US Defense Intelligence Agency [1]



4.5.3 Cyber offensive attacks

Satcom systems are primarily tasked at moving data on a network from one place to another, and networks are subject to cyberattacks. Offensive cyberattacks employ the concept that using these networks can disrupt, deny, degrade or destroy information residing on computers and computer networks, or disrupt, deny, degrade or destroy the computers and networks themselves. Cyber offensive operations are primarily related to the ground segment of network operations and TT&C links.

The primary forms of cyber offensive attacks include:

- Computer network exploitations (CNE), which compromise the network to which a ground station is connected through poorly configured or vulnerable technologies and phishing
- Backdoor attacks via cloud infrastructure
- Data corruption, either at rest or during communications
- Supply chain attacks in which malware is inserted into software, tools and common components
- Unpatched, outdated or legacy COTS software

Note: Cyber offensive operations also include misinformation, disinformation, propaganda and other forms of deception.

In 2017, a senior US military official went on record to state that cyberattacks are the "No. 1 counter-space threat". The Director of US National Intelligence, James R. Clapper, has also previously made similar observations (Pollpeter, et al.).

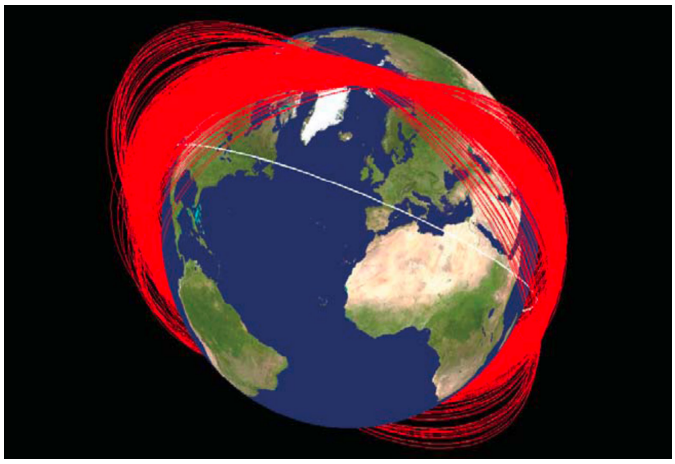
4.5.4 Offensive kinetic attacks

Although not strictly an electronic attack, an offensive kinetic attack is discussed here for completeness. Kinetic attacks can be accomplished through a direct ascent anti-satellite (AASAT) missile. In other words, a ground launched missile is targeted towards a satellite where it either collides with the satellite or detonates close to the target. A second form of kinetic attack utilizes a co-orbital ASAT missile. In this case, a space based weapon is positioned in a similar orbit, maneuvered close to target and detonated.

Kinetic attack is not usually preferred since it leads to space debris that compromises other space vehicles, including friendly and neutral assets. As an example, in 2007 China launched a DF-21 multi-stage ballistic missile from the Xichang Satellite Launch Center against a Chinese FY-1C polar orbit weather satellite, weighing 0.75 t (1 650 lbs). The FY-21 was traveling at 8 km/s (about 17 000 mph). The destruction of the FY-1C led to 10 000 pieces of debris, of which more than 2 800 are still in orbit and continue to pose a significant danger to space operations. NASA is tracking the FY-1C debris, as illustrated in Figure 12.

Figure 12: FY-1C debris orbit

Source: [4]



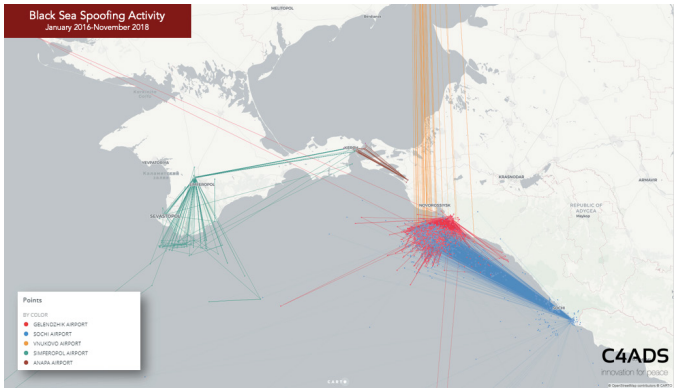
4.5.5 Navigation warfare

A specific form of space EW is navigation warfare (NAVWAR). NAVWAR is defined as offensive and defensive actions to ensure friendly use of positioning, navigation and timing (PNT) assets and to prevent an adversary's use of PNT information. NAVWAR is most commonly applied to GNSS satellite signals including GPS, GLONASS, Galileo, Beidou and QZSS/SBAS. Most NAVWAR activities are associated with jamming and spoofing of ground assets. Military systems depend on navigation satellite systems to move, attack, coordinate and communicate. Civil applications of PNT include air, land and sea navigation, power grid synchronization, financial transactions, air traffic control and rail traffic safety, weather monitoring, earthquake detection, and coordinating first responders.

NAVWAR is more than a theoretical possibility. For instance, in June 2017, about twenty ships in the Black Sea reported GPS anomalies. Vessels appeared to be miles from their actual location in what is believed was most likely a spoofing attack. GNSS anomalies around the Russian presidential palace and the Moscow Kremlin have led researchers to conclude that Russian authorities use GNSS spoofing wherever the Russian President is located, which commonly affects nearby GNSS users. There were additional incidents involving suspected Russian GNSS attacks in Norwegian territorial waters during a NATO exercise that led to a collision between two ships. GNSS spoofing in Syria by the Russian military affected flight operations at Ben Gurion airport in Tel Aviv, Israel, approximately 212 km (132 miles) away.

