REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
27-04-2018	FINAL	

4. TITLE AND SUBTITLE

Joint Force Operations in GPS-denied or degraded environment.

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Eric J. Radspinner, LT USN

Paper Advisor (if Any): Prof. Michael Crosskey

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

For Example Distribution Statement A: Approved for public release; Distribution is unlimited.
Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Since 1997, the Department of Defense has recognized the vulnerability of the Global Positioning System to jamming. Since 2011, technologies to simulate and override the signal a GPS receiver receives have been developed and now are in use. This paper looks at how the loss of GPS, either through jamming or spoofing, affects the Joint Force and its operations. Using a Position, Navigation and Timing framework, major weapon systems, launch platforms and critical processes are examined. This examination details how combat operations, while possible, will be significantly more challenging. Impacts on weapon accuracies and launch platforms navigation systems can be minimized through effective training. The impact on communication and coordination between multiple units and the resulting fog and friction created is harder to define without real-life research and practice. Current and ongoing Joint Force preparations for GPS-denied or degraded environments through two main lines of effort are described. The paper concludes with recommendations on where the Joint Force should focus to ensure it maintains its current capabilities.

15. SUBJECT TERMS

GPS, Denied, Degraded, Joint Force Operations

16. SECURITY CLASSIFICATION OF:	17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
			Chairman, JMO Dept

a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		20	401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, R.I.

Joint Force Operations in GPS-denied or degraded environments

By

Eric Jon Radspinner

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

27 April 2018

Paper Abstract

Since 1997, the Department of Defense has recognized the vulnerability of the Global Positioning System to jamming. Since 2011, technologies to simulate and override the signal a GPS receiver receives have been developed and now are in use. This paper looks at how the loss of GPS, either through jamming or spoofing, affects the Joint Force and its operations. Using a Position, Navigation and Timing framework, major weapon systems, launch platforms and critical processes are examined. This examination details how combat operations, while possible, will be significantly more challenging. Impacts on weapon accuracies and launch platforms navigation systems can be minimized through effective training. The impact on communication and coordination between multiple units and the resulting fog and friction created is harder to define without real-life research and practice. Current and ongoing Joint Force preparations for GPS-denied or degraded environments through two main lines of effort are described. The paper concludes with recommendations on where the Joint Force should focus to ensure it maintains its current capabilities.

Since its inception in 1973 by the Department of Defense, the Global Positioning System (GPS) has been the world's foremost Position, Navigation and Timing (PNT) source. Using a cluster of 24 satellites, GPS provides accurate and dependable signals for navigation across oceans, land and throughout the air. GPS satellites transmit using the Coordinated Universal Time (UTC) and provide a convenient and identical timing source for everything from computers to electrical power grids to airport operations. Without it, these systems are vulnerable and can report significant errors. Because of this, the U.S. takes great pains to ensure GPS timing accuracy of the system to ensure public safety and national security

Which makes what happened on June 22, 2017, a clear threat to national security. On that day, over 20 ships operating in the Black Sea reported that their GPS position was 20 miles inland at a nearby airport.[1] This was the first reported large-scale incident of GPS spoofing. Tourists visiting the Kremlin in Moscow have reported similar situations.[2]

Yet, these were not the earliest indications of GPS-spoofing. Iran newspapers reported that in September 2011, electronic warfare specialists had spoofed a CIA-drone into landing where they could disassemble and reverse engineer its technology.[3] To test how this was accomplished, the Department of Homeland Security requested University of Texas professor Todd Humphrey to spoof the GPS on a small helicopter drone in June 2012.[4] Prof. Humphrey was able to override the signal the drone was receiving. Using an altered altitude

[1] David Hambling, "Ships fooled in GPS spoofing attack suggest Russian cyberweapon," *Daily News*, August 10, 2017, https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon.
[2] Elizabeth Weise, "Mysterious GPS glitch telling ships they're parked at airport may be anti-drone measure," *USATODAY*, September 26, 2017, https://www.usatoday.com/story/tech/news/2017/09/26/gps-spoofing-makes-ships-russian-waters-think-theyre-land/703476001/.
[3] Connie Lee, "Spoofing Risks Prompt Military to Update GPS Devices," *National Defense*, January 4, 2018, http://www.nationaldefensemagazine.org/articles/2018/1/4/spoofing-risks-prompt-military-to-update-gps-devices.
[4] Mark L. Psiaki and Todd E. Humphreys, "Protecting GPS from Spoofers is Critical to the Future of Navigation," *IEEE* Spectrum, July 29, 2016, https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

signal, the drone nearly crashed itself before an operator intervened. In 2013, Professor Humphrey successfully spoofed the GPS onboard an $80 million yacht[5] at the owner's request. It is clear that the capability to spoof GPS position and timing signals exists, and can be accomplished against commercial signals with ease.

