Will GPS Jammers Proliferate in the Smart City?

Tegg Westbrook*

ABSTRACT

The Smart City will rely extensively on consented and unconsented information about people's location and movements in order to fulfil its many ambitions. Utilising the Global Positioning System (GPS) is necessary and practical for Smart City agendas, as it provides time and positioning information which is essential for tracking systems. Nevertheless, the emergence of GPS-enabled tracking technologies over recent decades has spurred an increase in the use of GPS jamming devices (or Personal Privacy Devices (PPDs)). This article therefore argues that the normalisation of tracking in the Smart City may lead to the wider ownership of GPS jammers. To overcome this, the article explores the ways in which jammer proliferation can be overcome or avoided entirely taking examples of military, security, and civilian counter-jamming technologies and strategies.

Keywords: Smart City, GPS, jammers, privacy, counter-technologies, tracking.

INTRODUCTION

Structure of the Article

The article begins by outlining what the "Smart City" is and why the Global Positioning System (GPS) is important for meeting its overriding agendas. It then provides a short chronology of the development of GPS and jamming technologies and identifies why jamming may become more prevalent in the Smart City. The next subsection provides an overview of literature relating to GPS jamming and identifies current gaps in our understanding, particularly about how higher

*Corresponding author: teggwestbrook@gmail.com

levels of tracking may lead to the proliferation of jammers. The findings section summarises the set themes relating to the proliferation of jamming devices based on an extensive review of media and literature. These themes are: globalisation and conflict; privacy concerns and other socio-technical forces; skewed and misleading marketing; and low risk, high reward criminality. Corresponding sections seek to identify causation between the present situation and the assumed increase in tracking in the Smart City by identifying ventures that pose risks of jamming due to their requirement of location, navigation and tracking information. It also explores the potential scale of interference based on known end-users and known ranges of jammers. The article offers possible counter-measures and alternative technologies, either built-in or as alternative navigation aids. Overall, the article concludes that privacy concerns must be seriously addressed by Smart City advocates if they want to avoid incentivising people to seek privacy illegally. To prevent this, more choice should be granted to current likely end-users of jammers – such as commercial truck drivers – to accept or decline being tracked. Greater reliance on GPS should also consider the possibilities this creates for criminals and even state actors.

What is the Smart City and why is GPS important?

The Smart City agenda endeavours to make cities more efficient, more environmentally friendly, more reactive, and more "liveable" places. It relies considerably on consented and unconsented access to data produced by people and objects to realise proactive and reactive societal, economic and planning solutions. Maintaining precision location and tracking information is necessary for achieving endeavours that involve, for example, autonomous vehicles, geofencing, and smart notifications. The Smart City utilises interconnected networks, such as the internet of things (IoT), cloud computing, remote sensors, artificial intelligence and the mobile infrastructure to merge "physical and virtual worlds," utilising various "electronics distributed in different places including houses, vehicles, streets, buildings, and many other environments" (Komninos, Schaffers, and Pallot, 2011, in Ijaz et al, 2016, p. 613; Biswas and Muthukkumarasamy, 2016). It requires real-time information about the functioning of the city and will involve the widespread use of radio waves at different frequencies coming from a range of devices and systems. Free-to-use GPS, however, will presently discount much of the need for built-in navigation- and tracking-based systems.

Tracking and location information are useful for the Smart City agenda as it can provide real-time manageable data about the movements of people and objects with minimal resources. GPS is thus especially important for the Smart City agenda. GPS is a satellite-based navigation system that provides position/location and time information for no cost to a multitude of users and systems. In finance, for example, it speeds up algorithmic financial transactions, thus accelerating global economic growth. For emergency services it helps save lives by improving efficiency in navigation and positioning information and speeding up emergency response times considerably. It also helps to improve public safety by enabling crime-mapping and tracking for police. For general business activities it supports millions of jobs and services worldwide in aviation, shipping, mobile networks and power supply, including time savings and reduction of fuel (Hall, 2018; Coffed, 2016, p. 4; Deogawanka, 2016; Rajendran, 2017). In the United States alone, it has been calculated that GPS generates approximately $122.4 billion in annual economic benefits (GPS World in Coffed, 2016, p. 4). In 2008, 6 to 7 percent of the European Union's gross domestic product (GDP) was directly dependent on the availability of GPS (Cameron, 2011 in Coffed, 2016, p.4).

A chronology of GPS and tracking

The modern, satellite-enabled roots of tracking dates back to the prelude of the Cold War, where in the 1950s navigation satellites were proposed, and eventually used, for the "prompt location and steering information to a variety of weapon systems," including aircraft, missiles, and nuclear weapons platforms, "thus increasing their accuracy and lethality" (York, 1985, p. 18). The use of jamming as a method of degrading and disrupting radio communications began in the early 20th century, where electromagnetic radio waves were first used in military maritime communications. From the 1920s, radio waves were used for distributing mass media – and propaganda – to millions of listeners in their homes and workplaces. Inevitably, this spurred new developments into jamming technologies and jamming methods. Soviet governments, for example, attempted to jam Western propaganda movements, such as Radio Free Europe, by strategically placing jammers on buildings in dense urban locations. The launch of GPS satellites in the 1980s, among other things, changed radio communication and modern warfare radically, spurring developments into "steerable" smart weapons systems and the miniaturisation of antenna systems. This inevitably created a market for

new military jamming technologies by the US's traditional adversaries: if you can jam smart weapons and your enemies' navigational and communication capabilities, you degrade their ability to fight and communicate effectively. To this day, military jamming is a daily occurrence in conflict zones such as the Ukraine and Syria.