Figure 13: Russian Black Sea spoofing activity

Source: [5]



4.5.6 Forms of GNSS jamming

Brute-force GNSS jamming

Intentionally denied GNSS is a commonly occurring phenomenon in contested parts of the world, such as the Korean Peninsula and the eastern Black Sea. Denied GNSS is achieved by overpowering the space based GNSS signal with a local, stronger signal that covers the frequency of operation of GNSS, such as the L1, L2 or L5 bands. Commonly used interferers include wideband Gaussian noise, wideband phase/frequency modulation, wideband spread spectrum, narrowband swept pulse, narrowband swept CW and wideband continuous CW. These brute-force denials of service are relatively easy to detect, and equally importantly, terrestrial jamming transmitters are relatively easy to geolocate.

GPS spoofing

A GNSS spoofing attack attempts to deceive a GNSS receiver by broadcasting fake GNSS signals structured to resemble normal GNSS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time. These spoofed signals may be modified in such a way as to cause the receiver to estimate its position to be somewhere other than where it actually is, or to be located at the correct position but at a different point in time. One common form of a GNSS spoofing attack, termed a carry-off attack, begins by broadcasting signals synchronized with the genuine GNSS signals observed by the target receiver. The power of the counterfeit signals is then gradually increased and drawn away from the genuine signal. It is believed that the Lockheed RQ-170 drone aircraft captured in northeastern Iran in December 2011 was the result of such an attack. A "proof-of-concept" attack was successfully performed in June 2013 when the luxury yacht White Rose of Drachs was misdirected with spoofed GPS signals by a group of aerospace engineering students from the Cockrell School of Engineering at the University of Texas in Austin. The students were aboard the yacht and allowed their spoofing equipment to gradually overpower the signal strength of the real received GPS constellation satellites and alter the course of the yacht.

Spoofing attacks can be classified as non-overlapped, overlapped, or by relative power.

Non-overlapped

In this case, the code and carrier phase of the spoofing signals are not synchronized with the authentic signals. The correlation peaks of the spoofing and authentic signals do not overlap. During a cold start, if the spoofing power is higher than that of the authentic signals, the acquisition engine may be deceived depending on the receiver search strategy. When a signal is in the tracking stage, the other regions of the cross-ambiguity function are invisible to the receiver. Therefore, a higher power spoofing signal might not affect the tracking procedure if the delays or Doppler frequencies are not aligned.

Overlapped

In a more sophisticated attack, a spoofer can synchronize its code phase and Doppler frequency with those of the authentic satellite signal. In an overlapped attack, the correlation peaks of spoofing and authentic signals combine to constructively or destructively alter the shape of the correlation peak. This type of spoofing attack might be generated by a receiver based spoofing generator where the spoofer knows the current time, observable satellites, location and parameters of the target receiver. Correct detection of an overlapped spoofing attack is challenging as the distortions caused by spoofing signals appear to be multipath errors.

Relative power

The relative RF power of spoofing attacks is an essential feature to deceive a target receiver. The relative power level of spoofing signals with respect to that of authentic signals can highly impact the effectiveness and error limit of spoofing interference. Identifying spoofing attacks based on their relative power is difficult as it requires information about the spoofer's propagation channel as well as the antenna gain pattern and its orientation.

NAVWAR mitigation

- Monitoring and quality of service measurements to detect jamming/spoofing
- Sources of alternate position, navigation and timing (A-PNT) when GNSS/GPS unavailable
- Hold-over clocks to maintain timing
- Controlled radiation pattern antennas (CRPA) to minimize ground based jamming
- DoD and friendly nations can use military GPS user equipment (MGUE) that utilizes the GPS M-code to autonomously detect jamming and spoofing
- GPS Block III satellites can use beam forming to increase signal to jamming (S/J) ratio by +20 dB to spot points on earth. This feature is known as "regional military protection".

4.6 Operational challenges of offensive space EW

In normal terrestrial jamming scenarios, the ideal situation is to position the jammer close to the target. In a space environment, this is not normally possible. The trajectory of a satellite cannot be controlled, but it can be predicted. This leads to the concept of getting enough power on the target. However, this is challenging due to free space losses and the distances involved, resulting in high jamming power requirements for terrestrial uplink and crosslink jamming.

Recall that received power decreases with the square of the distance ($1/R^2$). An example is GPS in which the received RF signal strength at the earth's surface is very low. GPS satellites have an orbit altitude of about 20 000 km. The satellite transmit power is typically approximately 45 W at the L1 frequency of 1 575.43 MHz. The typical antenna gain at the satellite is 12 dBi. Assuming that the receiver has a typical antenna gain of 4 dBi, the received signal power is –120 dBm using the free space loss model. Once antenna, connectors and atmospheric losses are included, the modeled receive power is –125 dBm while the noise power in the GPS bandwidth (approximately 2 MHz) is –110 dBm. Due to the direct spread-spectrum modulation employed in traditional GPS, there is an additional

processing gain of 43 dB. Overall, signals can be recovered down to –153 dBm. In practice, the received power needs a margin above this lower limit. Commonly accepted receive power during acquisition is > –135 dBm and during tracking > –147 dBm. With such small level signals, it is easy to see how effective a ground based jammer can be, requiring a low margin of J/S.

The logistical requirement of the jammer needing to be physically co-located within LOS to adversary's ground segment is problematic in a conflict zone. Since the jammer is relatively close to the adversary, geolocation of the jammer can be accomplished by the adversary using traditional direction finding techniques, leading to the potential of kinetic counter effects, including the use of anti-radiation missiles (ARM), which home in on the jammer.

Finally, obtaining actionable intelligence on an adversary's assets is always challenging.

5 DEFENSIVE SPACE ELECTRONIC WARFARE

In this section, we will discuss defensive space EW and jamming mitigation techniques.

5.1 Antennas

5.1.1 Directional antennas

One of the best defenses against jamming is to limit the effectiveness of the jamming signal on the receiving antenna. The traditional approach is to use a directional antenna, i.e. an antenna that has high gain in a specific direction. An example of such a directional antenna is a Yagi antenna (Figure 15). The radiation pattern of a Yagi antenna is shown in Figure 14. Another example of a highly directional antenna is a parabolic dish (Figure 17), which is commonly used in satellite communications. The radiation pattern of a parabolic antenna (Figure 16) contains a major lobe, which is directed along the axis of propagation, and several small minor lobes. Very narrow beams are possible with this type of reflector.