GPS spoofing is done by overriding the signals from the satellites using a land-based transmitter. The signals received from the satellites are relatively faint due to the satellite's locations over 12,000 miles above the Earth's surface and the low power transmitters they use. GPS spoofing technologies are readily available commercially. A few hundred dollars can buy a handheld GPS spoofing device the size of a pack of cigarettes that will interfere with all GPS receivers within a mile radius.

Commercial GPS receivers use a single frequency from multiple satellites to calculate the receiver's position. But for increased accuracy, military GPS receivers use an additional encrypted frequency that all GPS satellites broadcast. This encryption makes it significantly harder to falsify the data. So adversaries seek to jam the dual-use signals instead.

GPS jamming is simple to accomplish given the weak signal transmitted from the satellites. Random noise transmitted in the publicly known frequencies used by the satellites to raises the detection threshold above the level needed to establish a connection. This is done with relative ease; in fact, software code can be downloaded from the internet to change a simple radio transmitter into a simple GPS jamming device. The ability to spoof GPS and jam its signals indicates that the GPS is vulnerable.

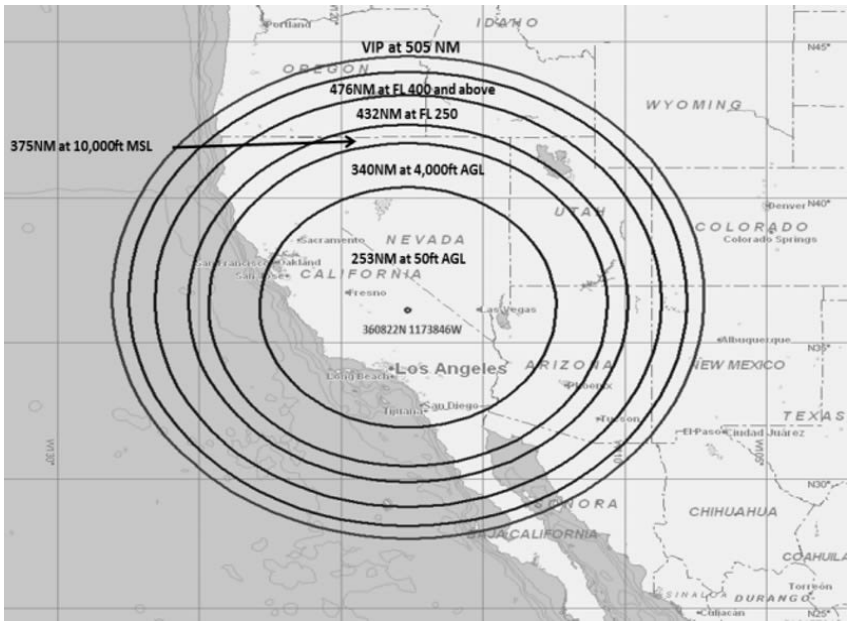
[5] Aviva Hope Rutkin, "'Spoofers' Use Fake GPS Signals to Knock a Yacht Off Course," *MIT Technology Review*, August 14, 2013, https://www.technologyreview.com/s/517686/spoofers-use-fake-gps-signals-to-knock-a-yacht-off-course/.

With the Joint Force's technological and relative combat power advantages, its dependency on the simple and vulnerable GPS system reveals a clear critical vulnerability. While the Joint Force can operate in current GPS denied/degraded systems, failure to continue to develop, test and refine these operations will significantly degrade a Task Force commander's ability to accomplish their mission.

This paper will examine how prepared the Joint Force is to operate in a GPS denied/degraded environment. Using the PNT framework, I will show how major weapon systems, launch platforms, and processes are impacted by the degradation or denial of GPS. A counterargument about how GPS denied/degraded operations are too challenging for the Joint Force is included. Then I will cover how the Joint Force is preparing for operations in these environments and finish with recommendations to ensure the Joint Force will be able to meet tomorrow's challenges.