In what ways is GPS vulnerable?

From a technical perspective, distant satellites provide weak signals and therefore antennae systems have to be very sensitive. This makes them susceptible to several types of natural and human interference, including built structure obstruction; terrain/foliage obstruction; solar activity; human or software error; satellite malfunction; control segment failure; space debris; and other factors (RNTF, 2016, p. 5; Lyidir and Ozkazanc, 2004; Borio, O'Driscoll, and Fortuny, 2012). Interference can affect precise timing and position/navigation information, leading to the disorientation of systems and inaccurate navigation and positioning data. From a socio-economic and political perspective, since the collapse of the Soviet Union, and when GPS became available for civilians in the 1990s, jamming and counter-jamming technologies have created new markets in the civilian realm and ceased to be confined exclusively to conflict zones and repressed states. Now incorporated into civilian infrastructures, this has widened the scale of vulnerability (or "attack surface") of the System and provided new opportunities for state actors and criminals.

Correspondingly, as the findings below indicate, the emerging market for cheap and concealable personal tracking devices, and the wide use of tracking systems in freight industries, are also factors incentivising people to buy jammers. Likewise, GPS-enabled monitoring can generate a plethora of information about familial, political, professional, religious, and sexual associations of individuals (Elmaghraby and Losavio, 2014). It could provide thieves with information about whether someone has left home or gone on vacation. GPS jamming is thus no longer a feature of military engagements (e.g. for disrupting communications or misdirecting GPS-enabled smart weapons, ships and surveillance UAVs); Because GPS is now integral to our everyday lives, the market and availability for personal, low-power and inexpensive GPS jammers is extensive.

"Jamming is the transmission of a noise signal across one or more of the GPS/GNSS frequencies to raise the noise level or overload the receiver circuitry and cause a loss of lock" (Royal Academy of Engineering, 2011).

Jammers prevent GPS receivers from computing positions intended to be locally stored or relayed via tracking networks (Mitch et al, 2012). Jamming signals can be done discriminately by disrupting specific systems or indiscriminately by causing unintentional damage as a result of intentional jamming. Spoofing, on the other hand, is the generation of false GPS signals that are intended to alter users' perceptions of time and location.

How widespread is the practice of jamming?

There are no reliable statistics of the ownership of jammers available. However, it has been concluded in various studies that a significant consumer group for "personal privacy devices" (PPDs) are drivers in the freight industry and other motorists. A project named Sentinel, for example, was commissioned to detect and locate interference near an airport where sensors were put in place (Espiner, 2011). It found marked peaks in jamming interference during rush hour times, suggesting commercial drivers of company vehicles are very likely to be the main users. In the same study, and in many media stories, it was argued that GPS-enabled car insurance tracking, criminal tagging and asset tracking are factors increasing ownership of jammers. Other studies have confirmed this, suggesting that up to 30 percent of commercial drivers use such devices (RNTF, 2016, p. 12). Blurring these lines between illicit use and extra-curricular business activities (mentioned later) is the legitimate, licensed use of jammers in some sectors such as prisons (denying use of contraband such as cell phones), governance and diplomacy (preventing spying and eavesdropping on secret meetings and conversations), critical infrastructure protection (denying use of civilian UAVs near airports, for example) military convoys (protection against explosives using radio detonators) and various law enforcement activities. These jammers are significantly higher in price and level of sophistication. Military jamming equipment, on the other hand, is likely in the arsenal of every national military. Varying in power and sophistication, they are used for disrupting communications, surveillance capability, target accuracy, and navigational reliability for offensive and counter-offensive purposes (Westbrook, 2019, p. 7).

Fundamentally, what does the future hold for Smart Cities that will utilise tracking technologies on a wider scale than the present situation? If privacy is diminished further, will this accelerate demands for privacy

seeking devices? A review of literature will identify current gaps in our understanding regarding these questions.

Literature review

Academic studies into jamming and counter-jamming technologies and countermeasures are largely confined to the science and engineering communities. These studies have provided a plethora of practical, technical and policy-relevant findings that have informed risk and vulnerability assessments for the practitioner/military sectors and which are applicable to the Smart City context (see for example Lyidir and Ozkazanc, 2004; Kundu et al, 2008; Borio, O'Driscoll and Fortuny, 2012; Mitch et al, 2012; Di Fonzo et al, 2014, and many more; as well as national governmental and non-governmental institutions). Research into the geographical scope and implications of jamming has recently received some attention (for example from the Resilient Navigation and Timing Foundation, C4ADS and members, Westbrook, 2019) as well as how risk to critical infrastructure has changed over time because of the emergence of new jamming technologies and counter-technologies. More popularised attention in recent years has raised awareness about the implications of jamming, the types of end-users, the consequences resulting in our over-reliance, and implications for law enforcement (e.g. Hambling, Rutkin, Gearin, 2016; McKinlay, 2016; see also MarketWatch, 2017). Nevertheless, little dedicated research addressed the possible consequences of non-consensual tracking has on law enforcement, municipalities and businesses. Likewise, no research addresses factors that may lead to the proliferation of tracking and jamming devices, nor addressed the possible implications of the wider ownership and use of jammers in urban areas.