Figure 14: Yagi antenna radiation pattern

Courtesy radartutorial.eu [6]

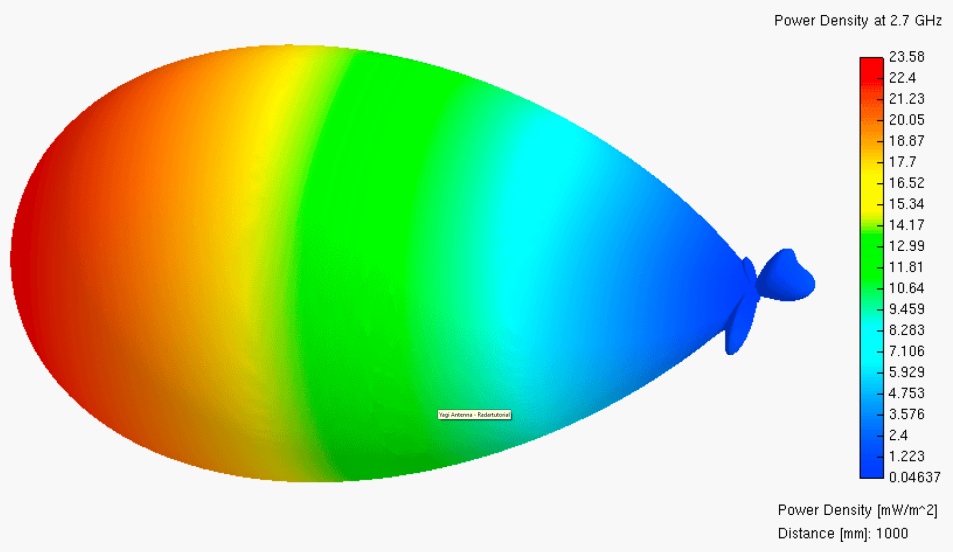


Figure 15: Yagi antenna

Courtesy radartutorial.eu [6]

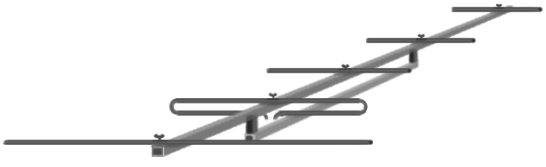


Figure 16: Parabolic dish radiation pattern

Courtesy radartutorial.eu [6]

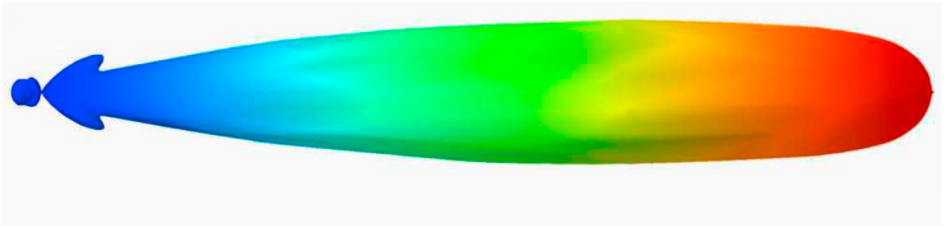
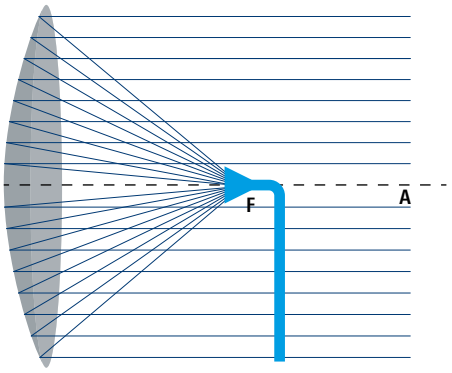


Figure 17: Principle of operation for a parabolic antenna

Courtesy radartutorial.eu [6]



Advantages of directional antennas

- Low cost
- Highly directional
- Greater gain compared to phased array (typically)
- Low/no processing

Disadvantages of directional antennas

- Mechanical steering required
- Slow change of beam direction
- Single beam
- Insensitive outside of main lobe (can also be considered as an advantage)

5.1.2 Phased arrays

The second type of antenna is a phased array, which uses space-time adaptive processing to form nulls against jamming. Phased arrays utilize many antennas in a two-dimensional array, and each element of the array can be fed with signals with different phase shifts and power levels. As a result, the antenna pattern can be steered electronically. Electronic steering is more flexible and requires less maintenance than a mechanically steered antenna. The antenna array usually employs a reflector to limit back lobes.

The transmitted signal is routed through a phase-regulating module which electronically controls the radiation pattern. The effectiveness of this antenna steering is greatest when it is perpendicular to the antenna array. On the other hand, extreme tilting of the main direction increases the number and size of the unwanted sidelobes while at the same time reducing the effective antenna area.

Advantages of phased array antennas

- High antenna gains possible with large sidelobe attenuation
- Fast change of beam direction
- High beam agility
- Arbitrary space scanning
- Selectable dwell time
- Multifunction operation by simultaneous generation of multiple beams
- Failure of some components does not result in a complete system failure

Disadvantages of phased array antennas

- Limited scanning range (up to max. 120° in azimuth and elevation)
- Deformation of the antenna pattern during beam steering
- Low frequency agility
- Complex structure (computer, phase shifter, data bus to each radiator)
- High costs

A specific form of antenna used in GPS jamming mitigation is the controlled radiation pattern antenna (CRPA). It uses an adaptive beam steering method to control the reception pattern, which can be adjusted to create nulls in the direction of interfering signals. The CRPA antenna creates a spatial filter that eliminates signals from a particular direction while permitting signal reception from other directions.

