Journal of Air Law and Commerce

Volume 86 | Issue 1 Article 2

2021

Will Harmful Interference Bring GPS Down?

Paul B. Larsen

WILL HARMFUL INTERFERENCE BRING GPS DOWN?

PAUL B. LARSEN*

TABLE OF CONTENTS

 The Author taught air and space law for more than forty years at Southern Methodist University and at Georgetown University Law Center. He is co-author of FRANCIS LYALL & PAUL B. LARSEN, SPACE LAW: A TREATISE (2d ed. 2018) and PAUL B. LARSEN, JOSEPH G. SWEENEY & JOHN E. GILLICK, AVIATION LAW: CASES, LAWS AND RELATED SOURCES (2d ed. 2012). The Author thanks Professors Francis Lyall, Bill Covington, and Jennifer Manner for their valuable comments.

INTRODUCTION

THE U.S. GLOBAL Positioning System (GPS) is in deep trouble and in need of remediation for the following reasons:

(1) Civilian GPS is operated and controlled by the Department of Defense (DOD).[1] It is an essential element of much military equipment and civilian infrastructure and devices.[2] Both military and civilian uses are growing rapidly, but the two uses have become increasingly estranged from each other, as military authorities build a new, separate secure system for military use only.[3] The future of civilian GPS is uncertain.[4]

(2) Military authorities are actively preparing for cyber warfare and want to retain freedom to use their offensive and defensive cyber warfare capabilities to interfere with adversaries' Global Navigation Satellite Systems (GNSS).[5]

(3) Increasingly, military interference harms civilian satellite navigation signals: examples include the forced diversion of shipping in the Black Sea and commercial airline traffic in the Eastern Mediterranean Sea.[6]

---

[1] *Frequently Asked Questions*, GPS.GOV, https://www.gps.gov/support/faq/ [https://perma.cc/ZM6H-MDZA].

[2] Justin Lee, *What Is M-Code and Where to Learn More About Next-Gen Military GPS*, MODERN BATTLE SPACE (Apr. 26, 2019), https://modernbattlespace.com/2019/04/26/what-is-m-code-and-where-to-learn-more-about-next-gen-military-gps/ [https://perma.cc/5L5K-LTHX]; *GPS Applications*, GPS.GOV, https://www.gps.gov/applications/ [https://perma.cc/54KC-2B6Z].

[3] Lee, *supra* note 2.

[4] *See* Mariam Baksh, *Federal Contracts to Require Secure Timing and Navigation Under Executive Order*, NEXTGOV (Feb. 12, 2020), https://www.nextgov.com/cybersecurity/2020/02/federal-contracts-require-secure-timing-and-navigation-under-executive-order/163084/ [https://perma.cc/7PFY-SLTH]; *see, e.g.*, *Contracts For Aug. 31, 2020*, U.S. DEP'T OF DEF., https://www.defense.gov/Newsroom/Contracts/Contract/Article/2331179/ [https://perma.cc/7WJM-FLWE] (describing DOD contract for a military alternative to GPS).

[5] *A New Global Ranking of Cyber-Power Throws Up Some Surprises, Digital Dominance*, ECONOMIST (Sept. 19, 2020), https://www.economist.com/science-and-technology/2020/09/17/a-new-global-ranking-of-cyber-power-throws-up-some-surprises [https://perma.cc/6L8P-QD92].

[6] *See* Hiroyuki Yamada, *IMO and the GNSS, Navigating the Seas*, INSIDE GNSS, Sept./Oct. 2017, at 40, 40, https://insidegnss.com/wp-content/uploads/2018/01/sepoct17-LAW.pdf [https://perma.cc/S52Y-YJNE]; *see also* Greg Milner, *How Vulnerable Is G.P.S.?*, NEW YORKER (Aug. 6, 2020) , https://www.newyorker.com/tech/annals-of-technology/how-vulnerable-is-gps [https://perma.cc/DFF6-UWG2]; Anusuya Datta, *Vulnerabilities of GPS Is a Big Concern: Dana Goward*, GEOS-

(4) Spectrum jamming and spoofing tools are cheaply, easily acquired and are used for illegitimate purposes.[7]

(5) The scarcity of—and the sharp competition for—radio frequencies cause harmful radio interference with the signals used by GPS and by the other GNSS, as exemplified by the 2020 Federal Communications Commission (FCC) award of frequencies to Ligado Networks (Ligado).[8]

(6) The existing four GNSS—EU's Galileo, U.S. GPS, Russia's GLONASS, and China's BeiDou—compete with each other, demonstrated by (1) Galileo requiring European Union (EU) GNSS operators have Galileo access and (2) the FCC restricting foreign GNSS access to U.S. sovereign space.[9]

(7) GNSS tracks (1) criminals; (2) civilians; and (3) COVID-19 victims in violation of life, liberty, and property—protected by the Fifth Amendment to the U.S. Constitution and by the Declaration of Human Rights.[10]

(8) Harmful interference with civilian GNSS signals causes increasing need for encryption of civilian signals, but encryption will establish a different, more limited access to GNSS.[11]

(9) U.S. government leadership of GPS policy is scattered. It should be unified. The FCC struggles with the executive branch over allocation of spectrum for GPS. Furthermore, GPS navigation safety is not adequately improved by prospective civilian GPS regulation on the basis of economics by the U.S. Department of Commerce (DOC), rather than on the basis of safety by the interagency National Executive Committee for Space-Based Positioning,

---

PATIAL WORLD (Sept. 5, 2020), https://www.geospatialworld.net/blogs/vulnerabilities-of-gps-is-a-big-concern-dana-goward/ [https://perma.cc/SXS7-SAUR].

[7] *See infra* Part III; *see also* Paul Tullis, *GPS Is Easy to Hack, and the U.S. Has No Backup*, SCI. AM. (Dec. 1, 2009), https://www.scientificamerican.com/article/gps-is-easy-to-hack-and-the-u-s-has-no-backup/ [https://perma.cc/8R3U-8X6W].

[8] *E.g.*, In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3783 (2020). In 2016, LightSquared Subsidiary LLC became Ligado Networks (Ligado). *LightSquared and GPS*, GPS.GOV, https://www.gps.gov/spectrum/lightsquared/ [https://perma.cc/56C2-AQHG].

[9] *LightSquared*, 35 FCC Rcd. at 3773 n.2; Paul B. Larsen, *International Regulation of Global Navigation Satellite Systems*, 80 J. AIR L. & COM. 365, 398 (2015); *What Is Galileo?*, EUR. SPACE AGENCY, http://www.esa.int/Applications/Navigation/Galileo/What_is_Galileo [https://perma.cc/M7AX-H2GJ].

[10] *See* U.S. CONST. amend. V; G.A. Res. 217 (III) A, Universal Declaration of Human Rights, arts. 3, 17 (Dec. 10, 1948); *see also infra* Section VI.A.

[11] *See* Larsen, *supra* note 9, at 411–12; *see also infra* Section IX.C.

Navigation, and Timing (PNT Committee), Department of Transportation (DOT), and Federal Aviation Administration (FAA).[12]

(10) All four GNSS are plagued by increased traffic congestion, debris accumulation, collision danger, and scarcity of radio frequencies and orbits in outer space.[13]

GPS is an essential pillar of support for U.S. and international infrastructure. Unless it is strengthened, the growing number of jammings, spoofings, and harmful interferences will destroy GPS. Silence and inactivity are implied acceptance of these activities. This Article discusses options and suggests solutions.

Aviation, shipping, the electric grid, computers, military equipment, and many other parts of our basic infrastructure now depend on vulnerable GNSS signals.[14] These signals are weak, able to be suspended or "jammed" by stronger signals, and easily subject to harmful interference.[15] For example, "spoofing" happens when a weak GNSS signal is hacked and changed by an outside agent.[16] Harmful interference may happen in multiple ways. An agent may disrupt the signal simply by buying a radio-frequency jamming device for as little as $200.00.[17] Or that agent may deviously substitute the existing

---

[12] *Agenda: 60th Meeting of the Civil GPS Service Interface Committee*, GPS.GOV, https://www.gps.gov/cgsic/meetings/2020/ [https://perma.cc/7KYC-FAMJ]; Civ. GPS Serv. Interface Comm., *DHS PNT Update*, at 2:18:48, YOUTUBE (Sept. 22, 2020), https://www.youtube.com/watch?t=8328&v=6FpKN018zSM&feature=youtu.be (last visited June 2, 2021) (featuring James Platt, Director, PNT Program Management Office, U.S. Dep't of Homeland Sec.); Civ. GPS Serv. Interface Comm., *Resilient PNT System Concepts for Critical Infrastructure*, at 2:50:14, YOUTUBE (Sept. 22, 2020), https://www.youtube.com/watch?t=10214&v=6FpKN018zSM&feature=youtu.be (last visited June 2, 2021) (featuring Arthur K. Scholz, Principal Engineer, The MITRE Corporation). The CGSIC met virtually Sept. 21–22, 2020. *Agenda: 60th Meeting of the Civil GPS Service Interface Committee*, *supra*. The meeting, which the Author attended, discussed the range of issues discussed in this Article. *Id.* References are based on the Author's personal notes. *See also infra* Section VII.B.

[13] Paul B. Larsen, *Minimum International Norms for Managing Space Traffic, Space Debris, and Near Earth Object Impacts*, 83 J. AIR L. & COM. 739, 742, 747, 751 (2018); *see also* Mark Harris, *Who Gets To Send Radio Waves in Space?*, MIT TECH. REV. (June 26, 2019), https://www.technologyreview.com/2019/06/26/134533/spectrum-wars-satellite-communication/ [https://perma.cc/JD4Q-7SWB].

[14] Lee, *supra* note 2.

[15] Datta, *supra* note 6.

[16] *Id.*

[17] Int'l Comm. Glob. Navigation Satellite Sys., *Presentation: Proliferation of GPS/GNSS Jammer Devices*, U.N. OFF. OF OUTER SPACE AFFS., https://unoosa.org/documents/pdf/psa/activities/2019/UN_Fiji_2019/IDM/2-06-1120.pdf [https://perma.cc/Q6YX-UBTY].

signal with a harmful message.[18] While signal interference is illegal and the agent can be arrested and prosecuted,[19] prosecution is rare because the agent may be embedded in a foreign country; in fact, the agent may be a foreign government using signal interference for its own national security reasons.[20] Furthermore, radio frequencies are in short supply and sometimes aligned too closely to forestall harmful interference.[21]

With the exception of Galileo, GNSS satellites are operated by military authorities.[22] U.S. GPS was the first position, navigation, and timing (PNT) service and was designed for military use.[23] It did not become available to civilian airlines until after the 1983 Korean Airline Disaster.[24] President Ronald Reagan realized that the Korean airliner could have avoided entry into Russian airspace if it could use the military's satellite navigation system.[25] The current availability of GNSS for civilian users is a huge benefit. Military use is still considered a primary purpose for GNSS,[26] although civilian use far exceeds military use.[27] Except

---

[18] *Id.* at 3.

[19] *See, e.g.*, Quinten Plummer, *FCC Fines Chinese Company Record $35 Million for Marketing, Selling Illegal Jamming Devices in U.S.*, TECH TIMES (June 23, 2014), https://www.techtimes.com/articles/8973/20140623/fcc-fines-chinese-signal-jammer-seller-record-35-million-for-marketing-and-selling-illegal-devices.htm [https://perma.cc/ML2R-F29X].

[20] *See, e.g.*, Yamada, *supra* note 6 (describing a GPS spoofing attack in the Black Sea in 2017).

[21] *See* In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3801–02 (2020). Previously, spectrum scarcity was handled by parceling out closely aligned and duplicative frequencies across the globe to geostationary satellites. *See generally* Harris, *supra* note 13. An issue arose when operators began sending out multiple low-Earth orbit (LEO) satellites, which orbit the earth multiple times a day and potentially interfere with those geostationary satellites and the PNT systems they support. *Id.*

[22] *Galileo Navigation Satellite System*, GLOB. SEC., https://www.globalsecurity.org/space/world/europe/nav.htm [https://perma.cc/JN84-5DYS].

[23] The Author served on the U.S. government task forces established to make GPS available for nongovernmental users after the 1983 Korean Airline disaster. He has followed GNSS development since that time. *See also* Berenice Baker, *A Position in History: 25 Years of GPS*, AIRFORCE TECH. (July 21, 2020), https://www.airforce-technology.com/features/a-position-in-history-25-years-of-gps/ [https://perma.cc/T679-2PLT].

[24] SCOTT PACE, GERALD FROST, IRVING LACHOW, DAVID FRELINGER, DONNA FOSSUM, DONALD K. WASSEM & MONICA PINTO, THE GLOBAL POSITION SYSTEM: ASSESSING NATIONAL POLICIES 180 (1995).

[25] *Id.*

[26] *See* FRANCIS LYALL & PAUL B. LARSEN, SPACE LAW: A TREATISE 340 (2d ed. 2018).

[27] *Id.* Only 16% of GNSS use is for military purposes. *Id.*

for Galileo, GNSS services are dual use (military and civilian).[28] While military signals are encrypted, free civilian signals are not, and thus are greatly exposed to harmful interference.[29]

There are four global GNSS in current use: GPS, GLONASS, BeiDou, and Galileo.[30] How do they interact? An airplane flying in a western direction around the Earth starts out in China and begins to navigate by the Chinese BeiDou system. As it approaches Russia, its navigation may automatically shift to the Russian GLONASS system. Proceeding further west, it may shift again to the EU Galileo system. On approaching the United States, it may pick up the U.S. GPS. When it returns to China, it may again use the Chinese BeiDou system. Each of the four systems is controlled by its government of origin.[31] GNSS augmentations, such as the European Geostationary Navigation Overlay System (EGNOS) and the U.S. Wide Area Augmentation System (WAAS), are available for landing at local airports.[32]

The four systems provide world-wide networks.[33] There are small differences in the number of satellites in each system, but each GNSS consists of about 24–30 satellites.[34] Fortunately, the GNSS operators cooperate closely in the United Nations (U.N.) General Assembly Committee on Peaceful Uses of Outer Space (COPUOS) International Committee on GNSS (ICG).[35] Consequently, all four GNSS have agreed to assist each other and be interoperable.[36] Most cell phones and many computers are programmed to use any of the four systems. While this Article will focus on all four GNSS, it will give special attention to interferences with the U.S. GPS.

---

[28] Larsen, *supra* note 9, at 411.

[29] *Id.* at 412.

[30] *Id.* at 392.

[31] *Id.* at 371 ("GPS, GLONASS, and BeiDou are controlled by their national governments. Galileo is governed by the EU, but it is largely delegated to the European Space Agency.").

[32] LYALL & LARSEN, *supra* note 26, at 347.

[33] *See BeiDou Begins: China's Home-Grown SatNav System Will Soon be Fully Functional*, ECONOMIST (July 18, 2020), https://www.economist.com/china/2020/07/18/chinas-home-grown-satnav-system-will-soon-be-fully-functional [https://perma.cc/3QKJ-4AR8].

[34] *GPS, Galileo, Beidou, Glonass . . . What Differences?*, TELLER REP. (May 4, 2020, 5:41 AM), https://www.tellerreport.com/tech/2020-05-04-gps--galileo--beidou--glonass%E2%80%A6-what-differences-.BJ8vb_6FL.html [https://perma.cc/N8MA-FMNE].

[35] Larsen, *supra* note 9, at 371–72.

[36] *See id.* at 372–73.

GNSS is incorporated into virtually all military equipment.[37] Besides its basic military uses, GNSS is essential for navigation of airplanes, ships, cars, space objects, and agricultural vehicles.[38] Previous navigation by reference to the stars is no longer a realistic option. There is increasing need for higher accuracy GNSS.[39] GNSS is now essential for timing financial transactions, managing disasters, providing emergency health services, maintaining all telecommunications functionality, and tracking people, vehicles, and other moving objects.[40] Surveyors need it for accurate land measurement.[41] It is an essential element of cell phone and computer networks.[42] Weather forecasting depends on GNSS.[43] The electric power grid is monitored by GNSS.[44] In short, "critical infrastructure" depends on GNSS.[45] Loss of GNSS due to interference with its signals would be globally disastrous.[46]

This Article discusses several forms of interference with (1) GNSS receivers; (2) GNSS satellites; and (3) in particular, the radio-frequency spectrum used by the GNSS signals. Some harmful interference is deliberate, but some radio interferences have natural causes. For example, solar flares and solar radiation may affect GNSS signals.[47]

---

[37] Sarah M. Mountin, *The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals*, 90 INT'L L. STUD. 101, 111 (2014).

[38] *Id.* at 110–11.

[39] Matteo Luccio, *New Players Offering GNSS Correction Services*, GPS WORLD (July 23, 2020), https://www.gpsworld.com/new-players-offering-gnss-correction-services/ [https://perma.cc/RK3Q-LXRD].

[40] Mountin, *supra* note 37, at 111.

[41] *Surveying Using GPS And Conclusion*, ANZLIC COMM. SURVEYING & MAPPING, https://icsm.gov.au/education/fundamentals-mapping/surveying-mapping/surveying-using-gps-and-conclusion [https://perma.cc/Q49D-JFH4].

[42] Mountin, *supra* note 37, at 111.

[43] *Id.* at 112.

[44] *Id.* at 103.

[45] Exec. Order No. 13905, 85 Fed. Reg. 9359, 9359 (Feb. 12, 2020) (defining critical infrastructure) ("Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on national security, national economic security, national public health or safety, or on any combination of those matters."); *see also* Memorandum on Space Policy Directive-7, The United States Space-Based Positioning, Navigation, and Timing Policy (Jan. 15, 2021), https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-7/ [https://perma.cc/P2YU-HPEC].

[46] Mountin, *supra* note 37, at 111.

