


Lethal empowerment and electronic crime: A focus on radio-frequency interference capabilities

Tegg Westbrook

tegg.westbrook@uis.no

 <https://orcid.org/0000-0002-9889-3673>

Department of Safety, Economics, and Planning, University of Stavanger, Kjell Arholms Gate 41, 4021 Stavanger, Norway

Abstract

This article focuses on the capabilities of criminals in using radiofrequency interference (RFI) devices to target systems that use the Global Positioning System (GPS). Surveying over a 22-year period during which GPS has been widely used by many industries, it seeks to understand how the electronic threat has evolved and changed. Focusing on the accessibility, usability, effectiveness, versatility, transportability, and concealability of RFI devices, and utilising a number of sources from engineering disciplines, hacker events, and media pieces, it argues that the more reliant we are on GPS, the more threat actors' target choices and means, ends, and, indeed, motivations for targeting systems will expand, elevating the risks to GPS users. This article finds that arguably some of the most disagreeable actors have elevated from unsophisticated to semi-sophisticated in the space of 20 years, and can target systems cheaply, easily, and effectively. In the space of two decades, the combination of war, the expansion of digitalisation, the commercialisation of military systems, and the demand and supply that feeds technological innovations, have left us with an entirely different threat picture.

Keywords:

global navigation satellite system, terrorism, cybercrime, electronic crime

Article info

Received: 19 September 2024

Revised: 22 November 2024

Accepted: 26 November 2024

Available online: 22 January 2025

Citation: Westbrook, T. (2025) 'Lethal empowerment and electronic crime: A focus on radio-frequency interference capabilities', *Security and Defence Quarterly*, 49(1), pp.22–39. doi: [10.35467/sdq/196515](https://doi.org/10.35467/sdq/196515).



© 2025 T. Westbrook published by War Studies University, Poland.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).

Introduction

The aim of this article is to understand how the threat of electronic crime and terrorism has manifested in line with the diffusion of the Global Positioning System (GPS)-dependent and GPS-aided systems in the past two decades. The objective is to establish how technological innovations have given criminal and politically violent actors the capabilities to target systems with radiofrequency interference (RFI) devices and how this relates to current literature in this area. Such analyses are important, as while cybercrime has received much focus, electronic crimes have received comparatively limited overview.

There are several examples where criminals have used electromagnetic energy to enable physical crimes. Criminals have used electromagnetic disruptors to interfere with gambling machines, to compromise security systems at banks, jewellers, and in expensive vehicles (US Department of Homeland Security (DHS), 2003). Bluetooth, WiFi, and 5G jammers are available on the market for users seeking privacy, but they can also be used for cyber-enabled property theft. Previous research has expanded on how criminals, from petty to serious, have used RFI to enable physical crimes (Westbrook, 2019a, 2023a, 2023b, 2023c, 2024). These have investigated different RFI strategies and considered how they fit with the modus operandi of various criminal actors. However, the focus on the capability and sophistication of actors has not been properly contextualised, which gives rise to concerns about the destructive capabilities of extreme groups.

Scholars of terrorism studies have long been interested in how technologies have empowered individuals or groups to cause mayhem. Dolnik's (2007) *Understanding terrorist innovation: Technology, tactics and global trends*, for example, puts forward the idea that weapon choice can be categorised into different opportunity parameters shaping the modus operandi of violent actors. Clark and Newman's (2006) *Outsmarting the terrorists* has also inspired much focus on the technological and environmental conditions that influence the decisions and actions of terrorist groups.

Cronin's (2020) book *Power to the people: How open technological innovation is arming tomorrow's terrorists* also seeks to understand why, and anticipate how, some technologies are adopted by violent actors. She argues that there are distinctions to be made about why some technologies rapidly diffuse and why others do not. She uses "lethal empowerment theory" to understand and anticipate why some "technologies hold the greatest potential to become popular tools for political violence in the future" (p. 13). Certain lethal technologies are more likely to be adopted by violent groups and individuals because they are: accessible, cheap, simple to use, transportable, concealable, effective (providing leverage and more "bang for the buck," for example), multi-use, not cutting-edge (usually in the second or third wave of innovation), bought off-the-shelf, part of a cluster of other emerging technologies (which are combined to magnify overall effects), symbolically resonant (which make them more potent than just their tactical effectiveness), and given to unexpected uses (p. 13). Cronin argues that such technologies extend the reach of criminal actors (p. 14).

While useful, such scholars noted above focus on traditional (kinetic) weapon choices, and do not deal with the prospect and impact of cyberterrorism or "electronic terrorism" in significant detail. There also remains a lack of historical contextualisation linking societal changes to specific elevated threat situations. This is perhaps due to the fact that it has been difficult to connect terrorist goals with the effects and impacts of cyberattacks. Gross *et al.* (2017) nonetheless write of a "stress-based cyber terrorism effect" that is also useful for considering the likelihood of electronic weapons being adopted by non-state

actors (NSAs) in their struggles. They argue that “[e]xposure to cyberterrorism is not benign and shares many traits with conventional terrorism.” Responses such as “stress, anxiety, insecurity, a preference for security over liberty, a re-evaluation of confidence in public institutions, a heightened perception of risk, and support for forceful government policies” are effects that can be achieved via cyberterrorism (Abstract).

There has been some focus on how sophisticated an actor needs to be to carry out headline-grabbing cyber-attacks. Overall, the “levels” of sophisticated RFI devices roughly correspond with the same categories of “cyberterrorists,” but they are imperfect generalisations. [Denning \(2000\)](#) defined “cyberterror” capability into: *simple-unstructured* (capable of conducting “basic hacks against individual systems using tools created by someone else,” with little need for target analysis or learning capability); *advanced-structured* (capable of conducting more sophisticated attacks against multiple systems/networks and able to modify or create basic hacking tools, with elementary target analysis and learning capability); and *complex-coordinated* (capable of coordinated attacks potentially causing mass-disruption against hard defences).

Focusing on RFI, [Ranganathan et al. \(2016\)](#) also provide detailed information about how use of RFI devices by sophisticated and unsophisticated actors can be defined. Additionally, scholars, such as [Humphreys et al. \(2008\)](#), [Shepard et al. \(2012\)](#), [Zeng et al. \(2018\)](#), and others, have attempted to classify various types of spoofing attacks into simple, intermediate, or sophisticated in terms of their effectiveness and subtlety. An issue with these articles is that while they seek to categorise levels of sophistication with “impact” as a barometer, they do not measure or delineate aspects of accessibility, usability as well as the versatility of specific cyber tools and how that broadly contributes to the threat picture. To summarise, electronic crime can be understood in similar ways to cybercrime, but it is necessary to place emphasis on equipment as well as end goals and the sophistication of the actor, which is where this article focuses most of its attention.

The threat of jamming and spoofing

What makes RFI attacks attractive for criminals? The answer is that very simple attacks can help with their activities in different ways. Radio jamming is used to intentionally block the signals emitted from satellites to receivers, which affect tracking and navigation systems. Terrorists have long used jamming systems to deny service to drone surveillance or to avert surveillance. Terrorists may also use jamming to complement physical attacks, for example, degrading communications for emergency responders following a physical attack ([Westbrook, 2023a](#)).

