# The Price of Precision: The Risks and Rewards of GPS in the Age of Navigation Warfare

Aaron E. Brown, Esquire[1]


## Abstract

As the reliance on Global Positioning System (GPS) technology grows, so does the vulnerability to intentional disruption. This article delves into the fundamentals of GPS, exploring its functionality and significance in modern warfare. Drawing upon this understanding, it proposes a set of Navigation Warfare tenets—Safeguard, Intercept, and Preserve—to address the emerging threats to GPS. The article also emphasizes the increasing concern within the Department of Defense (DOD) regarding Electromagnetic Interference (EMI) and GPS jamming. It argues that safeguarding GPS is of paramount importance to maintain operational advantage and protect military assets. By analyzing the potential consequences of a degraded or denied GPS environment, the article highlights the urgent need for proactive measures. To address these challenges, the article outlines a range of techniques, tactics, and procedures (TTPs) that senior military leaders can employ. Four key TTPs are proposed: Anticipation, Consistent Observation, Encryption, and Reporting. These measures aim to equip military forces with the necessary tools and strategies to effectively navigate and prevail in a degraded or denied GPS environment. Through this comprehensive examination, the article seeks to contribute to the discourse on the protection of GPS technology and provide practical guidance for military leaders in enhancing operational resilience. By adopting the proposed Navigation Warfare tenets and implementing


1 Judge Advocate, United States Army. Presently assigned as a National Security Law Attorney, 1st Multi Domain Command, Fort Shafter, Hawaii. Project Management Graduate Certificate, 2020, Fayetteville State University; J.D., 2011, Florida A&M University College of Law; B.S., 2008, University of Central Florida. Previous assignments include Command Judge Advocate & Contract Law Attorney, 418th Contracting Support Brigade, Fort Hood, Texas, 2020-2022; Trial Defense Counsel, Trial Defense Services, Fort Bragg, North Carolina, 2018-2020; Brigade Judge Advocate, 2nd Recruiting Brigade, Redstone Arsenal, Alabama, 2017-2018; Administrative Law/Operational Law Attorney, 1st Cavalry Division, Fort Hood, Texas, 2016-2017. Member of the Florida Bar.

The views presented are those of the author and do not necessarily represent the views of the Department of Defense or its components. CPT Brown may be contacted at aaronebrown.esq@gmail.com. Portions of this article's content are derived from lectures held during the Army Space Cadre Basic Course.

the outlined TTPs, military forces can better prepare themselves to confront and overcome the challenges posed by EMI and GPS jamming.

***Keywords:*** space law, space, national security, gps, gps jamming, electromagnectic intrusion

## El precio de la precisión: los riesgos y las recompensas del GPS en la era de la guerra de navegación

Resumen

A medida que crece la dependencia de la tecnología del Sistema de Posicionamiento Global (GPS), también crece la vulnerabilidad a la interrupción intencional. Este artículo profundiza en los fundamentos del GPS, explorando su funcionalidad y significado en la guerra moderna. Basándose en este entendimiento, propone un conjunto de principios de Navigation Warfare (Salvaguardar, Interceptar y Preservar) para abordar las amenazas emergentes para el GPS. El artículo también enfatiza la creciente preocupación dentro del Departamento de Defensa (DOD) con respecto a la interferencia electromagnética (EMI) y la interferencia del GPS. Argumenta que salvaguardar el GPS es de suma importancia para mantener la ventaja operativa y proteger los activos militares. Al analizar las posibles consecuencias de un entorno de GPS degradado o denegado, el artículo destaca la necesidad urgente de medidas proactivas. Para abordar estos desafíos, el artículo describe una variedad de técnicas, tácticas y procedimientos (TTP, por sus siglas en inglés) que pueden emplear los líderes militares superiores. Se proponen cuatro TTP clave: Anticipación, Observación consistente, Cifrado e Informes. Estas medidas tienen como objetivo equipar a las fuerzas militares con las herramientas y estrategias necesarias para navegar y prevalecer de manera efectiva en un entorno de GPS degradado o negado. A través de este examen integral, el artículo busca contribuir al discurso sobre la protección de la tecnología GPS y brindar orientación práctica para los líderes militares en la mejora de la resiliencia operativa. Al adoptar los principios de la guerra de navegación propuestos e implementar los TTP descritos, las fuerzas militares pueden prepararse mejor para enfrentar y superar los desafíos que plantean las interferencias de EMI y GPS.

***Palabras clave:*** derecho espacial, espacio, seguridad nacional, gps, bloqueo de gps, intrusión electromagnética

# 精度的代价：导航战时代GPS的风险与回报


## 摘要

随着对全球定位系统(GPS)技术的依赖不断增加，故意破坏（该技术）的脆弱性也随之增加。本文深入研究了GPS的基础，探究其在现代战争中的功能性和意义。基于这一认识，本文提出了一套导航战原则，即保卫、拦截和保护，以应对GPS面临的新威胁。本文还强调了国防部(DOD)对电磁干扰(EMI)和GPS干扰的日益关注。本文认为，保卫GPS对于维持作战优势和保护军事资源而言至关重要。通过分析GPS环境退化或失效的潜在后果，本文强调了采取主动措施的迫切需要。为了应对这些挑战，本文概述了高级军事领导人可以采用的一系列技术、战术和程序(TTP)。提出了四个关键TTP：预期、持续观察、加密、报告。这些措施旨在为军队配备必要的工具和战略，以便在GPS退化或失效的环境中进行有效导航并取得胜利。通过全面分析，本文试图为有关GPS技术保护的讨论作贡献，并在增强作战弹性方面为军事领导人提供实践指导。通过采用提出的导航战原则并实施TTPs，军队能更好地作准备，以应对和克服EMI和GPS干扰带来的挑战。


