HARVARD Kennedy School
BELFER CENTER

HOMELAND SECURITY POLICY PAPER #3

The City-Sized Hole in U.S. GPS Planning

Steven Polunsky*

Executive Summary

Our society has become highly dependent on constant, real-time information about position, navigation, and timing. We typically access this information through cell phones or other devices that receive global positioning system (GPS) signals. Cities are particularly vulnerable to GPS failures and will become more so as Smart City initiatives produce results. Yet, we are missing opportunities to protect localities from potential disaster. This paper recommends efforts at all levels of government that could improve local government resilience, coordinate efforts, involve the private sector, and integrate these initiatives with federal planning for the future.

Background

Do you have a paper map in your vehicle? Fewer and fewer people do. At least one state, Ohio, has reduced its highway map production by almost 60 percent since the mid-1990s.[1] Now we rely on getting information about where we are and where we are going from the taxpayer-funded global positioning system (GPS), a critical function of the U.S. government,[2] meaning "functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[3] The importance of GPS cannot be overstated: of the 16 infrastructure sectors identified by the U.S. Department of Homeland Security (DHS) as being critical, all but three require GPS for essential functions. What is your plan for when the signals stop, or worse, intentionally mislead you?

What we casually refer to as GPS began when scientists reverse-engineered Sputnik's trajectory[4] and today involves more than 30 satellites simultaneously beaming signals to earth (this is the American Global Navigation Satellite System (GNSS); there are others). A consumer does not need a license or a particular brand of radio or phone to receive and use the signals. Not too long ago, GPS receivers were purchased as freestanding units; now the function is built into smartphones. Freestanding units are still manufactured and sold, but they have diminished in popularity since 2011 when for the first time more people subscribed to the Waze app (crowdsourced traffic information overlaid on a GPS map) than purchased GPS devices. There are now about seven GPS receivers for every ten people on Earth.[5] Uses are getting more creative, from traffic condition crowdsourcing (Waze) to augmented reality (Pokémon Go) to being introduced as evidence in cases where bicyclists with fitness apps can prove they were hit by a car by showing a record of sudden, rapid acceleration in an unexpected direction.[6]

* **Steven Polunsky** (polunsky@ua.edu) has conducted and managed policy research in transportation, homeland security, and business/commerce for legislative, agency, academic, and policy making audiences. Polunsky is the Director of the Transportation Policy Research Center at the University of Alabama. He researched much of this paper during his time as a Founding Scholar in the HSx Program at the Center for Homeland Defense and Security, Naval Postgraduate School.

Travelers are not the only ones using GPS for position and navigation. GPS has been guiding tractors and agricultural machinery since the 1980s, and manufacturers have introduced self-driving tractors into the market.[7] The Virginia Department of Transportation saved $15 million and weeks of construction time on an interstate widening project by using GPS equipped bulldozers.[8] All New York City public school buses—some 10,000—will be tracked by GPS in 2020.[9] 911 services rely on it. Scientists use GPS to track animal migration patterns and detect earthquakes. Football teams are even using GPS to analyze athletes' speed and performance.[10] GPS is not the only tool available for location and navigation, but it is by far the predominant one—over 90 percent of context-aware apps rely on it.[11]

The value of GPS goes far beyond location-based services. The GPS signal includes time information that is accurate within 100 billionths of a second.[12] This aspect is used in industries where synchronizing stations is important, like wireless telephone and data networks, digital broadcast radio, and electric power grids. It is also used where time-stamped transactions are critical, such as retail businesses, where more than 80 percent of transactions involve credit or debit cards,[13] and financial markets, where multiple traders are simultaneously seeking to buy or sell stock and the exact time of a trade can have tremendous financial consequences (which is why federal rules require trader clocks to be synchronized within 50 milliseconds or 0.05 of a second).[14]

Research sponsored by the National Institute of Standards and Technology estimates that GPS has generated around $1.4 trillion in economic benefit in the United States—most of that in the last 10 years—and that a 30-day GPS outage would have an economic impact of $1 billion per day.[15] The U.S. Department of Defense's Defense Advanced Research Projects Agency determined that, within thirty seconds of a catastrophic GPS shutdown, a position reading would have a margin of error the size of Washington, D.C. After an hour, it would be Montana-sized.[16]