For the discussion, I will use the Federal Aviation Administration's warning given in June 2016 as the limits of a GPS denial/degraded operations area[6] from a single transmitter. These ranges include a safety factor to ensure public safety. However, this establishes the maximum range effects could be expected and allows for easy extrapolation.

[6] Matt Novak, "FAA Warns of GPS Outages This Month During Mysterious Tests on the West Coast," Gizmodo, June 7, 2016, https://gizmodo.com/faa-warns-of-gps-outages-this-month-during-mysterious-t-1780866590.



Position

The first part of the analysis examines positional accuracy impacts on platforms on weapon systems that use GPS mainly as an accurate (within 2.6 meter[7]) position source. From this, range and bearing to targets are calculated to support field artillery or Naval Surface Fire Support (NSFS). Changes in Circular Error Probability (CEP) are used as well as the time difference in establishing initial position using alternate methods to show the affects of GPS denial or degradation.

Modern artillery systems, including mobile howitzers and Fire Support Vehicles, use a combination of GPS and Inertial Navigation Systems (INS) to track their current location and determine their firing position. These artillery systems can use GPS-enabled INS, INS only or accept a manually entered position. In manual, Fire Support Teams can use a variety of other methods to determine their firing location such as field surveys or celestial positioning, but will incur a corresponding loss of accuracy.

[7] DoD Positioning, Navigation and Timing Executive Committee, "Global Positioning System Precise Positioning Service Performance Standard," (Washington DC: DoD, 2007), B-27.

Methods other than GPS increase the CEP from less than 4 meters to over 10 meters [8] depending on the method used. For modes other than GPS-enabled, the vehicles must periodically stop and use another source to determine their position every 5 or 10 minutes depending on the accuracy required.[9] This has a significant impact on their speed of advance.

Artillery units also need to determine target locations. The transition from GPS-assisted systems increases Target Location Error (TLE) from less than 6 meters up to over 200 meters, depending on the method used. Without GPS, artillery units can maintain a TLE of less than 6 meters using INS-only.[10]

Advanced Field Artillery Tactical Data System (AFATDS) is the Army and Marine Corps automated command and control network used to coordinate the 27 fire support tasks.[11] It allows for coordination from the platoon level to the Corp and enables the commander to utilize all of the fire support available to him. If GPS is degraded or denied, AFTADS can function in a stand-alone method but requires personnel to manually input data[12] and introduces human errors into an automated process.

The Tomahawk Land Attack Missile is the Navy's preferred first strike munition in preparation for tactical air strikes launched from carriers. Block III and IV TLAMs have a GPS-enabled INS navigation system coupled with Terrain Contour Matching (TERCOM) with a range of 1000 nautical miles. Older Block II TLAMs lack the GPS capability of the Block IV and instead rely on the INS for navigation.

---

[8] Col. Stephen J. Maranian, "Degraded Operations White Paper," (Fort Sill, 2016), 15.
[9] Ibid.
[10] Ibid., 9.
[11] Advanced Field Artillery Tactical Data System (AFTADS) Family of Systems (FoS), U.S. Marine Corps Concepts and Programs, last modified March 27, 2017, https://marinecorpsconceptsandprograms.com/programs/fire-support/advanced-field-artillery-tactical-data-system-afatds-family-systems-fos.
[12] Maranian, "Degraded Operations White Paper," 21.

The incorporation of GPS in Block III TLAMs decreased the mission planning time from 80 hours to under 2 hours. It also allowed for missiles to loiter in an area to create multiple missile strikes at the same time.

While the CEP for Block III and IV TLAMs is classified, Block II TLAM CEP is roughly 10 meters.[13] and is assumed for this analysis to be representative of the accuracy of Block III and IV TLAMs launched in a GPS denied/degraded environment.

How TLAMs respond to entering a GPS-denied area needs to be fully explored and tested to fully understand how the system responds to ensure effective targeting can be maintained. The Digital Terrain Contour Mapping system also needs testing in a GPS-denied environment. For example, how the system responds to a target on an island protected by a GPS-denial system and needs to be tested.