Spoofing, however, is much more sophisticated and malign than jamming, as spoofing is intended to inject falsified navigational data to influence a GPS-user, or the system, to make a choice favourable to the attacker. This can complement kidnappings, kinetic attacks, or enable physical attacks ([Westbrook, 2023a](#)). This is much harder to achieve than a jamming attack, but has, as this article shows, become much easier to do over a short time span.

The article provides a historical overview of the jamming and spoofing threat from its identification, particularly from the 1990s to the present-day situation. The findings of this article indicate that the spoofing and jamming capabilities of state and non-state actors have evolved as the global navigation satellite system (GNSS) has, itself, metamorphosed into something that is now taken for granted as much as tap water. What is it that turned an attack that was difficult to achieve, with once bulky, heavy, and expensive

equipment in the early 2000s, into something that someone with a modicum of technical knowledge can do rather cheaply, easily, and with a low chance of risking jail or death, in the last 20 years?

Methods

The research consisted of a meta-data analysis of research into jamming and spoofing mainly from engineering and computer science papers, government reports, risk assessments, and from media. From the documents, special attention was paid to the costs, manpower required (for successful spoofing), and associated consequences (impact) of the attacks. It also focused on gathering other information, including the size of devices, versatility, and the level of sophistication and manpower required to use them. The findings were organised into themes associated with [Cronin's \(2020\)](#) lethal empowerment theory. It also, though to a less systematic degree, linked the observations to the “stress-based cyber terrorism effect” proposed by [Gross *et al.* \(2017\)](#), and [Denning's \(2000\)](#) categories of sophistication. The results are expressed by way of subsections of the categorisations relevant to the lethal empowerment theory. The connections to the work of [Gross *et al.* \(2017\)](#) and [Denning's \(2000\)](#) theories are explored in the Conclusion.

What is electronic crime and “electronic terrorism”?

While terror groups have found rudimentary but effective means to enable violence, their influence on GPS-aided and GPS-dependent systems has received only recent attention ([Westbrook, 2023a, 2023b, 2023c, 2024](#)). However, first there is a need to distinguish the sometimes conflated notions of cyber terrorism, cyberattacks, cyber warfare, and cybercrime as opposed to electronic warfare, electronic attacks, and electronic terrorism, the former categories of which usually involve online activity via the Internet, the other uses and/or manipulates, offensively or defensively, the electromagnetic spectrum.

Academia is largely divided on the definition of cyberattacks, cybercrime, and cyber terrorism. Cybercriminals use computers, the Internet, or any networked activity for financial gains. A broad definition of cyber terrorism, which is usually not financially motivated, is “an act of politically motivated violence involving physical damage or personal injury caused by a remote digital interference with technology systems” ([Evan *et al.*, 2017](#)).

While crime using the electromagnetic spectrum to control or disrupt systems for financial gain is not widely seen (perhaps due to the limited financial benefit of interference alone), an adaptation of the term “international electromagnetic interference” was first described at the EMC Zurich Symposium in 1999. This was the “intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes” ([Giri *et al.*, 2020](#)). Scholars of “electronic terrorism” are in more agreement about what it is, perhaps due to the more applicable connection between brute force electromagnetic energy, violence (radiation), and physical damage (of critical technical infrastructure and computer systems), and thus easily attributable to terrorist means–ends objectives.

While state actors have special licences to control information sent via the electromagnetic spectrum, non-state actors, including terrorists, rebels, or insurgents have demonstrated ingenuity using mostly commercially available technologies to take advantage of it. Use of

radio receivers from toy planes, alarm clocks, and cell phones has allowed organisations like the Provisional Irish Republican Army (IRA), Al Qaeda, and many others to remotely detonate explosive materials. Using radio receivers from children's toys gave the Provisional IRA the ability to effectively remote detonate explosives and avoid accidental deaths of bomb makers. After the British security services jammed those signals, the Provisional IRA adapted, using “unjammable” radio initiation systems, including infrared and light sensor initiation systems (Gill, 2017), the techniques for which have reportedly been passed on to other violent organisations (Magnuson, 2007). Indeed decades later, in 2006, during the wars in Afghanistan and Iraq, the US military devoted huge efforts to developing systems that could jam remotely detonate improvised explosive devices (IEDs) using microwave emitters. Al Qaeda, in turn, like the Provisional IRA, found alternative means of remote detonation. The US military tried microwave emitters, which were supposed to damage IEDs' electronic circuitry, but they were simply shielded by the insurgents. The United States' use of lasers also failed to work effectively (Cronin, 2020). Al Qaeda's IED war on coalition forces in Afghanistan proved highly successful.

As for navigation systems, the potential that malign actors could create situations that elevate tensions between adversaries came to fruition in the 1980s following the liberalisation of GPS for non-military users. President Ronald Reagan released an executive order allowing civilian use of GPS in 1983 after the Soviet Union's downing of a Korean Airlines flight, which had strayed hundreds of miles off its planned course. While proving extremely useful for United States and coalition forces during Operation Desert Storm, the system eventually became fully operational in 1993 for civilian users, inevitably expanding the scalability of the “attack surface” (Jones, 2017).

As GPS (without military encryption) steadily became available in commercial/civilian sectors through the 1990s, the spoofing and jamming threat for GPS-aided and GPS-dependent systems became a theoretical possibility. Many conferences and research studies concluded that while jamming was certainly possible (Gerdan *et al.*, 1995), in reality spoofing was simply too difficult to be a realistic probability. Nevertheless, in reality such attacks posed a conceivable if very remote possibility given how many commercial, state sectors, and safety-critical systems were becoming increasingly reliant on the open source jammable and theoretically spoofable GPS system for timing and navigation. With the expansion of the Internet and increasing reliance on networked technologies in many sectors and industries, a discourse surrounding “cyberterrorism” and “electronic terrorism” also emerged in the early 1990s. It was thought that “tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb,” with terms such as “electronic Pearl Harbor” frequently being used in security circles (Weimann, 2004).

Global positioning system was becoming increasingly critical to business and societal functions in the early 21st century. Indeed, in 2000, President Bill Clinton announced that the United States would allow civilians, such as emergency services, sailors, and motorists, unrestricted access to a higher-grade GPS, previously left intentionally low grade before. It was perceived that such a move would have minimal impact on national security. This was in part due to the growing competition from other constellations, like Europe's Galileo, which was planned to provide improved signal accuracy. Following this liberalisation, and the subsequent liberalisations of satellite-based information from other constellations, the economic benefits of unrestricted access could be measured in billions of dollars of revenue for national economies.

The ever-increasing reliance on GPS for critical functions of society prompted a number of government initiatives, in particular for transportation infrastructure. President Clinton directed the Department of Transportation to study the issue and make recommendations.