[47] Solar flares jam GNSS satellites facing the sun at the time of the eruption. Space service companies position satellites in outer space to detect natural disturbances in outer space. *See* SATELLITE NAVIGATION & SPACE WEATHER: UNDERSTAND-

Jamming and spoofing are illegal in the United States.[48] As described further below, the FCC primarily leads enforcement.[49] Other agencies and actors also have enforcement interests.[50]

I. STAKEHOLDERS

A. National Government

GNSS is global. The four governmental operators (United States, Russia, China, and the EU) are each protective of their respective system. All countries use GNSS, so all countries are all anxious to preserve their access to and use of GNSS. Five U.S. agencies are closely involved in regulating GNSS. U.S. governmental GNSS interests, described below, are similar to interests of other governments.

1. Military Authorities

GPS (the U.S. GNSS) is owned and operated by DOD.[51] It was originally designed exclusively for the military's navigation and warfighting purposes.[52] Thus, U.S. military authorities have a strong proprietary interest in GPS because it is an indispensable part of guided missiles and many other military weapons.[53] Military authorities continue to administer and operate GPS.[54] The Deputy Secretary of Defense co-chairs the interagency PNT Committee, which coordinates civilian GPS.[55] The PNT Committee meets regularly to set U.S. governmental policy for GPS.[56] Civilian use now predominates GPS.[57] However, the military continues to control GPS.[58]

---

ing the Vulnerability & Building Resilience, Am. Meteorological Soc'y 27 (2011), https://www.ametsoc.org/ams/assets/file/spacwx_gps_2010.pdf [https://perma.cc/AZ7N-8WCR].

[48] *E.g.*, Plummer, *supra* note 19.

[49] *See supra* Section III.C.

[50] *Id.*

[51] Paul B. Larsen, *Regulation of Global Navigation and Positioning Services in the United States*, *in* National Regulation of Space Activities 459–65 (Ram S. Jakhu ed., 2010).

[52] *Id.* at 462.

[53] *Id.*

[54] *Id.*; 10 U.S.C. § 2281(a); *see also* Lyall & Larsen, *supra* note 26, at 465.

[55] *National Executive Committee*, GPS.gov, https://www.gps.gov/governance/excom/ [https://perma.cc/EVJ3-3E82]; Memorandum on Space Policy Directive-7, *supra* note 45.

[56] Larsen, *supra* note 51, at 461.

[57] *See* Lyall & Larsen, *supra* note 26, at 340.

[58] *Id.*

The military authorities in Russia and China also control their GNSS; only the EU Galileo system is controlled by civilian authorities.[59] All military GNSS uses remain subject to international and national military laws and regulations.[60] Thus, GNSS is subject to the U.N. Charter provisions on international peace and security.[61] Although the timing clocks on GPS satellites use nuclear materials for accurate timing signals, GPS is not considered subject to the Outer Space Treaty (OST) prohibition on placing nuclear materials in orbit.[62] GPS is not considered a nuclear weapon.

Encrypted military signals are more difficult to seize and divert than standard, unencrypted civilian signals. As a precaution, U.S. military authorities are experimenting with alternate PNT systems in case GPS suffers damage due to interference.[63] States involved in military conflicts may also deliberately interfere with radio frequencies of enemy states.[64] To avoid possible foreign diversion of U.S. military GPS, DOD is protective of the radio frequencies used for GPS signals.[65] DOD also watches carefully for any potential, harmful interference with GPS by commercial users who compete for use of scarce radio frequencies.[66] A recent example of tension between military and civilian uses is Ligado's FCC application for use of frequencies that are so close to nearby GPS signals that there could be harmful interference.[67]

As a practical matter, GPS is generously funded by the U.S. Congress as a military system.[68] This funding includes researching and building alternate systems based on different technol-

---

[59] *Id.*

[60] *Id.*

[61] *See, e.g.*, U.N. Charter arts. 39–51.

[62] *See* Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies art. 4, Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter OST].

[63] Yasmin Tadjdeh, *Executive Order Seeks Stronger PNT Systems*, NAT'L DEF. MAG. (May 8, 2020), https://www.nationaldefensemagazine.org/articles/2020/5/8/executive-order-seeks-stronger-pnt-systems [https://perma.cc/S2X7-LE7Y].

[64] LYALL & LARSEN, *supra* note 26, at 466.

[65] *See, e.g.*, In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3783 (2020).

[66] *Id.*

[67] *Id.* at 3780; *see also* The Communications Act of 1934, 47 U.S.C. § 151–646 (establishing the FCC).

[68] *Program Funding*, GPS.GOV, https://www.gps.gov/policy/funding/ [https://perma.cc/7664-ATGU].

ogy.[69] By contrast, how likely is it that Congress might approve such generous funding of a separate GNSS for civilians? The current government has not indicated a willingness to spend the money required to develop and build an alternate system based on different technology.[70]

2. Department of Transportation

GNSS is an essential part of all transportation safety.[71] Along with the Deputy Secretary of Defense, the Deputy Secretary of Transportation serves as PNT Committee co-chair.[72] The U.S. Congress appropriates funding for FAA to administer civilian GPS air navigation activities.[73] Thus, DOT (including FAA) has a strong interest in GPS as an indispensable element of civilian air safety.[74] FAA's air traffic control system depends on aircraft operators being able to navigate safely using GPS.[75] FAA also maintains WAAS, an augmented GPS system, which facilitates airport landing.[76] FAA's Office of Commercial Space Transportation issues launch permits to operators of nongovernmental satellites,[77] which gives FAA additional interest in GNSS for safe navigation of nongovernmental satellites. Furthermore, all modes of transportation, especially driverless cars, now depend on GPS for safe navigation.[78]

3. Department of Commerce

DOC's National Oceanic and Atmospheric Administration examines and may approve applications for satellite remote sensing,[79] which provides DOC with a real interest in the assignment

---

[69] Teresa Hitchens, *House Strategic Forces Fences Space Force, SDA, GPS Funds*, BREAKING DEF. (June 22, 2020, 4:33 PM), https://breakingdefense.com/2020/06/house-strategic-forces-fences-space-force-sda-gps-funds/ [https://perma.cc/29JG-QSB5].

[70] *See Program Funding*, *supra* note 68.

[71] Larsen, *supra* note 9, at 388, 409 (describing GNSS aviation, marine, rail, road, and highway applications).

[72] *National Executive Committee*, *supra* note 55; Larsen, *supra* note 51, at 460.

[73] Larsen, *supra* note 51, at 461.

[74] *Id.* at 462; Memorandum on Space Policy Directive-7, *supra* note 45.

[75] Mark Harris, *FAA Files Reveal a Surprising Threat to Airline Safety: The U.S. Military's GPS Tests*, IEEE SPECTRUM (Jan. 21, 2021), https://spectrum.ieee.org/aerospace/aviation/faa-files-reveal-a-surprising-threat-to-airline-safety-the-us-militarys-gps-tests [https://perma.cc/ZTN8-RHKY].

[76] LYALL & LARSEN, *supra* note 26, at 347.

[77] Commercial Space Launch Act of 1984, 51 U.S.C. §§ 50901–50923.

[78] *See generally* Larsen, *supra* note 9; Larsen, *supra* note 51.

[79] 51 U.S.C. § 60134.

of frequencies to remote sensing spacecraft. DOC's National Institute of Standards and Technology (NIST) establishes measurement standards for communication with GPS receivers.[80] The 2020 White House Executive Order (EO) on GPS (EO 13905) designated the Secretary of Commerce to lead the vital effort of defining GPS elements and associated risks (also known as PNT profiles).[81] Additionally, DOC's National Telecommunication Information Administration (NTIA)—independently from the FCC—advises the President on federal communication policy.[82] Congress adopted 51 U.S.C. § 50112, designating DOC to manage GPS and to "protect [the GPS electromagnetic] spectrum from disruption and interference."[83] Furthermore, Congress designated the Secretary of Commerce to lead the development of nongovernmental space policy regarding GPS.[84] However, Congress has not appropriated the necessary funding to DOC.[85] DOC also has a seat on the PNT Committee.[86]

4. National Aeronautics and Space Administration

The National Aeronautics and Space Administration (NASA) has an inherent interest in the safe operation and administration of all outer space activities.[87] GNSS can be used to track and facilitate the navigation of space objects.[88] NASA also observes the orbits of satellites to assure regularity of orbit.[89] NASA is an active member of the PNT Committee.[90]

---

[80] *About NIST*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/about-nist [https://perma.cc/GSM3-2LKS].

[81] Exec. Order No. 13905, 85 Fed. Reg. 9359, 9360 (Feb. 12, 2020); Memorandum on Space Policy Directive-7, *supra* note 45.

[82] *About NTIA*, NAT'L TELECOMM. & INFO. ADMIN., https://www.ntia.doc.gov/about [https://perma.cc/PHQ8-LJ94].

[83] 51 U.S.C. § 50112(3).

[84] *Id.*

[85] *Program Funding*, *supra* note 68.

[86] *National Executive Committee*, *supra* note 55.

[87] 51 U.S.C. § 20112; *see also* National Aeronautics and Space Act, Pub. L. No. 85-568, 72 Stat. 426 (1958).

[88] *Satellite Safety*, NASA, https://satellitesafety.gsfc.nasa.gov/ [https://perma.cc/XW5J-2YFN].

[89] *Id.*

[90] Larsen, *supra* note 51, at 460.

5. Department of Interior's Government Disaster Management

The U.S. Geological Survey uses GNSS to track movements of earthquakes and landslides.[91] GNSS sensors on the ground can communicate Earth movements to atomic clocks on satellites.[92] A large network of these sensors is planted as part of the Pacific Northwest Geodetic Array,[93] which can measure Earth movements as small as one-tenth of a millimeter.[94] The U.S. Geological Survey is part of the Department of Interior, which participates in the PNT Committee.[95]

6. Federal Communications Commission

Radio frequencies are a scarce resource; the competition for frequencies is fierce and highly regulated.[96] GNSS and commercial communication operators both require clear PNT signals. The competition between their urgent needs for these signals has resulted in several contests before the FCC, leaving the agency to make close decisions, some of which keenly affect GPS. For example, the FCC decision authorizing radio spectrum use by Ligado upset GPS operators and users who feared possible radio interferences with their GPS assigned frequencies.[97] In its decision, the FCC stated that making the award to Ligado was in the public interest.[98] That the FCC (which is not part of the executive branch) asserted its authority over military and claimed national security interests remains a contentious issue.[99]

---

[91] Paul B. Larsen, *The OSO Landslide: Disaster Management Law in the Space Age*, 40 WM. & MARY ENV'T L. & POL'Y REV. 335, 349 (2016).

[92] *Id.*

[93] *Id.*

[94] *Id.* at 350.

[95] *National Executive Committee*, *supra* note 55.

[96] Harris, *supra* note 13.

[97] In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3780 (2020); David Shepardson, *U.S. Agencies Ask FCC to Rescind Ligado Spectrum Decision*, REUTERS (May 22, 2020, 4:32 PM), https://www.reuters.com/article/us-usa-telecom-wireless/u-s-agencies-ask-fcc-to-rescind-ligado-spectrum-decision-idUSKBN22Y2WI [https://perma.cc/V62U-LNN7]; Sandra Erwin, *Coalition of GPS User Groups Joins Fight Against FCC's Ligado Decision*, SPACENEWS (June 23, 2020), https://spacenews.com/coalition-of-gps-user-groups-joins-fight-against-fccs-ligado-decision/ [https://perma.cc/FCB5-FKM5].

[98] *LightSquared*, 35 FCC Rcd. at 3783.

[99] *See* Univ. of Neb., *NE Virtual Space Law Symposium: Spectrum Issues Before FCC and ITU*, MEDIAHUB (Oct. 7, 2020, 10:56AM), https://mediahub.unl.edu/media/14616 (last visited June 2, 2021) (on file with the SMU Law Review Association) (featuring Jennifer Manner, Senior Vice-President, Reg. Affs., Echostar; Ruth Pritchard-Kelly, Vice-President, Reg. Affs., OneWeb; Jennifer Warren, Vice-Presi-

The large number of governmental and nongovernmental parties that participated in the Ligado FCC licensing proceeding illustrates the variety of interests claiming a stake in the issue of harmful radio-frequency interference.[100]

B. International Governmental Organizations

1. International Telecommunication Union

Radio frequencies are an essential GNSS element. GNSS users communicate with GNSS satellites via these frequencies, which are a scarce global resource.[101] The International Telecommunication Union (ITU) seeks to prevent harmful interference with the radio frequencies.[102] ITU keeps track of all radio-frequency assignments in its global Master International Frequency Register in accordance with the mandate of its Radio Regulations which are treaty obligations for all ITU member states.[103] Countries agree at the ITU World Radio Conferences to the ITU table of frequency allocations.[104] ITU works with national government agencies, such as the FCC and NTIA, to implement the findings of the ITU Radio Regulations Board.[105] ITU views GNSS from an international rather than a national point of view; it seeks maximum tolerance as well as minimum interference with radio frequencies.[106]

---

dent, Tech. Pol'y & Reg., Int'l Astronautical Fed'n). The Author attended this symposium discussion and references are to his personal notes. *See also* Sandra Erwin, *Pentagon Presses on With Campaign to Overturn FCC's Ligado Order*, SpaceNews (May 25, 2020), https://spacenews.com/pentagon-presses-on-with-campaign-to-overturn-fccs-ligado-order/ [https://perma.cc/DVR5-R54G].

100 In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772 (2020).

101 Harris, *supra* note 13.

102 Constitution of the International Telecommunication Union art. 45, Dec. 22, 1992, 1825 U.N.T.S. 331 [hereinafter ITU Constitution].

103 Radio Regulations of the Int'l Telecomm. Union art. 8.1 (2020 ed.) [hereinafter ITU Radio Regulations], https://www.itu.int/en/myitu/Publications/2020/09/02/14/23/Radio-Regulations-2020 [https://perma.cc/8KD4-KM3G].

104 *See, e.g.*, *id.* art. 5.89 (explaining that "the use of the band 1 605-1 705 kHz . . . is subject to the Plan established by the Regional Administrative Radio Conference").

105 *E.g.*, *LightSquared*, 35 FCC Rcd. 3772.

106 ITU Constitution, *supra* note 102, art. 45; *see also* Larsen, *supra* note 9, at 379–83.

2. United Nations Committee on Peaceful Uses of Outer Space

U.N. COPUOS is the international forum for discussion and negotiation of all outer space issues.[107] States meet in COPUOS to implement the OST.[108] COPUOS Guidelines promote the Long-Term Sustainability of Outer Space Activities.[109] The U.N. Office of Outer Space Affairs (UNOOSA), which services COPUOS, also administers the international registry of space objects, including GNSS satellites.[110] The COPUOS ICG meets to facilitate interoperability, as well as individual GNSS functionality.[111]

One nation's—or its authorized nongovernmental entities'—harmful interference with another nation's GNSS radio frequencies for military and national security reasons may involve the U.N. Security Council, which is tasked with resolving acts of aggression and other threats to the peace.[112] Multilateral discussions of military issues may be discussed in the U.N. Disarmament Conference.[113] Both institutions are therefore interested organizations. However, military GNSS interference issues have not been raised in either of these two fora as of December 2020.

3. International Civil Aviation Organization

Chicago Convention requires the International Civil Aviation Organization (ICAO) to regulate international navigation of airplanes.[114] Consequently, ICAO has sought to regulate GNSS because the instruments used in air navigation require GNSS.[115] All GNSS services must conform with the ICAO flight stan-

---

[107] *Committee on the Peaceful Uses of Outer Space*, U.N. OFF. FOR OUTER SPACE AFFS., https://unoosa.org/oosa/en/ourwork/copuos/ [https://perma.cc/5W9V-CCEM].

[108] *Id.*

[109] Rep. of the Comm. on the Peaceful Uses of Outer Space on Its Sixty-Second Session, U.N. Doc. A/74/20, annex II (June 12–21 2019).

[110] *See United Nations Register of Objects Launched into Outer Space*, U.N. OFF. FOR OUTER SPACE AFFS., https://unoosa.org/oosa/en/spaceobjectregister/index.html [https://perma.cc/EK2W-VNJF].

[111] Larsen, *supra* note 9, at 395–97.

[112] U.N. Charter arts. 34–35; *see also* Mountin, *supra* note 37, at 189.

[113] *About Us*, U.N. OFF. FOR DISARMAMENT AFFS., https://www.un.org/disarmament/about/ [https://perma.cc/QC2G-LAK3].

[114] Convention on International Civil Aviation Part II, Dec. 7, 1944, 61 Stat. 1180, 15 U.N.T.S. 295 [hereinafter Chicago Convention].

[115] *See* LYALL & LARSEN, *supra* note 26, at 354.

dards.[116] GNSS receivers on airplanes may receive GNSS signals from any of the four GNSS depending on which is nearest.[117]

GNSS has been in use by airplanes since the Korean Airline disaster in 1983.[118] It is now absolutely essential for air navigation.[119] The 1998 ICAO Assembly adopted the Charter on the Rights and Obligations of States Relating to GNSS Services.[120] It provides that (1) aviation safety is the most important purpose of GNSS; (2) aircraft shall have non-discriminatory use of GNSS; and (3) GNSS operators "shall ensure the continuity, availability, integrity, accuracy and reliability of such services."[121] ICAO's charter is not binding because aviation must share GNSS service with all non-aviation users, including those over which ICAO has no authority.[122] Nevertheless, ICAO continues to take a special interest in GNSS and asserts itself on air safety issues related to GNSS navigation.[123]

4. International Maritime Organization

The International Maritime Organization (IMO) has a vital interest in promoting GNSS use for navigation of ships.[124] Based on the IMO Convention on the Intergovernmental Maritime Consultative Organization, the IMO has established standards for navigation of ships.[125] International Convention for the Safety of Life at Sea regulations specifically require ships to be equipped with a GNSS receiver.[126] Maritime industry operators have urged IMO to protect shipping from GNSS jamming and spoofing.[127]

---

[116] *Id.*

[117] *See infra* Part I.