The Joint Direct Attack Munition (JDAM) is a guidance kit that provides advanced targeting guidance when mated to a free-fall bomb. With its GPS/INS navigational suite, its nominal CEP is less than 5 meters. Without internal GPS, the CEP grows to 30 meters if given GPS quality position data from the launch aircraft.[14] and a free fall less than 100 seconds. Current range of the JDAM is 15 nautical miles with efforts to increase that to 40 nautical miles. Laser JDAMs add a targeting laser on the nose cone that enables the bomb to attack mobile targets being lazed within the targeting area..[15]

Given the expected size of a GPS denied operations area, it is reasonable to assume that the launching platform's position handed to the JDAM will be affected. Cascading

[13] Tomahawk, CSIS Missile Defense Project, last modified September 19, 2016, https://missilethreat.csis.org/missile/tomahawk/.
[14] Joint Direct Attack Munition GBU-31/32/38, U.S. Air Force, June 18, 2003, http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104572/joint-direct-attack-munition-gbu-313238/.
[15] Joint Direct Attack Munition, Boeing, https://www.boeing.com/history/products/joint-direct-attack-munition.page.

positional errors can be statistically modeled to obtain the CEP, but live-fire testing is required to validate the model.

Alternate methods for determining a weapon systems position can be used if GPS is unavailable or unreliable. However, these alternatives introduce errors that decrease the weapons accuracy and can increase the time necessary to establish firing positions and target locations.

Navigation

After examining systems that use GPS as mainly a position source, the next step is to assess navigational processes and how GPS denial or degradation affects them.

The Harpoon is a multi-target type missile launched from a variety of platforms. It uses the same GPS-enabled INS system as the JDAM.[16] With a range of 67 miles, it has a CEP of 10 to13 meters.[17] The missile is capable of Over-The-Horizon (OTH) targeting using information shared from a targeting platform.

Because its launch platform will be inside a GPS-denial system, exact effects on its CEP or its effectiveness using targeting data is not fully known. The effect of position errors in OTH targeting needs further development if Harpoons are planned to be used while GPS-denial systems are still operational.

The next system examined is the Inter-Continental Ballistic Missile (ICBM). Land-based ICBMs use an INS-based navigation system that combines the missile's acceleration data, Earth's gravitational field and fixed initial position to achieve its accuracy.[18] Submarine

[16] Harpoon Block II Anti-Ship Missile, Naval Technology, https://www.naval-technology.com/projects/harpoon-block-ii-anti-ship-missile/.
[17] Harpoon, CSIS Missile Defense Project, last modified September 5, 2017, https://missilethreat.csis.org/missile/harpoon/.
[18] Minuteman Guidance System, Smithsonian National Air and Space Museum, https://airandspace.si.edu/collection-objects/guidance-system-minuteman-iii.

Launched Ballistic Missiles use the launching platforms initial location and compensates for errors and environmental factors using an INS coupled with stellar navigation.[19] Both of these systems are independent of GPS and not affected by its degradation or denial.

US Navy surface ships use a complex navigation suite that combines inputs from multiple inertial navigation systems, GPS receivers and other shipboard sensors such as radar. This PNT system is called the Navigation Sensor System Interface (NVSSI).[20] This system allows for the comparison of position data from different sources and distributes it to multiple stations throughout the ship, including its weapons systems.

The ability to compare position sources minimizes the impact GPS denial/degradation has on surface ship navigation. Yet, the effect of GPS denial on a mission like NSFS requires the understanding of how navigation errors are compiled across the firing unit's, the locating unit and the actual target locations.

Similar to surface ships, submarines rely on inertial navigation systems with GPS used to correct errors in position and heading due to INS drift. GPS is only available when at Periscope Depth although submarines can use other position sources when submerged. Submarines utilize both commercial and military GPS receivers with frequent comparisons between all PNT sources.

Submarine warfare is affected by GPS denied/degraded environments in two ways. The first is TLAM strikes with small location errors in submarine position and the effects on TLAM operations already discussed. The second is positional errors in target location

[19] FBM Weapon System 101, Strategic Systems Programs, http://www.ssp.navy.mil/fb101/functionalelements.html#IV.
[20] Peter Shaw and Bill Pettus, "An Integrated Approach to Electronic Navigation," (San Diego: Space and Naval Warfare Systems Center, 2001), 1.

information passed from and to a submarine. By nature, these errors are small and easily accounted for.