5.1.3 Other technologies

A commonly used method to mitigate jamming is to employ frequency agile techniques in which the signal moves or "hops" by varying the carrier among a set of discrete frequencies. The hopping frequency scheme is predetermined by both the transmitter and the receiver through the use of a pseudo random bit sequence (PRBS). One challenge of frequency hopping is to establish synchronized hops on both the transmitter and receiver. First, both the transmitter and receiver need high accuracy clocks to maintain their time synchronization. Second, the transmitter and receiver need to synchronize their hops. One common method is to ensure that the transmitter will use all the channels in a fixed period of time. The receiver can then find the transmitter by picking a random channel and listening for valid data on that channel. The transmitter's data is identified by a special sequence of data that is unlikely to occur over the segment of data for this channel. The segment can also utilize a checksum for integrity checking and further identification. The transmitter and receiver can use fixed tables or pseudo random sequences of frequency hopping patterns. In this manner, once they are synchronized, they can maintain communications. A jammer may utilize wideband jamming, sometimes known as barrage jamming, which uses white noise to cover all of the frequency "slots" of the hopping communications channels to effect a jam. This requires high jamming power due to the wideband nature of the jammer. Other jamming techniques used against hopping signals include imprecise follower jamming, partial band jamming and effective sweeper jamming.

Finally, encryption of the data is essential as it protects the data from interception by third parties and provides mechanisms to detect degradation and corruption of the data that can potentially occur under jamming conditions.

6 TECHNOLOGIES FOR SPACE ELECTRONIC WARFARE

In this section, we will review useful technologies that can be applied to space EW, including link budgeting, communications monitoring, signal analysis, carrier-under-carrier detection, interference hunting, capturing short-duration events, handheld interference hunting, and high bandwidth recording to capture long-term events.

6.1 Satellite link planning

Satellite link planning can be used to understand both the total budget for a satcom link, as well as to assess the potential impact of jamming and the associated required jamming power. R&S®GSASLP satellite link planner is a satcom analysis and optimization software solution, covering all aspects of modern satellite communications. R&S®GSASLP supports major parts of the satcom chain, such as satellite system design, transmission planning and transponder usage optimization. R&S®GSASLP accurately models weather conditions and atmospheric effects while covering all RF transmission impairments of transparent payloads among all satcom bands of interest (C, X, Ku, Ka band, etc.). Major signal impairments due to intermodulation and power robbing, for example, are accurately modeled and verified against vendor data and in orbit test campaigns.

6.1.1 Link budget calculation and optimization

R&S®GSASLP helps engineers to simulate and model the impact of dedicated transponder distortions on satcom carriers. In this respect, the impact of dedicated signal distortions on mission planning or payload design can be quantified in terms of carrier-to-noise ratio loss or capacity degradations. R&S®GSASLP link budget calculations are based on a set of internationally recognized methods and ITU recommendations.

6.1.2 Satellite network planning and optimization

Systems using R&S®GSASLP are capable of modeling ground stations with their specific parameters, e.g. the transmitting and receiving antenna gain, the maximum effective isotropic radiated power (EIRP) or the output power. Additionally, users can model the space segment as well by managing available satellites, transponders and their footprints. R&S®GSASLP offers a large database of satellites and footprints to simplify the user's job.

6.1.3 Route planning and satellite payload optimization

R&S®GSASLP helps users planning mobile satcom scenarios by managing route navigation. Based on the given route and data rate requirements, R&S®GSASLP searches for the best possible transponders according to criteria such as the data rate requirements, the coverage of transponder beams encompassing the entire route, or the satcom band of interest (C, X, Ku, Ka band, etc.).

6.1.4 R&S®GSASLP key features

- Link budget analysis of complex multi-carrier scenarios
- Modeling of transponder RF impairments (intermodulation, power robbing, gain compression)
- Link budgets and transponder optimization to minimize power/bandwidth consumption of satcom scenarios
- Ground station equipment and antenna management
- Antenna footprint visualization
- Satellite beacon reception analysis
- Impairment calculation due to adjacent satellite interference (ASI)
- Impairment calculation due to ITU weather recommendations
- Route planning and optimization for mobile VSAT terminals, satcom on the move (SOTM) or UAV operations
- Attenuation coverage analysis
- Carrier planning over time and frequency

- ► Adaptive graphical user interface and tailored special purpose solutions
- ► Data import/export, geopositioning and satellite footprint visualization
- ► Large satcom modem database (SCPC, meshed, DTH, military CDMA/DSSS)

Figure 18: Satellite link planner antenna footprint visualization

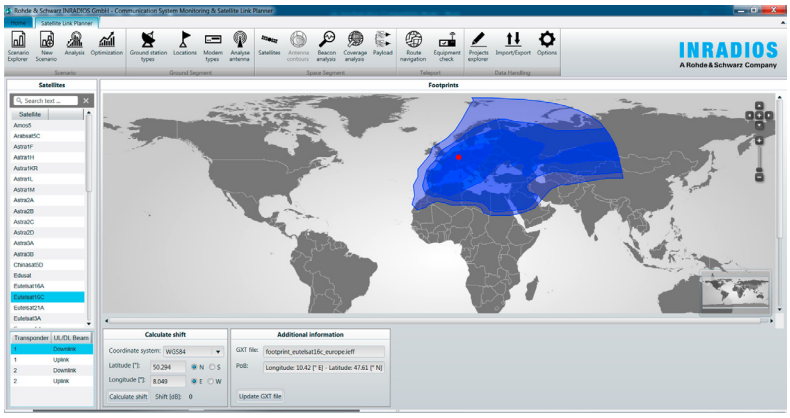
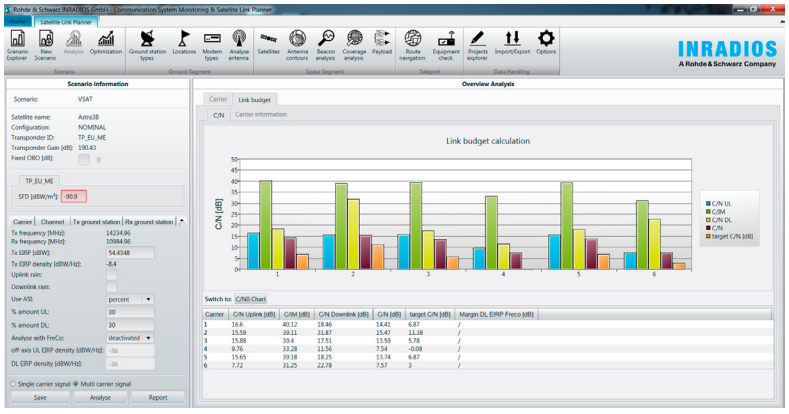