Occasionally, something goes awry. A New Jersey construction company employee, knowing his fleet vehicle was being GPS tracked but not wanting to reveal how long or where he took lunch, bought an inexpensive jamming device that he plugged into his pickup's power outlet and promptly took out a ground navigation system at Newark Liberty International Airport.[17] The cruise liner Royal Majesty ran aground after a loose GPS cable kicked off a series of errors.[18]

In January 2016, the process of decommissioning a GPS satellite caused a 13 microsecond (13 millionths of a second) error, which triggered 12 hours of timing equipment disruptions around the world, especially affecting telecom companies across England.[19] It disrupted commercial digital radio stations like the BBC for two days and threw some GPS systems off by as much as 3 miles.[20] In parts of the United States and Canada, police, fire, and emergency medical services (EMS) radio equipment stopped functioning.[21]

Of course, the military uses GPS as well, and it is vulnerable to GPS disruption. Uniformed services rely on GPS for monitoring troop movements and directing aircraft including unmanned aerial systems (UAS or drones). The military regularly experiences jamming (preventing the signal from reaching the receiver) and spoofing (sending a false signal to the receiver so the real one is ignored or rejected) in what are referred to as GPS-denied environments. In 2011, Iran brought down an American drone by redirecting its GPS system.[22] While Iran has used GPS attacks in other instances,[23] there are no reported repeats of the drone spoofing, suggesting our military expects and is prepared for malicious attacks of this nature. Protection for the civilian sector lags behind; a 2013 U.S. Government Accountability Office (GAO) report found shortcomings with DHS' GPS risk assessment and measurement of mitigation effectiveness as well as a lack of collaboration between DHS and the U.S. Department of Transportation (USDOT).[24]

Unfortunately, GPS attacks are becoming more common and are moving from the military space into the civilian arena as technology becomes more widely and cheaply available. Instructions for GPS attacks can be found on YouTube. Five years ago, a spoofing attack would have required expensive equipment costing $50,000 or more. Today, a user can launch an entry-level attack for $100.[25]

In the meantime, terrorists, adversarial and rogue nation-states, and those who would do us harm are taking battlefield technology and turning it on civilians.[26] Consider the following:

- North Korea jammed South Korea's GPS for 16 days in 2012[27] and again in 2016, disrupting airplanes, ships, and buoys out 100 nautical miles.[28] The capitol city of Seoul appeared to be the target. No injuries were reported.[29] Between 2010 and 2012, more than 1,000 airplanes and 250 ships experienced GPS errors attributable to North Korea's jamming.[30]

- In one 2017 incident, the GPS receivers for about 20 commercial ships near the Russian Black Sea port of Novorossyisk suddenly showed them at the Gelendyhik airport at Sochi, some 20 nautical miles away. Observers believe that Russia was behind the spoof[31] and that the intent was not to affect the ships but to deter any drones potentially launched from those ships.[32]

- Drug cartels on Ameica's southern border are using spoofing and jamming to prevent U.S. law enforcement from using drones to map drug and human smuggling routes.[33]

- As of August 2019, the Eastern Mediterranean Sea is under a GPS Interference Advisory issued by the U.S. Maritime Administration.[34]

Known targets include two recent technologies that are expected to proliferate in urban areas: drones and self-driving cars. Drones have rapidly become popular for civilian and commercial uses, including automated crop fertilization, livestock monitoring, traffic incident management, surveying, and transporting cargo and people. Thirty-four state transportation departments use drones, with 25 incorporating them into daily operations.[35] GPS is the predominant wayfinding method, although others are used. A recent Hong Kong incident shows the vulnerability: Malicious interference with GPS signals to drones in a synchronized nighttime light show caused more than 40 to crash resulting resulting in over $1 million HK ($128,000 US) in damage.[36]