关键词：空间法，太空，国家安全，GPS，GPS干扰，电磁入侵

---

## Introduction

*Consider this scenario: You are a senior military leader on temporary duty status at Fort Shafter, Hawaii. The base is relatively small but is mere miles away from one of the world's most visited beaches – Waikiki. On the day in question, you successfully complete two desk-side briefs and now decide to leave the base to grab some poke (seasoned diced raw fish) from a local vendor, you recall seeing on your commute into the base (Jackson, 2020). As you drive down a local road, traffic begins to pick up, and you simultaneously notice several traffic lights flickering erratically. At the same time, you begin to hear static emanating from your speaker. With abundant caution, you pull over and park on the shoulder of the road to better grasp the situation. As you initiate your hazard lights, you hear the radio broadcaster's distorted voice fill your car. You are deeply troubled by the news that follows. First, you faintly hear him advise that water treatment plants are offline. Next, the broadcaster informs listeners that pilots and unmanned aerial vehicles have reportedly lost contact with their respective air traffic controllers. Finally, and before the transmission becomes completely un-*

*intelligible, you hear him state that global missile warning systems appear to be down. Following the news, you immediately check your surroundings, shift your vehicle's gear into drive, and use familiar landmarks to find your way back to the base since your vehicle's built-in Navstar Global Positioning System (hereinafter GPS) appears inoperable.*

Though notional, these events can happen just as quickly as this fact pattern suggests and, in turn, can cause complete and utter chaos. These occurrences are just a tiny, and certainly not exhaustive, list of events that can occur if the precise position, timing, and navigation capabilities of the United States' (U.S.) GPS system is lost.

The GPS program can trace its origin to the Sputnik era when U.S. scientists were able to track the Soviet Union's first artificial satellite, Sputnike-1, by monitoring the shifts in radio signals. The ability the U.S. developed to trace and monitor an object in space was later classified as the "Doppler Effect" and paved the way for determining an object's location. Currently, the U.S.'s GPS is a satellite-based navigation system presently operated by the United States Space Force. This system is composed of a constellation of 31 operational satellites. Given the coverage, users are generally in view of at least four satellites at any given time, orbiting middle earth in both retrograde and prograde. Each satellite is arranged in six equally spaced orbital planes and circles the earth twice daily. The capabilities GPS has provided to the U.S. has proven and established benefits to both civilian and military applications. Systems such as Friendly Force Tracking (FFT), Defense Advanced GPS Receivers (DAGR), and even smartwatches are all capable due to the precise time synchronization and comprehensive coverage offered by our constellation of GPS satellites. As time progresses and technology advances, peer and non-peer threats establish capabilities that can and will impact the military's use of GPS-based applications. EMI and GPS jamming capabilities have proven to be asymmetric threats that can and will affect the DOD warfighting capabilities. These threats are crucial elements in the domain of Electronic Warfare (EW) and must not be left unchecked.

This article will discuss the fundamentals of GPS, propose Navigation Warfare tenets (Safeguard, Intercept, and Preserve), and then further analyze why the DOD should be increasingly concerned with EMI and GPS jamming. Ultimately, this article will outline several techniques, tactics, and procedures (TTPs) (1. Anticipation, 2. Consistent Observation, 3. Encryption, and 4. Reporting), senior military leaders can implement to equip forces to ensure they are prepared to fight and win in a degraded or denied environment. The DOD's proactive prioritization of navigation warfare is crucial in mitigating the asymmetric threats of GPS jamming and EMI, which have the capacity to disrupt and undermine various multi-domain military operations.

## The GPS Program

GPS capabilities have made tremendous strides in the last decade. From the increased understanding of the electromagnetic spectrum (EM) to the expanded navigational reach of space travel – GPS programs are now actively utilized as never before (Mai, 2017). Through the deployment of various GPS-based satellites, constant coverage (24 hours a day, 365 days per year) has become a reality (Maps GPS Info, 2019). The current GPS constellation of satellites ensures users can view at least four satellites from virtually any point on the planet (Maps GPS Info, 2019). This robust and persistent coverage allows civilian and military-based applications to receive accessibility and bandwidth capabilities like none other (GPS.Gov, 2022). In the following sections, this article will provide a brief overview of GPS, followed by a short synopsis of how GPS is utilized in the U.S. armed forces.

## Understanding the GPS

Satellite-based tracking devices are commonly referred to as GPS devices (Mai, 2017). Technically, GPS cites to a specific system of satellites created by and developed for the U.S., particularly the DOD (Herbert, 2011). Over the last three decades, GPS technology, which uses signals from satellites to determine a target's position, has evolved from developing and deploying military-based reconnaissance satellites to a comprehensive tracking and timing system widely used by civilians and military personnel alike (Herbert, 2011).

In its simplest form, the GPS consists of three main components: a space-based component (i.e., satellite), a receiver, and a command-and-control component (Joint DOD/DOT Task Force Report, 1993; Woodard, 2019). The space-based component consists of twenty-four satellites, which orbit the earth while broadcasting a positioning signal (Joint DOD/DOT Task Force Report, 1993; Woodard, 2019). The U.S. GPS constellation consists of 31 operational satellites covering at least 95% of the earth (Herbert, 2011). The spaced-based component involves satellites that cycle in medium earth orbit at an altitude of approximately 20,200 kilometers (around 12,500 miles) (GPS.gov, 2022). Initially, these satellites are launched as part of a payload package and then strategically placed into medium earth orbit so that any point on earth is directly in sight of at least four satellites (GPS.gov, 2022). The persistent presence of the GPS satellite constellation is a significant achievement, allowing coverage worldwide at any time of day or night (GPS.gov, 2022).