[118] PACE ET AL., *supra* note 24, at 180.

[119] Per Enge, Nick Enge, Todd Walter & Leo Eldredge, *Aviation Benefits from Satellite Navigation*, 20 NEW SPACE, no. 20, 2014, at 1, 1.

[120] Int'l Civil Aviation Organization [ICAO] Assembly Res. A32-19, Charter on the Rights and Obligations of States Relating to GNSS Services (1998), *in* Assembly Resolutions in Force, at V-8, ICAO Doc. 10022 (Oct. 4, 2013), https://www.icao.int/publications/Documents/10022_en.pdf [https://perma.cc/Q9EU-RBAF].

[121] *Id.* at V-9.

[122] *See* LYALL & LARSEN, *supra* note 26, at 354.

[123] *See* Int'l Civil Aviation Org., Working Paper: An Urgent Need to Address Harmful Interferences to GNSS, ICAO Doc. A40-WP/188 (May 8, 2019).

[124] Int'l Maritime Org. [IMO] Convention on the Intergovernmental Maritime Consultative Organization art. 1, Mar. 6, 1948, 9 U.S.T. 621.

[125] *Id.* arts. 16(i), 22(a).

[126] Yamada, *supra* note 6, at 40.

[127] *Id.* at 42.

5. World Meteorological Organization

The World Meteorological Organization has a stake in GNSS because it depends on GNSS to measure water moisture in the atmosphere.[128] Weather forecasting is linked to water vapor concentration in the atmosphere.[129]

6. European Union and the European Space Agency

The EU, consisting of twenty-seven European states, owns Galileo.[130] The European Space Agency manages Galileo for the EU's extensive infrastructure.[131] EU air traffic control uses a GNSS augmenting system called EGNOS—similar to the U.S. WAAS—for airport landings.[132] Thus, the EU has a significant GNSS stake.

C. Nongovernmental GNSS Users

1. Industry

The list of interested nongovernmental users of GNSS is extensive because GNSS has become such a large part of the world's social and economic infrastructure.[133] Both airlines and individual airplane and drone operators that navigate by use of GNSS are vitally interested, as both are totally dependent on GNSS.[134] Even low-Earth orbit (LEO) satellite operators benefit from GNSS for the navigation of their satellites.[135] Any interference with the GNSS radio signals may result in severe acci-

---

[128] World Meteorological Organization [WMO], Report No. 92: Instruments and Observing Methods, WMO/TD-No. 1340 (2006), https://library.wmo.int/doc_num.php?explnum_id=9329 [https://perma.cc/47PU-T2V8].

[129] *Macrotrends Affecting GNSS Across Market Segments*, Eur. Glob. Navigation Satellite Sys. Agency GNSS Mkt. Rep., no. 6, 2019, at 18, 20, https://www.gsa.europa.eu/system/files/reports/market_report_issue_6_v2.pdf [https://perma.cc/ARL8-5KA5].

[130] Larsen, *supra* note 51, at 369; *Countries*, Eur. Union, https://europa.eu/european-union/about-eu/countries_en [https://perma.cc/MJ3P-FEGB].

[131] *Galileo*, Eur. Comm'n, https://ec.europa.eu/growth/sectors/space/galileo/ [https://perma.cc/C4S5-ZAMZ].

[132] *See Galileo and EGNOS*, Eur. Space Agency, https://www.esa.int/Applications/Navigation/Galileo_and_EGNOS [https://perma.cc/2ESS-2RZX]; *EGNOS Navigation System Begins Serving Europe's Aircraft*, Eur. Space Agency (Mar. 2, 2011), https://www.esa.int/Applications/Telecommunications_Integrated_Applications/Technology_Transfer/EGNOS_navigation_system_begins_serving_Europe_s_aircraft [https://perma.cc/6HM6-8JY4].

[133] Mountin, *supra* note 37, at 103.

[134] *Id.* at 111, 120.

[135] *Id.* at 120.

dents.[136] Like airplanes and drones, ships cannot easily navigate without GNSS.[137] GNSS signal interference is extremely dangerous to ships and ship operators.[138] The communication networks use GPS for timing.[139] Financiers of airplanes, ships, cars, and all other GNSS-dependent instruments rely on GNSS signals.[140] Stock exchanges require the exact time of stock purchases and transfers; they would also suffer from GNSS signals interference.[141]

2. Individual Users

Most individuals may not realize the extent to which their daily lives depend on GPS. Car drivers depend on GPS to locate their destinations.[142] Rescue services, like On-Star for car drivers, rely on GPS.[143] Individual stock transactions are timed by GP via their electric grid.[144] However, the GPS signal may easily be disrupted. A sudden collapse of GPS by jamming or spoofing would quickly bring GNSS dependence to individual users' consciousness.[145] Thus, a number of options for greater GPS system security, as well as possible alternative technology, must be considered.

The Civil GPS Service Interface Committee (CGSIC) is an important general government forum for civilian GNSS users to learn about GPS operations and new developments.[146] The CGSIC, sponsored by the DOT and Coast Guard, holds a public meeting every year where military and civilian experts describe current GPS developments to the general public.[147] This meeting also provides an opportunity for members of the public to be heard.[148] CGSIC solicits individual contributions regarding the GPS network from GPS users around the world.[149] It has

---

[136] *Id.*
[137] *Id.* at 111.
[138] *Id.*
[139] *Id.*
[140] *Id.*
[141] *Id.* at 111, 120.
[142] *Id.* at 111.
[143] *Id.*
[144] *Id.*
[145] *See id.*
[146] *Civil GPS Service Interface Committee*, GPS.GOV, https://www.gps.gov/cgsic/ [https://perma.cc/6Q4C-QEZ5]; Memorandum on Space Policy Directive-7, *supra* note 45.
[147] *Civil GPS Service Interface Committee*, *supra* note 146.
[148] *Id.*
[149] *Id.*

formed specialized subcommittees.[150] CGSIC presents a unique opportunity for individual users to inform the U.S. government, which operates GPS, about problems with jamming, spoofing, and other harmful interference.[151] The existence of CGSIC should continue if the major civilian oversight of GPS is shifted from DOT to the DOC as envisioned by EO 13905.[152]

3. Competitors

Commercial satellite operators compete with GNSS for the use of radio spectrum. The challenges raised to Ligado's authorization to use adjacent frequencies for mobile communication illustrate (1) the scarcity of the radio-frequency source, and (2) the need for the FCC, as the government regulator, to make decisions that are in the public interest.[153] Ligado and similarly situated companies are interested in obtaining spectrum that military operators of GPS would prefer to have without challenge.[154] The outcome of this challenge is discussed further in Part IV.[155]

4. Nongovernmental Associations

The Institute of Navigation (ION) is the largest nongovernmental association specially focused on promoting the uses of GNSS.[156] Its members, including individual and corporate national and international GNSS users, meet every year to discuss new GNSS technology and applications, as well as to exchange ideas about how to avoid radio interference.[157] Members also include those involved in manufacturing both civilian and mili-

---

[150] *Id.* The 2020 CGSIC meeting included sessions and reports by International Subcommittees for International Information, Timing, and Surveying-Mapping-Geosciences. *See Agenda: 60th Meeting of the Civil GPS Service Interface Committee*, *supra* note 12.

[151] *Civil GPS Interface Committee*, *supra* note 146.

[152] *See* Exec. Order No. 13905, 85 Fed. Reg. 9359 (Feb. 12, 2020); Marcia Smith, *New Executive Orders for GPS, Space Council*, SPACE POL'Y ONLINE (Feb. 15, 2020), https://www.spacepolicyonline.com/news/new-executive-orders-for-gps-space-council/ [https://perma.cc/5A4J-EAG3]; Memorandum on Space Policy Directive-7, *supra* note 45.

[153] *See* In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3842 (2020); Shepardson, *supra* note 97; Erwin, *supra* note 97.

[154] *LightSquared and GPS*, *supra* note 8.

[155] *See infra* Part IV.

[156] *About the Institute of Navigation*, INST. OF NAVIGATION, https://www.ion.org/about/index.cfm [https://perma.cc/LD9H-6BLM].

[157] *Id.*

tary GNSS instruments.[158] In addition to professional meetings for all members, ION also organizes specialized meetings for groups of members (e.g., meetings for all ION members concerned with military GNSS).[159]

The German Institute of Navigation is also focused on promoting GNSS.[160] It sponsors the European Navigation Conference, which educates members on the latest GNSS technologies.[161] The conference is an excellent forum for exchanging ideas and information.

The International Federation of Air Traffic Controllers' Association (IFATCA), International Federation of Air Line Pilots' Associations (IFALPA), and International Air Transport Association (IATA), represent the views of their members in various fora.[162] In 2019, they jointly asked ICAO to resolve jamming and spoofing issues experienced by the aviation industry.[163]

D. Conclusion

GNSS has become an integral part of the national and international economic and social infrastructure. It is an essential utility like electricity or the internet. Virtually all people now depend on GNSS signal availability to conduct their lives. Thus, GNSS must be protected. If it is not possible to make the current GNSS dependable, then another technology must take its place.

II. GNSS JAMMING, SPOOFING, AND OTHER HARMFUL SPECTRUM INTERFERENCES

GNSS signals are easily overpowered due to the weakness of the radio-frequency signal emitted from GNSS satellites. Jamming and spoofing attempts to disrupt the already weak signal. Military GNSS is more difficult to jam due to its encryption, but civilian GNSS is not encrypted and thus easily subject to interfer-

---

158 *Id.*

159 *Id.*

160 *Our Mission*, Ger. Inst. of Navigation, https://www.dgon.de/en/about-us/our-mission.html [https://perma.cc/2RHA-8AC2].

161 *European Navigation Conference 2020*, Ger. Inst. of Navigation, https://www.enc2020.eu/en/home/ [https://perma.cc/7BV2-G55D].

162 *Partners and Supporters*, Int'l Civ. Aviation Org., https://www.icao.int/Meetings/AMC/NGAP/Pages/Partners.aspx [https://perma.cc/LQL6-NGSR].

163 *See* Int'l Civil Aviation Org., *supra* note 123, at 1.

ence.[164] All four GNSS are almost equally prone to interference.[165] Because of the desire to make GNSS interoperable, information about their signals is released, making them more easily accessible.[166] All GNSS signals are of approximately the same, weak strength.[167] Individuals, criminal gangs, and government actors have all been implicated in distorting signals.[168] Motivations include sheer convenience, theft of valuables, or military advantages.[169] One recent study found 500,000 GNSS frequency transmissions should not have been transmitted; approximately 10% of those transmissions were malicious and intentional, while the others may have been accidental, perhaps caused by signal testing or solar storms.[170]

A. Jamming

Jamming is "harmful interference" with radio frequencies.[171] By overpowering the weak GNSS signals with stronger signals, jamming can occur in two ways.[172] The first (terrestrial jamming) involves interference with signal receivers on Earth.[173] Alternatively, orbital jamming involves a conflicting signal drowning out the original signal to prevent it from reaching the satellite to be rebroadcast to users.[174] Therefore, "whereas orbital jamming effects can extend throughout a satellite's entire footprint, terrestrial jamming effects can be localized and limited to specific targets."[175]

The flow of the radio-frequency signal from the GNSS satellite to the GNSS receiver need only be interrupted sporadically in order to make the message meaningless.[176] The sporadic radio-frequency interruption accomplishes total communications in-

---

[164] Larsen, *supra* note 9, at 412. European Galileo GNSS is not a military operator, but has a limited high-level encrypted service available for payment. *Id.* at 369, 386–87.

[165] Datta, *supra* note 6.

[166] *Id.*

[167] *Id.* All GNSS are in medium-Earth orbit (MEO). Paul D. Groves, Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems 300 (2d ed. 2013).

[168] Datta, *supra* note 6.

[169] *Id.*

[170] *Id.*

[171] Mountin, *supra* note 37, at 129.

[172] *Id.*

[173] *Id.* at 130.

[174] *Id.* at 129–30.

[175] *Id.* at 130.

[176] *See id.* at 129.

terruption.[177] Military authorities may physically jam a GNSS signal for national security reasons.[178] Or civilians may jam a signal to gain some kind of advantage or to create havoc.[179] GNSS maintenance can also result in accidental or deliberate signal interference.[180] Radio-frequency jamming has occurred for many years. For example, during World War II, Germany jammed British Broadcasting Corporation radio broadcasts to German-occupied countries.[181]

B. SPOOFING

Spoofing is seizing control of a radio frequency and substituting a message different from the one in transit to or from the GNSS satellite.[182] Spoofing then tricks the end user by providing a fake signal that mimics a true signal's characteristics.[183] It occurs widely in telephone advertising, when outsiders pretending to be local businesses appear to call from a local area code.[184] Additionally, spoofing may occur in television broadcasting. In 1986, a disgruntled viewer managed to capture and replace a television broadcast with his own message.[185] In 2002, a Falung Gong broadcast hijacked a Chinese satellite television transmission to broadcast its own message.[186] A government may also spoof to mislead ships or airplanes by giving pilots misleading geolocation information.[187] Or, spoofing may lead away from sensitive national security places or persons, like the ruler of a country.[188]

---

[177] *Id.* at 129–30.

[178] *See id.* at 125.

[179] *See id.* at 121.

[180] *Id.* at 104.

[181] *BBC Broadcast Information About Britain's Military Setbacks to Win Hearts and Minds in Germany During World War II*, UNIV. OF EXETER, https://www.exeter.ac.uk/news/research/title_579867_en.html [https://perma.cc/GT4R-6BYP].

[182] Mountin, *supra* note 37, at 130.

[183] *Id.*

[184] *See Caller ID Spoofing*, FED. COMMC'N COMM'N, https://www.fcc.gov/spoofing [https://perma.cc/CK2Q-YPPJ].

[185] *See* Associated Press, *Video Pirate Interrupts HBO*, N.Y. TIMES (Apr. 28, 1986), https://www.nytimes.com/1986/04/28/arts/video-pirate-interrupts-hbo.html [https://perma.cc/2HS4-7NG4].

[186] *Jail for Falun Gong TV Hackers*, CNN (Sept. 20, 2002, 7:33 AM), https://edition.cnn.com/2002/WORLD/asiapcf/east/09/20/china.falun.gong/ [https://perma.cc/ZPB4-CBFG].

[187] *See* Mountin, *supra* note 37, at 106.

[188] Kyle Mizokami, *Report: Russia Engaging in Widespread Satellite Navigation Spoofing*, POPULAR MECHS. (Apr. 3, 2019), https://www.popularmechanics.com/

GNSS spoofing is more dangerous than jamming.[189] It substitutes false signals for the proper GNSS satellites signals, thus guiding the operators of GNSS receivers into wrong directions.[190] The European Space Agency suggests wide monitoring of all GNSS receivers to detect interference with GNSS signals.[191]

Extensive jamming and spoofing activities originate from military authorities, who consider outer space to be a warfighting domain.[192] The space powers (the United States, Russia, China, and, lately, India) compete for military dominance of outer space.[193] Reliance on outer space for warfighting leads the space powers to develop ways to jam, deceive, degrade, and deny access to GNSS.[194] These capabilities affect both military and civilian GNSS users. The OST prohibits the space powers from stationing weapons of mass destruction in outer space.[195] Thus, the space powers currently concentrate on warfighting from Earth's surface by engaging in electronic warfare such as jamming, spoofing, and other GNSS interference techniques.[196]

---

military/weapons/a27032602/report-russia-engaging-in-widespread-satellite-navigation-spoofing/ [https://perma.cc/HS3H-2KA3].

189 Datta, *supra* note 6.

190 *Id.*

191 *GIDAS: Real-Time Interference Detection Making Satnav Safer*, EUR. SPACE AGENCY (July 20, 2020), https://www.esa.int/Applications/Navigation/GIDAS_Real-time_interference_detection_making_satnav_safer [https://perma.cc/U53Y-VDJA].

192 Woodrow Bellamy III, *Are GPS Jamming Incidents a Growing Problem for Aviation?*, AVIATION TODAY (Jan. 31, 2017), https://www.aviationtoday.com/2017/01/31/are-gps-jamming-incidents-a-growing-problem-for-aviation/ [https://perma.cc/MD7PA9QB]; *see also* Bill Carey, *Aviation Groups Seek Action on Global Navigation Vulnerability*, AVIATION WK. & SPACE TECH. (Sept. 26, 2019), https://aviationweek.com/air-transport/aviation-groups-seek-action-gnss-vulnerability [https://perma.cc/CU3F-H2HX].

193 *See* SECURE WORLD FOUND., GLOBAL COUNTERSPACE CAPABILITIES: AN OPEN SOURCE ASSESSMENT, at x, xii, xiv, xvi (Brian Weeden & Victoria Samson eds., 2020), https://swfound.org/media/206970/swf_counterspace2020_electronic_final.pdf [https://perma.cc/6N4E-DG6F].

194 *See id.*

195 OST, *supra* note 62, art. IV. The OST also prohibits placing weapons of mass destruction in orbit. *Id.*

196 Ingo Baumann, *GNSS Cybersecurity Threats: An International Law Perspective*, INSIDE GNSS (June 3, 2019), https://insidegnss.com/gnss-cybersecurity-threats-an-international-law-perspective/ [https://perma.cc/4EGE-6S99]. GNSS is not considered a weapon of mass destruction. *See Weapons of Mass Destruction*, U.S. DEP'T OF HOMELAND SEC. (Aug. 14, 2008), https://www.dhs.gov/topic/weapons-mass-destruction [https://perma.cc/WM8V-AWF4].