Research shows that cell phone and auto navigation systems can be misdirected. Some autos can have functional control taken away, with possible outcomes including taking wrong exits, aggressive braking, steering, or acceleration, even the height of a car's suspension being changed while driving.[37] Automakers are working to stay ahead of the curve: in February 2019 Tesla patented a positioning system for its autonomous cars that relies on information from adjacent vehicles, roadside appurtenances, and onboard maps.[38] However, in June 2019 researchers working under very controlled conditions used GPS to steer two different Tesla models off course.[39] Terrorists are already exploring ways to turn autonomous vehicles into weapons.[40]

Analysis

Cities across the country are becoming "smart" by collecting, communicating, and analyzing data related to traditional local government functions, including street maintenance and operation, garbage and recycling services, and public transit. By collecting data, a city can report on weather, traffic and road conditions to allow real-time signal and routing adjustment and condition prediction; update transit riders with bus locations; and detect environmental hazards. The goal is to have universal, interoperable connectivity.[41] When the USDOT opened a Smart City Challenge, they received 78 applications, including such GPS-based uses as dynamic routing for truck traffic (Seattle), "radically programmable" city streets that can change from loading zones to thoroughfares (Boston), dynamically routed on-demand minibuses (New Orleans), and connected autonomous shuttles (Las Vegas).[42] Columbus, Ohio, won the challenge by proposing an integrated data platform including connected infrastructure and autonomous vehicles.[43] Smart Cities initiatives are forecast to drive $189 billion in spending globally in 2023, with priorities being resilient energy and infrastructure projects, data driven public safety, and intelligent transportation.[44]

As consumers track their Uber rides with GPS[45] and bicycle owners find their stolen bikes using GPS devices hidden in the handlebars,[46] cities are using the technology to connect, integrate, and adjust their traffic signals, with the goal of reducing traffic congestion and reducing greenhouse gas emissions.[47] The move toward self-driving cars only increases the critical nature of GPS.[48] Cities are in a unique position to set standards or requirements regarding position, navigation, and timing technologies, methodologies, and redundancies.

Given society's reliance on GPS, its unusual position as a many-faceted single point of failure, and the recent comparison of modern GPS receivers to radios from the 1960s in that "you tell it something, it believes it, it doesn't check,"[49] vulnerabilities in the system pose a growing and potentially serious threat to America's economy and security. What is being done to address those shortcomings?

- The private sector is responding with an array of products designed to detect GPS attacks, augment GNSS signals, and provide substitutes for GPS. DHS contracted the MITRE Corporation to operate the Homeland Security Systems Engineering and Development Institute to provide technical and engineering expertise. However, their reports are not generally available outside of DHS,[50] and they cannot recommend products because that would be perceived as government favoring one vendor over another. There currently is no clearinghouse to assist local governments in differentiating among these products, and with many products to choose from addressing a variety of GPS-related attacks (availability, integrity, incidental, targeted) along the entire hardware and software spectrum from antennas to cybersecurity aimed at different steps in the process (prevention, detection, reporting, mitigation, recovery), it is difficult for system operators to know what to purchase.[51] A proliferation of products without a requirement for standardization or minimal levels of security, while possibly beneficial for redundancy and a layered protection approach, increase the difficulty of maintaining interoperability among different users and creates disparities across systems (chains with weak links/single points of failure).

- GPS III satellites are going into orbit, with greater signal power than those they replace and other features.

- Foreign governments are implementing their own GNSS and regional augmentation systems[52] and allowing other nations to use their signals. FCC approval for civilian use for such systems[53] makes interoperable/ redundant/ backup

signals available to U.S. consumers, increasing the accuracy and reducing potential downtime. Reduced foreign reliance on our satellites also means less interest from other countries in maintaining/ defending the U.S. system. It also has the potential to introduce mischief into the signal system.