The second component is the receiver. The receiver is found within the user segment and is the aspect of GPS with which the average user is most familiar (Woodard, 2019). The receiver obtains the information supplied by the satellite and then calculates its three-dimensional location (longitude, latitude, and elevation above sea level) through trilateration (Joint DOD/DOT Task Force Report, 1993). Here, trilateration

can be understood as the process of determining the position of a point based on the known location and distance to three other points (India, 2022). Simply put, a GPS device receives a signal from a satellite, and the system calculates the distance between the receiver and the satellite, identifying the possible position of the device as anywhere within the satellite's signal radius (i.e., the satellite's footprint) (Hutchins, 2007). This process repeats with another satellite, creating two elliptical spheres. Here, the two signals provide a precise position, which could be any of the two points intersecting the two ellipses of signal coverage (Hutchins, 2007). Sadly, more is needed for the mission of the DOD, leading to a third satellite joining the process, revealing the device's precise location where all three ellipses intersect (Hutchins, 2007). For the receiver to provide 3- dimensional positioning information, a minimum of 4 satellites are required; due to the three-dimensional, spherical nature of the earth, this cross-section of satellite data ensures increased accuracy and information such as altitude, which would otherwise be incalculable (Dempsey, 2022).

The last is the command-and-control component (also known as the ground station or the master control station) (Ehrhart, 2000). This component is located strategically on earth and is responsible for telemetry operations (Ehrhart, 2000). Telemetry operations are defined as data transmitted and received from the satellite (Ehrhart, 2000). In addition to telemetry, the command-and-control component is also responsible for sending daily time and location updates to each satellite, ensuring that the entire network of satellites is appropriately synchronized (Ehrhart, 2000). Furthermore, the command-and-control component monitors the state and health of satellites and manages and controls the payload and mission data (Smithsonian National Air and Space Museum, 2012). To meet the GPS mission, the command-and-control component uses time, elevation, azimuth, range, and range rate to track their respective satellites and communicate for the duration of the satellite's life cycle (Smithsonian National Air and Space Museum, 2012). With regard to management, the United States Space Force Support and Operations Squadrons currently control our various satellite constellations and operate many of the command-and-control components (SpaceForce.Mil, 2020). Each Squadron plays a vital role in the Navigation Warfare (NAVWAR) construct, and all play a part in operating the GPS constellation and ensuring precise, three-dimensional position, velocity, and timing information is transmitted to both military and civilian users around the globe (SpaceForce.Mil, 2020).

In addition to the support offered by the Squadrons listed above, wideband satellite operation centers also play a vital role and control terminal access, responding to space anomalies and alarms, and monitoring the health and welfare of satellites (and spacecraft) within their area of responsibility (Segin, 2020). This is an increasingly important mission and equally significant in NAVWAR. To date, there

are five wideband space operation centers worldwide (Segin, 2020).

Despite the capabilities offered by systems that utilize the GPS program and the hard-working service members who labor tirelessly monitoring and ensuring each satellite's (and respective spacecraft's) functionality, limitations still exist in terms of optimizing utilization of the EM spectrum. The limitations addressed throughout this article provide an avenue for peer and non-peer threats to develop sophisticated capabilities to disrupt our systems and, in turn, our way of life (Orschel, 2005). As such, senior leaders must ensure adequate training is offered throughout their formations to ensure the members are cognizant of their environment, aware of the ever-looming threat of EMI and GPS jamming and working collectively to ensure proper encryption is always active in key systems.

## Utilizing the Electromagnetic Spectrum

The GPS program is an effective tool that the DOD utilizes to accomplish various missions, such as GPS-guided munition strikes, search and rescue operations, remote piloting of uncrewed aerial vehicles, and missile defense/warning (GPS.gov, 2022). The GPS Master Control Station monitors and controls the GPS satellite constellation and plays an enormous role in supporting the initiatives listed above (Wise, 2021). In addition to the duties mentioned above, the Master Control Station is also a support element that maintains the health and status of the GPS operational constellation (Wise, 2021). Relying on tracking and monitoring stations worldwide, service members supporting the Master Control Station are responsible for conducting 24-hour operations to monitor, control, and ensure GPS performance and reliability meet or exceed the requirements of both military and civilian users (Global Positioning System Precise Positioning Service Performance Standard, 2020).

Satellite communication is exceptionally relevant to the DOD because it enables leaders and forces on the ground to see and communicate beyond the line of sight (GPS.gov, 2022). In order to effectuate satellite communications, the GPS program effectively utilizes the EM spectrum to accomplish this mission. The three frequency bands within the EM spectrum that are employed for satellite communications are Ultra High Frequency (3000 megahertz (MHz)), Super High Frequency (3 gigahertz (GHz)-30GHz), and Extremely High Frequency (30GHz-300GHz). Satellites operate in various areas in these frequency bands, communicate, and receive data via wavelengths (Kueser, 2004). Though technological strides have allowed for increased understanding of wavelengths, various limitations and vulnerabilities are still associated with each satellite's communication frequency band (Joint Publication, 2018). For instance, in UHF, this frequency band has limited channels despite its boasted capability of smaller terminal capacity and ease of antenna pairing (Joint Publication, 2018). This

frequency is also highly susceptible to scintillation (i.e., space weather) and jamming (Joint Publication, 2018). SHF is a prominent frequency and is commonly utilized within the DOD, known most notably for its use in NIPR/SIPR/VOIP communications (Electrospaces.net, 2022). Unfortunately, despite its common usage, SHF also has frequency restrictions, including limited terminal mobility and high satellite costs, which are equally susceptible to jamming, earth weather, and scintillation (Electrospaces.net, 2022). Last is EHF. This frequency band is by far the most secure of the three (Electrospaces.net, 2022). To further expound, EHF is jam-resistant, has extensive bandwidth to operate with, and is also resistant to scintillation (Electrospaces.net, 2022). However, the downfall is ~~that~~ this band is expensive to operate within, is, ~~in fact,~~ susceptible to earth weather, and has a notable tradeoff between data rates and protection offered (Electrospaces.net, 2022).

