Statement Before the

House Armed Services Subcommittee on Strategic Forces
and
House Homeland Security Subcommittee on Emergency Preparedness, Response and Communications

"Threats to Space Assets and Implications for Homeland Security"

Testimony by:

Admiral Thad W. Allen, US Coast Guard (retired)

Former Commandant, US Coast Guard

March 29, 2017

Room 210, House Visitor Center

Chairman Rogers, Chairman Donavon, Ranking Member Cooper, Ranking Member Payne and distinguished members of the Committees, thank you for your invitation to appear today to discuss threats to our space assets and the implications of those threats to our homeland security. The is topic both timely and complex. I am honored to participate in this panel with my distinguished colleagues, General Shelton and Rear Admiral Nimmich. Given the breadth of knowledge represented by these professionals and the areas they intend to discuss I would like to focus my testimony on global navigation satellite systems (GNSS) which include the US Global Positioning System (GPS) and the threats and vulnerabilities associated with the services provided by those systems – positioning, navigation, and timing services or PNT.

For background, it is important to understand at the most basic level what space means to modern society because it is generally underappreciated and taken for granted, like oxygen. Access to space in our lifetimes has created the means for better communications, better knowledge of the earth and its environment, enhanced ability to know both friend and adversary, and connect societies in ways unimaginable just decades ago. It is undebatable we are a connected society and space is the linking and integrating domain that connects us all, not unlike weather. The ability to operate in space requires physical access and persistent presence, including the ability to communicate with and control assets in space. These elements are generally regarded as the space and ground control segments. The benefit and functionality derived from the space segment is generally divided into government or military users and public institutions and the public at large.

At the heart of this access and associated functionalities that both benefit and threaten its user is the ability to observe and transmit information through increasingly sophisticated sensing and communication platforms. Beyond the physical access to space created by human ingenuity, from Sputnik to deep space exploration, what connects us to space and space to us to is the electromagnetic spectrum. From micro wave and radio communications, to ionizing radiation, to light itself the presence and nature of the electromagnetic spectrum allow the transmission of energy and with it information. Accordingly, it is impossible to discuss the threats to space assets and their associated services without a discussion of electromagnetic spectrum as the unifying enabler in this domain.

As noted earlier, the purpose of my testimony today is to focus on the systems of satellites that provide autonomous geospatial positioning information to receiving equipment by line of sight radio frequency transmissions. Specifically, position (including altitude and elevation), movement or navigation, and time. The generic term for these systems is Global Navigation Satellite Systems (GNSS) indicating they have global coverage to provide autonomous geo-spatial positioning, navigation, and timing (PNT). The Global Positioning System (GPS) is the United States GNSS. Other GNSS include the European Union Galileo, Russian GLONASS, and Chinese Beidou systems, as well as other system that provide limited regional coverage in a particular area.

As noted earlier, the United States' GPS is divided into three segments: the space segment, the ground control segment, and the civil user segment. Today I would like to focus on the

relationship between the space segment and the civil user segment and associated vulnerabilities and risks. The US military developed, deployed, and continues to enhance GPS services and, accordingly, General Shelton is imminently qualified to address the remaining portions of the GPS infrastructure.

My testimony today if offered in my personal capacity and I am not representing any government or private sector entity. I would note that I do serve as a member of the Space Based Positioning, Navigation, and Timing Advisory Board (PNTAB) to the GPS Executive Committee, the federal governing body for GPS, that is co-chaired by the Deputy Secretaries of Defense and Transportation.

The GPS system was declared operational in 1993, after an extended period of test, evaluation, and discussion regarding public access to un-degraded GPS services. Since then GPS and GNSS have become ubiquitous in our lives and geolocation and timing services touch every American every day. Combined with advances in computation, miniaturization, access to spectrum, and mobility, GPS devices can be found in almost every electronic component and is the geolocation services backbone for the internet of things. Further, advances in timing technology have allowed GPS timing services, augmented by high performance clocks, to produce measures of time well below the micro second threshold. As a result, GPS is a critical service in ATM operations, the timing of computerized financial transactions, and the synchronization of telecommunications signals and phasing of power generation. Conservative estimates put worldwide GPS users at over 2 billion. Because of its widespread penetration in electronics and other devices the overall value of GPS services is difficult to calculate. Initial forays into estimating this impact have produced estimates from 30 to 90 billion dollars annually and the models continue to be refined. While GPS is not considered critical infrastructure, there is no critical infrastructure that is not dependent on or impacted by GPS, especially “Lifeline Sectors” such as Communications, Energy, and Emergency Services. Homeland Security officials have stated that our adversaries are interested in doing the Nation harm by disrupting GPS signals (Kolasky 2017). Earlier this year Spirent Communications, a leading provider of mobile network services warned of an “likelihood of disruptions this year” to GNSS.