The recommendations, informally called the [Volpe \(2001\)](#) report, called for improved receivers and the development of interference detection networks as well as non-satellite navigation systems for use alongside GPS. The key finding of the report predicted that “[a]s GPS further penetrates into the civil infrastructure, it becomes a tempting target that could be exploited by individuals, groups or countries” (2001). It also found that it would be relatively straightforward to spoof GPS signals using commercially available GPS simulators.

The Volpe report was published 12 days before the September 11th attacks (9/11) in New York and Washington in 2001, and most of the recommendations were understandably sidelined ([Goward, 2016](#)). The tragic events of 9/11 ignited discussion about spoofing and commercial air travel, especially on the subject of the Automatic Dependent Surveillance-Broadcast (ADS-B), which uses satellite navigation to broadcast position information to other aircraft ([Westbrook, 2024](#)). The possibility of hijackers simply switching off ADS-B onboard flights (and other tracking devices) was also a concern. The European Commission was similarly concerned about its emerging satellite constellation, Galileo, mentioning in a communication “Economic terrorists, criminals or hostile agents” as possible attackers. Targeting of the constellation, as the communication from the European Commission stresses, could seriously impair the efficiency of national security and police forces, affect economic activities, and even lead “to the complete shutdown of services in some areas. This would seriously undermine user confidence in the system” ([Communication from the Commission to the European Parliament and the Council, 2002](#)). Concerns about terrorists developing low-cost and portable electronic weapons, for example, high-powered microwave weapons, was also not misplaced. The US government-funded research found that a briefcase-sized microwave weapon could be constructed for as little as \$2,000 by terrorist organisations ([US Foreign Affairs, Defense, and Trade Division, 2008](#)).

Since GPS can be encrypted, the question was whether ADS-B should also be. Ideas about encrypting the ADS-B was in the end withdrawn due to it potentially undermining the “concept and associated benefits,” and even in later years after other hijackings and attempted hijackings, these concerns are still further substantiated. Similar concerns with the security of ADS-B’s marine equivalent—the Automatic Identification System (AIS)—have also been raised ([Westbrook, 2023b, 2024](#)).

A small number of academic publications exploring “practical spoofing attacks” followed the [Volpe \(2001\)](#) report and other government-level acknowledgements. These did not appear to dwell on terrorist or hostile state motivations or intentions, but rather more criminals targeting tracked cargo on trucks for theft. But they did show how criminals with varying capabilities and expensive equipment could create false time-shifting signals after tampering with the victim’s receiver, and also in limited situations when trucks are stationary or moving no further than 30 feet from the attacker. Others demonstrated that off-the-shelf equipment, such as signal simulators and amplifiers, could be used to lock on to a victim’s receivers, making spoofing for non-state actors more plausible.

There was optimism about solving the spoofing issue, however, with low-cost countermeasures for existing GPS receivers that could complicate attacks ([Warner and Johnston, 2003](#)). Spoofing in 2001 was still seen as difficult, detectable, and requiring expensive equipment that was usable only at short range by skilled and motivated attackers. The Department of Transportation noted that earlier tests were done on a limited budget and believed that better funding could enable more sophisticated attacks ([Warner and Johnston, 2003](#)).

Nevertheless, Pandora's box was opened and more and more businesses and sectors were becoming reliant on the "free" GPS service, including telecommunications, financial trading, power grids, and computer systems. There were also rapid advances in computer power which were making more possible more sophisticated and simple homemade spoofing devices utilising software and crude forms of artificial intelligence (crude by today's standards but advanced at that time). Certain events, such as the malfunctioning of a satellite on New Year's Day in 2004, as well as numerous military jamming events during the Iraq and Yugoslav wars, saw the issue of jamming, spoofing, and "GPS-denial" potentialities elevated.

Amid growing concerns over hostile state actors targeting the GPS constellation, President George W. Bush issued a directive stressing the need for GPS backup systems, as it was crucial to national infrastructure, security, and the economy ([Bush Administration, 2004](#)). For the maritime industry, for example, where there were concerns about navigation without GPS, this included upgrading the Loran system to eLoran, a ground-based service with stronger signals, making simultaneous jamming of both systems harder. However, the Obama Administration ([Dong-Hui, 2010](#)) rolled back the eLoran upgrade after the financial crisis, leaving satellite navigation as the primary system for many industries.

As predicted by some of the initial researchers, by the late 2000s the technologies required to reduce the costs and complexity of making a spoofer (and knowing how to use it and being able to conceal it) became increasingly real. A software-defined radio, which could much more easily lock on to a signal, was applied to a portable and low-cost civilian GPS spoofer ([Humphreys et al., 2008](#); [Su et al., 2016](#)). In 2008, researchers from the University of Texas at Austin, in collaboration with the Cornell GPS group, made a spoofer capable of targeting civilian GPS code. The spoofer they built was able to receive live GPS signals and then replay them to the victim's GPS receivers, but with subtly introduced incorrect navigation measurements. The spoofer could overcome then-available anti-spoofing technology, called receiver autonomous integrity monitoring ([Ju, 2012](#)). In theory, the still-bulky and awkward equipment, with laptops, wires, and other components, could be miniaturised, and increasingly multiple targets as opposed to singular targets could be attacked, although they were still restricted by techno-geographical factors.

As GPS became more embedded in ever-complex systems, this similarly widened the "attack surface" as well as the motivations to jam or spoof GPS signals. This is partly because the "commercial world was heavily focused on mass-market GPS receivers—reducing cost, increasing performance—with little care about jamming" ([Jones, 2017](#)). The privacy implications of tracking information were increasingly becoming more of a concern with the widespread ownership of cell phones. Jamming for privacy reasons, for avoiding tax payments (through tolls, for example) and fraud were being documented ([Westbrook, 2019a, 2024](#)).

While jamming was causing some collateral impact in cities and near airports (causing mostly inconvenience) ([Westbrook, 2019a, 2024](#)), perhaps the most notorious spoofing-related research that elevated the issue was when researchers successfully demonstrated that it was possible to cause a drone to crash ([Kerns et al., 2014](#)) and lead a luxury yacht off its course ([Bharti and Humphreys, 2017](#)), in both cases fooling the system (drone) or the pilots (of the yacht) to correct a false deviation. This was achieved with cheap and commercially available spoofing equipment. The drone crashed and the yacht captain followed the hoax navigational information on his dashboard, leading to many different hypotheses about what an unscrupulous actor could do. Popular science research undertaken by journalists, bloggers, and ethical and grey hackers have also made the spoofing phenomenon more accessible and entertaining to various audiences ([Westbrook, 2023a](#)).

Non-state actors have long used jamming to disrupt communications. Al Qaeda used jamming in the Middle East for averting surveillance and offensive drones, boasting of such capabilities in publicised pamphlets and magazines. A spoofing threat of destructive proportions was still, nevertheless, far-fetched. It was conceived that there were, at most, one hundred people in the world who could build a spoofer that could inflict damage on a ship or plane in the early 2010s ([Milner, 2017](#)), and that the possibility of significant risk to GPS was still years away.