Given the bandwidth issues identified in two of the three frequencies (UHF and SHF), techniques have been developed to allow multiple users to share the same frequency. These techniques are Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), and Code Division Multiple Access (CDMA) (Rouse, 2016). In FDMA, the available channel bandwidth is divided into non-overlapping frequency bands, wherein each is dynamically assigned to a specific user to transmit data (Rouse, 2016). TDMA is a channel access method for shared-medium networks (Ndungu, 2021). It allows several users to share the same frequency channel by dividing the signal into different time slots (Ndungu, 2021). The last technique, CDMA, is a spread-spectrum technology standard that assigns a pseudo-noise code to all speech and data bits, sends a scrambled transmission of the encoded speech over the air, and reassembles the speech in its original format (Ndungu, 2021). Collectively, these multiplexing techniques allow multiple users to effectively share the same bandwidth and increase the functionality of the DOD's use of the EM spectrum (Ndungu, 2021). In addition to having a firm understanding of the techniques used to increase capabilities, users must also remember that modern military operations are critically dependent on the EM spectrum. Accordingly, a key goal of our adversaries and enemies is to deny the DOD forces the ability to use it successfully (Joint Publication, 2020). As such, the DOD must always recognize the capabilities and vulnerabilities associated with EMI, GPS jamming, and other forms of signal interference. In order to combat this, service members must be cognizant of their system's capabilities and be prepared to fight signal interference/disruption with established TTPs to combat these threats.

## Critical Missions of the GPS Program

Before smart watches or DAGRs, mariners looked to the skies and used compasses to measure speed, time, and distance (Woodard, 2019). Over time, the DOD has

evolved from celestial navigation and dead reckoning to more sophisticated and precise technology geared toward helping service members accomplish their missions (Woodard, 2019). Today, with an expanded understanding of the EM spectrum, space, and space-based capabilities, the DOD must continue to increase its emphasis on the GPS program and three of its most critical mission sets. The first critical mission set is that the GPS satellite constellation must provide users with accurate positioning, velocity, and time data (Ehrhart, 2000). Accurate timekeeping has always been a critical mission of the DOD that impacts all its members (Ehrhart, 2000). In fact, Middle Age and Renaissance mariners typically used hourglasses to measure time – indeed dating the significance of this initiative system (Ehrhart, 2000). Without accurate position data, traditional GPS tracking systems would be unable to utilize trilateration, which could reduce the accuracy of positioning of DOD forces, assets, or systems (Ehrhart, 2000). The second critical mission is focused primarily on nuclear detection. In the era of hypersonic weaponry, one of the DOD's most important missions is providing clear and unequivocal nuclear missile detection (Ehrhart, 2000). In order to achieve timely and unequivocal missile detection, GPS satellites must be appropriately aligned and functional – at any time of day and night (Ramey, 2000). This is a highly salient and visible mission set since several countries have nuclear and hypersonic intercontinental ballistic missile capabilities, with some assets being able to reach speeds of Mach 5 and also capable of altering their course mid-flight (Ramey, 2000). In order to meet this mission set, DOD service members must be prepared to provide around-the-clock service and be fully versed in their assigned systems and their capabilities. The GPS program's third mission is to provide highly accurate timing information, especially for timing synchronization (GPS.gov, 2022). Timing synchronization is an essential function of the GPS program and one that is closely tied to the DOD's first mission (GPS.gov, 2022). In order to access this function, GPS receivers decode time signals to work appropriately, synchronizing each receiver to the atomic clocks (Time Machines, 2019). This enables users to determine the time to within 100 billionths of a second by utilizing atomic syncing clocks established in our GPS constellations (Time Machines, 2019). The capability of producing precise time is crucial to various military and economic activities worldwide, making this yet another critical mission of the GPS program.

## Understanding How Satellites Communicate

In order to operate GPS-enabled devices, service members should understand GPS signals and be knowledgeable about how GPS carrier frequencies are being utilized. In a nutshell, each GPS satellite continuously broadcasts navigation signals on two carrier frequencies – L1, the primary frequency, and L2, the secondary frequency (Mckenna, Gaudion, Evans, 2019). The L1 signal is centered

at 1575.42 (MHz), and the L2 signal is centered at 1227.6 MHz. (Mckenna, Gaudion, Evans, 2019).

GPS offers two types of services that enable users to navigate: Standard Positioning Service (SPS) and Precise Positioning Service (PPS) (Global Positioning System Standard Positioning Service Performance Standard, 2020). SPS is a free service available to everyone with a standard GPS receiver (Global Positioning System Standard Positioning Service Performance Standard, 2020). SPS provides navigation through the C/A (Coarse Acquisition) code which is broadcast on the L1 band only (Global Positioning System Standard Positioning Service Performance Standard, 2020). PPS, however, is available only to the U.S. military and various government agencies and requires encryption to acquire and use (Mckenna, Gaudion, Evans, 2019). The code that carries this encryption is known as P(Y) (Precise – Encrypted) and is broadcast on both the L1 and L2 frequency bands (Global Positioning System Standard Positioning Service Performance Standard, 2020).

Military receivers can access both the L1 and L2 frequency bands (Mckenna, Gaudion, Evans, 2019). The receiver must be encrypted for military receivers to move from unencrypted to encrypted (Global Positioning System Standard Positioning Service Performance Standard, 2020). The receiver achieves encryption by first acquiring the C/A code, finding what is known as a "Handover Word" embedded in the code, which then allows the receiver to synchronize and "lock" onto the P(Y) code that is broadcast on the L1 and L2 frequency (Global Positioning System Standard Positioning Service Performance Standard, 2020). While an encrypted receiver is not impervious to interference or jamming, the structure of the code is more robust than C/A, which makes it able to withstand interference or jamming effects longer (Global Positioning System Standard Positioning Service Performance Standard, 2020).