Likewise, academics interested in Smart Cities have contributed extensively in knowledge in the field of cyber-security and privacy implications, but, worryingly, none have addressed the potential implications of electronic interference from both a political and technical perspective, nor identified possible repercussions of the wider use of tracking and location technologies on the Smart City agenda. This article therefore addresses two significant gaps in literature relating to GPS jamming and cyber/electronic-security and privacy implications of the Smart City.

The next section outlines the various socio-technical, political and economic factors that currently influence the acquisition and use of jamming devices. Later, the article explores the implications for the Smart City, and later explores possible counter-measures and technologies.

FINDINGS

An extensive literature review has identified five prevailing themes driving the demand for acquiring and using jamming devices that may have implications for the Smart City agenda: (1) globalisation; (2) they provide low-risk, high-reward opportunities for criminals; (3) privacy concerns and other socio-technical factors; (4) skewed and misleading marketing and; (5) civilian jamming is not wholly separable from ongoing international political affairs. Many of these factors overlap with each other in various ways.

In reference to globalisation, consumers, even from the most remote parts of the world, are now able to access a range of products sold at competitive prices with little geographical restrictions. China is widely seen as the largest manufacturer and distributor of jammers. The rise of China as a significant economic power, and its vast industrial-base of producing cheap consumer electronics (such as tracking devices), is also a significant factor in the availability and competitive market for inexpensive GPS jammers (Westbrook, 2019, p. 10).

The easy availability and expense of jammers (less than 100 USD) means that there is a strong market and consumer base for both legal and legitimate commercial use (mentioned earlier) and illegal use. GPS jammers are often marketed as PPDs and this is appealing for people seeking privacy from distrustful partners, criminals, or the police. One catalyst for the PPD market is the corresponding market for cheap and accessible GPS-enabled tracking devices for civilian, police and security actors' use. GPS jammers are also marketed as cell phone jammers intended to create "quiet zones" in places such as on trains, in religious buildings, cinemas, theatres, restaurants, and to prevent distractions at work or in family settings. Cell phone jammers have also been used for practical jokes as well as cheating in video games such as Pokémon GO

(McNeil, 2016). This demonstrates that even the most trivial of matters – such as gaming – can influence consumer demand for jammers.

Jammers are also highly marketable because they are low-risk options for a variety of actors, not least because (1) they are easy to use (usually incorporating an on and off switch); (2) they are relatively inconspicuous, often pocket-sized devices that can be hidden and disguised as cell phones; (3) they can be difficult to detect and geolocate, particularly if used in vehicles where perpetrators are absent at the first point of alarm, or in cases where glitches and interference of a system, for example, could result from multiple eventualities (such as natural events or human/system errors) and; (4) they are relatively inexpensive.

Depending on the context and the intentions of the users, GPS jammers can provide high rewards proportional to various criminal objectives. Freight drivers might profit by working out of hours, and taxi drivers might avoid splitting profits with their management (GMT Connect, 2016). In Germany, some drivers have avoided GPS-enabled road tolling payments by using jammers (Messina, 2010). More determined actors – such as organised criminals – may acquire more expensive, sophisticated, reliable, high-power jammers to ensure that more high-stakes rewards are maximised. Criminals have been known to use GPS jammers successfully when stealing cargo or vehicles fitted with GPS tracking devices.

Importantly, whilst there is a high motive for privacy and criminality for a variety of users, there have been many reported instances of websites giving misleading information about laws governing the legal possession and use of jammers in some countries, and this should therefore be considered a factor influencing proliferation. GPS jammers are prohibited in countries such as the U.S., Canada, and Australia, while in the U.K., it is illegal to use GPS jammers, but not to purchase them. In France and Japan, cell phone jammers are legal for use in some public venues.

It has also been pointed out that marketers try to circumvent responsibility by including disclaimers "on their websites or in promotional material that the consumer bears sole responsibility for complying with all legal obligations regarding signal jammers" (Federal Communications Bureau, n.d.). Thus, these grey areas in domestic laws

are exploited and this inevitably leads to wider ownership of jammers and lower levels of accountability.

Existential to the above factors, global affairs, or more particularly ongoing conflicts and disputes in Eastern Europe, the Middle East and in South-East Asia, have national and local repercussions. As GPS gets incorporated into civilian infrastructure and systems, animosities between adversaries in military conflicts and political animosities in the civilian domain fuse together. Since GPS is owned by the United States, it is no coincidence that "privacy seeking" GPS jamming devices are produced en masse in China, and military jammers produced, sold and frequently used by Russia, North Korea and China in areas where the U.S. military operate. Indeed, GPS is undeniably a major soft and hard power tool for U.S. influence in so many strands of political and economic functions around the globe, so disrupting and degrading this system is a potential corrodent to its hegemony.