Manned aircraft have a GPS-enabled INS combination navigation system such as the Northup-Grumman LTN-100G Ring Laser Gyroscope.[21] Based on the expected range from a GPS denial system, incoming aircraft will see effects before entering land-attack weapons range. Air to air missions will be minimally impacted due to air-to-air missiles not utilizing GPS.

Similar to manned aircraft, larger drones such as the MQ-9 Reaper and RQ-4 Global Hawk have a GPS/INS combination navigation suite. Small drones lack the capacity to carry these larger systems and use Commercial GPS PNT. Breaking the communication signal between the drone and its base combined with spoofing the GPS signal is how Iran claims to have taken the CIA drone.[22]

The overall impact on navigation processes from a GPS denial or degradation system can be mitigated if the affected unit has been sufficiently trained and prepared for operations in those environments. The operational fires plan to destroy or neutralize an adversary's defenses needs to be developed and tested to maximize the effectiveness of the Joint Force.

Timing

After examining major weapons and the platforms used to launch them, the next step is to look at processes that use GPS as an accurate and precise timing source and how they are affected in a GPS denied or degraded environment. Disruptions in radio and satellite

[21] F22 Raptor Advanced Tactical Fighter, Air Force Technology, https://www.airforce-technology.com/projects/f22/.
[22] Scott Peterson, "Downed US drone: How Iran caught the 'beast'," *Christian Science Monitor*, December 9, 2011, https://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast.

communications will not be discussed although an adversary capable of interfering with GPS operations will most likely be capable of conducting additional types of EM warfare.

Command and control data links require precise and exact timing to be established among all net users. Data links, such as Link 11 or Link 16, are able to send and receive information near-simultaneously by using 7.8125-microsecond long time slots[23] allocated to different users. The Link 16 data link also changes frequencies every 13 microseconds[24] for increased jamming protection.

This precise time structure requires that all net users use the exact same time and frequency. Because of the precise timing signal, GPS makes creating, maintaining and joining a data net easier, more reliable and faster. Data links can create their own reference time for use in the net; however, any station wishing to join must first determine and then match the time from the master control station. Minor timing errors can and will cause the net to crash. Establishing and maintaining a data net is also a highly perishable skill.

The inability to use data links, such as Link 16, will have significant impacts on the Joint Force. Data links are how target information is shared between tactical units. Communication and coordination between different units will be degraded. Missions such as Close Air Support and Fires will most likely see the greatest impact if data links are unable to be maintained.

However, loss of the GPS timing signal can be overcome by the Joint Force. The data links that use the timing signal have the ability to establish their own reference time for redundancy but establishing and maintaining it in a combat environment requires continuous training and practice by all units using the net.

[23] Northrop Grumman, "Understanding Voice and Data Link Networking" (San Diego: Northrup Grumman, 2014), 2-32.
[24] Ibid, 2-15.

Counter-argument

After examining how GPS denied or degraded operations affect major weapon systems, platforms and processes, it can lead to the logical conclusion that loss of GPS introduces too much fog and friction for the Joint Force to operate effectively. Individual units will rely on less-capable alternate systems or devote large amounts of resources towards making GPS-dependent systems work.

While specific military-grade jamming signal strengths are classified as well as specific enemy capabilities, high power jamming sites can reach ranges of up to 476 nautical miles based on DOD testing in California.[25] Localized jamming can also be separately used to protect high-value targets against the precision weapons used by today's Joint Force. These two processes, combined, create a defense-in-depth scheme using a relatively large "stay out" area with additional safeguards provided for individual units and sites.

Additionally, advances in anti-satellite technology (ASAT) have placed the GPS satellites themselves at risk. In 2007, China shot down a failing Chinese satellite that was roughly 530 miles above the surface.[26] While GPS satellites are placed in Medium Earth Orbit around 12,000 miles above the Earth's surface, the Chinese conducted a rocket launch in 2013[27] assessed to be capable of hitting GPS or other satellites.

By denying the use of GPS as a PNT source, US enemies can remove the technological advances the Joint Force has over them. This enables the adversary to potentially isolate and defeat selected units of the Joint Force.