Government-initiated projects contributed to the accumulating work during this period. After the [Volpe \(2001\)](#) report, the US DHS and other experts released two 2012 reports on risks to US critical infrastructure from GPS disruptions, concluding that “GNSS spoofing scenarios posed the highest threat” ([US DHS, 2011](#)). Similar reports from Western governments highlighted the severe economic impacts of GPS interruptions. President Obama signed the National Defense Authorization Act in 2014, expressing concern about space system vulnerabilities ([GPS World, 2014](#)). The [Trump Administration \(2021\)](#) followed with Space Policy Directive 7, emphasising GPS resilience, while agencies like the DHS and the National Science Foundation increased grants and guidance from 2018 onward. The Biden Administration followed with key funding commitments ([Goward, 2021](#)).

The status today shows that the threat posed by non-state actors to GPS-reliant and GPS-dependent systems is both evidence- and theory-based. There are several reports indicating up to and beyond 2000% increase in RFI over previous years ([Goward, 2023](#); [Westbrook, 2024](#)). The threat actors have diversified and now include gamers, privacy seekers, quiet seekers, grey/black hats, activists, businesses, terrorists, cyber mercenaries, lone wolves, or state actors arming non-state actors with advanced electronic warfare (EW) technologies ([Westbrook, 2023a, 2024](#)). The motives and incentives have expanded as GPS has metamorphosed to include intimidation, harassment, economic damage, tax avoidance, fraud, and physical encroachments for hijackings, sanctions evasion, reconnaissance, and sabotage ([Westbrook, 2023b, 2024](#)). Spoofing and jamming strategies have also diversified, including cyber-physical encroachments, decoy tactics, and jamming-enabled crime ([Westbrook 2023a, 2024](#)). The opportunity costs are immeasurable. For example, the promising benefits of (semi-)autonomous aerial vehicles, UAV deliveries, or smart city initiatives for improved quality of life and sustainable development are arguably being held back by the electronic and cyber threat against GPS ([Westbrook 2024](#)). The lost financial and economic growth opportunities are similarly immeasurable. Although the economic and societal benefits of GPS’s ubiquity are tremendous, considerable costs and efforts have gone into the manufacture, use, and updates of countermeasures, both technological and procedural ([Westbrook, 2024](#)).

In summary, numerous government actions have followed the liberalisation of GPS, and there is considerably more knowledge about the prevalence and consequences of intentional and collateral radio interference than what was known in 2001, and the users and intentions are also now better understood. As GPS became more embedded in ever-complex systems, this similarly widened the “attack surface” as well as the motivations to jam or spoof GPS signals.

Results—The status of the RFI threat today

The accessibility of RFI devices

Spoofing devices are accessible not least because there are a number of how-to-build guides online in writing, podcasts, and via videos (with instructions of what hardware

and software are required). There are several types of spoofing equipment, including repeaters, errant signals, collateral spoofers, and targeted spoofers ([Fernández-Hernández *et al.*, 2019](#)) and the required materials and components (appropriate for certain targeted spoofing tasks) are easily accessible. These include software-defined radios (SDRs), TX (like BladeRF, HackRF, and USRP), Raspberry Pi's, and aluminium foil (to make a faraday cage), much of which can be ordered online.

User-friendly GPS simulators are used by companies to test their systems. These simulators can be used to create spoofing devices, are used by various companies to test whether their GPS receivers are available to buy or rent from suppliers without a license. The production of jammers has a niche but healthy market, driven largely by high demand from certain individuals (privacy seekers), businesses, and organisations (like theatres wanting to silence cell phones), prisons (to deny use of cell phone contraband), and diplomatic services (to prevent eavesdropping) ([Westbrook, 2019a, 2019b](#)).

The codes required to target signals are also available in online repositories like GitHub. Such guides have been published by tech hobbyists and hackers (usually following hacker conventions), and have been proven to be accurate by university researchers (albeit in some cases with slight modifications). Other materials are accessible via various hacker conventions and chat rooms. All in all, this is a vast change from over a decade ago when “malicious spoofers needed a special-purpose device coupled with high cost and high complexity in order to perform” spoofing attacks ([Jansen, 2018](#)).

The affordability of RFI devices

Spoofers and jammers are also now very cheap. The latter can cost around UAUS\$200, and the former as little as US\$50. But spoofers and jammers for certain tasks may require additional modifications that raise the price. Jammers, for example, can be made for special purposes, such as concealment, for mounting in vehicles, or inside the hood of a vehicle with battery connectors ([G4S Global, 2017](#)). Some jammers can only target one frequency whereas more sophisticated ones can target others provided by Galileo and GLONASS—the European and Russian constellations.

When we consider “time as money,” it may also require different numbers of “attackers” or accomplices to use successfully, as well as time to put the contraptions together and test them. It could be a “matter of a few days,” for example, to “completely replicate the entire GNSS satellite system transmission” with a purchased SDR (Roi Mitt in [Lo, 2019](#)). It has been argued that it “...would be something that would only takes a few hours for someone who has a little bit of experience with radio frequency work” ([Brunker, 2016](#)).

The publicised costs of certain contraptions, either purpose-built or sold in various parts, could easily have risen or fallen in price as competition, demand, inflation, etc. change (see Table 1). For example, a successful attack on a drone in 2012 cost US\$1,000. Attacking a vessel in 2013 with different equipment would cost US\$2,000. Since then, researchers have demonstrated successful attacks on drones and other systems with US\$200 devices.

It is important to note that those making spoofers were not necessarily attempting to do so with limited manpower. Nonetheless, it can be assumed that at least two individuals can make a reliable and workable spoofing device.

Table 1. Equipment and manpower required for spoofing devices over time.

Manpower	Cost of equipment
One assistant professor, two postgraduate students, or “anybody technically skilled..”	US\$1,000 UAV spoofer in 2012 (Bhatti et al., 2012 ; Noel Sharkey in BBC News, 2012).
One assistant professor and one postgraduate student	US\$2,000–\$3,000 spoofer in 2013 (Bhatti and Humphreys, 2017).
Two researchers from an Internet security company	US\$300 in 2015 (Huang and Yang, 2015).
Undisclosed number of “researchers,” including a PhD student, a professor, and security consultant	More than US\$90,000 for surface vehicle in 2016 (pzduple1 [pseudonym], 2016).
Eight researchers	US\$223 in 2018 (Zeng et al., 2018).
Four researchers	US\$600 (SDR) targeting instrument landing system in 2018 (Sathaye et al., 2019).

The usability of RFI devices

To expand on works regarding sophistication mentioned in the Introduction ([Denning, 2000](#); [Humphreys et al., 2008](#); [Ranganathan et al., 2016](#); [Shepard et al. et al., 2012](#); [Zeng et al., 2018](#)), the “unsophisticated” user, for example, is one that does not need advanced knowledge of the radio spectrum but can execute a spoofing attack with the right equipment—equipment that is “low complexity,” portable and easy to use ([Ranganathan et al., 2016](#)), using easy or accessible instructions. Different RFI devices will need actors of different levels of “sophistication.” For the purpose of this study, we focus on the simplest spoofing devices.