The United States has announced that it is preparing for war in outer space and considers outer space to be a "warfighting domain."[197] To that end, the United States has established the U.S. Space Force to focus specifically on outer space warfare.[198] DOD's Counter Communication System is developing ways to jam and spoof GNSS satellites.[199] The Naval Warfare Program can now frustrate adversaries by blocking GNSS use in local areas.[200] The program sometimes tests its capabilities by engaging in extensive jamming during naval exercises in waters and land of the southeastern United States.[201]

Russia is also focused on outer space as a warfighting domain.[202] Thus, in competition with the United States, Russia has similarly established a special military Space Force for outer space warfare.[203] Russia has developed a large variety of ways to jam and spoof the flow of information on GNSS satellites and receivers.[204] Russia has also indicated that it has the capability to misguide both ships and airplanes, including unmanned airplanes.[205] The Russian Army has electronic warfare capability focusing on GNSS receivers in specific localities—for example, the immediate environment around President Vladimir Putin, including wherever he travels.[206] Russia is able to jam and spoof communication in large areas—for example, near the Eastern Mediterranean Sea and the Black Sea off southern Russia.[207]

China, like the United States and Russia, has designated outer space as a military domain with the objective of achieving Chinese military dominance in outer space.[208] China has developed

---

[197] SECURE WORLD FOUND., *supra* note 193, at 3-20; *see also Agenda: 60th Meeting of the Civil GPS Service Interface Committee*, *supra* note 12; Civ. GPS Serv. Interface Comm., *Keynote Address*, at 12:02, YOUTUBE (Sept. 22, 2020), https://www.youtube.com/watch?t=722&v=Rr11pyY79-M&feature=youtu.be (last visited June 2, 2021) (featuring Maj. Gen. John E. Shaw, Combined Force Space Component Commander, U.S. Space Command, and Commander, Space Operations Command, U.S. Space Force). Major General Shaw predicted massive wartime GNSS jamming. Civ. GPS Serv. Interface Comm., *supra*.

[198] SECURE WORLD FOUND., *supra* note 193, at 3-20 to -21.

[199] *Id.* at 3-11.

[200] *Id.* at 3-12.

[201] *Id.* at 3-13.

[202] *Id.* at xiii.

[203] *Id.* at 2-29.

[204] *Id.* at 2-19.

[205] *See id.* at 2-17 to -18.

[206] *Id.*

[207] *Id.* at 2-18.

[208] *Id.* at 1-1.

electronic warfare capability to deter foreign aggression.[209] Toward that purpose, China jams GNSS signals to control access to PNT data.[210] For example, the Chinese military authorities are reported to have jammed GNSS in the South China Sea.[211] Chinese military authorities are also reported to have engaged in spoofing in the Shanghai area.[212]

Iran is also capable of engaging in electronic interference with GNSS signals.[213] On several occasions it has demonstrated an ability to interfere with civilian GNSS signals.[214]

GPS jamming affects not only military activities but also frustrates civilians. In 2017, the police in northern Norway noticed GNSS signals were being jammed.[215] The Norwegian National Security Agency investigation found that the GNSS signal jamming originated in Russia.[216] Twenty ships lost navigation in the Black Sea due to local Russian spoofing of their GNSS receivers, endangering the people on board the ships.[217] One London Economics study estimated that spoofing events in the maritime sector could potentially cause losses totaling over one billion dollars.[218] A similar spoofing event happened near Moscow, where people were charged for transportation services for which they had not contracted.[219] Spoofing is extensive. From 2016 to 2018, ten thousand spoofing events involving 1,300 ships were reported.[220]

Spoofing and jamming are intense in the eastern parts of the Mediterranean Sea, which is related to the military conflicts in the Middle East.[221] The Mediterranean entrance to the Suez Canal has been particularly spoofed.[222] Airline pilots complained to the ICAO that false GNSS signals endangered airline access to

---

209 *Id.*

210 *Id.* at x.

211 *Id.* at 1-16.

212 *Id.*

213 *Id.* at 6-3.

214 *Id.*

215 Peter Bakkemo Danilov, *GPS Jamming Still Causing Problems in Finnmark*, HIGH N. NEWS (June 26, 2020), https://www.highnorthnews.com/en/gps-jamming-still-causing-problems-finnmark [https://perma.cc/ZJ3X-LEM6].

216 *Id.*

217 Yamada, *supra* note 6, at 40.

218 *See id.*

219 Milner, *supra* note 6.

220 *Id.*

221 *Id.*

222 Carey, *supra* note 192, at 32.

Israeli airports.[223] Airplanes flying at high altitudes reported that their GNSS signals were being overpowered by strong "fake" signals from a military airbase in Syria.[224] Consequently, the ICAO Regional Aviation Safety Group for the Middle East has warned airplane operators about spoofing and jamming in the area.[225] "[T]he nonprofit organization [Center for Advanced Defense Studies] used data from a GPS receiver on the International Space Station to detect GPS spoofing in Syria by the Russian military for airspace denial purposes."[226]

There are also existing reports of jamming and spoofing in Asia.[227] Ships arriving in Shanghai and other ports off the eastern coast of China reported that the GNSS signals of three hundred commercial ships showed an incorrect location for those ships.[228]

The spoofing and jamming perpetrators appear to be both military and non-military as the objectives of these events vary.[229] While military authorities influence the military conflict in the Middle East, the civilian purpose may be to defraud or smuggle illegal supplies into a country.[230] The technology is very simple and does not require sophisticated military software.[231]

In 2019, the IFATCA, IFALPA, and IATA jointly urged the ICAO Assembly to (1) avoid jamming and spoofing dangers to air safety; (2) warn military authorities that their operations adversely affect the air safety of civilian aircraft flight; (3) protect GNSS radio frequencies as mandated by ITU radio regulations; and (4) support alternative air navigation technology.[232] The University of Texas reported research estimates spoofing signals to be 500 times stronger than the true GNSS signals.[233]

---

[223] *Id.*

[224] *Id.*

[225] *Id.*

[226] *Id.*

[227] *See* Milner, *supra* note 6.

[228] *Id.*

[229] *See* Mountin, *supra* note 37, at 118–20.

[230] *See* Milner, *supra* note 6.

[231] *See* Mountin, *supra* note 37, at 131.

[232] Int'l Civil Aviation Org., *supra* note 123.

[233] Ctr. for Advanced Def. Studs. [C4ADS], Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria 25 (2019).

C. Enforcement of Civilian and Military Harmful Interference

1. International Telecommunication Union

ITU is a treaty organization.[234] Virtually all countries in the world are members of ITU.[235] ITU regulates the radio frequencies used for GNSS signals.[236] Article 44 of the ITU Constitution requires ITU to administer the allocation of radio frequencies as "limited natural resources" which must be used in accordance with ITU Radio Regulations.[237] ITU has, by virtue of the ITU Constitution, legal authority over the entire radio-frequency spectrum.[238] And ITU, which requires stations be established and operated to avoid significant "harmful interference" with radio frequencies used by other countries, maintains a register of all radio frequencies in use.[239]

ITU administers the radio frequencies through its radio regulations.[240] Interference with registered radio frequencies is contrary to the ITU Radio Regulations.[241] Article 15 of the ITU Radio Regulations prohibits "transmission of superfluous signals, or the transmission of false or misleading signals, or the transmission of signals without identification."[242] However, States have not been willing to give ITU effective authority to administer its registered frequencies.[243] Allocations are thus only enforced through ITU's control over the Master International Frequency Register and its refusal to register assignments that would cause significant harmful interference.[244] Member states enforce harmful interference restrictions based on treaty obligations.[245] The FCC represents the United States in ITU and

---

234 *See* Lyall & Larsen, *supra* note 26, at 194.

235 *Id.* at 195.

236 *Id.* at 192. The ITU Radio Regulations Board administers the Master International Frequency Register as provided by the organization's constitution. ITU Constitution, *supra* note 102, art. 14.

237 ITU Constitution, *supra* note 102, art. 44.

238 *Id.*

239 *Id.* arts. 14, 45.

240 *Id.* art. 44; Lyall & Larsen, *supra* note 26, at 192.

241 ITU Constitution, *supra* note 102, art. 45.

242 ITU Radio Regulations, *supra* note 103, art. 15.1.

243 Mountin, *supra* note 37, at 122.

244 *Id.* at 134.

245 *Id.*

obtains ITU-cleared radio frequencies for assignment to United States operators.[246]

2. FCC Enforcement of Harmful Interference

Administration and enforcement responsibilities fall primarily on the national governments, supplemented by the efforts of individual users. The FCC enforces the prohibition on harmful interference with GNSS signals.[247] A typical FCC enforcement example involved Gary Bojczak, a construction company employee who inadvertently jammed GPS at Newark Liberty International Airport.[248] He had acquired a cheap jamming device for his truck "to keep his boss from tracking his whereabouts at all times."[249] Unknown to him, the device also jammed GPS at the airport.[250] An FCC agent, using a tracking device, located his truck and its illegal jamming device.[251] Based on its investigation, the FCC issued the driver a fine of $31,875.00.[252] Seizing control of a satellite is a crime.[253]

3. U.S. Criminal Enforcement

The 1986 Electronic Communications Privacy Act[254] prohibited interference with radio frequencies used for communication with satellites, which is now considered a felony and enforced by the U.S. Department of Justice.[255] The Act protects electronic communication and electronically stored data.[256]

---

[246] *International*, NAT'L TELECOMM. & INFO. ADMIN., https://www.ntia.doc.gov/category/international [https://perma.cc/8P87-3S89].

[247] *Jammer Enforcement*, FED. COMMC'N COMM'N, https://www.fcc.gov/enforcement [https://perma.cc/JWM8-PST7].

[248] *In re* Gary P. Bojczak, 28 FCC Rcd. 11589 (2013); *see also* Raymond Fisman & Tim Sullivan, *How GPS Transformed Trucking and Made the Open Road a Lot Less Open*, WALL STREET J. (Oct. 23, 2013), https://www.wsj.com/articles/BL-ATWORKB-1367 [https://perma.cc/C738-D2G4].

[249] Fisman & Sullivan, *supra* note 248.

[250] *Id.*

[251] *In re Gary P. Bojczak*, 18 FCC Rcd. at 11590. GNSS jamming violates 47 U.S.C. §§ 301, 302(b), 333. *Id.* at 11591.

[252] *Id.* at 11594. The FCC also prosecutes the sale of jamming devices. *See In re* Supply Room, Inc., 28 FCC Rcd. 4981 (2013). The Cyber Security Principles for Space Systems, published in the Federal Register, seek to protect against jamming and spoofing, but they do not establish new enforcement sanctions. *See* Cybersecurity Principles for Space Systems, 85 Fed. Reg. 56155 (Sept. 4, 2020).

[253] 18 U.S.C. § 1367.

[254] *Id.* §§ 2510–2523.

[255] *See id.* § 2511(2)(g)(iv).

[256] *Id.* § 2510(12).

4. Harmful Interference Related to National Security by Agents of Foreign Governments

Government interference with GNSS signals is a different matter. Government authorities interfere with the use of radio frequencies if they determine that interference is in their national interests.[257] One state's jamming and spoofing can affect another state's national security and sovereignty, causing a responsive intervention. One author, Sarah Mountin, suggests that retaliation against another state can be legally justified if one country seriously affects another state by jamming or spoofing "fake" information.[258] Interference with military objectives may justify military response.[259] Possible retaliation is limited by U.N. Charter Article 2, which requires states to refrain from use of force or threats of use of force "inconsistent with the Purposes of the United Nations."[260] For example, deliberate interference with a commercial airplane's GNSS navigation, resulting in a crash and killing hundreds of passengers, could constitute illegal use of force, thus justifying retaliation.[261] Likewise, jamming or spoofing GNSS signals in violation of basic space law and ITU Radio Regulations to cause a satellite's destruction could be considered an armed attack that would also justify retaliation.[262] Similarly, Mountin asserts that intense GNSS spoofing and jamming, which critically disturbs state infrastructure, could justify legal use of retaliatory force.[263] Nevertheless, states are reluctant to react to jamming and spoofing because they may wish to engage in such acts themselves, or they may wish to avoid causing international tensions.[264]

GNSS interference by nongovernmental agencies does not trigger Article 2 of the U.N. Charter, which applies only to actions by states.[265] An exception would exist if the interference can be traced to a state.[266] OST Article VI provides that:

---

[257] Mountin, *supra* note 37, at 105.

[258] *Id.* at 105–06, 130, 156–57, 173. The principle of non-intervention was clarified by the ICJ in *Nicaragua v. United States.* Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 106 (June 27).

[259] Mountin, *supra* note 37, at 162.

[260] U.N. Charter art. 2(4).

[261] Mountin, *supra* note 37, at 172, 177.

[262] *Id.* at 177.

[263] *Id.* at 177–78.

[264] *Id.* at 178.

[265] *Id.* at 179.

[266] *Id.*

> States Parties to the Treaty shall bear international responsibility for national activities in outer space, including the moon and other celestial bodies, whether such activities are carried on by governmental agencies or by non-governmental entities, and for assuring that national activities are carried out in conformity with the provisions set forth in the present Treaty.[267]

This provision could make states responsible for GNSS interference by nongovernmental entities.[268]

5. International Settlement of Disputes About Harmful Interferences

OST Article IX provides:

> If a State Party to the Treaty has reason to believe that an activity or experiment planned by it or its nationals in outer space, including the moon and other celestial bodies, would cause potentially *harmful interference* with activities of other States Parties in the peaceful exploration and use of outer space, including the moon and other celestial bodies, it shall undertake appropriate international consultations before proceeding with any such activity or experiment.[269]

In her study of harmful interference, Mountin traced Article IX's reference to harmful interference to the famous U.S. West Ford Experiments in 1961 and 1963, which deposited 500,000 copper metal needles into orbit to test the effect on global communication.[270] Some of the needles still remain in orbit as space debris.[271] The experiments caused international protests, which were expressed in OST Article IX.[272] Mountin suggests that jamming and spoofing could justify offended states invoking OST Article IX to request consultation.[273] However, as of the time of this writing, no state has invoked Article IX, despite repeated instances of harmful interference.[274]

---

[267] OST, *supra* note 62, art. VI.

[268] LYALL & LARSEN, *supra* note 26, at 60.

[269] OST, *supra* note 62, art. IX. (emphasis added).

[270] Mountin, *supra* note 37, at 148–49; William W. Ward & Franklin W. Floyd, *Thirty Years of Space Communications Research and Development at Lincoln Laboratory*, NASA HIST. DIV., https://history.nasa.gov/SP-4217/ch8.htm [https://perma.cc/QZK4-E7JD].

[271] *West Ford Needles: Where Are They Now?*, 17 ORBITAL DEBRIS Q. NEWS, Oct. 2013, at 1, 3–4, https://orbitaldebris.jsc.nasa.gov/quarterly-news/pdfs/odqnv17i4.pdf [https://perma.cc/A588-BHTK].

[272] Mountin, *supra* note 37, at 149–50.

[273] *Id.* at 150.

[274] *Id.* at 150–51.

The OST Article III reference to the U.N. Charter and other international law makes relevant the possibility of dispute settlement by the U.N.[275] The OST does not in any way delimit dispute settlement by the U.N. Security Council, because Article 103 of the U.N. Charter supersedes all other international law in case of conflicts.[276]

III. FCC'S ORDER REGARDING POSSIBLE HARMFUL INTERFERENCE WITH GPS FREQUENCIES BY LIGADO

Nongovernmental entities cannot represent themselves in ITU. The Department of State represents the United States, but the FCC interacts on behalf of U.S. nongovernmental entities.[277] The FCC is an independent U.S. government agency.[278] 47 U.S.C. §§ 301 and 307 authorize the FCC to assign ITU-cleared frequencies based on what it finds to be in the public interest.[279] Ascertaining the public interest is a wide-ranging search, which is becoming increasingly more extensive.

The 2020 FCC Ligado ruling was seventeen years in the making.[280] Ligado plans to establish a high-tech (5G) communication system using low-power signals similar to the GPS system.[281] The problem is whether Ligado's frequencies are too close to the existing GPS frequencies, which might cause harmful interference.[282] As previously discussed, GPS needs to have radio frequencies that are free of radio interference in order to send unhindered signals to GPS receivers. Therefore, the FCC needed to answer whether this assignment of radio frequencies would cause harmful interference with the radio frequencies allocated to GPS.[283]

---

[275] OST, *supra* note 62, art. III.

[276] U.N. Charter art. 103.

[277] *See International Telecommunication Union Radiocommunication Sector (ITU-R)*, INT'L TELECOMM. & INFO. ADMIN., https://www.ntia.doc.gov/legacy/osmhome/international/ITUR.html [https://perma.cc/RJ77-Y867].

[278] *What We Do*, FCC, https://www.fcc.gov/about-fcc/what-we-do [https://perma.cc/MD2J-RM7Z].

[279] 47 U.S.C. §§ 301, 307(b).

[280] *See* In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3774 (2020) ("The genesis of this proceeding, however, dates back to 2003.").

[281] Datta, *supra* note 6.

[282] *Id.*

[283] *See id.*

The Ligado case raises a policy issue for the United States that other countries also encounter—meeting the demands of commercial systems by using frequencies close to those of existing services. The radio spectrum is a scarce resource, and there is competition for its use.[284] In the Ligado case, the competition was primarily between a commercial communication company and DOD, an executive branch government agency.[285] The FCC, which is not part of the executive branch, but an independent government agency governed by its own laws, decided the issue.[286] The executive branch agencies were represented by the NTIA, located in the executive branch's DOC.[287] The Communications Act, 47 U.S.C. §§ 305 and 902, delegates to the NTIA authority over radio stations "belonging to and operated by the United States," whereas 47 U.S.C. §§ 303 and 301 delegates to the FCC legal authority to license and regulate nongovernmental uses of the radio spectrum.[288] The FCC and NTIA coordinate their regulation through a Memorandum of Understanding.[289]

As the Ligado case well illustrates, the consequence of this bifurcation is that the FCC, using its own separate legislative mandate, made an ultimate ruling on GPS use of radio spectrum by its own standards, which were different from those advocated by the executive branch agencies.