We must keep in mind that GPS was originally designed as a low power, line of sight signal that allowed terrestrial receivers to determine a position on earth. In fact, were it not for the encoding of the signal so that it could located, the signal would be lost in cosmic background noise. The rapid expansion of these services has placed a premium of their value but has also increased the risks associated with a loss or denial of service. The ultimate vulnerability of a weak signal was something not anticipated in the development of GPS but it now a structural part of the service that must be understood and dealt with.

As reported by GPSWORLD.COM in 2014, Stanford Professor Emeritus and an original architect of the US GPS capability opened his presentation at the European Navigation Conference (ENC-GNSS 2014) in Rotterdam, The Netherlands, with the following question, “What can we do to reduce the vulnerability (of GPS) and ensure that the expectations of the public are going to be met?” In 2016, Dr. Parkinson was awarded the Marconi Prize by the Marconi Society

recognizing his contribution in the field of information and communication science which benefit humanity.

Dr. Parkinson's presentation has evolved to become the backbone of the strategy to ensure GPS services by the PNTAB in their recommendations to the GPS EXCOM. The strategy revolves around three lines of effort that are needed to create "assured PNT" for all users: Protect, Toughen, and Augment. These lines of effort address two basic features of reliable GPS: signal availability and integrity. The most critical feature to insure service is "availability." That means the availability of a signal at the specified accuracy of the system. The second critical aspect is "integrity." That means the user receives the expected accuracy and the system is not providing false, incorrect, or inaccurate information.

While the public generally associates positioning, navigation, and timing as GPS-related services, Dr. Parkinson would argue that the goal should be to assure public access to all three in a systemic, redundant, and resilient manner. Accordingly, my remarks today align with that construct. We need assured PNT regardless of the source, space based or terrestrial. Further, we need to understand the services available from the other GNSS and their potential to provide redundancy and assured PNT with the overall goal to be the assured availability and integrity of the information.

"The first prerequisite for GPS-based PNT is a receivable, clear, and truthful (truthful implies full integrity) ranging signal ... the second is satellite geometry ... the user who cannot see enough of the sky."

Dr. Bradford Parkinson, 2014

The second challenge cited above requires a denser constellation and a means to deal with obstructions like urban canyons. Regarding the first, five challenges are presented by Dr. Parkinson:

1. Adjacent spectrum interference: Power signals in adjacent bands to GPS can drown out the signal denying use. In some cases, this is caused by FCC authorized users where the implications of licensing decisions are not understood or issued with insufficient testing.

2. Natural Interference: Phenomena such as solar flares (space weather) can cause signal interference, attenuation, or delays. Progress in tracking these events and improving prediction has been made and the Space Weather Prediction Center has been established by NOAA in Boulder CO.

3. Inadvertent Natural or Manmade Jamming: In these cases nearby devices can create spurious or destructive emissions.

4. Collateral Interference: Many personal privacy devices that are intended to elude geolocation can impact nearby users.

5. Deliberate Jamming or Spoofing: This continues to be a major concern for all developers and users of GNSS.

Protect, Toughen, Augment
(Advocated by Dr. Parkinson and supported by the PNTAB)

Protect the Signal

The first protect element of the PTA strategy to protect the signal and delivery system. This must begin with protection of the spectrum for GNSS operations. Current concerns center on nearby spectrum licensed for broadband use. Satellite based signals are rebroadcast from terrestrial antennas at a much higher power jamming nearby GNSS receivers.

The second protect element is to create a deterrent to illegal jamming by enacting stiff, behavioral influencing penalties in terms of fines and jail sentences. GPS jammers are currently available on the internet. While FCC penalties exist, they are not a credible deterrent and rarely employed.

The third protect element is to control the manufacture and web sale of jammers. The FCC has indicated they are committed to doing this. That commitment needs to be honored.

The fourth protect element is to improve jamming detection. This can involve independent sensors or improvements to firmware and software by manufacturers to create more "competent" receivers.

The fifth protect element is to localize and pinpoint jammers. This technology is advancing and needs to be sustained.

The sixth protect element is to eliminate jammers. We need a committed national effort at the federal, state, and local level to "find and fix" inadvertent or illegal jamming.

The seventh and final protect element is to prosecute offenders. Prosecutorial discretion can be used based on circumstances when warranted but consequences must be equal to the effects cause by illegal intentional jamming.