Figure 19: IBO/OBO [1] charts and gain vs. IBO charts for a non-linearized TWTA [2] in single carrier and multi-carrier operation mode



6.2 Communications system monitoring

R&S®GSACSM communications system monitoring is a satmon software solution for remote spectrum monitoring and signal analysis. R&S®GSACSM combines traditional spectrum analyzer functions, trapping systems, advanced signal detection and identification algorithms. The modern, adaptive GUI makes it easy to implement use cases, e.g. interference identification or satcom transponder analysis.

6.2.1 Remote spectrum monitoring

R&S®GSACSM provides an interface for communicating with remote spectrum analyzers via remote connections; users can access their devices from anywhere in the world. R&S®GSACSM supports monitoring of signals for one device at a time and for many different devices at once. R&S®GSACSM also handles different users monitoring the same device. Both a standalone application and a server/client solution are supported.

[1] IBO/OBO stands for transponder input back-off/transponder output back-off.
[2] TWTA stands for traveling wave tube amplifier.

6.2.2 Satellite transponder monitoring

R&S®GSACSM autonomously scans transponder signals and identifies carriers, e.g. DVB-S, DVB-S2 and DVB-CID. By scanning and evaluating signals continuously, it is possible to detect wanted carriers with detailed information such as baud rate, modulation scheme, FEC rate, C/N and carrier frequency offset. It is also possible to track and identify unwanted interference.

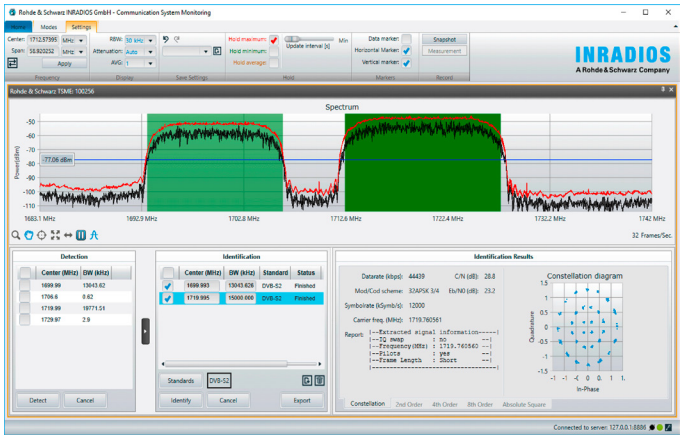
6.2.3 Carrier-in-carrier detection

Systems using R&S®GSACSM can perform carrier-in-carrier (CiC) detection tasks, which are a major feature in modern VSAT systems. Tasks such as paired carrier multiple access (PCMA) detection and signal identification and under-carrier signal analysis can be executed to find unwanted interferers in such systems.

R&S®GSACSM key features:

- Multichannel power measurement, history logging and alarm trapping
- Classic software based spectrum analyzer functions
- Adaptive graphical user interface and tailored special purpose solutions
- Autonomous detection and identification of terrestrial and satellite signals (e.g. GSM, DECT, DVB-S, DVB-S2)
- Autonomous detection and identification of paired carrier multiple access (PCMA) and time-division multiple access (TDMA) signals
- Autonomous detection and identification of under-carrier signals
- Autonomous detection and identification of DVB carrier identification (DVB-CID) signals
- Simultaneous operations on multiple remote spectrum analyzers
- Remote spectrum monitoring over narrowband low latency connections

Figure 20: Signal detection and identification



R&S®GSACSM supports the following Rohde&Schwarz sensor instruments:

- R&S®TSME6 ultracompact drive test scanner
- R&S®NRQ6 frequency selective power sensor
- R&S®FPS signal and spectrum analyzer
- R&S®FSW signal and spectrum analyzer
- R&S®FSV/FSVA signal and spectrum analyzer
- R&S®FPL1000 signal and spectrum analyzer
- R&S®ESMD wideband monitoring receiver
- R&S®ESME wideband monitoring receiver
- R&S®MSR200 wideband receiver
- R&S®EM200 digital compact receiver
- R&S®MSR4 multipurpose satellite receiver

6.3 R&S®MSR4 multipurpose satellite receiver

The R&S®MSR4 is a hardware monitoring receiver that provides up to four receive channels from 500 MHz to 3 GHz, with each input providing 200 MHz I/Q bandwidth. The R&S®MSR4 also provides two transmit channels from 900 MHz to 2.5 GHz for replay purposes. The R&S®MSR4 is designed to work with external upconverters and downconverters. The R&S®MSR4 is compact in size, occupying 1 RU of height. The heart of the R&S®MSR4 is a software defined radio with cognitive capabilities. It can run a CSM server with no extra computing hardware required.

Figure 21: R&S®MSR4 multipurpose satellite receiver

6.4 Signal analysis

Signal analyzers, or spectrum analyzers, are useful in analyzing many aspects of space EW. Spectrum analyzers are wide bandwidth instruments used to acquire, analyze, display and demodulate RF signals. They can give unique insights into:

- Tracking, logging, displaying and monitoring interference
- Jamming effects in time-frequency and amplitude domains simultaneously
- Demodulation of signals of interest
- Streaming interfaces to record signals of interest
- Autonomous monitoring of uplink and downlinks

The R&S®FSW is an example of a high-performance spectrum analyzer. It can provide up to 8.3 GHz of internal I/Q analysis bandwidth, up to 800 MHz of real-time bandwidth and up to 1 GHz of streaming bandwidth. It can tune to center frequencies between 9 kHz and 90 GHz. The FSW provides wide dynamic range which enables tracking of small signals and includes integrated preselection to reject out of band signals.