A. FCC Regulation of Possible GPS Signal Interference by Ligado

For its administration of harmful interferences with radio frequencies, the FCC adopted the ITU's Radio Regulation 1.169, which defines "harmful interference" as "[i]nterference which endangers the functioning of radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with [ITU] Radio Regulations."[290] GPS, by previous allocation of

---

[284] *Radio Frequency Spectrum is a Scarce, Natural Resource*, Fin. Express (Feb. 12, 2003, 5:30 AM), https://www.financialexpress.com/archive/radio-frequency-spectrum-is-a-scarce-natural-resource/64215/ [https://perma.cc/8KVU-5LTF].

[285] *See LightSquared*, 35 FCC Rcd. at 3816.

[286] *Id.* at 3773; *see also What We Do*, *supra* note 278.

[287] *LightSquared*, 35 FCC Rcd. at 3821; *About NTIA*, *supra* note 82.

[288] 47 U.S.C. §§ 301, 303, 305, 902.

[289] Press Release, Fed. Commc'n Comm'n, FCC and NTIA Sign New Memorandum of Understanding on Spectrum Coordination (Jan. 31, 2003), https://www.fcc.gov/document/fcc-and-ntia-sign-new-memorandum-understanding-spectrum-coordination [https://perma.cc/44Z4-WNXD].

[290] ITU Radio Regulations, *supra* note 103, art. 1.169 (emphasis omitted).

frequencies, became free to use the 1559–1610 megahertz (MHz) band for PNT signal services.[291] Additionally, GPS receivers are also increasingly enabled to use the signal frequencies of the three non-U.S. GNSS operators because interoperable receivers are built into many U.S. GNSS receivers.[292]

Various governmental, as well as nongovernmental, interests opposed the assignment of frequencies to Ligado, alleging that the requested frequencies were too close to and might weaken the existing GPS signals and cause potential harmful interference with GPS.[293] DOD was most concerned because of the military origin and management of GPS, as well as the extensive use of GPS by military authorities.[294]

Previously, in 2012, United States government agencies had urged the FCC to seek an appropriate balance between the potential harmful interference caused by the applicant's transmitters and the GPS receivers.[295] Achieving this balance became an objective of the FCC. The FCC order in the Ligado case claimed to have established this necessary balance.[296] However, other governmental departments do not agree and seek reversal of the 2020 ruling.[297] They have subsequently requested the FCC to reconsider its decision.[298]

The FCC rationalizes that its creation of a 23 MHz quiet band will sufficiently isolate Ligado's downlink at the 1526–1536 bandwidth from the GPS band at 1559–1610.[299] Second, the Ligado uplink bands at 1627.5–1637.5 and from 1646.5–1656.5 will similarly be sufficiently isolated from the GPS bandwidths by a quiet guard band.[300] The FCC therefore concluded that this arrangement was in the public interest and should be permitted, subject to a range of further conditions to ensure the elimination of several possibilities for harmful interference with previously allocated and assigned frequencies.[301] The FCC decided that the Ligado license thus constructed was a rational, efficient,

---

[291] *See LightSquared*, 35 FCC Rcd. at 3773 n. 2.

[292] *Id.* However, note that only Galileo has FCC authority to beam signals into U.S. territory. *See id.*

[293] *Id.* at 3805–06.

[294] *Id.* at 3821.

[295] *Id.* at 3777.

[296] *See id.* at 3823.

[297] *See* Datta, *supra* note 6.

[298] *Id.*

[299] *See LightSquared*, 35 FCC Rcd. at 3773.

[300] *Id.* at 3788 n.95.

[301] *See id.* at 3785–86.

and economical use of the radio-frequency spectrum,[302] and that this ruling would advance the FCC's goal of making additional spectrum accessible for Ligado to provide fast 5G level services to a wide range of users.[303]

In its decision, the FCC declined to provide further protection for GPS receivers experiencing possible harmful interference from transmissions coming from outside of the bandwidth designated for GPS.[304] The FCC suggested that GPS receivers could be built so as not to experience problems with interference, although some receivers may have to be retrofitted.[305]

The FCC found "little or no" harmful interference from Ligado's modified "base station or handset operations to the hundreds of millions of" cell phones connected to GPS.[306] The FCC decision concluded that its order did "not cause harmful interference" with "general location and navigation devices."[307] High-precision GPS receivers were examined, and the FCC concluded that those kinds of receivers could be upgraded with better antennas and thus made "immune" to interference.[308]

Importantly, the FCC declined to measure possible harmful GPS signals interference by the measurement advocated by DOD and DOT.[309] The FCC stated that the metric measurement would "examin[e] the GPS receivers to determine whether a receiver could experience a 1 dB degradation to the C/N[0] with respect to any satellite within view of the receiver."[310] The FCC reasoned that such measurement would not measure the actual GPS receiver performance.[311] Instead, the FCC decided to measure harmful interference by its own measurement methods used in the allocation of spectrum to radio operators.[312] Consequently, the degree of GPS interference became evaluated as if GPS were a radio operator rather than a PNT operator.[313] DOT and the FAA claimed and continue to argue that the FCC's mea-

---

302 *See id.* at 3783, 3823; ITU Constitution, *supra* note 102, art. 44.

303 *LightSquared*, 35 FCC Rcd. at 3785; *see infra* Part V (discussion of 5G technology).

304 *LightSquared*, 35 FCC Rcd. at 3806.

305 *Id.*

306 *Id.* at 3818.

307 *Id.*

308 *Id.*

309 *Id.* at 3799.

310 *Id.*

311 *Id.*

312 *See id.*

313 *See id.*

surement of actual performance failed to measure GPS's PNT performance, since the accuracy requirements of the two performance measurements differ substantially.[314]

In its decision, the FCC referred to the ability of the European GNSS operator, Galileo, to operate in and send signals into U.S. space, thus suggesting that Galileo is an alternate service avenue for GNSS receivers in the United States.[315] However, reliance on a foreign GNSS at a roughly similar radio frequency satisfies neither the United States' governmental interest nor the interests of nongovernmental operators. For example, DOD would not be able to use Galileo for guidance of weaponry.

The FCC was particularly concerned about harmful interference with military GPS.[316] GPS is operated by the U.S. Air Force and, thus, most of the objections to Ligado's license were and continue to be raised by Air Force.[317] The FCC reasoned that the Air Force objection to harmful interference caused by Ligado relates to interference with high-precision GNSS receivers.[318] The FCC concluded that its decision results in "a 99.3% reduction" of the power level of Ligado operations.[319] The order states that the reduction will greatly reduce the possibility of harmful interference with high-precision weaponry.[320] The FCC also states that its order will reduce the need to retrofit military machinery.[321] Further, the order required Ligado to cooperate with the U.S. government to remove other possible interferences from Ligado's ancillary terrestrial component stations.[322] The FCC also ordered Ligado to exchange information with the U.S. government about Ligado's efforts to remove these concerns.[323] Furthermore, the FCC ordered the Air Force to inform Ligado of specific GPS receivers that experience harmful interference in order for Ligado to resolve interference problems with those receivers.[324]

---

[314] *See supra* notes 309–13.

[315] *LightSquared*, 35 FCC Rcd. at 3819.

[316] *See id.* at 3823.

[317] *See* Mountin, *supra* note 37, at 110 ("The U.S. Air Force's GPS constellation . . . provides the foundation for nearly all global commercial space-based navigation and timing.").

[318] *LightSquared*, 35 FCC Rcd. at 3821–23.

[319] *Id.* at 3823.

[320] *Id.* at 3823–24.

[321] *Id.* at 3818.

[322] *Id.* at 3824.

[323] *Id.*

[324] *Id.*

The government departments had conducted several technical examinations and tests of possible Ligado harmful interference with governmental operations of GPS signals—in particular, DOD's concern with interference with military weaponry and FAA's concern with interference with navigation of commercial airplanes and, consequently, with air traffic control.[325] As a result, the NTIA expressed "significant concerns" with the possible grant of radio frequencies to Ligado by the FCC.[326] DOD and FAA's concerns were sufficiently serious for the NTIA to state that the governmental agencies were "unable to recommend" grant of license to Ligado.[327] DOD stated that grant of spectrum license to Ligado would have "a potential significant negative impact on military operations."[328]

The military concerns with the granting of Ligado's license have considerable momentum because of concerns with national defense. Those concerns are shared by congressional representatives who support and approve the national defense budget, and in particular the DOD GPS budget, which is mainly funded because of its military functions.[329]

Nevertheless, the FCC was not persuaded by the governmental evidence presented by NTIA. The FCC resolved its difference with the executive branch agencies by exercising its statutory power to make its decision based on what it determines to be in the public interest of the United States.[330] Congressional members' interest in the Ligado decision is particularly important because Congress controls the budget of the executive branch agencies and the FCC.[331] Furthermore, Congress can overrule the Ligado decision by adopting legislation contrary to it.

On April 22, 2020, the FCC issued its order authorizing Ligado to use radio frequencies to provide service.[332] On May

---

[325] *See id.* at 3808, 3821.

[326] *Id.* at 3832.

[327] *Id.*

[328] *Id.*

[329] *See generally* KELLY M. SAYLER & JOHN R. HOEHN, CONG. RSCH. SERV., IN11400, DOD CONCERNS ABOUT THE FCC-APPROVED LIGADO NETWORK (2020).

[330] *LightSquared*, 35 FCC Rcd. at 3841–42. The FCC's legal duty is to administer U.S. spectrum, so as to "ensure that this valuable resource is used as efficiently as possible without causing harmful interference to important applications, such as GPS." *Id.*

[331] *Power of the Purse*, HISTORY, ART & ARCHIVES — U.S. HOUSE OF REPRESENTATIVES, https://history.house.gov/institution/origins-development/power-of-the-purse/ [https://perma.cc/3V3R-9G89].

[332] *LightSquared*, 35 FCC Rcd. at 3773.

22, 2020, the NTIA, on behalf of DOD, DOT, and five other executive branch agencies, asked the FCC to reconsider its order and to postpone the effective date of the Ligado order until the issue of harmful interference with GPS could be finally resolved.[333] The petition was supported by a substantial part of the aviation industry, including aircraft manufacturers.[334] Furthermore, a thirty-two member bipartisan group of United States senators joined to ask the FCC to reconsider.[335] Members of the House Armed Services Committee also supported the petition to reconsider.[336] The Air Line Pilots Association was particularly concerned that uncertified private pilots and drone operators using GPS receivers would collide with commercial airlines.[337] The Assocation also expressed concern that airline passengers could use cell phones to disrupt pilot contact with air traffic control.[338]

B. DOD's Adversarial Role as the Government Operator of U.S. GPS

DOD operates and controls GPS.[339] Virtually all military equipment with computer features has some GPS connection. An additional function of the Air Force is to track space objects

---

[333] *See* Petition for Reconsideration or Clarification of the National Telecommunications and Information Administration at iii, 15, IB Docket Nos. 11-109, 12-340 (filed May 22, 2020).

[334] Letter of Support of NTIA Stay Petition, IB Docket Nos. 11-109, 12-340 (filed June 3, 2020).

[335] David Shepardson, *32 U.S. Senators Urge FCC to Reconsider Ligado Spectrum Order*, Reuters (May 15, 2020), https://www.reuters.com/article/us-usa-telecom-wireless/32-u-s-senators-urge-fcc-to-reconsider-ligado-spectrum-order-idUSKBN22R2WQ [https://perma.cc/AQ7G-N9A8]. On August 13, 2020, the General Accounting Office (GAO) ruled that the FCC had not violated 5 U.S.C. § 801(a)(1)(A)–(B), which requires the FCC to consult with Congress before issuing a ruling and before it can take effect. U.S. Gov't Accountability Off., B-332233, Federal Communications Commission—Applicability of the Congressional Review Act to Ligado Amendment to License Modification Applications 1 (2020).

[336] Press Release, U.S. House of Representatives Armed Servs. Comm., Smith, Thornberry, and 20 Bipartisan Members Demand Answers From FCC: Ligado Spectrum Order Inconsistent with Federal Law (May 8, 2020), https://armedservices.house.gov/2020/5/smith-thornberry-and-20-bipartisan-members-demand-answers-from-fcc [https://perma.cc/95FC-3SCJ].

[337] Petition for Reconsideration of Air Line Pilots Association, International at 14, IB Docket Nos. 11-109, 12-340 (filed May 20, 2020).

[338] *Id.* at 16.

[339] Mountin, *supra* note 37, at 110.

that may cause interference with military space objects, such as GPS satellites.[340]

GPS offers two different kinds of services: (1) the Standard Positioning Service (SPS), and (2) the Precise Positioning Service (PPS).[341] The SPS is not encrypted and, therefore, easy to jam or spoof; it is generally available all over the world free of charge.[342] However, it is less precise than the PPS, which is encrypted and, therefore, is secure and less easy to jam or spoof.[343] The PPS is dedicated to use by DOD and United States allies.[344]

Being heavily dependent on GPS, DOD is deeply concerned with jamming, spoofing, and other harmful interference with the GPS signal.[345] Experience has proved that existing encryption alone is ultimately not sufficient to protect military signals.[346] Therefore, the new military M-code is being developed and installed.[347] It will not only have a higher-powered GPS signal, but it will also be faster and more secure.[348] The strength and bandwidth needs are at issue in the Ligado case, which seeks to avoid harmful interference by separating and isolating the radio frequencies of competing parties.[349] However, it will still be possible (even likely) that some hacker will find a way to interfere with GPS. Protection may only come with the development of a radically different new technology.

C. DOD's Potential Freedom from ITU Spectrum Management

Article 48 of the ITU Constitution provides that national defense services' use of the radio-frequency spectrum remains free

---

340 *See* Paul B. Larsen, *Space Traffic Management Standards*, 83 J. Air L. & Com. 359, 364–65 (2018).

341 Larsen, *supra* note 9, at 367.

342 *Id.* at 367, 412.

343 *Id.*

344 *Id.* at 367.

345 *See supra* Section II.A.1. There is an Army saying that "bits and bytes are as dangerous as bullets and bombs." Lee, *supra* note 2. Therefore, the military plans to build—and is currently building—protective devices. *See id.*

346 Sally Cole, *Securing Military GPS from Spoofing and Jamming Vulnerabilities*, Mil. Embedded Sys. (Nov. 30, 2015), https://militaryembedded.com/comms/encryption/securing-military-gps-spoofing-jamming-vulnerabilities [https://perma.cc/HR4H-U67V].

347 *See infra* Section VIII.B (discussion of M-Code).

348 *See id.*

349 *See* In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3804–06 (2020).

of ITU regulation.[350] Nevertheless, the military installation may, in general, cause harmful interference. Therefore, to avoid harmful interference, the military services comply with ITU Administrative Regulations regarding radio frequencies and generally with ITU regulatory provisions.[351]

Military stakes in outer space are escalating. The United States has created a Space Force with a special military branch in order to establish "American dominance in space."[352] The United States now considers outer space to be a "warfighting domain in and of itself."[353] Russia and China have also established special military forces for outer space activities.[354] Possible interference with GNSS-equipped military weaponry and GNSS operation in outer space is therefore a high priority.

The upshot is that the military authorities could use ITU Constitution Article 48 to claim freedom from subjection to ITU radio frequency regulation. That would free GPS from ITU bandwidth availability restrictions. However, military and civilian activities increasingly intermingle so that it is difficult to distinguish military from civilian operations.[355] However, operating radio frequencies outside the ITU framework would also subject military bandwidths to harmful interference by the nongovernmental users to whom ITU and FCC allocated radio frequencies. The military authorities are therefore better served by subjecting themselves to, and participating in, the ITU radio frequencies allocation.

D. Evaluation of FCC's 2020 Spectrum Management Order Regarding Possible Harmful Interference with GPS Frequencies by Ligado

The Ligado decision brings into question the FCC's suitability to decide the issue of harmful interference with the GPS signal

---

[350] ITU Constitution, *supra* note 102, art. 48.

[351] *Id.*; *see also* Lyall & Larsen, *supra* note 26, at 195.

[352] Stephen A. Hildreth, Jennifer K. Elsea, Lawrence Kapp & Kathleen J. McInnis, IF10950, Cong. Rsch. Serv., Toward the Creation of a U.S. "Space Force" 1 (2018).

[353] Press Release, U.S. Dep't of Def., Department of Defense Establishes U.S. Space Force (Dec. 20, 2019), https://www.defense.gov/Newsroom/Releases/Release/Article/2045981/department-of-defense-establishes-us-space-force/ [https://perma.cc/ATE2-GDU7]; ITU Constitution, *supra* note 102, art. 48.

[354] Secure World Found., *supra* note 193, at 1-22, 2-29; *see generally* Pavel Podvig & Hui Zhang, Russian and Chinese Responses to U.S. Military Plans in Space (2008).

[355] Mountin, *supra* note 37, at 119.

using radiocommunication standards.[356] GPS is a new technology, developed after the Communications Act was adopted in 1934.[357] That legislation was intended to regulate radiocommunication issues.[358] However, the harmful interference with GPS raises issues that do not involve radiocommunication. The FCC, operating with "archaic" legislation and regulation, was arguably not qualified to decide the Ligado case. New federal law needs to be enacted to protect GPS from radio interference.[359]

The current arrangement whereby NTIA and the FCC coordinate spectrum assignment to government-operated GPS presented a new issue that they could not resolve satisfactorily.[360] Their interrelationship needs to be streamlined. GPS harmful interference issues need a more unified decisionmaker.[361]

IV. ARGUMENT THAT CHINESE 5TH TECHNOLOGY (5G) COULD INTERFERE WITH U.S. GPS SIGNALS

In 2019, 5G technology was introduced on mobile telephones with internet access.[362] 5G technology establishes small digital networks of cells that connect better and faster than 4G technology.[363] 5G has its own independent network, which is used for cell phone and computer internet access, and is much faster than 4G technology.[364] The troubling issue with 5G is whether GPS signals may be subject to infiltration by Chinese advanced 5G technology when used for access to United States GPS.[365] The 5G technology is particularly embedded in cell phone and computer technology produced by the Chinese high-technology

---

[356] Univ. of Neb., *supra* note 99.