WHAT DOES THIS MEAN FOR THE SMART CITY AGENDA?

Fundamentally, whilst Smart Cities promise better living standards and more economic and social opportunities, they will challenge "our security and expectations of privacy" (Elmaghraby and Losavio, 2014). The simple hypothesis that this article puts forward is that based on the present situation where numerous individuals have sought privacy by subverting GPS tracking, future and present Smart City agendas will need take into consideration the possible implications of their actions. Not only is it the question of whether increased tracking might motivate people to buy privacy devices, but what opportunities will Smart City functions offer criminals? What intentional and unintentional damage might be caused if there are more end-users and more systems that rely on GPS?

Whilst we cannot answer these questions without speculating, we can try to identify the possible scales of interference based on Smart City initiatives that seek to utilise GPS at the present time, and also based on the known jamming ranges.

Scales of interference

Interference on GPS-reliant systems in Smart Cities will cause varying degrees of disruption that are not equally critical. At the lower-end of the scale, jamming could cause general inconvenience. At the opposite, there might be an increase in intentional and unintentional incidents leading to deaths and injuries, as well as disruptions to critical infrastructures, and impacts on business continuity.

Some forms of jamming – particularly military jamming and spoofing – could in theory seriously damage a nation, but in practice are unlikely ever being carried through. Other threats could cause only minor damage, but that damage is inflicted every day in many locations (RNTF, 2014, p. 2). The overall impact can depend "upon the number and type of affected users, duration of the disruption" and other factors, and the degradation of service can be insidious, without even noticing it is happening (ibid). At the extreme end of the scale, communications, power grids, traffic systems, financial transactions and stock exchanges could be affected. Nevertheless, aviation, shipping, and financial industries typically have backup systems and alternative navigation methods.

Overall, apart from some examples of accidental military jamming in San Diego in 2007, and intentional military jamming by North Korea directed at Seoul (on numerous occasions in early 2010s), both of which affected critical infrastructures, as serious as they were, they only caused general inconvenience for people in these cities – blocking cell phones, navigation data, malfunctioning ATMs, for example. Nevertheless, prolonged interference of the GPS system, like the aforementioned examples, also needs to consider the possibility that other opportunistic crimes may increase (ibid, p. 13). The increased pressure placed on governments to respond to malicious military jamming or spoofing activity could also escalate into conflict, as was in the case of the Iranian spoofing of an U.S. UAV in 2011 (Westbrook, 2019, p. 8-9).

Whilst disruption to satellite navigation system in normal road vehicles might disrupt many operations in the freight industry, disruption to Smart City ventures, including automated vehicles (including personal vehicles, buses, trams, trains and UAVs) and GPS-enabled geofencing technologies (incorporated into infrastructure and in vehicles), may have more serious consequences in terms of loss of life and major disruption to traffic networks. Such systems will rely on "centimetre- or millimetre-

precise coordinates for navigation or avoiding other objects" (Shaw, 2018). Motor vehicles will also provide a plethora of data for national authorities and private entities relating to an individual's everyday activities and consumer habits.

GPS-reliant vehicles could potentially present spoofing opportunities for criminals and terrorists. Recent tests have confirmed that jammers were able to affect an 80,000 USD UAV by making the receiver believe that it was rising, not hovering, which made it plummet "...towards the ground in rather dramatic fashion" (Wood, 2013). Similar tests have been carried out on ships, which have revealed the vulnerabilities occurring because of momentary disruption of positioning information of up to 10 meters, which with poor visibility, narrow straits and rocky areas, could prove disastrous (University of Nottingham, 2016).

Will multiple users cause wider interference?

The implications of jamming cannot only be comprehended solely in qualitative terms, but in quantitative terms relating to their effective ranges and the possibility there will be multiple end-users (Westbrook, 2019, p. 10). This allows us to grasp the implications of jamming based on their effective ranges. Despite being inexpensive, the price of small devices does not appear to provide an accurate account of their power and ranges, thus manufacturer specifications are not accurate. Prominent researchers agree that the effective "ranges from a few meters to several tens of meters are advertised" online, "but the actual effective ranges are significantly greater. Claimed and true power consumptions range from a fraction of a watt to several watts" (Mitch et al, 2012). Overall, this makes it hard to predict if or how receivers are vulnerable to what devices and what ranges. Adding to this, companies and infrastructure managers can be reluctant to expose the weaknesses of their systems which inevitably makes it harder to understand or comprehend the implications of jamming in urban contexts.