Given the ease of use of today’s spoofer contraptions, here we narrow them down to the typically US\$200 SDR spoofer used at hackathons. The SDRs are easily tuneable to replicate a GPS signal/code. Overall, in the space of 4 years, it was believed that the “difficulty of mounting a spoofing attack has dropped by maybe a factor of a hundred since 2012” ([Brunker, 2016](#)).

However, ease of use can of course vary by the location, tactics, and victim(s) being targeted. A single person may be able to affect multiple receivers with a jammer or collateral spoofer, but with the aid of a co-attacker, it may be easier to achieve accurate distance, trajectory of victim, and line of sight challenges if targeting a certain receiver ([Ranganathan et al., 2016](#)). If the victim has certain systemic and procedural countermeasures (alarms, detection, and back-up systems), further assistance and technical expertise may be required.

Certain types of spoofing may require more specialist “step-by-step” planning and resources in order to make the attack successful (see Table 2), and something akin to the skillset of a simple spoofer. The attacker often has to have the ability to “real-time track and synchronise with the original signals at the victim’s location.” The second step often requires the attacker to “manipulate the GPS receiver by either shifting the signals” in their arrival time or modifying the navigation messages ([Zeng et al., 2018](#)). A “smooth takeover begins by transmitting signals synchronised with the original ones and then gradually overpowering the original signal to cause the migration” ([Zeng et al., 2018](#), p. 1530). It would take a lot of skill to temporarily shift a time of arrival in real time, and introduce a time delay to induce a navigational error ([Ranganathan et al., 2016](#); [Zeng et al., 2018](#)).

Separate from the US\$200 spoofer, there are other advanced spoofers used by more “sophisticated” and motivated actors, which are more difficult to construct and use,

Table 2. Changes in cost in tandem with resources required and likelihood of use.

Year	Cost	Resources	Likelihood of malicious end-use against civilians	Academic and governmental interest
2001	Very high	Highly specialised computer science backgrounds	Low	Concept stage (disputable) and proof of concept
2008	High	Strong computer science backgrounds	Low to medium	
2012	Low	General computer science backgrounds	Medium	Evidence-based practice. Evident use “in the wild” and counter-measures
2015	Very low	Online manual, some science background, downloadable spoofing apps	High to very high	

but also more difficult for the victim to detect (Jafarnia-Jahromi *et al.*, 2012). Perhaps the most sophisticated actors and equipment are needed for “multi-antennae” attacks, otherwise known as a “sophisticated coordinated spoofing attack” (Humphreys *et al.*, 2008). These attacks utilise multiple coordinated and synchronised spoofing devices which give the attacker(s) “more freedom for the transmission of signals and [they] can send potentially different signals from various locations” (Tippenhauer *et al.*, 2011). Such attacks are “the most complex to implement and deploy, the most expensive (both in hardware costs and in developer efforts) and the hardest to defend against” (Humphreys *et al.*, 2008).

The attacker will also need to know when the spoofing has succeeded and try not to lose the lock—a skill in itself. The “takeover phase” and “post-capture control” of a spoofing attack are key phrases used to describe when a system is “hypnotised” or a person is fooled by incorrect information. Spoofing a UAV, for example, will require the attacker to specify the “UAV’s position and velocity estimates” before manipulating them (Kerns *et al.*, 2014). As for targeting a vessel, Shepard *et al.* (2012) argue that “[t]here is a point when the spoofed signals have moved more than 600 meters in position or 2 microseconds in time away from the authentic signals, [and] the receiver can be considered completely owned by the spoofer.” The attacker may also have to know the distance from him/herself to the victim and avoid misalignment between arrivals of the signal from the antennas (Tippenhauer *et al.*, 2011). Being that stealth is important, the higher the offset, the greater the likelihood that this may cause “a noticeable jump” in the victim’s reported position (Tippenhauer *et al.*, 2011, p. 10).

The transportability and concealment of RFI devices

Jammers can be barely the circumference of a cell phone, and a spoofer could be about the length and width of a pen (Zeng *et al.*, 2018), which make them easy to transport and conceal. Bulkier specialist equipment could fit into a briefcase. To improve concealability, systems can be separated into various parts and components, and reassembled later (Westbrook, 2019b). Media have also reported that a sophisticated eight-antenna jamming device was built into a suitcase (Brunker, 2016). Size matters for other reasons, too, particularly involving attacks where the spoofer or related equipment needs to be planted in the victim’s vehicle/location. These are sometimes referred to as static spoofers or “limpet spoofers.” For example, one study found that with a Raspberry Pi platform, a HackRF One SDR, a portable power source and an antenna and other components, small enough to fit in one hand and costing no less than US\$250, can be planted inside a targeted car

or operated from a following car. Bulkier and heavier spoofers can, of course, benefit by having high-power amplifiers, “which can help them generate strong spoofing signals to compromise distant receivers” ([Khan et al., 2021](#)).

The effectiveness of RFI devices

The effectiveness (or “bang for your buck”) of jammers and spoofers is ambiguous and depends on the target, motivation, and required outcomes.

But if the motivation is to achieve the seven Ds (degrade, deny, delay, deter, detect, distract, and destroy), or if it requires “covert capture” (e.g., with the user not knowing they are being fed incorrect navigation information), then certain low-cost and available spoofers could prove effective for certain tasks. Homemade spoofers can transmit on frequencies covering most of the radio spectrum used in modern technology. Even at low power levels (a minimum of 2-dB power is an advantage ([Khan et al., 2021](#), p. 22), spoofers and jammers are able to affect some commercial and widely used UAVs ([Sathyamoorthy et al., 2020](#)), which for some attackers might be enough to avert surveillance, affect emergency responders, and such. The cheapest spoofer will be able to penetrate materials like walls, and the target device will likely be able to “latch onto the false signals without losing connections” ([Zeng et al., 2018](#)). Getting more bang for your buck, attackers can use directional antennae or collateral ones depending on their intentions. If the victim is far away, they can use “antennas with wide-beam propagation patterns” ([Jansen, 2018](#)) or use a transmitter and a large amplifier on a hill top or a tall tower.

Line of sight is important, and the need to overcome physical obstructions and power lines may limit the chances of success. Two types of spoofing can be equally effective. There is measurement spoofing, which introduces “RF waveforms that cause the target receiver to produce incorrect measurements of time of arrival or frequency of arrival or their rates of change,” and data spoofing, which “introduces incorrect digital data to the target receiver for its use in processing of signals and the calculation of PNT [positioning, navigation, and timing]. Either type of spoofing can cause a range of effects, from incorrect outputs of PNT to receiver malfunction” ([US DHS, 2016](#)).

In all tests recently completed, the data in Table 3 indicates that attackers can execute a successful attack from very far away, albeit in the right conditions. Although the test on

Table 3. Successful spoofing attacks and ranges based on victim and types of spoofers (based on available research).