[357] *Id.*; The Communications Act of 1934, 47 U.S.C. §§ 151–646.

[358] *See* 47 U.S.C. § 151.

[359] Univ. of Neb., *supra* note 99.

[360] *Id.*

[361] *See id.*

[362] Todd Haselton, *5G Reality Check: You Won't Need A 5G Phone Next Year*, CNBC (Dec. 4, 2018), https://www.cnbc.com/2018/12/04/5g-phones-are-coming-next-year-heres-what-that-means-for-you.html [https://perma.cc/9VPH-PBJE].

[363] Michael R. Bradley & Vincent Rotty, *Fixing the Glitch: The Smart Rollout of 5G Small Cell Wireless Networks Balancing Private and Public Interests*, 63 S.D. L. Rev. 483, 486–87 (2019).

[364] *Id.* A late development is that civilian users will become able to authenticate Galieo signals. Peter Gutierrez, *Galileo to Transmit Open Service Authentication*, Inside GNSS (Feb. 3, 2020), https://insidegnss.com/brussels-view-galileo-to-transmit-open-service-authentication/ [https://perma.cc/ZS9D-3V6J].

[365] *See* Larry W. Thorpe, *The History & Future of 5G*, 16 SciTech Law., Winter 2020, at 4, 8.

company, Huawei.[366] The United States fears that China may program technology to report to Chinese intelligence authorities because Chinese companies are subject to the Chinese government's direction.[367] This is particularly disturbing to United States military authorities. The immediate issue centers on whether Huawei should be permitted to market its 5G technology in the United States and its allied countries, such as the United Kingdom (UK).[368] The United States government has adopted a policy to exclude Huawei technology from entering the country in order to protect GPS from potential Chinese interference.[369]

The United States ban of Huawei causes political and technical difficulties for other states, which depend on its technology.[370] The UK has now joined the United States in banning Huawei 5G technology and has told its telecommunications companies to remove Huawei 5G technology from UK telecommunications networks.[371] Other states concerned with Chinese access to their military technology may also ban Huawei 5G technology.[372] In addition to loss of foreign business, Huawei now faces production difficulties because the United States recently deprived the company from using semiconductor chips.[373] The company cannot build 5G technology without these chips.[374] One consequence of banning Huawei may be a slower conversion of United States technology to 5G.[375]

V. OTHER LIMITATIONS ON USE OF GNSS

A. Privacy and Human Rights Restrictions

GNSS is used to track people through GNSS receivers in their cell phones.[376] GNSS users also attach tracking devices to cars and even to children and people who have Alzheimer's dis-

---

366 *Id.*

367 *See* Hadas Gold, *UK Bans Huawei from Its 5G Network in Rapid About-Face*, CNN Bus. (July 14, 2020), https://www.cnn.com/2020/07/14/tech/huawei-uk-ban/index.html [https://perma.cc/H3BW-HXQU].

368 *Id.*

369 *Id.*

370 *Id.*

371 *Id.*

372 *Id.*

373 *Id.* ("[N]ew sanctions . . . further reduced the company's ability to manufacture and maintain semiconductor chips using American-made technology.").

374 *Id.*

375 *Id.*

376 *See* Larsen, *supra* note 9, at 388–89.

ease.[377] A great benefit is finding those who are lost or stranded.[378] Privacy laws govern the ability to track people through GNSS.[379] Tracking people may interfere with constitutionally guaranteed basic liberty rights.[380]

The laws on information tracking differ among countries.[381] Most countries have some interest in protecting privacy and place restrictions on use of collected information.[382] The EU is particularly keen on protecting people's privacy.[383] Europe can directly regulate the collection of data by its own GNSS, Galileo.[384] However, it is difficult for a European court to obtain jurisdiction over U.S. GPS, Russian GLONASS, and Chinese BeiDou, where sovereign immunity becomes an issue.[385]

A new GNSS privacy issue has arisen concerning the tracking of people who have COVID-19 or who have recently had contact with persons known to have the disease. Norway, for example, used the "Smittestopp" computer application to trace people suspected of carrying COVID-19 and then used GNSS to upload such information without permission of the persons involved.[386] That caused Amnesty International to complain to the Norwegian Institute of Public Health and to Norway's data protection agency about invasion of privacy.[387] Consequently, Norway agreed to stop collecting this data.[388] However, certain other

---

[377] *Id.* at 389.

[378] *Id.* GPS is also used to track animals. *Id.*

[379] *Id.*; *see* ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 891–908 (5th ed. 2015) (discussing constitutional protections for travel and control over information); U.S. CONST. amends. V, XIV.

[380] *See* U.S. CONST. amends. V, XIV.

[381] Larsen, *supra* note 9, at 389.

[382] *Id.*

[383] Commission Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 2016 O.J. (L 119) 1, 3–4; Monika Zalnieriute, *The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgment*, 24 AM. SOC'Y INT'L L. INSIGHTS 1, 1–2 (Nov. 5, 2020), https://www.asil.org/sites/default/files/ASIL_Insights_2020_V24_I28.pdf [https://perma.cc/3VT7-VS4B].

[384] Larsen, *supra* note 9, at 369.

[385] *Id.* at 389–90.

[386] *Norway: Halt to COVID-19 Contact Tracing App a Major Win for Privacy*, AMNESTY INT'L (June 15, 2020), https://www.amnesty.org/en/latest/news/2020/06/norway-covid19-contact-tracing-app-privacy-win/ [https://perma.cc/E9A5-UNRC].

[387] *Id.*

[388] *Id.*

countries, such as South Korea, continue using GNSS to track individuals affected by COVID-19.[389]

The main legal issue concerns the purpose for which the tracking and tracing information is used. Does the collecting state use the information to control COVID-19 or to control a wider range of issues—for example, terrorism? Is it used to discriminate between persons who have the disease and those who do not have it? Is the tracking of people proportionate to the danger of the disease? Does it comply with local privacy laws and policies? Does it effectively reach its goal of controlling COVID-19? On analysis, Norway found that the tracking was not effective.[390] Use of GNSS to collect COVID-19 information may also violate Article 12 of the Universal Declaration of Human Rights, which provides everyone freedom from "arbitrary interference with his privacy, family, home or correspondence."[391] Article 13, which guarantees everyone the right to freedom of movement, also presents an issue.[392]

B. Use of GNSS to Collect Evidence in Criminal Cases

GNSS is frequently used to track people in criminal cases. In the case of *United States v. Jones*, the local police attached a GNSS receiver to the suspect's car in defiance of a geographically limited warrant.[393] Without Jones' consent, the GNSS receiver remained attached to his car, tracking his movements for one month.[394] The prosecution used the evidence at his criminal trial to prove the charge.[395] On appeal to the U.S. Supreme Court, the Court concluded that the privacy of the suspect had been violated.[396] The Court concluded that the evidence was

---

[389] *See* Civ. GPS Serv. Interface Comm., *China BeiDou Update*, at 15:07, YouTube (Sept. 21, 2020), https://www.youtube.com/watch?v=P6s42dYHTBY&t=907s (last visited June 2, 2021) (featuring Changjiang Geng, Test & Assessment Rsch. Ctr., China Satellite Navigation Off.); *Agenda: 60th Meeting of the Civil GPS Service Interface Committee*, *supra* note 12.

[390] Scott Ikeda, *After Being Ranked Among the World's Most Privacy-Invasive, Norway Suspends Use of Contact Tracing App*, CPO Mag. (July 2, 2020), https://www.cpomagazine.com/data-privacy/after-being-ranked-among-the-worlds-most-privacy-invasive-norway-suspends-use-of-contact-tracing-app/ [https://perma.cc/FYG8-6U7U].

[391] G.A. Res. 217 (III) A, Universal Declaration of Human Rights art. XII (Dec. 10, 1948).

[392] *Id.* art. XIII.

[393] United States v. Jones, 565 U.S. 400, 402–03 (2012).

[394] *Id.* at 403.

[395] *Id.*

[396] *Id.* at 404, 413.

collected in violation of the Fourth Amendment to the U.S. Constitution protecting "the right of the people to be secure in their persons houses, papers, and effects, against unreasonable searches and seizures."[397] The Court found that the attachment of the GNSS device to the car and its use to monitor the movements of the suspect constituted an illegal search, and the evidence it provided must be excluded.[398]

VI. POSSIBLE REMEDIES FOR HARMFUL INTERFERENCES WITH GNSS: WHITE HOUSE EXECUTIVE ORDER 13905 STRENGTHENING NATIONAL RESILIENCE THROUGH RESPONSIBLE USE OF PNT SERVICES

A. The Order

EO 13905, issued by President Trump on February 12, 2020, recognizes that, despite precautions taken to protect GNSS from harmful interferences, it remains vulnerable.[399] The EO characterizes the U.S. GPS as a basic utility like the electrical power grid which supports life and which constitutes a "critical infrastructure."[400] Consequently, EO 13905 expresses that:

> It is the policy of the United States to ensure that disruption or manipulation of PNT [GPS] services does not undermine the reliable and efficient functioning of its critical infrastructure. The Federal Government must increase the Nation's awareness of the extent to which critical infrastructure depends on, or is enhanced by, PNT [GPS] services, and it must ensure critical infrastructure can withstand disruption or manipulation of PNT [GPS] services.[401]

This EO took several steps to protect GPS security and continued availability. The EO assigned DOC the major task of implementing the new policy by developing GPS "standards, guidelines, and sector-specific requirements" necessary to protect GPS and to prevent its disruption by harmful interference.[402] These standards, guidelines, and requirements are

---

[397] U.S. Const. amend. IV; *Jones*, 565 U.S. at 405.

[398] *Jones*, 565 U.S. at 405; *see also* Larsen, *supra* note 9, at 390.

[399] Exec. Order No. 13905, 85 Fed. Reg. 9359, 9359 (Feb. 12, 2020).

[400] *Id.*

[401] *Id.* at 9359–60. GPS is known as the service for PNT. *Id.* at 9359. *See also* Peter Behr & Christian Vasquez, *Trump Orders 'Overdue' Grid, EV Defense*, Env't & Energy News, https://www.eenews.net/stories/1062336293 [https://perma.cc/48MF-WC9X].

[402] Exec. Order No. 13905, 85 Fed. Reg. 9359, 9359 (Feb. 12, 2020).

scheduled to be available one year after the EO's issuance.[403] DOC's NIST must define PNT services and describe the possible disruptive dangers facing these services.[404] NIST will compile a list of possible defenses that users may deploy to detect and manage risks associated with GPS signal disruptions.[405] NIST will also develop and distribute a new global timing standard that will measure time independently of GPS.[406] This new time measure will be 1,000 times more accurate than current timing available on the Internet.[407]

An important provision of EO 13905 is that "[n]othing in this order shall be construed to impair or otherwise affect . . . the authority granted by law to an executive department or agency, or the head thereof."[408] The EO ordered several studies.[409] However, it does not affect or change existing laws granting authority or providing funding for DOD, DOT, DOC, or FCC.[410]

The EO asks DOD and other government departments to assist the White House Office of Science and Technology Policy and the Secretary of Homeland Security with their assigned task of ascertaining government agencies' capability to apply DOC-developed GPS "standards, guidelines, and sector-specific requirements."[411] DOC's contribution to the effort primarily involves improved risk management by GNSS users stated in the 2020 Space Policy Directive 5, entitled Cybersecurity Principles for Space Systems.[412] The directive recommends GNSS users adopt cybersecurity best practices, monitor and reduce risks inherent in their GNSS equipment, and estimate their jamming

---

[403] *Id.* at 9360.

[404] *Id.* at 9359–60; *see also Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services – Frequently Asked Questions*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/pnt/faqs [https://perma.cc/E827-NKNR].

[405] *Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and Timing Services – Frequently Asked Questions*, *supra* note 404.

[406] *Responsible Use of Positioning, Navigation and Timing Services*, NAT'L INST. OF STANDARDS & TECH., https://www.nist.gov/pnt [https://perma.cc/H7XQ-CJ8P].

[407] *Id.*; Exec. Order No. 13905, 85 Fed. Reg. at 9360.

[408] Exec. Order No. 13905, 85 Fed. Reg. at 9360.

[409] *Id.* at 9359–60; Memorandum on Space Policy Directive-7, *supra* note 45.

[410] *See* Exec. Order No. 13905, 85 Fed. Reg. at 9360; Memorandum on Space Policy Directive-7, *supra* note 45.

[411] Exec. Order No. 13905, 85 Fed. Reg. at 9360.

[412] Memorandum on Space Policy Directive-5, Cybersecurity Principles for Space Systems, 85 Fed. Reg. 56155, 56156–57 (Sept. 9, 2020).

and spoofing risk tolerance as well as their ability to recover after disruptions.[413]

B. Evaluation of Executive Order 13905

GPS is in deep trouble. Harmful interference with GPS signals threatens basic safety and security of the GPS users.[414] The government needed to deal with this harmful interference, and the EO, as well as associated presidential directives on the subject, reflect the serious need for this attention.[415] EO 13905 assigned major responsibility for its execution to DOC, which has an economic laissez-faire attitude towards GPS safety, in contrast to FAA's safety mission, which currently maintains safety oversight of GPS for airplane navigation.[416] In the past, the joint military and civil PNT Committee, established by the 2004 U.S. Space-Based Positioning, Navigation, and Timing National Security Presidential Directive (NSPD-39), has had interagency oversight responsibility for GPS.[417] The PNT Committee coordinates GPS activities among the government agencies and issues national guidance.[418] Co-chaired by DOD and DOT, it coordinates spectrum management among the government departments.[419] Members also include the Departments of State, Commerce, Homeland Security, Interior, Agriculture, as well as the Joint Chiefs of Staff and NASA.[420] The PNT Committee, which has a permanent staff, has several subcommittees and working groups on specific GPS issues.[421] The PNT Committee meets regularly and provides national and international guidance.[422] DOD's membership in the PNT Committee establishes important policy and operative cooperation between the military GPS pro-

---

[413] *Id.*; *see Agenda: 60th Meeting of the Civil GPS Service Interface Committee*, *supra* note 12; Civ. GPS Serv. Interface Comm., *DHS PNT Update*, *supra* note 12; Civ. GPS Serv. Interface Comm., *Resilient PNT System Concepts for Critical Infrastructure*, *supra* note 12.

[414] *See* Larsen, *supra* note 9, at 392.

[415] Exec. Order No. 13905, 85 Fed. Reg. 9359; Memorandum on Space Policy Directive-5, Cybersecurity Principles for Space Systems, 85 Fed. Reg. 56155; Memorandum on Space Policy Directive-7, *supra* note 45.

[416] Exec. Order No. 13905, 85 Fed. Reg. at 9360; Larsen, *supra* note 51, at 462.

[417] National Security Presidential Directive-39, U.S. Space-Based Position, Navigation, and Timing Policy (Dec. 15, 2004), https://fas.org/irp/offdocs/nspd/nspd-39.htm [https://perma.cc/JSA9-KEAZ].

[418] *Id.*

[419] *Id.*

[420] *Id.*

[421] *Id.*

[422] *Id.*

vider and other government users.[423] The Civil GPS Service Interface Committee provides important coordination with non-governmental users.[424] The EO does not change NSPD-39, nor does it mention the PNT Committee established by that presidential directive.[425] The EO review of GPS barely mentions DOD, DOT, or FAA.[426] Because interference with GPS signals mostly affects safety,[427] the following observations are made about the effect of the EO.

GPS is a military service located in and administered by DOD on a particular legal mandate from Congress and funded by Congress.[428] Thus, DOD is the key agency. GPS is a basic ingredient of the military structure.[429] Other agencies are basically in the position of making recommendations.[430] DOD has been willing to make GNSS available for civilian uses.[431]

GPS is a GNSS just like the other three services (GLONASS, BeiDou, and Galileo).[432] GPS was the first GNSS and remains the most popular one around the world.[433] GPS is part of other countries' national infrastructures just as it is part of the U.S. infrastructure.[434] The issue of dependability and possible harmful interference with its signals is as much an international problem as it is a national one.[435] The international issues are discussed more extensively elsewhere in this Article.[436]

Jamming, spoofing, and other harmful spectrum interference disruptions are basic safety problems that can result in collisions and loss of human life.[437] Harmful interference with air navigation can result in accidents involving loss of cargo and hundreds

---

423 *Id.*

424 *Civil GPS Service Interface Committee*, *supra* note 146.

425 *See* Exec. Order No. 13905, 85 Fed. Reg. 9359, 9360 (Feb. 12, 2020).

426 *See id.* DOD and FAA were the moving government parties in the FCC Ligado proceeding. In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3776 n.18, 3783 (2020).

427 Lee, *supra* note 2.

428 DOD administers GPS pursuant to 10 U.S.C. § 2281. *See* Larsen, *supra* note 51, at 459, 461–62.

429 Larsen, *supra* note 51, at 462.

430 *Id.*

431 *Id.* at 460.

432 Larsen, *supra* note 9, at 366–70.

433 *Id.* at 366.

434 *Id.* at 367–68.

435 *See id.* at 382.

436 *See* discussion *supra* Section II.B.

437 LYALL & LARSEN, *supra* note 26, at 352–53.

of passengers.[438] DOC's suggestion to analyze the economic risks involved in outer space activities will probably fail to resolve these basic safety problems effectively.[439]

The basic safety problems caused by the harmful interference with GPS signals described in this Article[440] can best be examined and prevented by an agency that is basically concerned with *safety*. The PNT Committee, FAA, and DOD should therefore continue overseeing basic safety of civilian GPS.