Table 1. Likely users and ranges of GPS jammers

Likely End-users	Approximate Power	Approximate Distance	Urban Areas Affected and Potential Consequences	Notable Examples
Privacy seekers; criminals	one deciwatt < >	Few meters to 9.3 miles	Dense urban locations, civilian systems	London Stock Exchange, numerous airports.
Organised criminals; terrorists; state proxy actors, state/private security actors	one kilowatt < >	31 miles < >	Cities, regions, civil and military systems	No open access information available.
State-assisted terrorist and rebel groups, state militaries	10 kilowatts < >	94 miles – 124 miles < >	Cities, regions, small countries, civil and military systems	South Korea, San Diego Harbour (unintentional), Finnmark (Norway), Ukraine, Syria, Iraq, East Europe, Black Sea, South China Sea, and others.

From open access sources (Scott, Shaw, and Lo, 2013; Mims, 2011; Lynne, 2003; Westbrook, 2019)

Most non-state actors will not be able to acquire military-grade jammers because they are not available without an appropriate license in most countries. Nevertheless, drug cartels succeeded in spoofing surveillance UAVs used by Custom and Border Protection on the Mexico-U.S border, which required a high level of sophistication to accomplish (RNTF, 2016, p.14). Thus, it is clearly possible to produce or acquire

military-grade jammers and spoofers through the black market, especially in countries that lack laws and legislation for manufacturers, distributors, as well as related parts and components and intellectual property. But if one low-power jammer can impact dense urban locations, then multiple users could hypothetically affect systems in whole cities and regions. Thus, the quality and quantity of jammers are significant in different ways.

A recurring theme relating to the GPS jamming phenomena, however, is the increased use of intentional military jamming of urban civilian areas. Russia's "Zapad" military drills, involving thousands of soldiers in as near as 10km from Norway is likely to be deliberately provocative (Staalesen, 2018). The Norwegian Ministry of Foreign Affairs confronted Russian authorities over concerns that civilian aviation and communications systems had been repeatedly "jammed in connection with nearby Russian military activities" near Norway's Eastern Finnmark region (ibid; Westbrook, 2019, p. 7). South Korea's capital Seoul has been targeted frequently by North Korean military jamming; affecting aerial, naval navigation, as well as cell towers and vehicle navigation. Seoul and its major airport are close enough to the demilitarised zone to be affected by intentional and unintentional interference. Thus, some cities may require military anti-jamming systems incorporated into civilian infrastructures, while others in relative safety may opt for more accessible technologies available in the civilian market (Westbrook, 2019).

POSSIBLE COUNTERMEASURES AND ALTERNATIVE TECHNOLOGIES

Counter-jamming strategies and technologies

It is not within the scope of this study to outline the technical, legal, political and operational ways to mitigate jamming, as they vary between each study and country (see for example, Kundu et al, 2008; Borio, O'Driscoll, and Fortuny, 2012; Di Fonzo et al, 2014; Mitch et al, 2012). Since jamming affects the accuracy and reliability of smart weapons and communication systems, significant research has gone into counter-jamming strategies and technologies for military markets. Iraq's jamming of U.S. and coalition's smart weapons during the Second Gulf War spurred interest into lethal and non-lethal detection and geolocation technologies.

The U.S.-made home-on GPS Jam, or HOG-J, is a lethal example. Anti-jamming systems themselves have miniaturised, have become lighter and less power-consuming, and therefore have become more versatile for users and for installation in numerous devices and infrastructures.

For law enforcement especially, this has significantly improved monitoring, identification, tracking, and responses to, jamming, or GPS interference more broadly. One example is hand-held battery-operated radar systems, which can, for example, identify vehicles illegally using jammers. Devices the size of mobile phones also assist in detecting and geolocating jamming. Seizures at airports and international mail packages can also be an effective counter-jamming strategy. Whilst tightening laws on the trade and possession of GPS jammers as well as implementing rigid laws and legislation on privacy rights might be the most effective approach, there are some counter-measures in the military, security and civilian markets that could provide some measure of protection against jamming.

One of the many factors that makes GPS susceptible to jamming is the size of the antenna systems, as well as issues concerning standardisation and modernisation. This has already initiated state and private initiatives for modernisation as well as miniaturisation of antenna systems and receivers. Since antennas and receivers can be large and heavy; small and lightweight receivers, preferably low in power consumption, are being produced to allow more flexibility and versatility.

Whilst small antenna systems are less vulnerable to interference, fitting them to UAVs does not necessarily decrease their vulnerability, but as moving objects, they can be fitted with alert and fault detection systems (incorporated into receivers) that enable the vehicles to automatically steer away from interference, and even notify authorities and geolocate where interference is coming from. Lightweight technologies would be key to UAVs, whilst heavier systems can be incorporated into land vehicles. Whether this is practical or even a realistic countermeasure, however, is open to question (composite studies address this, for example Perkins et al, 2015).

Since fixed-reception antennas are also generally more susceptible to jamming than moving objects, adaptive array antennas (or “smart antennas”) could theoretically be adapted to emerging Smart City functions like UAVs and other vehicles that rely on GPS. Some smart

antennas have hemispherical coverage, allowing them to receive radio frequencies from more satellites than conventional antennas. Electrically steerable directional antennas could also potentially overcome jamming (Cole, 2015).