Toughen Receivers

Advances are being made to toughen or develop more competent receivers. Some techniques can be accommodated in market driven improvements and upgrades. Improve receiver performance should be supported. There are five general options but the goal should be to make these changes/upgrades affordable.

Local antenna shading: The creation of a physical barrier to shield the receiver.

Signal beam steering by antennas: this is an effective but expensive way toughen receivers but creates expense for ordinary users.

Integration of GPS with other navigational tools such as inertial systems

Increased GPS signal power. An option but not likely due to the expense.

Physical separation of the GPS signals to allow more effective, discrete processing.

Augment the Signal

This element of PTA focuses on augmenting or substituting PNT sources to increase redundancy. The first source can be exploiting existing GNSS with all-GNSS receivers that diversify frequencies and signals, thereby reducing vulnerabilities. This approach also addresses the needs of sky impaired users. However, this approach will require international cooperation similar to that historically achieved by the International Maritime Organization (IMO) or the FAA and International Civil Aviation Organization (ICAO) in their domains. International GNSS governance remains a work in progress. Regardless, there is merit to pursuing this course of action with three objectives related to GNSS integrity: compatibility, interoperability, and interchangeable systems. Standards for integrity monitoring need to be developed and implemented.

Receivers can also conduct integrity monitoring if enough satellites are in view. Standardization among GNSS (interchangeability) would enhance this option greatly. Other sources of augmentation and improved signal integrity include:

Global Differential GPS (GDGPS): This NASA administered real time tracking network provides integrity tracking and the ability to augment the signal for improved performance.

Pseudolites: or Pseudo-Satellites. These are ground based transceivers that could provide additional ranging information. However, the coverage is limited and may involve frequency interference with GNSS.

Distance Measuring Equipment (DME): This modernized FAA system supplements GPS for airborne users. However, ground users are limited by line of sight.

eLORAN: This terrestrial system uses a low frequency powerful signal and presents an attractive relatively low cost alternative to assured PTA and is widely supported.

Summary

This testimony regarding the vulnerability of GPS/PNT and the PTA strategy for assuring service is a condensation of extensive work done by others: government, industry, and the PNTAB. My

goal has been to summarize the key issues and I do not represent myself as having the technical solutions to all the issues and options raised. I have, however, been involved in operational issues related to radio navigation my entire career, including a tour as Commanding Officer LORAN Station Lampang, Thailand at the close of the war in Viet Nam. From that vantage point I have two closing comments.

As Commandant, I watched as OMB removed Coast Guard funding in 2009 for modernizing LORAN C and potentially developing eLORAN consistent with domestic and international commitments to seek alternatives to back up GPS. With a new DHS Secretary and new administration there was little appetite in 2009 to appeal this arbitrary reduction made under the guise of "cost savings." We are now eight years later poised to reconsider the development of an eLORAN system to support assured PNT. We should make up our minds and finish the job.

At the same time, the overall governance of the US GPS continues under the Executive Committee governance model. Issues regarding adjacent spectrum interference are difficult to address with overlapping roles and responsibilities between the federal agencies and independent regulatory agencies such as the FCC. Spectrum allocation, management, and governance continue to be critical to protecting the GPS signal. As stated in their June 13, 2016 letter to the GPS EXCOM the PNTAB objected use of adjacent spectrum to GPS for wireless terrestrial broadband without testing that satisfactorily meets 6 criteria:

1. Adhere to previous EXCOM guidance to ensure new spectrum proposals "are implemented without affecting existing and evolving uses of space-based PNT services"

2. Strictly apply the 1dB degradation Interference Protection Criterion (IPC)

3. Protect all classes of GPS receivers, including precision and timing receivers.

4. Protect GPS receivers in all receiver operating modes, including signal acquisition/reacquisition

5. Protect all users of all emerging GNSS signals.

6. Use maximum authorized transmitted interference powers and propagation models that do not underrepresent the maximum power of the interfering signal (particularly consider the impact of the multiple transmitters creating additive interference).

The PNTAB further endorsed "the Department of Transportation Adjacent Band Compatibility assessment as the most scientific valid approach to date for Protecting space-based PNT based on the above criteria."

Finally, any infrastructure investment program developed to address the current challenges facing this country, regardless of political origin, should require assured PNT and the associated resiliency as a basic design parameter

My recommendation is that these committees also endorse this extensive work done to date to protect GPS and assure PNT to civil users.

Thank you for the opportunity to testify before this joint hearing today and I look forward to your questions.