## Tenets of Navigation Warfare

Establishing a core set of principles that are universally adopted throughout the DOD is essential to unifying efforts to combat NAVWAR. Joint Publication 3-14, Space Operations, defines Navigation NAVWAR as deliberately offensive and defensive actions to ensure friendly use and prevent adversary use of Position, Navigation, Timing (PNT) information through coordinated employment of space, cyberspace, and electromagnetic warfare EW capabilities (Joint Publication, 2020). Given the guidance outlined in Joint Publication, 3-14, the DOD should remain increasingly vigilant in the space of NAVWAR and implement tenets to align our warfighting functions (Joint Publication, 2020). There are several reasons why this initiative should be pursued. First, GPS has been historically used as the default PNT system for DOD forces. For example, FFT and DAGR systems rely heavily on GPS data for timing and accuracy, and the inability to utilize these systems could have dire or catastrophic consequences (MAJ

Nowels, MAJ Fechter, 2014). In order to properly operate on the encrypted L1 and L2 code, there must be timing synchronization between the application and the GPS satellite (Joint Publication, 2020). The critical timing element is vitally important. If rendered inoperable due to EMI or GPS jamming, the system(s) at issue risk having a significant political and/or economic impact (Joint Publication, 2020). These are but a few reasons why the DOD should be concerned about GPS jammers and EMI capabilities (Joint Publication, 2020). In addition to the abovementioned concerns, the DOD should also be solicitous about GPS jammers and EMI from a susceptibility standpoint. For starters, GPS signals are inherently weak, which in and of itself makes them more prone to becoming a victim of GPS jamming (Larsen, 2021). Secondly, GPS jamming technology is simple but highly effective (Larsen, 2021). In fact, recent articles have highlighted the increased capabilities and accessibility of cheap, effective, and commercially accessible GPS jamming devices (Larsen, 2021). Last and certainly not least, jamming systems can appear anywhere and without warning (Larsen, 2021). The concern mentioned above, combined with the nominal financial burden it takes to develop and implement GPS jammers, makes the DOD warfighting function vulnerable in every sense of the manner. In response to the issues raised, the DOD should create tenets to emphasize the significance of NAVWAR and highlight the roles and responsibility of each service member that utilizes GPS-based applications.

To prepare and protect service members from denial and deception-based jamming efforts, senior leaders should develop tenets to ensure NAVWAR is at the forefront of warfighting functions. For example, *Safeguard, Intercept, and Preserve* could serve as tenets in the NAVWAR operational construct. In its simplest form, *Safeguard* could memorialize the DOD's efforts to protect personnel and friendly forces from GPS disruption. By implementing the *Safeguard* tenet (in addition to proper education and system familiarization), service members can minimize the likelihood or impact of signal interruptions. The second proposed tenet is *Intercept. Intercept* can symbolize the DOD's efforts to prevent or expropriate hostile forces from using EMI techniques with minimal effects on friendly forces. The *Intercept* tenet can and should be echoed down to the lowest element of DOD formations. If done correctly, tenets *Safeguard* and *Intercept* can ensure that service members are equipped with the tools they need to combat signal interference, recognize vulnerabilities, and offer steps to identify signal interruptions' origins. If done in conjunction with routine systems familiarization, service members will have the tools they need to overcome EMI or GPS jamming and engage the proponent of said disruption. Last, the DOD could focus its efforts on *Preservation*. By preserving the civil use of GPS systems outside the theatre of operations, the DOD can decrease the likelihood of signal interruption. The three proposed tenets are simple but effective ways to

communicate the NAVWAR initiative across all formations. As a warfighting function, the DOD must be prepared to control the battlefield and be confident in its understanding of EMI and GPS jamming. Establishing and enforcing NAVAWAR tenets will allow the DOD to react more efficiently, respond more intelligibly, and engage the EW threat more credibly.

In addition to establishing and championing well-defined tenets, it is imperative that government funding to support space-related technologies be continued. On March 28, 2022, the Biden-Harris Administration submitted to Congress a proposed Fiscal Year 2023 Budget request of $813.3 billion for national defense (Secretary of Defense Austin, 2022). Out of the proposed request, approximately $130 billion was solicited to be allocated to research and development (H.R.7776, 2022). Also, the National Defense Authorization Act provided a specific line item dedicated to applied research and educational activities to support space technology development (House Armed Services Committee, 2023). Given the figures and allocation requested by the present Commander in Chief, it is clear that the U.S. government understands the need to sharpen readiness in advanced technologies, such as GPS. Presently, governmental appropriations are sufficient to meet the growing need for support in the NAVWAR construct. However, this focus must stay steadfast as the race to disrupt GPS-based capabilities shows no sign of slowing down.

## Understanding Electromagnetic Interference

A firm understanding of EMI is vital to combat signal interference. In the arena of EMI, there are two main categories – Denial and Deception (Joint Publication, 2020). Denial is a less sophisticated means of signal interruption and prevents friendly antennas from receiving data transmitted via the electromagnetic spectrum (Joint Publication, 2020). This category is straightforward. To accomplish denial, the adversary will use a form of EW (e.g., an impediment to network access) to deny service members the right to unimpeded access to the EM environment. If done correctly, communication efforts, satellite access, and computer systems may prove ineffective. The second is deception. Deception is a more sophisticated means of signal interruption (Joint Publication, 2020). This category of EW attempts to mislead decision-makers by manipulating their understanding of reality (Joint Publication, 2020). If used successfully, the deception technique can genuinely affect the DoD's flexibility on the battlefield by emulating other signals or conflating current data, thereby confusing the battlefield and relaying inaccurate or untimely information (Joint Publication, 2020).

The most common forms of deception are repeaters and spoofers (Bagaria, 2020). Repeaters and spoofers are increasingly prevalent in the EW space. GPS spoofing alters the signals or data associated with GPS to produce

different PNT information (Bagaria, 2020). Put another way, it is a way to trick the GPS receiver (and the application it is running on) into thinking that you are in another place or another time (Bagaria, 2020). Next is Repeaters. Repeaters transmit signals to places that they usually cannot reach (Bagaria, 2020). Essentially, this form of EW intentionally sends radio frequency signals to interfere with radar operation by saturating its receiver with noise or false information (Annulli). Both these subcategories of deception and denial are highly effective and can impact multiple military-based applications at any given time (Annulli).