Type of vehicle	Range
Road vehicle	0.05 km (Zeng et al., 2018)
	1.2 km (Schneier, 2008)
	10 km (provided you have line of sight) (Bradbury, 2019 ; Regulus, 2019)
UAV	0.62 km (Kerns et al., 2014)
	0.48 km (Ju, 2012)
	20–30 km away (provided you have line of sight), or 2 km at sea (Farivar 2013 ; Bhatti et al. 2012)
Vessel	<0.01 km (onboard) (Farivar, 2013)

the vessel was onboard, at sea there is a significant opportunity to have light of sight and thus vessels can be targeted from a significant distance.

Conclusions

The literature review of the events and government actions over the years has demonstrated that non-state actors' use of jamming and spoofing technologies has conformed to some aspects of the "stress-based cyber terrorism effect" proposed by [Gross *et al.* \(2017\)](#). Through government actions, tests by researchers, and reports from "the wild," the risk perception of spoofing and jamming has increased, and confidence in GPS has been challenged in all industries, with direct and high-level references to national security. There is a strong kinetic element to electronic interference, whether an attack is an ends to means (direct kinetic) or means to ends (to enable physical attacks). Actors with some level of knowledge of the radio spectrum have also reached the level of "advanced-structured" according to [Denning's \(2000\)](#) categorisations, and this has become possible within only two decades. Within roughly 10 years, what was only possible to a handful of highly educated engineers (operating under limited conditions) has now become possible for anyone with a comprehension of the radio spectrum.

Where was the tipping point of this transition? While jamming is seen as relatively unsophisticated in most cases, between 2008 and 2015, the availability of a multipurpose, low cost, portable, and concealable spoofing device requiring one to two persons to operate became a reality. This was during a period of expansion of GPS-dependent and GPS-aided services and systems in many industries, in concurrence with the miniaturisation and versatility of software-defined radios and computer systems, such as the Raspberry PI. With the ubiquity of GPS, combined with the availability of unsophisticated (jammers) and semi-sophisticated (spoofers) systems, this has increased the likelihood of end-use, with evidence demonstrating up to and beyond a 2,000% increase in RFI in some sectors over a short period.

It is also important to emphasise that the combination of war, the expansion of digitalisation, the commercialisation of military systems, and the demand and supply that feeds technological innovations, has left us with an entirely different threat picture than in 2001. The commercialisation and hence ubiquity and variety of GNSS-aided/dependent systems has opened the attack surface for a range of potential attackers.

How the ends justify the means for spoofing and jamming, however, is deeply contextual and cannot be concluded with broad strokes. Some tactics and intentions are strategically rational for one actor and strategically unwise and devoid of general benefits for another. What \$200 RFI devices do, at least, is allow the option to choose what is "rational" in accordance with the actors' specific situation, opportunistically, and dynamically in ever-changing criminal as well as geopolitical and social landscapes.

Simply put, what has not been established is whether the potential harm they can do (and other "rewards") is sufficient to warrant the effort (motivation) for extremist groups. Indeed, terrorist groups have long been considered "conservative" in their weapon and target choices—choosing bombs, firearms, knives, and cars above all else to target people, buildings, and infrastructure. We know that groups will use the Internet to spread fear and boast of their activities, but the Internet does not have the same kinetic expression. The open-source GPS system, used by civilian actors, at least helps us identify on the likely civilian targets. However, whether spoofing and jamming may supplement more

“traditional” forms of political violence is, up to now, a theoretical question that requires further investigation.

Indeed, while anti-jamming GPS technologies have their roots in the Cold War, the market for GPS-jamming and GPS-spoofing countermeasures, including intrusion detection systems, in both military and civilian sectors, has flourished and still maintains the status quo, arguably making it increasingly difficult for criminals to keep pace without assistance and educated knowledge of the radio spectrum. Upon reflection, if innovations like this can happen within 20 years, what will 2045 look like? Indeed, as new technologies evolve through time, violent political actors will, in their asymmetrical nature, evolve too.

Funding

This research received no external funding.

Data Availability Statement

Not applicable.

Disclosure statement

No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

References

BBC News (2012) ‘Researchers use spoofing to “hack” into a flying drone’, 29 June. Available at: www.bbc.co.uk/news/technology-18643134 (Accessed: 07 November 2023).

Bhatti, J.A. and Humphreys, T.E. (2017) ‘Hostile control of ships via false GPS signals: Demonstration and detection navigation’, *Journal of the Institute of Navigation*, 64(1), pp. 51–66. doi: [10.1002/navi.183](https://doi.org/10.1002/navi.183).

Bhatti, J.A. Shepard, D.P. and Humphreys, T.E. (2012) ‘Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle’, *Aviation* (August). Available at: https://radionavlab.ae.utexas.edu/images/stories/files/papers/drone_hack_shepard.pdf (Accessed: 07 November 2023).

Bradbury, D. (2019) ‘Tesla 3 navigation system fooled with GPS spoofing’, *Naked Security*, 27 June. Available at: <https://nakedsecurity.sophos.com/2019/06/27/researchers-fool-tesla-3-navigation-system-with-gps-spoofing/> (Accessed: 07 November 2023).

Brunker, M. (2016) ‘GPS under attack as crooks, rogue workers wage electronic war’, *NBC News*, 8 August. Available at: <https://www.nbcnews.com/news/us-news/gps-under-attack-crooks-rogue-workers-wage-electronic-war-n618761> (Accessed: 07 November 2023).

Büchel, M., Schwerdtfeger, B., Pohle, R., Aust, D., Bollmann, C. and Arndt, H.J. (1999) ‘Evaluation of the high power electromagnetic pulse threat for information systems and infrastructures’, *Proceedings of the 13th International Zurich Symposium and Technical Exhibition on Electromagnetic Compatibility*, 16–18 February, Zurich, Switzerland, pp. 1–17. Available at: <https://www.tib.eu/en/search/id/TIBKAT%3A266621848/> (Accessed: 07 January 2025).

Bush Administration (2004) *NSPD-39: US space-based position, navigation, and timing policy fact sheet*, National Security Presidential Directives [NSPD], 15 December. Available at: <https://fas.org/irp/offdocs/nspd/nspd-39.htm> (Accessed: 07 November 2023).

Clarke, R.V. and Newman, G.R. (2006) *Outsmarting the terrorists*. Westport, CT: Praeger Security International.

Communication from the Commission to the European Parliament and the Council (2002) *State of progress of the Galileo programme (COM(2002) 518 final, 24/8/02)*. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52002DC0518&from=FR> (Accessed: 07 November 2023).

Cronin, A.K. (2020) *Power to the people: How open technological innovation is arming tomorrow's terrorists*. New York, NY: Oxford University Press.

Denning, D.E. (2000) 'Cyberterrorism', testimony before the special oversight panel on terrorism committee on armed services US House of Representatives, 23 May. Available via Wayback Machine at: <https://web.archive.org/web/20140310162011/http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> (Accessed: 07 November 2023).

Department of Homeland Security (2003) *The threat of radio frequency weapons to critical infrastructure facilities*. TSWG and DTEO Publication. Available at: <https://apps.dtic.mil/sti/citations/ADA593293> (Accessed: 07 January 2025).