Figure 22: R&S®FSW signal and spectrum analyzer

6.4.1 Modulation analysis

The R&S®FSW-K70 vector signal analysis option is designed to work with the R&S®FSW to analyze digitally modulated single carriers down to the individual bit level. The clearly structured operating concept simplifies measurements, despite the wide range of analysis tools. The R&S®FSW-K70 option provides analysis lengths up to 64 000 symbols with up to 8.3 GHz of signal analysis bandwidth.

Supported modulation formats

- 2FSK, 4FSK to 64FSK
- MSK, GMSK, DMSK
- BPSK, π/2-BPSK, π/2-DBPSK, QPSK, offset QPSK (O-QPSK),
- DQPSK, π/4-DQPSK, 3π/4-QPSK, 8PSK, D8PSK,3π/8-8PSK, π/8-D8PSK
- 16QAM, 32QAM, 64QAM, 128QAM, 256QAM,512QAM, 1024QAM, 2048QAM, 4096QAM
- 16APSK (DVB-S2), 32APSK (DVB-S2), 2ASK, 4ASK
- π/4-16QAM (EDGE), –π/4-32QAM (EDGE), SOQPSK

6.4.2 Monitoring of satellite communications links

In conjunction with the R&S®FSW, the R&S®FSW-K70M multi-modulation analysis option (multi-carrier) and the R&S®FSW-K70P BER PRBS measurements option can be used to ensure the integrity of satcom links.

DVB-S2X modulation analysis

The R&S®FSW-K70M multi-modulation analysis option allows DVB-S2X signals to be analyzed. The R&S®FSW-K70M detects the start of frame, demodulates both the header and payload parts of the signal, and displays the constellation diagram and relevant modulation analysis parameters.

Uncoded bit error rate

The R&S®FSW-K70P bit error rate (BER) pseudo random binary sequence (PRBS) measurements option is an extension of the R&S®FSW-K70 option that allows measurement of raw BER on PRBS data up to PRBS23. In addition, the R&S®FSW-K70P offers the ability to measure BER based on user-defined bit sequences.

6.5 Signal generation

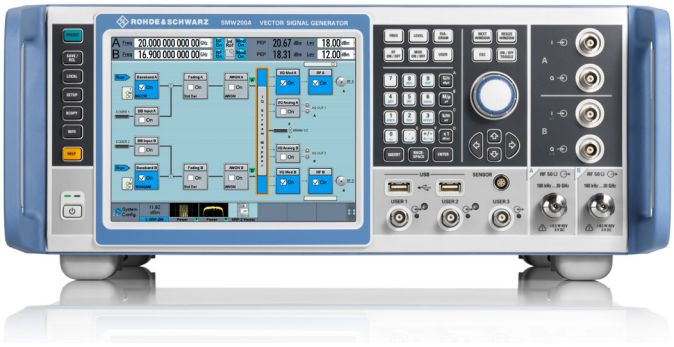
Signal generators, or more specifically RF vector signal generators (VSG), are used to create realistic RF environments through the use of arbitrary digitally modulated RF signals. The main uses for a VSG in space EW include:

- Creation of reference payload signals, for example DVB-S2X
- Generation of realistic jamming signals to measure the susceptibility of a system to jamming during development
- Generation of actual jamming signals with the addition of a wideband RF power amplifier and associated antenna
- Generation of non-standard waveforms to enable research and deployment of proprietary modulation schemes
- Multi-channel RF generation, enabling generation of bona-fide signals and interference signals in a single box

The R&S®SMW-200A vector signal generator is an example of a high-performance VSG, and includes the following characteristics:

- Frequency range from 100 kHz to 67 GHz
- Optional dual RF paths with a frequency range of 100 kHz to 44 GHz
- Channel bonding to give up to 4 GHz of modulated RF output
- Up to 2 GHz I/Q modulation bandwidth (in RF) with internal baseband
- Options for all important digital communications standards
- Optional integrated fading simulator with up to 800 MHz bandwidth
- Support of all key MIMO modes including 3x3, 4x4, 8x4, 4x8 and 4x2x2

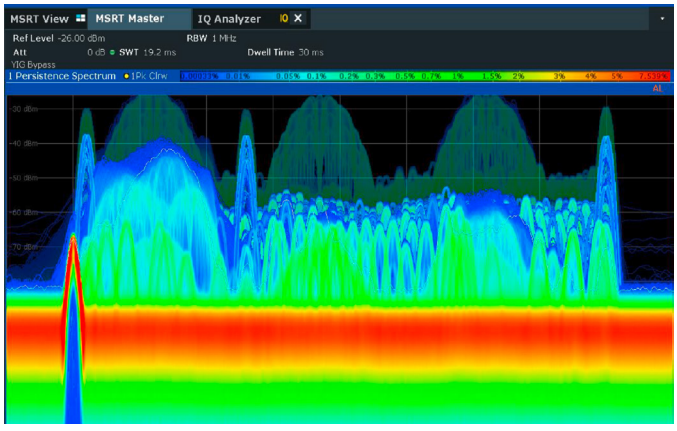
Figure 23: R&S®SMW200A vector signal generator



6.6 Short-term events and interference

Capturing short-duration interference events requires a spectrum analyzer with real-time spectrum analysis (RTSA) capability. An RTSA utilizes dedicated FGPA processing, providing over 2 343 750 FFT per second to trigger and visualize the transient signals. The R&S®FSW can reveal unknown signals greater than 460 nsec minimum event duration for 100 % probability of intercept (POI).