On the above points, some procedures for identifying and responding to jamming events in airports, for example, could also be replicated in the Smart City. Instead of having in-built systems or multiple people responding to and reporting jamming, it could be more cost-effective to have one jammer geolocation system that identifies instances of jamming to a single entity. It may be argued, however, that whilst managing this would be possible for an airport, a city with unique and complex physical and human landscape with possibly more end-users, as well as multipath reflections and "urban canyons," might be less practical.

Some advocates have argued that finding alternatives to, or reducing our dependence on, GPS is most appropriate. Indeed, many governments, militaries and critical infrastructure managers have invested their resources into appropriate responses to GPS outages, including undertaking operations independent of GPS, utilising alternative technologies and improving risk assessments. This is transferable knowledge for cities and municipalities invested in Smart City initiatives. As for vehicle navigation, alternative or complementary systems from military technologies, such as laser-guidance, pre-programmed navigation images (of physical structures, roads, streets, pedestrian crossings etc.) and inertial, self-calibrating navigation aids (fitted with stable and precise clocks) are just some systems that could replace GPS as a navigation tool.

Indeed, considerable investment already goes into back-up navigation systems such as Loran (LOng-RAnge Navigation: China, Iran, Russia), and eLoran (Enhanced-Loran: U.K., U.S. and Europe). The superior eLoran system provides a means to maintain high-quality timing in the event of GPS vanishing by enabling "navigation by triangulating via low-frequency/longwave radio signals transmitted by fixed land-based radio beacons" (Vaas, 2014). Indeed, the connected and autonomous vehicle industry is already developing alternative technologies that address existing limitations of GPS. GPS black spots are created in dense urban locations (due to minimised satellite coverage) and GPS is sufficiently less effective underground, in buildings, tunnels and in crowded areas. Considerable investment also goes into internal navigation aids, collision

avoidance systems, intelligent speed adaptation, automatic braking systems, and geofencing technologies. These could provide potential alternatives in relation to inaccurate GPS information.

On the other hand, as an accompaniment to investing in alternative systems, strengthening GPS signals could overcome weak jamming signals. Indeed, recent military jamming aimed at disrupting Western military operations has prompted "much more significant investment in counter-space capabilities" (Lewis, 2004). One countermeasure has involved producing future generations of satellites with stronger signals, creating a more "distinctly separate GPS system for civilians and military […] to avoid the targeting and disabling of all GPS systems" in military operations (GPS Jammers, 2013). Thus, improving signals might minimise the risk to GPS reliant systems if jamming "noise" is effectively weakened.

On the above point, the enduring capability race between major powers – on earth and in space – means that GPS signals are destined to become stronger and more reliable. The move of some great powers, aware of the potential threat of zero or minimal satellite navigation capabilities during wartime, have developed their own independent systems (The U.S. (GPS), Russia (GLONASS), China (BeiDou) and Europe (Galileo), IRNSS (India) and QZSS (Japan)) which include modernisation projects.

In summary, there are a range of developments in the military, security, and civil industries that might make the Smart City agenda more achievable if tracking technologies are, as they currently expected to be, important to realising its potential.

CONCLUSIONS AND DISCUSSIONS

Any aspect of privacy may disappear if people are more willing to sacrifice information about their location and activities in order to receive better services and or improve their living standards. This raises the question of whether the Smart City agenda may irrecoverably motivate people to seek privacy by illegal means.

Whilst we are not at the stage at which everyone is knowingly tracked, the real question is: where will the boundaries lie? Taking one example, electric vehicle manufacturers operating in China are obliged to incorporate systems that provide information about the location of cars to the government (Kinetz, 2018). Chinese officials state that this data is used to improve public safety and facilitate industrial and infrastructure planning, but civil society more broadly argue that this facilitates mass surveillance (ibid). There appears to be no open-source information indicating that this has led to a proliferation of jamming devices in China, but since there is a large industrial-base for such devices in the country, it cannot be ruled out that jammers are produced in the country for these very reasons.

Reducing the motivation to buy jammers could also be achieved by implementing stricter laws on privacy and possession and use of jammers, but also identifying the likely users. Since some commercial drivers are motivated to buy jammers, should "more" privacy be granted to these users? It is a legal paradox that in most Western countries companies seek consent from their workers to track their locations, but their refusal may result in dismissal, limited work, or outright rejection for hiring. The question remains whether citizens of Smart Cities going to have to sacrifice their privacy without refusal.

If tracking is necessary to create "liveable cities," some military, security, and civilian technologies could reduce reliance on GPS or improve its strength, and therefore reduce possible widespread interference. But fundamentally, whilst jammers are, for good reason, illegal to use without license in most of the world, the goal should be to enable people to seek privacy legally and ensure that privacy is safeguarded to the point that privacy cannot be achieved only by illegal means.

The wider policy implications are glaring due to the multitude of actors using jammers – military or non-military. Overall the practice of jamming has become potentially deadlier as reliance on GPS expands and opportunities for criminality or military provocations increases (Westbrook, 2019, p. 12). Cross-border military jamming may become more prevalent if relations between states – on Russia's and North Korea's borders, for example – deteriorate further. Drug cartels spoofing U.S. government UAVs suggests that other Smart City functions might present

new opportunities for criminal and state actors and lead to more sophisticated criminal methods of achieving certain goals. Smart City advocates should consider the wider implications tracking not only on their agenda, but on the societies and economies as a whole.