- The U.S. Navy has reinstated training in celestial navigation[54] but the Army has moved land navigation training from basic combat training to later training.[55]

DHS provides resources to state, local, tribal, and territorial governments through its US-CERT program, which is focused on cybersecurity generally,[56] and through its state, local, tribal, and territorial program. Research for this paper discovered no public evidence of DHS communication with local governments regarding GPS; in fact, their web page on GPS has not been updated since before April 2017.[57] USDOT's plan for autonomous vehicles assumes GPS.[58] Their method for addressing local government needs is to work through the Federal Highway Administration's connections with state departments of transportation.[59]

Spurred by Congress, the federal government is taking steps to modernize and address the future of GPS. On December 4, 2018, President Trump signed the Frank LoBiondo U.S. Coast Guard Authorization Act of 2018, which included the National Timing Resilience and Security Act of 2018.[60] The act tasks the Secretary of Transportation with establishing a terrestrial backup timing system for GPS within two years. USDOT received 22 responses to a request for information regarding GPS backup technologies and intends to move some to demonstration testing and ultimately create the backup system for civilian use, which currently is unfunded.[61]

Unfortunately, there are some shortcomings in this approach, a major one being that our cities have not been at the table as policy has been developed. With the push toward Smart Cities by 2/3 of American cities[62] and an increasing reliance on technology, cities have perhaps the most to lose by a GPS failure.

Created in 2004 by National Security Presidential Directive 39,[63] the National Executive Committee for Space-Based Positioning, Navigation, and Timing guides the federal government's GPS efforts and is assisted by a National Advisory Board.[64] There are no local government representatives on the Executive Committee[65] or the Advisory Board.[66] Local governments may participate in a Civil GPS Service Interface Committee (CGSIC), the "recognized worldwide forum for effective interaction between all civil GPS users and the U.S. GPS authorities."[67] CGSIC had a subcommittee for state and local governments that was retired in 2015, its duties being rolled into the Surveying, Mapping, and Geo-Sciences Subcommittee as the subject matter discussed in the subcommittee was "typically relating to use of differential reference stations."[68] No one representing a city or county attended the most recent meeting.[69]

The U.S. government needs to focus its efforts on preparing for the inevitable attacks and disruptions to GPS with an emphasis on involving those stakeholders like local governments that would be severely affected. Local governments also bear responsibility for implementing current best practices and anticipating the coming technological advances and threats.

Recommendations

Recommendation 1: Congress should mandate formation of a national commission to review GPS vulnerabilities and recommend measures for all levels of government and the private sector to improve resiliency.

All levels of government, including local governments, and the civilian/private sectors are rapidly expanding their reliance on GPS, but the extent to which they are preparing for loss singly or collectively is unknown as is the extent to which those preparations are being taken into account in federal, non-military planning.

Given the extent of reliance on GPS and the potential consequences of failures in the system (or as a result of attacks on it), Congress should constitute a National Commission on Position, Navigation, and Timing (NC-PNT). Similar to the National Commission on Military, National, and Public Service,[70] for example, the NC-PNT would be a nonpartisan, military-public-private-civilian body charged with considering methods to improve the nation's GPS system and resiliency in an integrated fashion. The NC-PNT would hold hearings on GPS resilience at all levels, receive input from the public, and advise Congress on addressing GPS-related risks.

Among the issues the Commission would consider are strengthening the federal regulatory framework and incentivizing the private sector to address these issues. In addition to uses noted above, the Internet of Things (IoT) is bringing us GPS-enabled appliances and other innovations beyond our current imagination. New devices should be made with a backup or redundant system that anticipates and accommodates or rejects failure as well as feeding data to artificial intelligence implementations that can fill data gaps and provide predictive services.[71] Systems should be designed to recognize nodal failure and route around or recover. Testing requirements and metrics should be established for products with safety implications such as self-driving vehicles.

Standards can be developed and administered in much the same way as we have seen in the autonomous vehicle industry. An industry association with standing should take the lead on creating a universal syntax and approach, similar to what the Society of Automotive Engineers has done for autonomous vehicles. A federal agency could then emulate the National Highway Traffic Safety Administration's approach in this area.

Further, at the present, the private sector seems primarily focused on military uses of GPS, which is understandable given defense spending levels and the military's interest in technology in this area. However, the Smart City movement is expected to continue growing, which means opportunities for private sector participation should expand. These should be attractive markets for private sector solutions to problems local governments face resulting from GPS reliance. Efforts are needed to encourage the acceleration of local government-oriented solutions, and the federal government should consider policy options such as tax credits and grant programs to support such a shift.

Recommendation 2: Congress should accelerate and fully fund GPS research and development.