---

[25] Novak, "FAA Warns of Outage,".
[26] Edward Cody, "China Confirms Firing Missile to Destroy Satellite," *Washington Post*, January 24, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/01/23/AR2007012300114.html.
[27] Andrea Shalal-Esa, "U.S. sees China launch as test of anti-satellite muscle:source," *Reuters*, May 15, 2013, https://www.reuters.com/article/us-china-launch/u-s-sees-china-launch-as-test-of-anti-satellite-muscle-source-idUSBRE94E07D20130515.

Rebuttal

Because there are numerous ways to deny or degrade GPS, each country will develop a separate strategy and scheme based on their current technology and defense budget. These differences require the Joint Force to approach and attack each one separately and allows the Joint Force to develop a sequential and systematic method of dismantling individual portions of GPS-denial/degradation schemes. For example, using TLAMs to target high power jammers followed by Harpoons launched at low-power jammers as a common tactic with the timing and preparations operationally different.

ASAT weapons are expensive, difficult to develop and preparations for launch are usually visible to US intelligence. This limits the countries who pose a credible threat to GPS satellites. In February 2018, Dan Coates, the Director of National Intelligence, stated "Russian and Chinese destructive ASAT weapons probably will reach initial operational capability in the next few years."[28]

In addition, the GPS constellation consists of 36 satellites flying in a 27-slot constellation. This means there are multiple satellites available as replacements if necessary. GPS satellite orbits can also be changed to provide short-term coverage.

Because of its worldwide usage, denying the US GPS will also affect any adversary themselves unless they possess an alternative to GPS. Due to the high technological and financial requirements to develop and maintain GPS alternatives, these are limited to India[29], Russia, China and the European Union. These systems are also subject to same jamming, spoofing and destruction possibilities as GPS.

---

[28] Director of National Intelligence, *Worldwide Threat Assessment of the US Intelligence Community*, (Washington DC: February 2018).

[29] Defenceupdate, "Beidou v/s IRNSS – Where Did India's Own GPS stand against Chinese?," *Indian Defence Update*, July 10, 2017, https://defenceupdate.in/beidou-vs-irnss-india-gps-stand-chinese/.

Current Preparations

As early as 1997, The Joint Force has recognized its dependency on GPS and the system's vulnerability. Preparations for operations in GPS denied/degraded environments have focused along two main lines of effort: personnel and equipment. The Department of Defense has been investigating ways to increase the protection of friendly use of GPS and deny enemy usage.[30] New M-code satellites use a spectral separation from the civil signals that enables higher accuracy with less impact on civil operations. They create a more jam-resistant signal through higher power levels and directed spot beams vice whole-earth signals. This separation also allows for selective US jamming of GPS signals to reduce the enemy usage of GPS without degrading use by the Joint Force.

The Air Force tested the new M-code signals on a B-2 at Edwards Air Force Base in December 2017.[31] Rockwell Collins has partnered with the Army and Air Force to test smart weapons using M-code.[32] Of note, neither test was performed in a GPS denied or degraded environment.

DARPA is developing and testing alternatives to GPS. The Adaptable Navigation System (ANS) collects and compares time and location signals from different sources such as cell towers, television towers, and radio towers. Similar to how GPS works, this system then calculates the receiver's position.

The second main effort is down the personnel side. Platforms utilizing GPS also regularly train on its loss or degradation and how to operate in such environments. Artillery

[30] Col. Richard L. Reaser, Jr, "What are the major characteristics (improvements) of M-code relative to (over) the existing P-code?," *Inside GNSS*, May/June 2006, 25.
[31] Tracy Cozzens, "New M-code GPS capability tested onboard B-2 bomber," GPS World, December 5, 2017, http://gpsworld.com/new-m-code-gps-capability-tested-onboard-b-2-bomber/.
[32] Michael Peck, "Rockwell tests M-code GPS for smart weapons," *Military Times*, July 17, 2017, https://www.militarytimes.com/intel-geoint/2017/07/17/rockwell-tests-m-code-gps-for-smart-weapons/.

units are required to practice using the survey methods. Surface ships and submarines practice using alternate position methods such as Celestial Navigation. Establishing data nets without using the GPS timing signal is practiced as well.

All of this training is performed in a simulated GPS denied/degraded environment. The units being tested are usually the ones removing it and so know beforehand. This limits the effectivenesss and does not subject the units to the additional fog and friction they would experience in a GPS denied or degraded environment.