Department of Homeland Security (2011) *National risk estimate: Risks to US critical infrastructure from global positioning system disruptions*. Available at: <https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf> (Accessed: 07 November 2023).

Department of Homeland Security (2012) *National risk estimate: Risks to US critical infrastructure from global positioning system disruptions*. Available at: <https://www.gps.gov/news/2013/06/2013-06-NRE-fact-sheet.pdf> (Accessed: 07 November 2023).

Dolnik, A. (2007) *Understanding terrorist innovation: Technology, tactics and global trends*. Abingdon: Routledge.

Dong-Hui, Y. (2010) 'Study of alternative navigation systems for GNSS in South Korea', *Journal of Information and Communication Convergence Engineering*, 8(5), pp. 524–527. doi: [10.6109/jicce.2010.8.5.524](https://doi.org/10.6109/jicce.2010.8.5.524).

Evan, T., Leverett, E., Ruffle, S., Coburn, A., Bourdeau, J., Gunaratna, R. and Ralph, D. (2017) *Cyber terrorism: assessment of the threat to insurance*. Cambridge Risk Framework Series. Cambridge: Cambridge Centre for Risk Studies, University of Cambridge.

Farivar, C. (2013) 'Professor fools \$80M superyacht's GPS receiver on the high seas', *Ars Technica*, 30 July. Available at: <https://arstechnica.com/information-technology/2013/07/professor-spoofs-80m-superyachts-gps-receiver-on-the-high-seas/> (Accessed: 07 November 2023).

Fernández-Hernández, I., Walter, T., Alexander, K., Clark, B., Châtre, E., Hegarty, C., Appel, M. and Meurer, M. (2019) 'Increasing international civil aviation resilience: A proposal for nomenclature, categorization, and treatment of new interference threats', in *Proceedings of the 2019 International Technical Meeting of the Institute of Navigation*, Reston, VA, January, pp. 389–407. doi: [10.33012/2019.16699](https://doi.org/10.33012/2019.16699).

G4S Global (2017) 'Supply chain: Defeating the security watchdog', *Corporate Risk Services, Intelligence Bulletin*. Available at: https://www.g4s.com/en-ca/-/media/g4s/canada/files/whitepapers/usa/supply_chain_defeating_the_security_watchdog.ashx?la=en&hash=7682972D229DB660B9EA9A982644AB07#:~:text=In%20July%202010%2C%20British%20police,being%20tracked%20after%20the%20thefts (Accessed: 07 November 2023).

Gerdan, G.P., Lucinda, L.J.C. and Frank, T. (1995) *The effects of RF interference, multipath and signal obstruction on the GPS observables*, Department of Land Information, Royal Melbourne Institute of Technology. Available at: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.128.4955&rep=rep1&type=pdf> (Accessed: 07 November 2023).

- Gill, P.** (2017) 'Tactical innovation and the provisional Irish Republican Army', *Studies in Conflict & Terrorism*, 40(7), pp. 573–585. doi: [10.1080/1057610X.2016.1237221](https://doi.org/10.1080/1057610X.2016.1237221).
- Giri, D.V., Hoad, R. and Sabath, F.** (2020) 'The threat of intentional electromagnetic interference (IEMI)', in Arduini, F.R. (ed.) *High-power electromagnetic effects on electronic systems*. Pan-European Training, Research and Education Network on Electromagnetic Risk Management (PETER). Available at: <https://etn-peter.eu/2021/06/22/the-threat-of-intentional-electromagnetic-interference-iemi/> (Accessed: 07 November 2023).
- Goward, D.** (2016) 'Opinion: Were US sailors "spoofed" into Iranian waters?' *The Christian Science Monitor*, 15 January. Available at: <https://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0115/Opinion-Were-US-sailors-spoofed-into-Iranian-waters> (Accessed: 07 November 2023).
- Goward, D.A.** (2021) *Averting catastrophe: Why we need to rethink GNSS vulnerability*. Available at: <https://rntfnd.org/wp-content/uploads/ION-Summer21-GOWARD.pdf> (Accessed: 07 January 2025).
- Goward, D.** (2023) 'Increasing GNSS interference: UK and EU warn aviation', *GPS World*, 11 April. Available at: <https://www.gpsworld.com/increasing-gnss-interference-uk-and-eu-warn-aviation/> (Accessed: 21 November 2024).
- GPS World** (2014) *Out in front: Complements of the season*. Available at: <https://www.gpsworld.com/out-in-front-complements-of-the-season/> (Accessed: 07 November 2023).
- Gross, M.L., Canetti, D. and Vashdi, D.R.** (2017) 'Cyberterrorism: Its effects on psychological well-being, public confidence, and political attitudes', *Journal of Cybersecurity*, 3(1), pp. 49–58. doi: [10.1093/cybsec/tyw018](https://doi.org/10.1093/cybsec/tyw018).
- Huang, L. and Yang, Q.** (2015) 'Low-cost GPS simulator—GPS spoofing by SDR', *DEFCON 23*, 7 August. Available at: <https://infocondb.org/con/def-con/def-con-23/low-cost-gps-simulator-gps-spoofing-by-sdr> (Accessed: 07 November 2023).
- Humphreys, T.E., Ledvina, B.M., Psiaki, M.L., O'Hanlon, B.W. and Kintner, P.M., Jr.** (2008) 'Assessing the spoofing threat: Development of a portable GPS civilian spoofer', in *Proceedings of ION GNSS*, The Institute of Navigation, Savannah, Georgia. Available at: https://radionavlab.ae.utexas.edu/images/stories/files/papers/ion2008r01_for_distributionW.pdf (Accessed: 07 November 2023).
- Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J. and Lachapelle, G.** (2012) 'GPS vulnerability to spoofing threats and a review of antispoofing techniques', *International Journal of Navigation and Observation*, July, pp. 1–16. doi: [10.1155/2012/127072](https://doi.org/10.1155/2012/127072).
- Jansen, K.** (2018) 'Crowd-GPS-Sec: Leveraging crowdsourcing to detect and localize GPS spoofing attacks', in *2018 IEEE Symposium on Security & Privacy*, May 21–23, San Francisco, CA. Available via YouTube at: <https://www.youtube.com/watch?v=tsrOKeIeLc> (Accessed: 07 November 2023).
- Jones, M.** (2017) 'Anti-jam technology: Demystifying the CRPA', *GPS World*, 12 April. Available at: <https://www.gpsworld.com/anti-jam-technology-demystifying-the-crpa/> (Accessed: 07 November 2023).
- Ju, A.** (2012) 'Spoofed GPS signals can be countered, researchers show', *Cornell Chronicle*, 23 July. Available at: <https://news.cornell.edu/stories/2012/07/researchers-counter-gps-spoof-attacks> (Accessed: 07 November 2023).
- Kerns, A.J., Shepard, D.P., Bhatti, J.A. and Humphreys, T.E.** (2014) 'Unmanned aircraft capture and control via GPS spoofing', *Journal of Field Robotics*, 31(4), pp. 617–636. doi: [10.1002/rob.21513](https://doi.org/10.1002/rob.21513).
- Khan, S.Z., Mohsin, M. and Iqbal, W.** (2021) 'On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions', *Peer J Computer Science*, 7, doi: [10.7717/peerj-cs.507](https://doi.org/10.7717/peerj-cs.507).