Congress appropriated $10 million in the FY 2018 National Defense Authorization Act to carry out the GPS backup demonstration scheduled for late 2018, a full year after 13 technologies were demonstrated in a private sector challenge.[72] Steps beyond the federal demonstration, including system development, test, launch, and operation, are not currently funded. Pending the report of the national commission, Congress should continue to fund GPS-related research to mitigate current security gaps and improve the state of understanding around this technology.

Recommendation 3: The White House should revise National Security Presidential Directive 39 to mandate inclusion of a representative of local government on the Advisory Board to the National Executive Committee for Space-Based PNT.

The Executive Branch can take near-term actions to improve planning around GPS resiliency. Failure to include all relevant levels of government in these efforts creates additional vulnerabilities. Local governments should be integrated into national level planning for GPS. The appropriate committees or advisory boards should be created or expanded to integrate substantive input from local governments at both the policy and technical levels.

The timing for this action is appropriate as NSPD-39 is currently being updated.[73] USDOT should reconstitute the U.S. State and Local Government Subcommittee of the Civil GPS Service Interface Committee and reach out to information technology, operations technology, information security officers, and innovation officers at all levels of government.

Recommendation 4: State and local governments should independently organize and coordinate to identify and mitigate risks associated with their increased use and reliance on GPS.

Local governments should not wait passively for action at the federal level. Instead, local governments should take the initiative to recognize the threats from reliance on GPS and the need for resilience. Such includes efforts to build coordination structures among themselves and to act independently to address GPS-related risk and improve resiliency.

Through national associations, regional multi-government pacts, and sister city arrangements, local government technology expenditures (procurement) should ensure that efforts do not have the unintended consequence of preventing an expanded scale, compatibility, or interoperability with neighboring jurisdictions. Experiments, pilot projects, and testbeds should be used with thought toward how the results can be widely disseminated and, if positive, replicated with an eye toward prudent use of tax dollars. While needs vary from city to city, information sharing and combined efforts should improve the potential for effective responses. Local governments should create an overarching coordinating mechanism, potentially leveraging current institutions such as the United States Conference of Mayors and/ or the National League of Cities.

Among the specific actions local governments should take is to examine their own GPS-dependent systems and local GPS-reliant and consumer-facing networks, evaluate their vulnerabilities and consequences of failure, identify potential mitigative measures and establish their own methods for maintaining necessary services in the event GPS becomes unavailable. They should set priorities for systems to be addressed based on risk assessment (potential for compromise and economic or social cost of consequences) and identify appropriate redundant measures or countermeasures. A solution could involve using cities as testbeds for GPS alternatives and augmentations as well as improving local resilience through GPS generators similar to the

standby electric generators now commonly found in homes, businesses, hospitals and other structures. A variety of existing methods are available, for example maintaining their own atomic clock sources like the financial services sector does; broad-area mesh coverage via amateur radio; and putting up signs for analog wayfinding. It may also be time for re-evaluating the regulatory relationship between cities and telecommunications companies with an eye toward these companies' abilities to use ground and cloud-based services as backup measures.

Local governments also should include GPS enabled products in cybersecurity practices and continuity of operations plans and require the same from their vendors. Governments should at the least seek to comply with the current GPS interface specifications and incorporate DHS best practices.[74] Maintaining current GPS standards and practices would have avoided the April 6, 2019, incident where New York City's wireless network went down, temporarily disabling 38 police department license plate readers and taking down 12,389 traffic signal controllers although the signals continued to operate normally.[75]

Endnotes

1 Julie Carr Smith, "State Mapmaker Brings Creativity, Whimsy to Ohio Road Maps," *Associated Press*, July 2, 2019.

2 Brian E. Humphreys, *Critical Infrastructure: Emerging Trends and Policy Considerations for Congress*, CRS Report R45809 (Washington, DC: Library of Congress, Congressional Research Service, July 8, 2019).

3 "National Critical Functions Set," Cybersecurity & Infrastructure Security Agency, April 2019, https://www.dhs.gov/sites/default/files/publications/national-critical-functions-set-508.pdf .