REFERENCES

Biswas, K., Muthukkumarasamy, V. (2016, December). *Securing Smart Cities Using Blockchain Technology,* 2016 IEEE 18th International Conference on High Performance Computing and Communications. Abstract only. doi: 10.1109/HPCC-SmartCity-DSS.2016.0198

Borio, D., O'Driscoll, C., Fortuny, J. (2012, December). *GNSS Jammers: Effects and countermeasures.* 2012 6th ESA Workshop on Satellite Navigation Technologies (Navitec 2012) & European Workshop on GNSS Signals and Signal Processing, doi: 10.1109/NAVITEC.2012.6423048

Cameron, A. (2011). Galileo from the Top: Interview with the EC's Paul Verhoef. *GPS World*, in Coffed, J. (2016). The Threat of GPS Jamming; The Risk to an Information Utility, *Harris Corporation*, https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf

Coffed, J. (2016). The Threat of GPS Jamming; The Risk to an Information Utility, *Harris Corporation*, https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf

Cole, S. (2015) Securing military GPS from spoofing and jamming vulnerabilities, *Military Embedded Systems*, retrieved from mil-embedded.com/articles/securing-military-gps-spoofing-jamming-vulnerabilities/

Deogawanka, S. (2016). How GIS Supports the Planning and Development of Smart Cities, *GIS Lounge*, Retreived from https://www.gislounge.com/how-gis-supports-the-planning-and-development-of-smart-cities/

Di Fonzo, A., Leonardi, M., Galati, G., Madonna, P., and Sfarzo, L. (2014). *Software-Defined-Radio techniques against jammers for in car GNSS navigation.* 2014 IEEE Metrology for Aerospace (MetroAeroSpace). doi: 10.1109/MetroAeroSpace.2014.6865942

Elmaghraby, A. S. and Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy, 5(4): 491–497. doi: 10.1016/j.jare.2014.02.006

Espiner, T. (2011) UK Sentinel study reveals GPS jammer use, *ZDNet*, retrieved from https://www.zdnet.com/article/uk-sentinel-study-reveals-gps-jammer-use/

Federal Communications Bureau, (n.d.). GPS, Wi-Fi, and Cell Phone Jammers Frequently Asked Questions (FAQs), retrieved from https://transition.fcc.gov/eb/jammerenforcement/jamfaq.pdf

GMT Connect (2016). Thousands Using GPS Jammers On UK Roads Pose Risks Say Experts, retrieved from https://www.gmtconnect.com/thousands-using-gps-jammers-uk-roads-pose-risks-say-experts/

GPS Jammers (2013). How GPS Jammers are used, retrieved from www.gpsjammers.org/what-gps-jammers-are-used-for/

GPS World, The Economics of Disruption: $96 billion annually at Risk, in Coffed, J. (2016). The Threat of GPS Jamming; The Risk to an Information Utility, *Harris Corporation*, p.4, https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf

Hall, K. (2018). Forget cyber crims, it's time to start worrying about GPS jammers – UK.gov report. *The Register*, Retreived from https://www.theregister.co.uk/2018/01/31/gps_signal_jammers_critical_infrastructure/

Komninos, N., Schaffers, H., and Pallot. M. (2011). *Developing a policy roadmap for smart cities and the future internet*, eChallenges e-2011 Conference Proceedings, IIMC International Information Management Corporation. IMC International Information Management Corporation in: Ijaz, S., Shah, M. A., Khan, A., and Ahmed, M. (2016) Smart Cities: A Survey on Security Concerns. *International Journal of Advanced Computer Science and*

Applications, 7(2), 612-625. citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.742.883&rep=rep1&type=pdf

Hambling, D. (2017). Change in the air: Disruptive Developments in Armed UAV Technology. *United Nations Institute for Disarmament Research*. Retrieved from www.unidir.org/files/publications/pdfs/-en-726.pdf

Hambling, D., Rutkin, A., Gearin, C. (2016). How drones are learning to find their own way in the world. 27 July, *The New Scientist*, retrieved from https://www.newscientist.com/article/mg23130842-600-how-drones-are-learning-to-find-their-own-way-in-the-world/

Kinetz, E. (2018). Electric vehicles send real-time data to Chinese government, *TechXplore*, retrieved from https://techxplore.com/news/2018-11-electric-vehicles-real-time-chinese.html#nRlv

Kundu, A., Mukhopadhyay, M., Sarkar, B. K., Chakrabarty, A. (2008, January). *Incorporation of Anti-Jamming Techniques in a GPS Receiver.* 2008 International Conference on Signal Processing, Communications and Networking. doi: 10.1109/ICSCN.2008.4447175

Lewis, J. (2004) Iraq and GPS Jamming, *Arms Control Wonk*, Retrieved from https://www.armscontrolwonk.com/archive/200039/iraq-and-gps-jamming/