VII. NEW TECHNOLOGY TO PERFORM THE TASKS PRESENTLY DONE BY GPS

A. Strengthening Existing GPS Technology

Military authorities are developing a new generation of GPS-III satellites to remedy some existing GPS system weaknesses.[441] The new technology will digitalize and fully encrypt signals with anti-jamming and anti-spoofing features.[442] The satellites will "have three times greater accuracy and eight times improved anti-jamming capability."[443] The military authorities have contracted for even more sophisticated technology, including a "fully digital navigation payload [and] something called a regional military protection which is a new, more powerful regional signal for our warfighters that will help give an increased anti-jam and anti-spoofing capability."[444] Furthermore, it will have a "laser retroreflector array," enabling users to send a laser to the satellite for more accurate information.[445] Despite these technological advances, others remain focused on developing even more sophisticated jamming devices to overcome anti-jamming efforts.[446]

---

[438] *Id.*

[439] *See GPS Economic Study*, Off. of Space Com. (Aug. 9, 2019), https://www.space.commerce.gov/gps-economic-study-presentation/ [https://perma.cc/E7KN-46ZY].

[440] *See supra* Part III.

[441] Tadjdeh, *supra* note 63.

[442] *Id.*

[443] *Id.*

[444] *Id.* (quoting Jonathan Caldwell, Vice President for Navigation Sys., Lockheed Martin).

[445] *Id.*

[446] *See* Daniele Borio & Pau Closas, *A Fresh Look at GNSS Anti-Jamming*, Inside GNSS, Sept./Oct. 2017, at 54, 54–55, https://insidegnss.com/auto/sepoct17-BORIO_0.pdf [https://perma.cc/3N8Q-CPWG].

B. The New GPS Military M-Code Encryption

The difference between civilian and military GPS continues to grow. The military specially developed M-code to protect military uses from jamming, spoofing, and other harmful interferences with the GPS signals.[447] The M-code is further encrypted and protected and thus even more different from the unprotected standard signals available to the civilians.[448] The M-code, when fully deployed, will enable the military GPS to become an autonomous system, meaning receivers will be able to acquire the M-code signal without access to other signals.[449] The M-code is transmitted on the existing GPS radio frequencies.[450] It uses a special "high-gain directional antenna" in addition to the existing antenna.[451] The signal is sent by the directional antenna functioning like a "spot beam" aimed at a specific destination.[452] Thus, the signal is 100 times stronger than existing GPS signals.[453] The extra strength will make the signals more difficult to jam, spoof, or otherwise be subject to interference.[454]

The M-code is being built into a dozen advanced GPS-III satellites and will gradually take the place of the previously encrypted military satellites.[455] Eventually, DOD will have only one uniform system for its use.[456] All equipment will be aligned with the M-code, and will thus be better protected.[457] The military services will be able to operate totally independently of the standard GPS while still using the same frequencies but without interfering with the standard GPS.[458]

---

[447] Jan Van Sickle, *The M-Code*, Pa. State Univ., https://www.e-education.psu.edu/geog862/node/1862 [https://perma.cc/DZ6P-6JT2].

[448] Brian Barker, John W. Betz, John E. Clark, Jeffrey T. Correia, James T. Gillis, Steven Lazar, Kaysi A. Rehborn & John R. Straton, *Overview of the GPS M Code Signal*, *in* Proc. of the 2000 Nat'l Tech. Meeting of the Inst. of Navigation 542, 543 (2000).

[449] *Id.* at 545–46.

[450] *Id.* at 546.

[451] Tracy Cozzens, *GPS III Finally Aloft, Benefits on the Way*, GPS World (Jan. 9, 2019), https://www.gpsworld.com/gps-iii-finally-aloft-benefits-on-the-way/ [https://perma.cc/N7AB-2PDU].

[452] *Id.*

[453] *Id.*

[454] *Id.*

[455] Van Sickle, *supra* note 447.

[456] *Id.*

[457] *Id.*

[458] *Id.* The U.S. military will rely on the M-code in times of war. Nathan Strout, *Allies Begin Ordering M-Code-Enabled GPS Receivers*, C4ISRNet (Nov. 24, 2020),

As became apparent in the Ligado proceeding,[459] changes in existing military equipment will increase M-code compatibility. The M-code requires an expensive transition to new technology, which will take some years.[460] Overlap with older GPS codes will remain for some time, until all military devices gradually convert to M-code.[461] All new GPS signal equipment will be built to incorporate the M-code.[462] The change to full compatibility with the M-code is expensive, and Congress must budget for the additional cost.[463] Thus, the President must ask Congress for increases in the military budget.[464] For the 2020 military budget, President Trump asked Congress for an additional $330 million for M-code conversion, and DOD will likely need an additional $1.76 billion to convert all military equipment.[465]

M-code development shows how military GPS is becoming increasingly separated from civilian GPS.[466] The military authorities wish to become unburdened of responsibility for civilian GPS.[467] However, civilian GPS use far exceeds total military use.[468] Separating civilian and military GPS would require Congress to appropriate billions of dollars for an independent civilian GPS system.[469] That seems unlikely.

C. Encryption of Civilian GNSS Signals

Civilian standard GNSS signal encryption might require each person who wants to use GNSS to enter into an agreement.[470] That would place the service on an entirely different legal basis because the GNSS provider would be subject to the agreement's terms.[471] Furthermore, the existing ease of use would be gone: each user would have an individual relationship with the provider.[472] GNSS would no longer be free like the air or open

---

https://www.c4isrnet.com/battlefield-tech/space/2020/11/24/allies-begin-ordering-m-code-enabled-gps-receivers/ [https://perma.cc/X8HF-U7T9].

459 *See supra* Section IV.A.

460 Lee, *supra* note 2.

461 *Id.*

462 *Id.*

463 *Id.*

464 *Id.*

465 *Id.*

466 Larsen, *supra* note 9, at 412.

467 *Id.* at 411.

468 *Id.* at 412.

469 *Id.*

470 Milner, *supra* note 6.

471 *See id.*

472 *Id.*

roads.[473] It would also change the relationship between GPS and its users. Civilian users would have to be screened for dependability and trustworthiness before being told the secret GPS encryption, and a special government bureaucracy would likely be created to administer permit issuance. That would probably result in charging money to use GPS navigation services, perhaps similar to how Canada now charges airlines for use of Canadian air traffic control.[474]

How would a change from free GPS to one that the user pays for affect GPS PNT? Such a change would probably also affect the other three GNSS (GLONASS, Galileo, and BeiDou) that now provide free global GNSS services.[475] If they continue to provide free services, global use of civilian GPS would probably cease. Other GNSS services would also likely shift to a system of encryption and charges.

Administration would be expensive and would create an additional, probably unwanted burden for DOD. Also, the process of permitting and charging would involve a different legal relationship between governmental GPS and its users because the users might hold GPS responsible for service quality.[476]

VIII. ALTERNATIVE GNSS TECHNOLOGIES

Jamming, spoofing, and other interference has motivated interest in PNT technology other than GPS.[477] Three alternative services are in development. One is a terrestrial system.[478] The other two are satellite systems in LEO instead of in medium-Earth orbit (MEO) like the four current GNSS.[479] Ideally, the alternative technologies would be speedier and send stronger

---

[473] Larsen, *supra* note 9, at 385.

[474] Scott McCartney, *The Air-Traffic System U.S. Airlines Wish They Had*, WALL ST. J. (Apr. 27, 2016), https://www.wsj.com/articles/the-air-traffic-system-u-s-airlines-wish-they-had-1461776053 [https://perma.cc/A49M-WCY4].

[475] Larsen, *supra* note 9, at 385.

[476] *See id.*

[477] Michelle V. Rafter, *U.S. Transportation Officials Seek Alternative Tech for GPS*, IEEE SPECTRUM (Apr. 24, 2020), https://spectrum.ieee.org/aerospace/satellites/us-transportation-officials-seek-alternative-tech-for-gps [https://perma.cc/XA5C-4V5C].

[478] Jeff Shepard, *eLoran A Terrestrial Alternative to GPS*, MICROCONTROLLER TIPS (Oct. 6, 2020), https://www.microcontrollertips.com/eloran-a-terrestrial-alternative-to-gps/ [https://perma.cc/Z7EM-7DM3].

[479] Nathan Strout, *COVID, OneWeb And How The Space Development Agency Has Coped*, C4ISRNET (May 26, 2020), https://www.c4isrnet.com/battlefield-tech/space/2020/05/26/covid-oneweb-and-how-the-space-development-agency-has-coped/ [https://perma.cc/7MLF-XBAG].

signals that would be more difficult to jam, spoof, or otherwise be interfered with.[480]

A. eLoran: Terrestrial Substitute for Outer Space GNSS

The question of alternative GNSS technology initially focused on pre-GPS navigation technology, the Loran-C navigation system.[481] After the change to GPS, countries began to do away with the Loran-C system.[482] However, jamming, spoofing, and other interference problems provoked interest in advanced Loran-C, called eLoran,[483] which is difficult to jam or spoof because of the huge, easily-detectable antennas required.[484] eLoran would be a standardized, international PNT service.[485] It would meet performance requirements for aviation, shipping, and automobiles.[486] eLoran would build on old Loran-C facilities.[487] Other countries have also expressed interest in this alternative to GPS.[488] The U.S. National Timing, Resilience, and Security Act authorized DOT to develop a terrestrial substitute for GNSS.[489] DOT is ready to submit the results of its study to Congress.[490] EO 13905 includes development of national PNT "that are not dependent on global navigation satellite sys-

---

480 Rafter, *supra* note 477.

481 *See* Larsen, *supra* note 9, at 383–84.

482 *Id.*

483 *Id.*

484 Georg T. Becker, Sherman Lo, David De Lorenzo, Di Qiu, Christof Paar & Per Enge, *Efficient Authentication Mechanisms for Navigation Systems – A Radio-Navigation Case Study*, *in* Proc. of the 22nd Int'l Tech. Meeting of the Satellite Div. of the Inst. of Navigation 901, 902 (2009).

485 Arthur Helwig, Gerard Offermans, Chris Stout & Charles Schue, *eLoran System Definition and Signal Specification Tutorial*, *in* 40th Int'l Loran Ass'n Ann. Convention & Tech. Symp. (Nov. 18, 2011), https://www.loran.org/proceedings/Meeting2011/ILA%202011%20Tutorial.pdf [https://perma.cc/CAS5-RFLE].

486 *Id.*

487 *House Committee Moves to Block Loran-C Teardowns*, Inside GNSS (Feb. 14, 2014), https://insidegnss.com/house-committee-moves-to-block-loran-c-teardowns/ [https://perma.cc/VQ4C-9KC8].

488 Larsen, *supra* note 9, at 384.

489 49 U.S.C. § 312(a).

490 Datta, *supra* note 6; *see generally Agenda: 60th Meeting of the Civil GPS Service Interface Committee*, *supra* note 12; Civ. GPS Serv. Interface Comm., *DOT PNT Update*, at 43:40, YouTube (Sept. 22, 2020), https://www.youtube.com/watch?v=6FpKN018zSM&t=2620s (last visited June 2, 2021) (featuring Andrew Hansen, Volpe Nat'l Transp. Sys. Ctr. & Karen Van Dyke, PNT & Spectrum Manager, U.S. Dep't of Transp.).

tems."[491] However, other countries, such as the UK, have since decided against a terrestrial substitute for GNSS.[492]

B. DOD's SDA Contract for a Military Alternative to GPS

In 2019, DOD's new Space Development Agency (SDA) began plans for a military alternative to GPS, to be ready by 2023, which would replace GPS if the M-code encryption and other precautionary changes fail to protect the military GPS from disruptive interference.[493] Toward that purpose, DOD contracted with two companies, Lockheed Martin and York Space Systems, to each build ten small satellites (twenty total) for delivery in 2022.[494] These satellites will be placed in LEO and will be the first step towards placing a constellation of several hundred small satellites in LEO.[495] This new satellite system will provide navigation for and communication with military equipment if the GPS system is compromised.[496] DOD plans to deploy 100 small satellites by 2024, which will be sufficient to allow use of the system as planned.[497] The new satellite system will enable DOD to control and direct military equipment on the surface more effectively than with GPS.[498] Besides the existing PNT signals, the new satellite network will have additional PNT capabil-

---

491 Exec. Order No. 13905, 85 Fed. Reg. 9359, 9360 (Feb. 12, 2020); *see also* Memorandum on Space Policy Directive-7, *supra* note 45.

492 Reuters, *Europe Gives Up on eLoran*, Maritime Exec. (Feb. 9, 2016, 7:23 AM), https://maritime-executive.com/article/europe-gives-up-on-eloran [https://perma.cc/6XRY-896R].

493 Sandra Erwin, *Lockheed Martin, York Space to Produce 20 Satellites for Space Development Agency*, SpaceNews (Aug. 31, 2020), https://spacenews.com/lockheed-martin-york-space-win-contracts-to-produce-20-satellites-for-space-development-agency/ [https://perma.cc/7TZQ-HPC6].

494 *Id.*

495 *Id.* The DOD satellite constellation will compete with the thousands of small satellites now being launched into LEO. Greg Ritchie & Thomas Seal, *Why Low-Earth Orbit Satellites Are the New Space Race*, Wash. Post (July 10, 2020 9:15 PM), https://www.washingtonpost.com/business/why-low-earth-orbit-satellites-are-the-new-space-race/2020/07/10/51ef1ff8-c2bb-11ea-8908-68a2b9eae9e0_story.html [https://perma.cc/RK6R-K3SC].

496 Erwin, *supra* note 493.

497 Eric Berger, *The US Military Took a Big Step Toward a Future Space Network This Week*, Ars Technica (Sept. 1, 2020), https://arstechnica.com/science/2020/09/the-us-military-took-a-big-step-toward-a-future-space-network-this-week/ [https://perma.cc/ZK4S-5DER].

498 *Id.*

ity.[499] The SDA Director announced: "We're not going to broadcast like GPS does, but folks that are on our comm[unication] channel can get navigation using our backbone."[500]

The military alternative would serve a wider purpose than GPS. Whether it could be considered a weapon of mass destruction in violation of OST Article IV would depend on its wider uses.[501] The military could fall back on the new satellite network in case GPS is compromised. The SDA and the new satellite network will be transferred to the newly established U.S. Space Force in 2022.[502]

C. OneWeb as Alternative GNSS

The UK has bought control of OneWeb Satellites (OneWeb).[503] The UK will turn the company into an alternative global PNT service.[504] The objective is similar to DOD's plan to place a new PNT system in LEO, except that it will service both civilian and military customers.[505] OneWeb is a small satellite company which has already placed seventy-four small satellites in LEO and has existing authority and plans to place a satellite constellation of 648 satellites in LEO.[506] The use of LEO and of the Ku-band of radio frequencies—rather than the L-band used by GPS—will make OneWeb's signals stronger and harder to jam, spoof, or otherwise be interfered with.[507] OneWeb has requested further authority to place 48,000 small satellites in

---

[499] Kimberly Underwood, *Military Aims to Urgently Provide Disruptive Satellite Capability*, AFCEA Int'l (Aug. 1, 2020), https://www.afcea.org/content/military-aims-urgently-provide-disruptive-satellite-capabilities [https://perma.cc/2E7G-C84U].

[500] *Id.* (quoting Derek Tournear, Director, Nat'l Space Dev. Agency).

[501] Bruno Hasselmann, *Weapons of Mass Destruction, Article IV Outer Space Treaty and the Relation to General Disarmament*, *reprinted in* Proc. Twenty-Fifth Colloq. L. of Outer Space 99, 108 (1982); *see also* Lyall & Larsen, *supra* note 26, at 449.

[502] Valerie Insinna, *Space Development Agency on Track to Become Part of Space Force in 2022, Director Says*, Def. News (Jan. 23, 2020), https://www.defensenews.com/space/2020/01/21/space-development-agency-on-track-to-become-part-of-space-force-in-2022-director-says/ [https://perma.cc/WSX5-DC2L].

[503] Tony Osborne, *OneWeb Buy Could Pave Way to UK Sovereign GNSS*, 182 Aviation Wk. & Space Tech., no. 14, 2020, at 70, 70.

[504] *Id.*

[505] *Id.*

[506] *Id.*

[507] *Id.*; *see also* Steve Nichols, *L/Ku/Ka-Band Satellites – What Does It All Mean?*, Get Connected (Sept. 11, 2017), https://www.getconnected.aero/2017/09/lkuka-band-satellites-mean/#:~:text=the%20terms%20L%2Dband%2C%20Ku,are%20bandied%20around%20quite%20freely.&text=L%2Dband%20uses

LEO.[508] "OneWeb will offer something new into the [PNT] arena, and not simply another alternative system."[509] OneWeb will also provide access to "broadspeed-band internet . . . without the additional cost of ground infrastructure."[510] The new service will serve civilians but will also be linked to and used by UK military services.[511] However, OneWeb's different satellite technology would require different receivers than currently used for GNSS.[512]

D. Evaluation of Alternatives

The eLoran terrestrial navigation system would bring the satellites much closer to the users, which would increase the speed of the service and considerably strengthen the signal.[513] DOD's SDA contract for a GPS alternative in LEO is intended for military use.[514] It does not help nongovernmental users who are left with the existing, increasingly dangerous PNT system. OneWeb, the other LEO satellite service, has yet to develop into a PNT system that could be considered seriously.[515] It may become relevant if it remains a U.S. system, but if it becomes a UK system, then it is less likely to replace GPS. As a foreign service, it would need FCC permission to beam signals into the United States.[516] Consequently, OneWeb's ability to take the place of the current GNSS networks is questionable.

IX. SOLUTIONS AND OPTIONS

Jamming, spoofing, and other harmful interferences have exposed a basic fault in GNSS. A fundamental weakness has developed. Silence is consent to the weakened system. Unless and until the structure is repaired and fortified, the weakness will grow until the system collapses.