4 Steven Johnson, "Where Good Ideas Come From," *TEDGlobal 2010*, July 2010, https://www.ted.com/talks/steven_johnson_where_good_ideas_come_from.

5 Greg Milner, "What would happen if GPS failed?," *New Yorker,* May 6, 2016.

6 John Markoff, "Bike crash wiped details; GPS data filled them in," *New York Times*, September 5, 2011.

7 "Autonomous Tractors -- The Future of Farming?" Big Ag, January 18, 2018, http://www.bigag.com/topics/equipment/autonomous-tractors-future-farming/.

8 SaraRose Martin, "GPS Equipped Bulldozers Help I-64 Expansion," *The Virginia Gazette*, June 21, 2019.

9 "Seen & Heard," *GPS World,* September 2019, 50.

10 Shannon Ryan, "Illinois Joins a Growing Number of Football Programs that use GPS Technology for 'Smarter' Practices. But For Some Players, It's All About Speed," *Chicago Tribune*, April 20, 2019.

11 Yoav Zangvil, "Research on GPS Resiliency and Spoofing Mitigation Techniques Across Applications," 4, last visited June 6, 2019, https://www.gps.gov/governance/advisory/meetings/2019-06/zangvil.pdf.

12 "Timing," GPS.gov, last visited August 3, 2019, https://www.gps.gov/applications/timing/.

13 "50 Uses or Applications of GIS," Grind GIS, August 1, 2018, https://grindgis.com/gps/50-uses-or-applications-of-gps.

14 Michael A. Lombardi et al., "Accurate, traceable, and verifiable time synchronization for world financial markets," *Journal of Research of the National Institute of Standards and Technology* 121 (2016), 441.

15 Alan C. O'Connor et al., *Economic Benefits of The Global Positioning System (GPS),* RTI Report No. 0215471 (Research Triangle Park, NC: RTI International, June 2019), 14-1.

16 Milner, "What would happen if GPS failed?"

17 Iain Thompson, "Feds arrest rogue trucker after GPS jamming borks New Jersey airport test." *The Register*, August 12, 2013.

18 Bob Couttie, "The Case of the Wandering Monarch," *Maritime Accident Casebook*, last visited August 3, 2019, http://maritimeaccident.org/library2/the-case-of-the-wandering-monarch/.

19 Chris Baraniuk, "GPS error caused 12 hours of problems for companies," *BBC*, February 4, 2016.

20 Chris Baraniuk, "UK radio disturbance caused by satellite network bug," *BBC*, February 2, 2016.

21 Dan Glass, "What Happens if GPS Fails?" *The Atlantic*, June 13, 2016.

22 David Cenciotti, "Captured U.S. Stealthy Drone was Hijacked Exploiting GPS Vulnerability. But Hack Description Does Not Solve the Mystery," *The Aviationist*, December 15, 2011.

23 Lukas Mikelionis, "Iran using GPS Jammers, Pretend to be American Warships to Trick Vessels, US Says," *Fox News,* August 8, 2019.

24 "GPS Disruptions: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced," GAO Report 14-15 (Washington, DC: U.S. Government Accountability Office, November 2013.

25 Zangvil, "Research on GPS Resiliency and Spoofing Mitigation Techniques Across Applications," 6.

26 "Summary of Terrorism Threat to the U.S. Homeland," U.S. Department of Homeland Security, National Terrorism Advisory System, July 18, 2019.

27 Sebastian Anthony, "Our terrifying reliance on GPS, and the need to develop a ground-based alternative," *Extreme Tech*, November 7, 2014.

28 "State Department Issues Notice on North Korean Jamming," *GPS World*, April 8, 2016.

29 "South Korea issues warning over suspected North Korean GPS disruption," *GPS World,* March 31, 2016.

30 PierLuigi Paganini. "British navigation tech 'eLoran' is under examination of US military to thwart GPS jamming," *Security Affairs*, May 27, 2015.

31 Dana Goward, "Mass GPS Spoofing Attack in Black Sea?" *Maritime Executive,* July 11, 2017.

32 Diana Furchtgott-Roth, Deputy Assistant Secretary, Office of the Assistant Secretary for Research and Technology, U.S. Department of Transportation, speech to the Civil GPS Service Interface Committee Annual Meeting, Miami, Florida, September 17, 2019.