The US Air Force ran Developmental Test Navigation Festival (DT NAVFEST) in August 2017 and invited two civilian universities to utilize the GPS denied operating area for testing for their research.[33] Conducting additional exercises with research universities and defense contractors broadens the opportunities for development and understanding of how to counteract a GPS denied or degraded environment.[34]

Recommendations

While the Joint Force can adapt and overcome current potential adversary's GPS denial/degradation capabilities, research in GPS-hardening technologies and real-life practice in such environments is required to maintain the Joint Force's capabilities.

I recommend the creation of static GPS-denied operations areas that can be used for testing and unit evaluation. These areas could be part of a base that already have access and overflight restrictions to minimize the impact of other operations. The GPS-jamming equipment would be prepared and ready for use with the coordination with outside agencies already completed.

---

[33] Christopher Ball, "Dod, academia test systems for GPS denial," U.S. Air Force, September 13, 2017, http://www.af.mil/News/Article-Display/Article/1309991/dod-academia-test-systems-for-gps-denial/.
[34] Samantha Masunaga, "GPS guidance can be fooled, so researchers are scrambling to find backup technologies," *LA Times*, March 15, 2018, http://www.latimes.com/business/la-fi-gps-alternatives-20180315-story.html.

These sites could be used for testing the concerns in weapons, equipment, and processes previously discussed. Conducting multi-unit exercises in these environments would allow for the creation and dissemination of lessons learned at the operational level of war.

These sites would also be a key part of my second recommendation. The Joint Force needs to re-evaluate its methods and priorities when conducting operational fires at the start of a conflict.

Wargaming Phase I and II operations, focused on operational fires, will build processes in how we systemically neutralize or destroy the adversary's defenses, but the results cannot model the fog and friction that would actually be felt. The GPS-denied exercise areas can be used to validate the war game results and give commanders experience in such environments.

This leads to my final recommendation. The Joint Force needs to continue developing alternatives to GPS. These alternatives do not need to be on the same scale as GPS; they only need to function when GPS is disrupted. ANS is a good example that would work in parallel with GPS but in limited environments. Similiarly, a network of drones, using celestial navigation, and transmitting time and location signals in different frequencies, can be established for short-term use by the Joint Force in hostile environments. It would be a parallel, limited scope and duration alternative established only when needed. This would make it harder for the adversary to deny or degrade its operation while providing the Joint Force the same capabilities as GPS.

Bibliography

2017. "Advanced Field Artillery Tactical Data System (AFTADS) Family of Systems (FoS)." *US Marine Corps Concepts and Programs.* March 27. Accessed March 25, 2018. https://marinecorpsconceptsandprograms.com/programs/fire-support/advanced-field-artillery-tactical-data-system-afatds-family-systems-fos.

Air Force Technology.com. n.d. "F-22A Raptor Advanced Tactical Fighter." *Air Force Technology.* Accessed March 28, 2018. https://www.airforce-technology.com/projects/f22/.

Ball, Christopher. 2017. "DoD, academia test systems for GPS denial." *U.S. Air Force.* September 13. Accessed March 30, 2018. http://www.af.mil/News/Article-Display/Article/1309991/dod-academia-test-systems-for-gps-denial/.

Boeing. n.d. *Joint Direct Attack Munition Historical Snapshot.* Accessed March 26, 2018. https://www.boeing.com/history/products/joint-direct-attack-munition.page.

Coats, Dan R. 2018. "Worldwide Threat Assessment of the US Intelligence Community." Statement for the Record, Diretor of National Intelligence, Washington, DC.

Cody, Edward. 2007. "China Confirms Firing Missile to Destroy Satellite." *Washington Post.* January 24. Accessed March 29, 2018. http://www.washingtonpost.com/wp-dyn/content/article/2007/01/23/AR2007012300114.html.

Cozzens, Tracy. 2017. "New M-code GPS capability tested onboard B-2 bomber." *GPS World.* December 05. Accessed March 30, 2018. http://gpsworld.com/new-m-code-gps-capability-tested-onboard-b-2-bomber/.

CSIS Missile Defense Project. 2017. *Harpoon.* September 05. Accessed March 26, 2018. https://missilethreat.csis.org/missile/harpoon/.

Defenceupdate. 2017. "Beidou v/s IRNSS- Where Did India's Own GPS stand against Chinese." *India Defence Update.* June 18. Accessed March 30, 2018. https://defenceupdate.in/beidou-vs-irnss-india-gps-stand-chinese/.