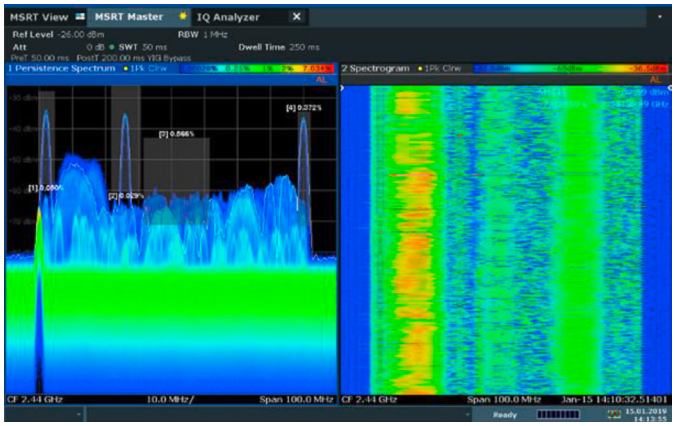
Figure 24: R&S®FSW persistence display of transient signals



Since these signals are very transient in nature, dedicated triggering mechanisms are useful in capturing them. The R&S®FSW supports two triggering mechanisms: a frequency mask trigger, where an upper and lower frequency vs. amplitude mask can be applied, and any signals exceeding the mask are captured, and a probability mask trigger. The probability mask trigger can be applied to up to four zones and is based on a signal probability exceeding the thresholds in each of up to four zones.

Figure 25: Frequency mask triggering

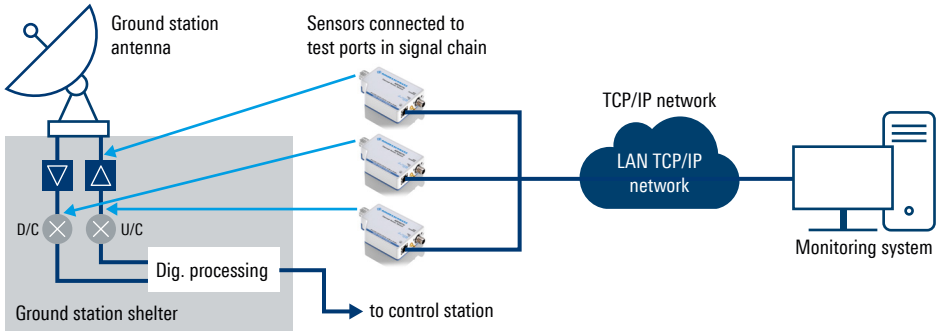
Figure 26: Probability mask triggering



6.7 RF power measurement

RF power sensors can be used to provide remote, autonomous monitoring of RF signal levels at the antenna feed as well as intermediate points via USB and LAN. The sensors are able to deliver traceable, calibrated measurements with simple operation. The sensors operate without affecting the standing wave ratio (SWR) and provide low insertion loss and excellent intermodulation characteristics. The uses for RF power meters include monitoring of IF and RF power levels to ensure correct operation, and long-term trend monitoring of power levels for failure prediction. The power meters from Rohde&Schwarz are also able to directly measure the total power of multi-carrier signals, a very useful feature in many satcom applications.

Figure 27: Power sensors in satcom applications



6.8 Handheld interference hunting

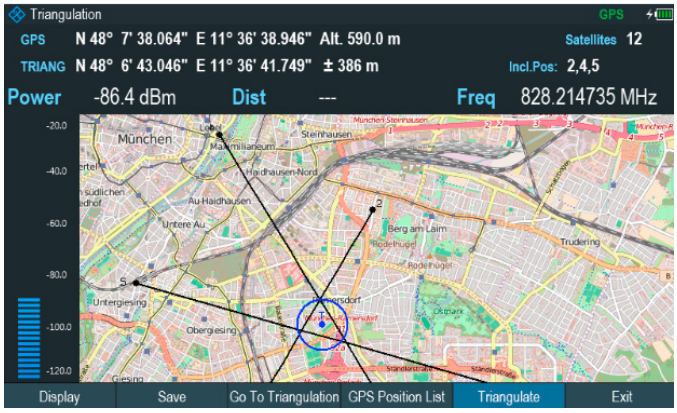
Handheld interference hunting can be used to geolocate the location(s) of sources of interference, whether intentional, in the case of jamming, or accidental, such as an RF source emitting on an incorrect frequency. Portable receivers and directional handheld antennas give operators lightweight, flexible solutions for interference hunting in the field. Portable direction finders can be used to take bearing measurements, even on short-duration emissions. The heart of an interference hunting system is a portable handheld spectrum analyzer, such as the R&S®Spectrum Rider FPH handheld spectrum analyzer.

R&S®Spectrum Rider FPH main characteristics

- 5 kHz to 44 GHz frequency coverage
- 6 hour battery life
- Excellent RF performance, DANL: typ. –163 dBm, TOI measurement: +10 dBm
- Interference hunting and signal strength with geolocated maps
- Unique, high performance wideband directional antennas
- Portable, lightweight: 2.5 kg (5.5 lbs)

Figure 28: R&S®Spectrum Rider FPH handheld spectrum analyzer

Figure 29: R&S®Spectrum Rider FPH displaying georeferenced interference



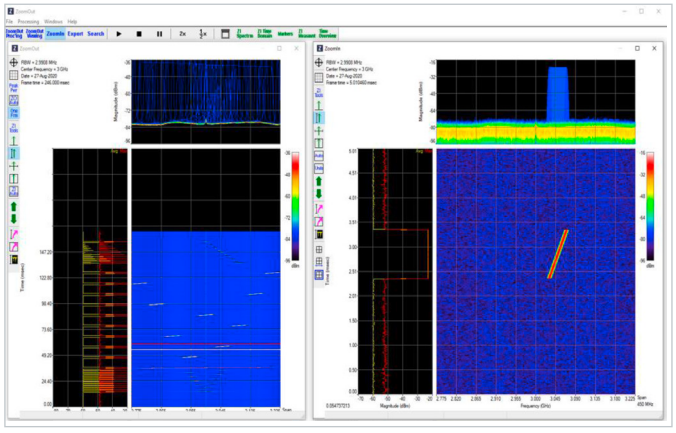
6.9 RF recording, analysis and playback

The R&S®IRAPS™ integrated record, analysis and playback system is a complete high bandwidth RF record and playback solution based on commercial off the shelf (COTS) products. R&S®IRAPS™ can be used to capture long-duration RF events and later replay those signals in a controlled environment. It can also be configured to trigger and record anomalies in the uplink, downlink and TT&C of a satcom system. Furthermore, R&S®IRAPS™ can be used to capture, document and analyze the interactions between systems, such as a jammer and a satcom link.