33 Patrick Tucker, "DHS: Drug Traffickers are Spoofing Border Drones." *Defense One*, December 17, 2015.

34 "2019-005-Eastern Mediterranean and Red Seas-GPS Interference," MCSI Advisory, U.S. Department of Transportation Maritime Administration, May 2, 2019.

35 Joanne Costin, "Infrastructure," *Inside Unmanned Systems,* April/May 2019, 15.

36 "Criminal Investigation Underway in GPS Jamming Incident that Crashed Drones, Caused KH$1M in Damage," *Inside GNSS*, October 31, 2018.

37 Zangvil, "Research on GPS Resiliency and Spoofing Mitigation Techniques Across Applications."

38 "Tesla Granted US Patent for Positioning Tech," *GPS World*, February 6, 2019.

39 "Tesla Model S and Model 3 Prove Vulnerable to GPS Spoofing Attacks as Autopilot Navigation Steers Car Off Road, Research from Regulus Cyber Shows," *PRNewswire*, June 19, 2019. But see Jim Salter, "Claims of Tesla Hack Wide of the Mark – We Dig Into GNSS Hacking," *ARSTechnica*, June 22, 2019.

40 Javed Ali, "Opinion: Collaboration key to preventing autonomous vehicle terror," *Detroit News*, July 21, 2019.

41 "Smart Cities Readiness Guide: The Definition of a Smart City," Smart Cities Council, last visited July 23, 2019, https://rg.smartcitiescouncil.com/readiness-guide/article/definition-definition-smart-city.

42 "Smart City Challenge," U.S. Department of Transportation, June 29, 2017, https://www.transportation.gov/smartcity/.

43 "The Winner: Columbus, Ohio," U.S. Department of Transportation, January 3, 2017, https://www.transportation.gov/smartcity/winner.

44 Serena Da Rold and Michael Shirer, "Smart Cities Initiatives Forecast to Drive $189 Billion in Spending in 2023, According to a New Smart Cities Spending Guide from IDC," IDC, June 25, 2019, https://www.idc.com/getdoc.jsp?containerId=prUS45303119.

45 Daniel Matthews, "GPS is huge for business, the Internet of Things – and for Surveillance," Netrightdaily, last visited August 25, 2019, http://netrightdaily.com/2016/02/gps-is-huge-for-business-the-internet-of-things-and-for-surveillance/ .

46 Nathan Sykes, "What does the Coming of the Internet of Things (IoT) Mean for the future of GPS?" *Anthill Magazine*, February 23, 2018.

47 Ryan Citron, "Advanced Traffic Management is the Next Big Thing for Smart Cities," GreenBiz, last visited August 25, 2019, https://www.greenbiz.com/article/advanced-traffic-management-next-big-thing-smart-cities .

48 Michelle Krause, "For Self-Driving Vehicles, Accuracy in GPS Mapping is Crucial," Accenture, last visited August 25, 2019, https://insuranceblog.accenture.com/for-self-driving-vehicles-accuracy-in-gps-mapping-is-crucial .

49 Harold "Stormy" Martin, Director, National Coordination Office for Space-Based Positioning, Navigation, and Timing, Speech to Civil GPS Service Interface Committee Annual Meeting, Miami, Florida, September 17, 2019.

50 "Homeland Security Systems Engineering and Development Institute," DHS Science and Technology Directorate, September 17, 2018, https://www.dhs.gov/sites/default/files/publications/FFRDC_HSSEDI_FactSheet_v2_edito9172018.pdf

51 Arthur Scholz, "Resilient PNT for the Civilian Sector," MITRE Corp, presentation to the 59th Meeting of the Civil GPS Service Interface Committee (CGSIC), Monday, September 16, 2019, https://www.gps.gov/cgsic/meetings/2019/scholz.pdf .

52 George Frousiakis, "The Business Advantages of a Multi GNSS Setup," *Telit*, March 6, 2018, https://www.telit.com/blog/multi-gnss-business-advantages/ .