In addition to denial and deception tactics mentioned above, there are two additional types of EM attacks: EMI and EM jamming (i.e., GPS jamming) (Joint Publication, 2020). EMI is the intentional insertion of EM energy into transmission paths in any manner to deceive operators or cause confusion (similar to deception) (Joint Publication, 2020). Similarly, EM jamming is the deliberate radiation, re-radiation, or reflection of EM energy to prevent or reduce an enemy's effective use of the EM spectrum, used to degrade or neutralize the enemy's combat capability (Joint Publication, 2020). If done correctly, these techniques can be highly effective and degrade the communication network (SHF or EHF) utilized during military operations.

Techniques such as repeaters, spoofers, EMI, and EM jamming are just a short list of tactics that are taken to impede the DOD's ability to communicate and operate freely. To combat these threats, the DOD must remain vigilant, ensure forces are educated and aware of ever-growing EW threats and be cognizant of techniques they can utilize to resist the same.

## Tactical Training Points

To combat EMI and GPS jamming, senior leaders must ensure that their respective forces are educated on jamming and EMI capabilities, understand the tenets of NAVWAR, and implement TTPs to ensure, as an organization, they are prepared to fight in a degraded or denied environment. For the last twenty years, the DOD has operated with complete freedom of maneuver in the United States Central Command area of operation (*Air Force Times*, 2021). This maneuverability was a considerable strength and allowed forces to operate freely within the operational space without genuine fear or disruption caused by GPS jamming or EMI (aside from those disruptions caused by earth and terrestrial weather) (*Air Force Times*, 2021). However, times have changed and the battlespace has evolved. At this very moment, the DOD must be prepared to operate in any environment, including those denied or degraded. In order to accomplish this mission, the DOD must ensure that forces are educated on EW (GPS jamming and EMI), have a firm understanding of the capabilities and limitations of their systems, and recognize NAVWAR tenets. Lastly, senior leaders must focus their efforts on developing TTPs to ensure fidelity of the NAVWAR mission.

In order to create fidelity in this effort, leaders can develop short but effective TTPs that resonate with service members, in garrison, during exercises, and in deployed settings. To assist, this article will highlight four TTPs that can be implemented without delay. The first proposed TTP is *anticipation*. In this technological era, senior leaders should anticipate the likelihood of GPS jamming and EMI. As mentioned, the DOD should consider the current environment, be vigilant, and expect frequent EMI-based and cyber-related attacks. The second proposed TTP is *continuous and deliberate observation*. DOD forces should monitor and understand their system's operational environment. In the event systems become degraded due to jamming or EMI, service members should implement alternate means of communication and know, with an outstanding level of detail, what actions they will take when their system is denied or degraded (e.g., celestial navigation, map, compass, protractor navigation, or assembling alter communication methods). With a keen knowledge of their systems and the EM spectrum, forces can create primary, alternate, contingency, and emergency (commonly referred to as PACE) plans to simulate what steps they will need to take in the event of a signal intrusion. The third TTP should be *encryption*. Forces at all levels need to be reminded to encrypt everything that is GPS enabled. The constant encryption concept may seem commonsensical, but the failure to encrypt systems (i.e., DAGRS or FFT) is an often-overlooked task and can prove costly when desperately needed. Last, and certainly not least, is *reporting*. One of the most essential training points this article highlights is to remind service members of the requirement to report instances of GPS jamming or EMI under the procedures outlined in the Joint Spectrum Interference Resolution (JSIR) (Chairman of the Joint Chiefs of Staff Instruction, 2013). The JSIR addresses persistent and recurring EMI problems in joint operations, including those between civil and DOD systems and those involving space systems (Chairman of the Joint Chiefs of Staff Instruction, 2013). Further, the JSIR outlines reporting, response, and resolution procedures for spectrum interference, and provides detailed guidance to the DOD regarding standard EMI detection, characterization, reporting, identification, geo-location, and resolution procedures for space and terrestrial systems (Chairman of the Joint Chiefs of Staff Instruction, 2013). Effective EMI management is crucial to obtaining and maintaining information superiority, an essential foundation of information operations. Timely and accurate identification, verification, characterization, reporting, geolocation of the source, analysis, and resolution of EMI during military operations is vital to maintaining command and control of U.S. forces and responding to adversary EW actions. Consider the notion that if a service member does not report a deliberate EMI attack, no one will know to investigate the intrusion or develop a means to prevent it from impacting them or a fellow battle buddy in the future.

## The Benefits of Legal Counsel

Each EMI, jamming activity, or proposed countermeasure has unique legal considerations. Senior leaders must routinely engage their assigned judge advocate to develop a legal framework for operating in these particular cyber, space, and electronic areas of operations. Similarly, judge advocates assigned to provide counsel must have a firm understanding of the EM network, know the appropriate policy considerations, and be familiar with relevant authorities related to the concepts of NAVWAR (Joint Publication, 2018). Assigned judge advocates must also be prepared to add value by understanding what makes up the legal framework, which includes international treaties, regulations, and host nation laws, where applicable (Joint Publication, 2020).

International space treaties are bodies of work that establish fundamental principles of public international space law (Durkee, 2019). To date, several multilateral treaties govern extraterrestrial extensions of State sovereignties (Durkee, 2019). The most notable treaties are as follows: the 1963 Limited-Test-Ban Treaty (Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, 1962), the 1972 Liability Convention (Convention on International Liability for Damages Caused by Space Objects, 1972), the 1967 Outer Space Treaty (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 1967), the 1968 Rescue Agreement (Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 1968), the 1979 Moon Agreement (Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 1979), and the 1975 Registration Convention (Convention on the Registration of Objects Launched into Outer Space, 1975). In order to be influential legal advisors, judge advocates should be aware of existing and emerging international authorities and stay abreast of efforts undertaken by the United Nations Office for Outer Space Affairs (United Nations Office for Outer Space Affairs, 2023).