R&S®IRAPS™ consists of an R&S®FSW spectrum analyzer, an R&S®SMW vector signal generator and the SigPro processing system. SigPro runs the record, playback and analyzer software, which collectively is known as ZoomOut. The ZoomOut software enables the operator to observe the RF spectrum, down to individual samples in time, frequency and amplitude. R&S®IRAPS™ can support 1 GHz of end-to-end record and playback with up to 6 hours of recording time.

Figure 30: R&S®IRAPS™ configuration

Figure 31: ZoomOut software capturing a chirp signal



7 CONCLUSION

Space EW is a complex and emerging warfighting domain that presents a number of unique operational challenges. The ability to operate without constraint in space provides integral support to military, commercial and civilian applications. Traditional cost barriers to space are rapidly falling, enabling more countries and a wider range of commercial endeavors to be undertaken. These advancements are creating new opportunities, but they are also creating new risks to space and ground based communications, navigation, weather and reconnaissance activities. Foreign governments have recognized the benefits of space based operations and are taking steps to maximize their advantages and formulate methods to minimize their adversaries' capabilities.

In the 1960s, the space race commenced. 60 years later, the race is on to field technologies that facilitate control over the space environment and the ground support services. At the forefront of this new space race is the invisible fight for control of the electromagnetic domain.

8 REFERENCES

[1] Defense Intelligence Agency – US Security Challenges In Space, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf

[2] GAO analysis of DoD documentation GAO-20-80, https://www.gao.gov/products/gao-20-80

[3] Electronic Warfare – The Forgotten Discipline, Commander Malte von Spreckelsen, DEU N, NATO Joint Electronic Warfare Core Staff, Joint Airpower Competence Center, https://www.japcc.org/electronic-warfare-the-forgotten-discipline/

[4] Image - NASA Orbital Debris Program Office, http://www.orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv11i2.pdf

[5] Exposing GPS Spoofing in Russia and Syria, https://rntfnd.org/2019/03/27/exposing-gps-spoofing-in-russia-and-syria-9000-incidents-in-new-c4ads-report/

[6] Radar Basics, https://www.radartutorial.eu/index.en.html

9 FURTHER INFORMATION

1. Silent Sentry, Staff Sgt. Alexandre Montes, 379th Air Expeditionary Wing Public Affairs, https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/885152/operation-marks-10-years-of-interstellar-combat-support-protecting-centcoms-sat/

2. Space EW, Massimo Annulli, EURODASS Consortium, https://www.emsopedia.org/entries/space-ew/

3. Declassified US national archives, https://www.archives.gov/files/declassification/iscap/pdf/2014-033-doc01.pdf

4. Pierluigi Paganini, Infosec, https://resources.infosecinstitute.com/topic/hacking-satellite-look-up-to-the-sky/

5. Cognitive Anti-jamming Satellite-to-Ground Communications on NASA's SCaN Testbed, S, Jayaweera, S. Feng, D. Mortensen, A. Holland, M. Piasecki, M. Evans, C. Christodoulou, https://ntrs.nasa.gov/api/citations/20190001548/downloads/20190001548.pdf

6. WGS, Dr. Paul LaTour, Lieutenant Colonel, United States Air Force (USAF), http://www.milsatmagazine.com/story.php?number=1909521651

7. Rapid Attack Identification Detection and Reporting System (RAIDRS), https://www.globalsecurity.org/space/systems/raidrs.htm

8. Brian Garino and Jane Gibson, "Space System Threats", AU-18 Space Primer, Maxwell Air Force Base: Air University Press, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/AU-18.PDF

9. Todd Harrison, Future of MILSATCOM, Center for Strategic and Budgetary Assessments, https://csbaonline.org/research/publications/the-future-of-milsatcom

10. Todd Harrison, Kaitlyn Johnson and Thomas G. Roberts, Space Threat Assessment 2019, CSIS, https://www.csis.org/analysis/space-threat-assessment-2019

11. Garino and Gibson, "Space System Threats", CSIS, https://aerospace.csis.org/wp-content/uploads/2018/09/Space-System-Threats.pdf

12. Ronald G. Wilgenbusch and Alan Heisig, "Command and Control Vulnerabilities to Communications Jamming", Joint Force Quarterly, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-69/JFQ-69_56-63_Wilgenbusch-Heisig.pdf

13. "GPS, Wi-Fi, and Cell Phone Jammers Frequently Asked Questions", Federal Commerce Commission Enforcement Bureau, https://transition.fcc.gov/eb/jammerenforcement

14. David Bosco, "When Can States Jam Radio Broadcasts?", Foreign Policy, https://foreignpolicy.com/2012/10/05/when-can-states-jam-radio-broadcasts/

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

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

17. GPS: The Global Positioning System, www.gps.gov

18. "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community", Office of the Director of National Intelligence, February 13, 2018, https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community

Note: All links have been checked and were functional when this document was created.
However, we cannot rule out subsequent changes to the links in the reference list.

Rohde & Schwarz

The Rohde & Schwarz technology group is among the trailblazers when it comes to paving the way for a safer and connected world with its leading solutions in test & measurement, technology systems and networks & cybersecurity. Founded more than 85 years ago, the group is a reliable partner for industry and government customers around the globe. The independent company is headquartered in Munich, Germany and has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support

PD 3683.9434.52 | Version 02.00 | June 2023 (ch) | White Paper
An overview of space electronic warfare
Data without tolerance limits is not binding | Subject to change

3683943452
3683.9434.52 02.00 PDP/PDW 1 en