53 Neil Grace, "FCC Approves Use of Galileo Global Navigation Satellite System in the United States," Federal Communications Commission News, November 15, 2018, https://docs.fcc.gov/public/attachments/DOC-355098A1.pdf .

54 Tim Prudente, "Naval Academy Reinstates Celestial Navigation," *Military Times*, November 1, 2015.

55 Matthew Cox, "Low Recruit Discipline Prompts Army to Redesign Basic Training," *Military.com*, February 9, 2018.

56 "Resources for State, Local, Tribal, and Territorial (SLTT) Governments," Cybersecurity and Infrastructure Security Agency, accessed September 2019, https://www.us-cert.gov/resources/sltt.

57 "Global Positioning System (GPS) Program," DHS Science and Technology Directorate, accessed September 21, 2019, https://www.dhs.gov/science-and-technology/gps-program.

58 "Preparing for the Future of Transportation: Automated Vehicles 3.0." U.S. Department of Transportation, December 3, 2018, 60, https://www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

59 Karen Van Dyke, Director, PNT and Spectrum Management, U.S. Department of Transportation, Chair, CGSIC, Civil GPS Service Interface Committee Annual Meeting, Miami, Florida, September 17, 2019.

60 Pub L. 115-282.

61 Dana Goward, "US DOT Moves Aggressively on GPS Backup, RFP This Month," *GPS World,* September 4, 2019.

62 Teena Maddox, "66% of US Cities Are Investing in Smart City Technology," *TechRepublic*, November 6, 2017.

63 The White House, "NSPD-39: U.S. Space-Based Position, Navigation and Timing Policy Fact Sheet," December 8, 2004, available at https://fas.org/irp/offdocs/nspd/nspd-39.htm.

64 "Space-Based Positioning Navigation & Timing: National Executive Committee," National Coordination Office for Space-Based Positioning, Navigation, and Timing, last visited March 7, 2019, https://www.gps.gov/governance/excom/.

65 "Charter, National Space-Based Positioning, Navigation, and Timing Executive Committee," Secretaries of Defense and Transportation, National Coordination Office for Space-Based Positioning, Navigation, and Timing, last visited June 19, 2019, https://www.gps.gov/governance/excom//charter/.

66 "Space-Based Positioning Navigation & Timing: National Advisory Board Membership, 2019-2021," National Coordination Office for Space-Based Positioning, Navigation, and Timing, last visited June 19, 2019, https://www.gps.gov/governance/advisory/members/.

67 "Civil GPS Service Interface Committee," National Coordination Office for Space-Based Positioning, Navigation, and Timing, last visited June 19, 2019, https://www.gps.gov/cgsic/.

68 "Civil GPS Service Interface Committee: U.S. State & Local Government Subcommittee," National Coordination Office for Space-Based Positioning, Navigation, and Timing, last visited June 19, 2019, https://www.gps.gov/cgsic/states/ .

69 Conversation with conference staff, September 17, 2019

70 For information regarding the Commission, please see its website at https://www.inspire2serve.gov/.

71 Laña, Ibai et al., "On the imputation of missing data for road traffic forecasting: New insights and novel techniques," *Transportation Research Part C: Emerging Technologies* 90 (May 2018), 18-33.

72 "The 2018 Combating Terrorism Technology Startup Challenge," U.S. Department of Defense (CTTSO), the Israel Ministry of Defense (MAFAT), and the MIT Enterprise Forum of Israel, accessed September 2019, https://cttsc-x.com/.

73 Harold Martin, Director, National Coordination Office for Space-Based Positioning, Navigation, and Timing, Speech to Civil GPS Service Interface Committee Annual Meeting, Miami, Florida, September 17, 2019.

74 "Improving the Operation and Development of Global Positioning System Equipment Used by Critical Infrastructure," U.S. Department of Homeland Security, January 2017, https://www.us-cert.gov/sites/default/files/documents/Improving_the_Operation_and_Development_of_Global_Positioning_System_%28GPS%29_Equipment_Used_by_Critical_Infrastructure_S508C.pdf.

75 William Neuman, "New York City Has a Y2K-Like Problem, And It Doesn't Want You to Know About It," *New York Times,* April 10, 2019.