Regulations also play a significant role in the space legal framework. Agencies generally issue regulations to provide specific guidance on space-related activities (Durkee, 2019). Though typically non-binding or punitive, these bodies of work are living documents and can prove extremely helpful to judge advocates looking to learn more about unique or specifically tailored areas within the space construct.

Spacefaring nations generally promulgate laws and policies that are developed to regulate anything from military use of satellites to private companies looking to offer commercial space services. Over the years, nations have taken various approaches to conduct and adjudicate space activities and tailor their regulatory framework for how they regulate/monitor their space-based activities. Given the nuances involved, judge advocates will not likely

know every host nation's law. However, they should be cognizant of the various bodies of authority that may play a role in space operations.

By understanding the legal framework and being involved in the planning process, judge advocates can spot issues, advise on rules of engagement, provide legal reviews on proposed concepts of operations, understand and interpret various and evolving levels of authority, and offer counsel on policy-related matters. Their involvement is critical and will serve not only as risk management but as possible conflict avoidance.

Finally, judge advocates must work to learn and understand space and space-based capabilities. Judge advocates assigned to support space operations must actively seek opportunities to enhance their understanding of space-based assets, enablers, and capabilities. In order to accomplish this, judge advocates can seek and obtain training from their respective institutions or connect with organizations such as the Army Space Professional Development Office, which offers courses such as the space planners and space fundamentals course throughout the year. Though not rooted in law, these courses will undoubtedly increase a judge advocate's capacity to understand this dense area of multi-domain operations and also allow those interested in space an opportunity to learn the technical and force enhancement functions the Army and United States Space Force currently possess.

## Conclusion

GPS is an integral component of the DOD and its mission. Applications such as mapping and surveying; air, land, and sea-based timekeeping and navigation; traffic control; agriculture; and civilian-based emergency management for disasters like Super Typhoon Marwar all depend on our GPS constellation to function correctly with limited to no signal interference. However, as adversaries actively seek to disrupt GPS systems, it is imperative to be prepared to defend against these threats. Both peer and non-peer threats work tirelessly to ensure that DOD systems are impacted to gain an edge in the current NAVWAR battlespace. EMI and GPS jamming can affect ground-based missions, cyberspace, space, and even air and maritime operations. As such, the DOD and senior governmental leaders must understand NAVWAR concepts and increase capabilities during intentional EMI or GPS jamming by outside threats and unintentional fratricide by friendly forces.

Additionally, Combatant Commanders and subordinate commanders at all levels should consider the points raised in this article and also contemplate standing up EMI/GPS jamming operation centers. Strategically, these centers can be developed as a subset of the Multi-Domain Task Force construct and play an integral role in the DOD's "integrated deterrence" concept (Lopez, 2021). These centers should be staffed by cyber electromagnetic warfare officers, capable of massing EW effects on

adversaries, and geospatial intelligence imagery analysts, with comprehension of imagery exploitation software and mastery in analyzing fixed/moving targets. Once formally activated, the center will be a network of knowledge, expand our situational awareness, and increase the likelihood of successfully defending against EMI and GPS jamming attacks. In closing, by prioritizing NAVWAR and taking proactive measures to counter EMI and GPS jamming, the DOD can maintain superiority when operating within the EM spectrum and ensure the success of its missions across all domains. This article should serve as a starting point for understanding NAVWAR and a constant reminder that the DOD must continue to shape the battlefield and prepare its forces to win in the NAVWAR space.

## References

Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, U.N. GAOR. (1979, December 18). U.N. Doc. A/34/46, 1434.

Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, U.N. GAOR. (1968, April 22). U.N. Doc. A/6716, 584.

Air Force Times. (2021, October 6). Compass Call squadron is coming home after 20 years of hacking and jamming enemies in CENTCOM. *Air Force Times.* Retrieved from https://www.airforcetimes.com/news/your-air-force/2021/10/11/this-compass-call-squadron-is-coming-home-after-20-years-of-hacking-and-jamming-enemies-in-centcom/

Annulli, M. (n.d.). Repeater Jamming. RADA USA. Retrieved from https://radausa.com/blog/electronic-warfare-jamming- deception.

Austin, L. (2022, March 28). *The Department of Defense releases the President's fiscal year 2023 defense budget*. Retrieved from https://www.defense.gov/News/Releases/Release/Article/2980014/the-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg/.

Bagaria, A. (2020, November 12). *Electronic warfare: Jamming, spoofing, and ground stations*. RBC Signals. Retrieved from https://rbcsignals.com/blog/electronic-warfare-jamming-spoofing-and-ground-stations/.

Chairman of the Joint Chiefs of Staff Instruction (2013, March 8). CJCSI 32000.02F.

Convention on International Liability for Damages Caused by Space Objects, U.N. GAOR. (1972, March 29). U.N. Doc. A/8429, 262.

Convention on the Registration of Objects Launched into Outer Space, U.N. GAOR. (1975, January 14). U.N. Doc. A/9631, 552.

Dempsey, C. (2022). What is the difference between GIS and Geospatial? *GIS Lounge*. Retrieved from https://www.gislounge.com/difference-gis-geospatial/.

Durkee, M. (2019, January 1). Interstitial space law. *Washington University Law Review*. *423*, 442.

Ehrhart, B. (2000). A technological dream turned legal nightmare: Potential liability of the United States under the Federal Tort Claims Act for operating the Global Positioning System, *33 Vanderbilt Journal of Transnational Law. 371*, 376.

Electrospace.net. (2015, March 11). *U.S. military and intelligence computer networks*. Retrieved from https://www.electrospaces.net/2015/03/us-military-and-intelligence-computer.html.

GPS.gov (2022, June 28). *Department of Defense*. Retrieved from https://www.gps.gov/governance/agencies/defense/.