DoD Positioning, Navigation and Timing Executive Committee. 2007. *Global Positioning System Precise Positioning Service Performance Standard.* Washington DC: Department of Defense.

Hambling, David. 2017. *Daily News.* Agust 10. Accessed March 24, 2018. https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/.

Lee, Connie. 2018. *National Defense.* January 4. Accessed March 24, 2018. http://www.nationaldefensemagazine.org/articles/2018/1/4/spoofing-risks-prompt-military-to-update-gps-devices.

Maranian, Stephen J. 2016. *US Army Field Artillery Degraded Operation White Paper.* White Paper, US Army.

Masunaga, Samantha. 2018. "GPS guidance can be fooled, so researchers are scrambling to find backup technologies." *LA Times.* March 15. Accessed April 01, 2018. http://www.latimes.com/business/la-fi-gps-alternatives-20180315-story.html.

Naval Technology.com. n.d. *Harpoon Block II Anti-ship Missile.* Accessed March 27, 2018. https://www.naval-technology.com/projects/harpoon-block-ii-anti-ship-missile/.

Northup Grumman. 2014. *Understanding Voice and Data Link Networkinig.* San Diego: Northup Grumman.

Novak, Matt. 2016. "FAA Warns of GPS Outages This Month During Mysterious Tests on the West Coast." *GIZMODO.* June 07. Accessed March 24, 2018. https://gizmodo.com/faa-warns-of-gps-outages-this-month-during-mysterious-t-1780866590.

Peck, Michael. 2017. "Rockwell tests M-code GPS for smart weapons." *Military Times.* July 17. Accessed March 30, 2018. https://www.militarytimes.com/intel-geoint/2017/07/17/rockwell-tests-m-code-gps-for-smart-weapons/.

Peterson, Scott. 2011. "Downed US drone: How Iran caught the 'beast'." *Christian Science Monitor.* December 9. Accessed March 28, 2018. https://www.csmonitor.com/World/Middle-East/2011/1209/Downed-US-drone-How-Iran-caught-the-beast.

Psiaki, Mark L, and Todd E Humphreys. 2016. "Protecting GPS from Spoofers is Critical to the Future of Navigation." *IEEE Spectrum.* July 29. Accessed March 24, 2018. https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation.

Reaser, Col. Richard. 2006. "What are the major characteristics (improvements) of M-code relative to (over) the existing P-code?" *Inside GNSS,* May/June: 25.

Rutkin, Aviva Hope. 2013. ""Spoofers" Use Fake GPS Signals to Knock a Yacht Off Course." *MIT Technology Review.* August 14. Accessed March 24, 2018. https://www.technologyreview.com/s/517686/spoofers-use-fake-gps-signals-to-knock-a-yacht-off-course/.

Shalal-Esa, Andrea. 2013. "U.S. sees China launch as test of anti-satellite muscle: source." *Reuters.* May 15. Accessed March 29, 2018. https://www.reuters.com/article/us-

china-launch/u-s-sees-china-launch-as-test-of-anti-satellite-muscle-source-idUSBRE94E07D20130515.

Shaw, Peter, and Bill Pettus. 2001. *An Integrated Approach to Electronic Navigation.* San Diego: Space and Naval Warfare Systems Center.

Smithsonian National Air and Space Museum. n.d. *Minuteman Guidance System.* Accessed March 27, 2018. https://airandspace.si.edu/collection-objects/guidance-system-minuteman-iii.

Strategic Systems Programs. n.d. *FBM Weapons Systems 101.* Accessed March 27, 2018. http://www.ssp.navy.mil/fb101/functionalelements.html#IV.

2016. "Tomahawk." *CSIS Missile Defense Project.* September 19. Accessed March 26, 2018. https://missilethreat.csis.org/missile/tomahawk/.

US Air Force. 2003. *Joint Direct Attack Munition GBU-31/32/38.* June 18. Accessed March 26, 2018. http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104572/joint-direct-attack-munition-gbu-313238/.

Weise, Elizabeth. 2017. *USATODAY.* October 3. Accessed March 24, 2018. https://www.usatoday.com/story/tech/news/2017/09/26/gps-spoofing-makes-ships-russian-waters-think-theyre-land/703476001/.