Lyidir, B. and Ozkazanc, Y. (2004, April). *Jamming of GPS receivers.* Proceedings of the IEEE 12th Signal Processing and Communications Applications Conference, 2004. doi: 10.1109/SIU.2004.1338639

MarketWatch (2017). Spirent Security Experts Predict Greater Risk to Civil and Military Global Navigation Applications In 2017, retrieved from https://www.marketwatch.com/press-release/spirent-security-experts-predict-greater-risk-to-civil-and-military-global-navigation-applications-in-2017-2017-02-02

McKinlay, R. (2016). Technology: Use or lose our navigation skills. *Nature*, 531, 573-575, doi:10.1038/531573a

McNeil, B. (2016). Battling Pokémon trespassers with GPS Jamming, *AM insights on location*, retrieved from https://www.directionsmag.com/article/1130

Messina, J. (2010). GPS Jamming Devices Pose Many Threats, *Phs.org*, retreived from https://phys.org/news/2010-02-gps-devices-pose-threats-video.html

Mitch, R. H., Psiaki, M. L., O'Hanlon, B. W., Powell, S. P., Bhatti, J. A. (2012). *Civilian GPS Jammer Signal Tracking and Geolocation*. 25th, Institute of Navigation; 2012; Nashville, TN. 4, 2901-2920. citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.721.7129&rep=rep1&type=pdf

Perkins, A., Dressel, L., Lo, S., and Enge, P. (2015). Antenna Characterization for UAV Based GPS Jammer Localization. *Semantic Scholars.* Retrieved from https://pdfs.semanticscholar.org/3692/8bd059d7c1d30a0d348edebae4ba91d1121b.pdf

Rajendran, V. (2017). Location Based Services and Smart City Initiatives on a Global Scale, *Geoawesomeness*, Retreived from https://geoawesomeness.com/lbs-and-smart-city-initiatives-on-a-global-scale/

RNTF (Resilient Navigation and Timing Foundation), (2016). *Prioritising Dangers to the United States from Threats to GPS: GPS Ranking Risks and Proposed Mitigations*, White Paper, https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf

Royal Academy of Engineering, (2011). Global Navigation Space Systems: reliance and vulnerabilities, in Coffed, J. (2016). The Threat of GPS Jamming; The Risk to an Information Utility, *Harris Corporation*, p.6, https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf

Scott, L., Shaw, G., Lo, S. (2013). *GNSS-Denied Environments: Living in a vulnerable world*, Presentation webinar, Inside GNSS, May 12, 2013, www.insidegnss.com/pdf/GNSS_in_Denied_Environment_Webin

ar_slides_5_2_13.pdf; Mims, C. (2011). How Cruise Missiles Would Beat GPS Jammers in Libya, *MIT Technology Review*, retrieved from https://www.technologyreview.com/s/423363/how-cruise-missiles-would-beat-gps-jammers-in-libya/; Lynne, D. (2003) GPS-jammer contractor plays both sides of war, *WND*, Retrieved from, https://www.wnd.com/2003/03/17996/

Shaw, K. (2018). How Microlocation Will Open New Frontiers for Robotics, Smart Cities, *RB*, retrieved from https://www.roboticsbusinessreview.com/news/microlocation-will-open-new-frontiers-for-robotics-smart-cities/

Staalesen, A. (2018). Norway requests Russia to halt GPS jamming in borderland, *The Barents Observer*, retrieved from https://thebarentsobserver.com/en/security/2018/04/norway-requests-russia-halt-gps-jamming-borderland

The University of Nottingham (2016). GPS jamming: keeping ships on the 'strait' and narrow, retrieved from https://www.nottingham.ac.uk/news/pressreleases/2016/july/gps-jamming-keeping-ships-on-the-strait-and-narrow.aspx

Vaas, L. (2014). Revamping an old technology to go where GPS signals cannot reach, *Sophos*, retrieved from https://nakedsecurity.sophos.com/2014/02/13/revamping-an-old-technology-to-jam-the-gps-jammers/

Westbrook, T. (2019). The Global Positioning System and Military Jamming: The geographies of electronic warfare. *Journal of Strategic Security* 12(2), 1-16. doi: https://doi.org/10.5038/1944-0472.12.2.1720

Wood, M. (2013). Forget GPS jamming, drone 'spoofing' is all the rage, *Market Place*, retrieved from https://www.marketplace.org/2013/03/11/forget-gps-jamming-drone-spoofing-all-rage/

York. H. F. (1985). Nuclear Deterrence and the Military Uses of Space. *Daedalus, The MIT Press, Weapons in Space*, 114(2), 17-32. Retrieved from www.jstor.org/stable/20024976

ABOUT THE AUTHORS

Dr Tegg Westbrook holds a PhD in Global Studies, Nottingham Trent University, UK. For last 3 years he has worked for humanitarian NGOs that specialise in arms control. He is currently Associate Professor at the University of Stavanger, Norway, where he teaches at the Faculty of Science and Technology, Department of Safety, Economics and Planning. His current research interests include terrorist risk, urban resilience, and emerging security technologies.