GPS.gov. (2020, April). *Global Positioning System Precise Positioning Service Performance Standard*. Retrieved from https://www.gps.gov/technical/ps/2020-SPS-performance-standard.pdf

GPS.gov. (2022, June 28). *Space segment*. Retrieved from https://www.gps.gov/systems/gps/space/

H.R.7776. (2022). *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, Title XVI-Space Activities, Strategic Programs, and Intelligence Matters, Section 1607.

Herbert, I. (2011). Where we are with location tracking: A look at the current technology and the implications on Fourth Amendment jurisprudence, *16 Berkeley Journal of Criminal Law*. 442, 442.

Housed Armed Service Committee. (2023). *FY23 National Defense Authorization Act*. Retrieved from https://armedservices.house.gov/sites/republicans.armedservices.house.gov/files/Final%20FY23%20NDAA%20Conf%20Highlights.pdf.

Hutchins, R. (2007). *Tied up in knotts? GPS technology and the Fourth Amendment*,

55 UCLA L. Rev. 409, 417.

Jackson, K. (2020, August 29). What is a Hawaiian poke bowl? How to make a poke bowl. *Today***.** Retrieved from https://www.today.com/food/what-hawaiian-poke-bowl-how-make-poke-bowl-t189956

Joint DOD/DOT Task Force Report. (1993). *The Global Positioning System: Management and operation of a dual use system***.**

Joint Publication. (2018, June 8). *Cyberspace Operations,* 3-12, I-2.

Joint Publication. (2018, June 8). *Cyberspace Operations*, 3-12, I-8.

Joint Publication. (2020, May 22). *Electromagnetic spectrum operations*, 3-85, I-3.

Joint Publication. (2020, May 22). *Joint Electromagnetic Spectrum Operations*, 3-85, Appendix B.

Joint Publication. (2020, October 26). *Space Operations,* 3-14, II-3.

Joint Publication. (2020, October 26). *Space Operations*, 3-14, I-7(d).

Kueser, J. (2004, April 1). *This LAN is my LAN, This LAN is your LAN: The case for extending private property rights to Wireless Local Area Networks***,** *University of Missouri-KansasCity Law Review***,** 787, 789.

Larsen, P. (2021, January 1). *Will harmful interference bring GPS down?* 86 Journal of Air Law & Commerce, 3, 23.

Lopez, C. T. (2021, April 30). *Defense Secretary says 'integrated deterrence' is cornerstone of U.S. defense*. U.S. Department of Defense. Retrieved from https://www.defense.gov/News/News-Stories/Article/Article/2592149/defense-secretary-says-integrated-deterrence-is-cornerstone-of-us-defense/

Mai, T. (2017, August 7). Global Positioning System history. *National Aeronautics and Space Administration (NASA)*. Retrieved from https://www.nasa.gov/directorates/heo/scan/communications/policy/GPS_History.html

Maps GPS Info. (2019, March 29). *GPS History - How it all started*. Retrieved from http://www.maps-gps-info.com/gps-history.html**.**

Mckenna, A., Gaudion, A., & Evans, J. (2019). The role of satellites and smart devices: Data surprises and security, privacy, and regulatory challenges, *123 Penn*

*State Law Review.* 591, 609.

Ndungu, S. (2021, March). *CDMA (Code-Division Multiple Access).* Tech Target. Retrieved from https://www.techtarget.com/searchnetworking/definition/CDMA-Code-Division-Multiple-Access.

Nowels, R. & Fechter, M. (2014). *Understanding GPS: The importance of a militaryreceiver in a GPS-contested environment*. Retrieved from https://www.benning.army.mil/infantry/magazine/issues/2015/Apr-

Orschel, B. (2005, October 1). *Assessing a GPS-based global navigation satellite system within the context of the 2004 U.S. space-based positioning, navigation, and timing policy*, 70 Journal of Air Law & Commerce. 609, 623-624.

Ramey, R. A. (2000, January 1). *Armed conflict on the final frontier: The law of war in space*, **48** *The Air Force Law Review. 1*, 15-16.

Rose India. (2022). *What is trilateration?* Retrieved from http://roseindia.net/technology/gps/what-is-trilateration.shtml

Rouse, M. (2016, December 5). *Frequency Division Multiple Access (FDMA)*. Techopedia. Retrieved from https://www.techopedia.com/definition/5669/frequency-division- multiple-access-FDMA.

Segin, S. (2020). *New battalion satellite communications operations center, fully operational on Fort Carson*. Retrieved from https://www.army.mil/article/232134/new_battalion_satellite_communications_operations_center_fully_operational_on_fort_carson

Smithsonian National Air and Space Museum. (2012). *How does GPS work?* Retrieved from https://timeandnavigation.si.edu/multimedia-asset/how-gps-works.

Time Machines Corp. (2019, October 8). *What is a GPS clock system?* Retrieved from https://timemachinescorp.com/2019/10/08/what-is-a-gps-clock-system/

Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, UN, (1962, August 5), U.S.T. 1313 (ratified by the United States on Oct. 7, 1963; entered into force on Oct. 10, 1963).

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, U.N. GAOR. (1967, January 27). U.N. Doc. A/6316, 613.

U.S. Space Force. (2020). *Space Delta 8.* Retrieved from https://www.spoc.spaceforce.mil/About-Us/Fact-Sheets/Display/Article/2334040/space-delta-8.

United Nations Office for Outer Space Affairs (2023). *About us***.** Retrieved from https://www.unoosa.org/oosa/en/aboutus/index.html.

Wise, B. (2021, December 14). The magic of GPS simplified. *United States Space Force.* Retrieved from https://www.spoc.spaceforce.mil/News/Article-Display/Article/2874327/the-magic-of-gps-simplified.

Woodard, J. (2019). Oops. My GPS made me do it: GPS manufacturer liability under a strict products liability paradigm when GPS fails to give accurate directions to GPS end users, *34 Dayton Law Review*, 429, 434.