%20frequencies%20in,segment%20of%20the%20electromagnetic%20spectrum [https://perma.cc/7MNS-3EAL].

[508] Osborne, *supra* note 503.

[509] *Id.*

[510] *Id.*

[511] *Id.*

[512] *OneWeb LEO PNT: Progress or Risky Gamble?*, Inside GNSS (Sept. 28, 2020), https://insidegnss.com/oneweb-leo-pnt-progress-or-risky-gamble/ [https://perma.cc/SJ4N-GHQX].

[513] Becker et al., *supra* note 484, at 902.

[514] Erwin, *supra* note 493.

[515] Strout, *supra* note 479.

[516] *See* In the Matter of LightSquared Tech. Working Grp. Report, 35 FCC Rcd. 3772, 3773 n.2 (2020).

A. Solutions

1. Ultimate Viability of GNSS?

The first question is whether the existing highly vulnerable GNSS in MEO are dependable and ultimately viable. The existing GNSS have been jammed, spoofed, and interfered with.[517] Encrypted GNSS signals are more secure than unencrypted signals, but all are vulnerable. Failure to remedy the problem could result in loss of confidence in the crucial GNSS infrastructure.[518] What is required to establish a GNSS sufficiently resilient to withstand harmful interference? One solution might be to rebuild all GNSS receivers to filter out harmful interferences, like those caused by Ligado. Another option is to greatly increase GNSS signal strength, making it more difficult for the signals to be overpowered by stronger signals.[519] However, such changes could involve huge cost. This solution might also require larger constellations, with hundreds of LEO satellites per system, instead of the 24–30 MEO satellites required by the existing GNSS.[520] As an interim solution, Congress is considering legislation prohibiting DOD compliance with the FCC Ligado order until a satisfactory solution has been negotiated.[521]

2. Harmful Interference is an International Problem

Can one country, even a leading space power like the United States, resolve the international problem of GNSS jamming and spoofing, much of which is caused beyond national borders? Each GNSS is separately operated and controlled by the European Space Agency, as well as U.S., Russian, and Chinese military authorities.[522] All the GNSS are interoperable.[523] They serve as back-ups for one other in case an existing system fails. Each operator can and does encrypt and modify parts of their system to avoid harmful interferences, but all the systems are vulnerable.[524] Nevertheless, all the systems are global, so any changes affect the entire world. The U.S. GPS system is even more glob-

---

[517] Larsen, *supra* note 9, at 382.

[518] *Id.* at 383.

[519] Osborne, *supra* note 503, at 70.

[520] Lyall & Larsen, *supra* note 26, at 340; Milner, *supra* note 6.

[521] Dawn M.K. Zoldi, *Ligado Soars Over Another Obstacle to 5G Domination*, Inside GNSS (Sept. 23, 2020), https://insidegnss.com/ligado-soars-over-another-obstacle-to-5g-domination/ [https://perma.cc/X66H-JFFN].

[522] Lyall & Larsen, *supra* note 26, at 465.

[523] *Id.* at 348.

[524] *Id.*

ally ingrained into existing ways of living and operating than the other systems, and in that sense, it is the most dependent on reliable GNSS.[525] But all countries are vulnerable when GNSS is attacked. Therefore, there is a prevailing international interest in and need for secure GNSS. Harmful interference is an international problem in need of international solution.

3. Effect of Military Encrypted M-code that Excludes Civilians

Suppose the military authorities abandon GPS in favor of the special M-code PNT system in LEO. If not the military, which agency would operate nongovernmental GNSS and protect it from harmful interference? The M-code's extensive military GNSS signals encryption may satisfy military authorities' immediate need to avoid harmful interference with GNSS signals, but that presents a dilemma for the nongovernmental users.[526] Providing protection against harmful interference is outside the inherent functions of the military.[527] M-code moves military users further from responsibility for nongovernmental users and their unencrypted standard signals.[528] It increases the likelihood of separation of nongovernmental from governmental GNSS.[529] It leaves unencrypted nongovernmental GNSS in an increasingly dangerous situation.

4. Need for a U.S. Government GPS Decision Maker

A nonmilitary decision maker like the FCC is probably not qualified to decide whether the military GPS is adequately protected from radio interference from other users of radio frequencies. The Ligado case illustrates how differences on spectrum policy can endanger services.[530] The United States is not well served by having GPS spectrum policy decided by a government agency that is not part of the executive branch.[531] Better government policy coordination is needed.[532] Congress

---

[525] *Id.* at 341.

[526] Tadjdeh, *supra* note 63.

[527] LYALL & LARSEN, *supra* note 26, at 475.

[528] Larsen, *supra* note 9, at 412.

[529] *Id.*

[530] *See also* Jeff Foust, *GPS Committee Calls FCC Ligado Order a "Grave Error"*, SPACENEWS (July 1, 2020), https://spacenews.com/gps-committee-calls-fcc-ligado-order-a-grave-error/ [https://perma.cc/6UVX-HPRN].

[531] *Id.*

[532] Theresa Hitchens, *Iridium Publicly Threatens Lawsuit to Overturn FCC's Ligado Vote*, BREAKING DEF. (July 10, 2020), https://breakingdefense.com/2020/07/irid-

needs to give the executive branch authority for unitary decision-making on GPS spectrum assignment.[533]

5. Which U.S. Government Agency Could Best Supervise Civilian GPS?

GNSS is indispensable for traffic safety both on Earth and in space. Civilian GNSS is increasingly subject to harmful interference.[534] However, the White House 2020 GPS policy decision to assign GPS oversight responsibility to the DOC created a new problem.[535] GNSS is basically a technological safety tool—it performs basic PNT functions.[536] It has become a pillar of the national infrastructure.[537] The White House's decision, via EO 13905, to treat GPS as an economic issue by assigning policy leadership to the DOC does not suit civilian GPS technological and safety policy requirements.[538] DOT has a practical technical stake in GPS technology.[539] NSPD-39 placed civilian GPS in DOT/FAA, where it should remain.[540]

B. OPTIONS

An option that would provide quick GNSS reinforcement across the board is badly needed, but does not exist. Combining military and civilian GNSS complicates the search for and achievement of a 100% solution. A recent study shows that the space powers have invested heavily in offensive cyber technology capable of interfering with communication networks.[541] The United States outspends the other space powers, indicating that the United States would have difficulty in giving up cyber technology capable of harmful interference with GNSS.[542] The fol-

---

ium-publicly-threatens-lawsuit-to-overturn-fccs-ligado-vote/ [https://perma.cc/2D8Z-ELAY].

[533] *Id.*

[534] Larsen, *supra* note 9, at 379, 382.

[535] Exec. Order No. 13905, 85 Fed. Reg. 9359, 9360 (Feb. 12, 2020); Smith, *supra* note 152; *see also* Memorandum on Space Policy Directive-7, *supra* note 45.

[536] LYALL & LARSEN, *supra* note 26, at 337–38.

[537] *Id.*

[538] Exec. Order No. 13905, 85 Fed. Reg. at 9360.

[539] *See supra* Section II.A.2.

[540] *See* National Security Presidential Directive-39, *supra* note 417.

[541] *See A New Global Ranking of Cyber-Power Throws Up Some Surprises*, *supra* note 5. *The Economist* reports that the United States invested $17 billion in offensive cyber technology in 2020, most of which was expended by the National Security Agency. *Id.* China spent almost as much. *Id.*

[542] *Id.*

lowing scale of possible options and solutions begins with the easiest but also weakest solution. It ends with the most difficult, but also the strongest solution.

1. Voluntary International Harmful Interference Guidelines

The easiest option may be to use the U.N. Space Debris Guidelines as a model for resolving the GNSS problem with harmful interferences with civilian GNSS. In 2007, COPUOS adopted space debris guidelines which were approved by the U.N. General Assembly in 2008.[543] While the space debris guidelines are voluntary, the individual states are asked to adopt them as mandatory regulations.[544] Many states, including the United States, have done so.[545] The adoptions have not been uniform, and COPUOS guidelines on harmful interference with GNSS would at least establish an international baseline or standard for national regulation.[546]

GNSS harmful interference guidelines, similar in form, that might apply to GNSS would include the following elements:

(1) Apply the COPUOS interference guidelines only to jamming, spoofing, and harmful interference with civilian GNSS;[547]

---

[543] U.N. Off. for Outer Space Affs., Space Debris Mitigation Guidelines, U.N. Doc. V.09–88517 (Jan. 2010); G.A. Res. 62/217, International Cooperation in the Peaceful Uses of Outer Space (Dec. 22, 2007).

[544] G.A. Res. 62/217, *supra* note 543, ¶ 27; Ram S. Jakhu & Md Tanveer Ahmad, *The Outer Space Treaty and States' Obligation to Remove Space Debris: A US Perspective*, SPACE REV. (Nov. 13, 2017), https://thespacereview.com/article/3370/1 [https://perma.cc/33HP-QQCE].

[545] Jakhu & Ahmad, *supra* note 544; Kevin Conole, Head of Delegation, U.S. Statement at 2020 COPUOS Scientific and Technical Subcommittee (Feb. 5, 2020), https://vienna.usmission.gov/2020-copuos-stsc-u-s-on-space-debris/ [https://perma.cc/H7MZ-CB3U].

[546] The ICG agenda already includes the issues of spectrum interference. LYALL & LARSEN, *supra* note 26, at 356–58 (discussing the ICG). The ICG has adopted recommendation for interference and spectrum protection. *See also* GPS Serv. Interface Comm., *U.S. National Space-Based PNT Update*, YOUTUBE, at 52:05, (Sept. 22, 2020), https://www.youtube.com/watch?v=Rr11pyY79-M&t=3125s (last visited June 2, 2021) (featuring Harold Martin, Director, Dir. Nat'l Off. for Space-Based Positioning, Navigation, and Timing); Civ. GPS Serv. Interface Comm., *GPS User Perspectives*, YOUTUBE, at 1:14:01, (Sept. 22, 2020), https://www.youtube.com/watch?v=Rr11pyY79-M&t=4441s (last visited June 2, 2021) (featuring Adm. Thad Allen, U.S. Coast Guard (Ret.), U.S. PNT Advisory Bd. Chair); G.A. Res. 59/2, Review of the Implementation of the Recommendations of the Third United Nations Conference on the Exploration and Peaceful Uses of Outer Space (Oct. 20, 2004).

[547] *See generally* G.A. Res. 62/217, *supra* note 543.

(2) Recognize the OST Article IX obligation to engage in cooperation and mutual assistance so as to avoid harmful interferences with civilian GNSS;[548]
(3) Express recognition of state sovereignty;
(4) Acknowledge that GNSS is a necessary tool for Earth infrastructure;[549]
(5) Recognize the mutual benefits of preserving civilian GNSS without jamming, spoofing, or other harmful interference;[550]
(6) Declare the urgency of eliminating all civilian GNSS jamming, spoofing, and harmful interference;[551] and
(7) Place the burden on each state to prohibit governmental and nongovernmental jamming, spoofing, and other radio interferences with civilian GNSS uses.

COPUOS guidelines on harmful interference with civilian GNSS radionavigation frequencies would recommend that states make the guidelines subject to mandatory application and enforcement. That could become the first step towards international prohibition on harmful interference.

The existing COPUOS ICG would be the logical group to prepare U.N. guidelines on GNSS harmful interference.[552] Action by COPUOS should be expedited if this option is accepted. This option's weakness is the lack of uniformity, universal adoption, and enforcement.

2. Changing the FCC Definition of Harmful Interference

The Ligado decision brought into question the FCC's competency to decide the harmful GPS signal interference issue using radiocommunication standards.[553] GPS technology is new and outside the scope of the Communications Act, which Congress intended to regulate radiocommunication issues.[554] New federal law, or at the very least new FCC definition of harmful interference, should be enacted to protect GPS from radio interference.

---

[548] OST, *supra* note 62, art. IX.

[549] Larsen, *supra* note 9, at 365.

[550] *Id.* at 392–93.

[551] *Id.* at 382–83.

[552] *International Committee on Global Navigation Satellite Systems*, U.N. OFF. FOR OUTER SPACE AFFS., https://www.unoosa.org/oosa/en/ourwork/icg/icg.html [https://perma.cc/64JT-TYDK].

[553] Foust, *supra* note 530.

[554] Univ. of Neb., *supra* note 99; 47 U.S.C. § 151.

3. A Unified U.S. Government Decision Maker

The current NTIA and FCC coordination of GPS spectrum allocation should be streamlined. A more unified decision-maker for harmful interference issues needs to be established. The United States scatters decision-making regarding GPS harmful interference among too many agencies.[555] The harmful interference issue involves all the government members of the interagency PNT Committee.[556] EO 13905 could result in even greater dilution of decision-making authority.[557] A more unified government decision structure for administration and policy formation would establish greater confidence in GPS.[558]

4. Encrypting All Civilian GNSS Signals

Encryption of the civilian standard GNSS signals is looming. It may require each service to enter into an arrangement with individual GNSS service users.[559] That would place GNSS service on a different legal basis because the GNSS service provider would be subject to the arrangement's terms.[560] The existing ease of use would be replaced by a more complex strategy. Each user would have an individual relationship with the provider.[561] The current concept, with GNSS service free like the air or open roads, would no longer pertain.[562]

5. Using Galileo for Global Civilian GNSS

The current practice, free civilian use of military GNSS, may not be able to continue if military GNSS radically increases encryption and other defensive technology. Sharing such new technology with civilians free of charge may no longer be possible.[563] What would happen to civilian users if they were ejected from the military GNSS? Civilians' huge and still increasing need for GNSS would continue. Under these pressures, there could be a powerful impetus for a special civilian GNSS. Could

---

555 *See Federal Agencies*, GPS.GOV, https://www.gps.gov/governance/agencies/ [https://perma.cc/8FD7-SBSC].

556 *Id.*

557 *See* Exec. Order No. 13905, 85 Fed. Reg. 9359, 9360 (Feb. 12, 2020) (splitting authority further by adding DOC and DOE to the PNT Committee).

558 Mountin, *supra* note 37, at 122.

559 Milner, *supra* note 6.

560 *See id.*

561 *Id.*

562 Larsen, *supra* note 9, at 385.

563 *Id.*

Galileo, as the only entirely civilian system, become GNSS for civilians?[564] The United States, China, India, and other major countries might not wish to be beholden to and captive of the European system, just as the Europeans did not want to become dependent on the U.S. GPS, and therefore built Galileo.[565]

6. Greater Legal Authority to ITU to Resolve Harmful Interference with GNSS

ITU member states could also give ITU legal authority to enforce the Radio Regulations that now govern distribution of radio frequencies.[566] Currently, ITU is without effective legal enforcement power.[567] ITU might receive adequate enforcement oversight authority over radio interferences with assigned frequencies. A strong, enforceable, international agreement to protect the existing systems from all harmful interference would fit into the existing regulation of radionavigation by ITU.[568] This is especially true because ITU, as a principle, only accepts and records radio frequencies that do not cause significant harmless interference in its International Master Frequency Registry.[569] ITU should include adoption of a more refined definition of harmful interference in order to manage the GNSS interference problems.[570] Such authority would require ITU, in cooperation with the individual states, to prohibit and enforce a ban on jamming, spoofing, and other radio interference. This would be a huge change for ITU because the enforcement measures against radio interferences would probably not be solely directed against GNSS interferences. Such a change would not only benefit civilian GNSS; it would also benefit military GNSS.[571] The likelihood of accomplishing such a major change in ITU is not great. It could undermine military authorities' plans to use radio interference as a possible military tactic.[572] Furthermore, ITU is also under obligation to give special consideration to the needs of the developing countries.[573]

---

564 *Id.*

565 *Id.*

566 Mountin, *supra* note 37, at 133–34.

567 *Id.* at 136.

568 *Id.*

569 *Id.*; *see also* ITU Radio Regulations, *supra* note 103, arts. 8.1, 8.3.

570 *Id.* art. 1.169.

571 Mountin, *supra* note 37, at 105. Note that ICAO has limited international authority to enforce air safety. *See supra* Section II.B.3.

572 *Id.* at 107.

573 ITU Constitution, *supra* note 102, art. 44(2).

7. A Ban Only on Military Interference with GNSS

Military authorities in the major space warfighting states are now planning cyber wars that include extensive interference with GNSS signals. Much of present interference can be traced to military authorities.[574] In fact, banning jamming and spoofing could be accomplished by international agreement in the Disarmament Conference.[575] Such an arrangement would leave it to the individual states to resolve criminal and other incidental harmful jamming and spoofing.

8. New International Agreement on Harmful Interference with GNSS

The most effective option would be for all states to enter an international agreement outlawing GNSS interference. All states have a huge investment and interest in unhindered GNSS use.[576] It is in their self-interest to recognize current GNSS vulnerability to interference, but they might also agree to leave the current GNSS undisturbed. The ban would be like the 1963 Nuclear Test Ban Treaty.[577] It would limit or preclude harmful interference with GNSS and it would be enforced by the individual states.

Harmful interference is a deadly threat to the national and international PNT systems. This threat must motivate action. It is in the interest of the entire world to preserve them.

---

[574] Nerijus Adomaitis, Terje Solsvik & William Maclean, *Norway Says It Proved Russian GPS Interference During NATO Exercises*, REUTERS (Mar. 18, 2019), https://www.reuters.com/article/uk-norway-defence-russia-idUKKCN1QZ1VP?edition-redirect=UK [https://perma.cc/WH3L-AM56]; SECURE WORLD FOUND., *supra* note 193, at xvii.

[575] *About Us*, *supra* note 113.

[576] Larsen, *supra* note 9, at 374–75.

[577] Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and Under Water art. 1, Aug. 5, 1963, 16 U.S.T. 1313, 480 U.N.T.S. 47.