Lo, C. (2019) 'GPS spoofing: What's the risk for ship navigation?' *Ship Technology*, 15 April. Available at: <https://www.ship-technology.com/features/ship-navigation-risks/> (Accessed: 07 November 2023).

Magnuson, S. (2007) 'Bomb making skills spread globally', *National Defense*, 1 June. Available at: <https://www.nationaldefensemagazine.org/articles/2007/6/1/2007june-bomb-making-skills-spread-globally> (Accessed: 07 November 2023).

Milner, G. (2017) *Pinpoint: How GPS is changing technology, culture, and our minds*. New York, NY: Norton.

pzduple1 (Pseudonym) (2016) 'Hackers show how they tricked a Tesla into hitting objects in its path', *Business Insider*, 8 August. Available at: www.businessinsider.com/defcon-tesla-jamming-spoofing-autopilot-2016-8?r=US&IR=T (Accessed: 07 November 2023).

Ranganathan, A., Olafsdottir, H. and Capkun, S. (2016) 'SPREE: A spoofing-resistant GPS receiver', in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (MobiCom '16)*, October, pp. 348–360. doi: [10.1145/2973750.2973753](https://doi.org/10.1145/2973750.2973753).

Regulus (2019) *Tesla Model 3 spoofed off the highway—Regulus navigation system hack causes car to turn on its own*, August 4. Available at: <https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-navigation-system-hack-causes-car-to-turn-on-its-own> (Accessed: 07 November 2023).

Sathaye, H., Schepers, D., Ranganathan, A. and Noubir, G. (2019) 'Wireless attacks on aircraft instrument landing systems', *Proceedings of the 28th USENIX Security Symposium*, August 14–16, Santa Clara, CA, pp. 375–372. Available at: <https://www.usenix.org/system/files/sec19-sathaye.pdf> (Accessed: 07 November 2023).

Sathyamoorthy, D., Amin, Z.F.M., Selamat, E., Hassan, S.A., Kazmar, A.F.A. and Zaimy, Z. (2020) 'Evaluation of the vulnerabilities of unmanned aerial vehicles (UAVs) to global positioning system (GPS) jamming and spoofing', *Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia*. Available via ResearchGate at: https://www.researchgate.net/publication/345150887_EVALUATION_OF_THE_VULNERABILITIES_OF_UNMANNED_AERIAL_VEHICLES_UAVS_TO_GLOBAL_POSITIONING_SYSTEM_GPS_JAMMING_AND_SPOOFING (Accessed: 07 November 2023).

Schneier, B. (2008) 'GPS spoofing', *Schneier on Security*, September 17. Available at: https://www.schneier.com/blog/archives/2008/09/gps_spoofing.html (Accessed: 07 November 2023).

Shepard, D., Wesson, K. and Humphreys, T.E. (2012) 'Straight talk on anti-spoofing: Securing the future of PNT', *GPS World*, pp. 32–63. Available at: https://radionavlab.ae.utexas.edu/images/stories/files/papers/antiS-pooofStraightTalk_Wesson.pdf (Accessed: 07 November 2023).

Su, J., He, J., Cheng, P. and Chen, J. (2016) 'A stealthy GPS spoofing strategy for manipulating the trajectory of an unmanned aerial vehicle', *IFAC-Papers*, 49(22), pp. 291–296. doi: [10.1016/j.ifacol.2016.10.412](https://doi.org/10.1016/j.ifacol.2016.10.412).

Tippenhauer, N.O., Pöpper, C., Rasmussen, K.B. and Capkun, S. (2011) 'On the requirements for successful GPS spoofing attacks', in *Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS '11)*, 17–21 October, Chicago, IL. Available at: <https://www.cs.ox.ac.uk/files/6489/gps.pdf> (Accessed: 07 November 2023).

Trump Administration (2021) *Space Policy Directive 7—The United States space-based positioning, navigation, and timing policy*. 15 January. Available at: www.govinfo.gov/content/pkg/DCPD-202100025/pdf/DCPD-202100025.pdf (Accessed: 07 November 2023).

US DHS (2016) *Improving the operation and development of Global Positioning System (GPS) equipment used by critical infrastructure*. National Cybersecurity & Communications Integration Center and National

Coordinating Center for Communications, pp. 1–21. Available at: <https://www.dhs.gov/science-and-technology/pnt-program> (Accessed: 07 January 2025).

US Foreign Affairs, Defense, and Trade Division (2008) *High altitude electromagnetic pulse (HEMP) and high power microwave (HPM) devices: Threat assessments*, Document No. 14, 26 March. Available at: https://www.wired.com/images_blogs/dangerroom/files/Ebomb.pdf (Accessed: 07 November 2023).

Volpe, J.A. (2001) *Vulnerability assessment of the transportation infrastructure relying on the global positioning system*, National Transportation Systems Center, Office of the Assistant Secretary for Transportation Policy, US Department of Transportation. Available at: https://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf (Accessed: 07 November 2023).

Warner, J.S. and Johnston, R.G. (2003) 'GPS spoofing countermeasures', *Homeland Security Journal*, 25(2), pp. 19–27. Available at: <https://www.semanticscholar.org/paper/GPS-Spoofing-Countermeasures-Warner-Johnston/36e17f723bff8d429aca4714abe54500a9edaa49> (Accessed: 07 November 2023).

Weimann, G. (2004) *Cyberterrorism: How real is the threat?*, Special Report 119, United States Institute for Peace, December, pp. 1–12. Available at: <https://www.usip.org/sites/default/files/sr119.pdf> (Accessed: 07 November 2023).

Westbrook, T. (2019a) 'Will GPS jammers proliferate in the smart city?', *Salus Journal*, 7(2), pp. 45–67. Available at: <https://view.salusjournal.com/article/view/102/96> (Accessed: 07 November 2023).

Westbrook, T. (2019b) 'The global positioning system and military jamming: The geographies of electronic warfare', *Journal of Strategic Security*, 12(2), pp. 1–16. doi: [10.5038/1944-0472.12.2.1720](https://doi.org/10.5038/1944-0472.12.2.1720).

Westbrook, T. (2023a) 'A taxonomy of radiofrequency jamming and spoofing strategies and criminal motives', *Journal of Strategic Security*, 16(2), pp. 68–80. doi: [10.5038/1944-0472.16.2.2081](https://doi.org/10.5038/1944-0472.16.2.2081).

Westbrook, T. (2023b) 'Radiofrequency interference strategies targeting marine navigation systems: Political motives and consequences', *Journal of Baltic Security*, 9(1), pp. 1–28. doi: [10.57767/jobs_2023_003](https://doi.org/10.57767/jobs_2023_003).

Westbrook, T. (2023c) 'Trojan spoofing: A threat to critical infrastructure', *Security and Defence Quarterly*, 42(2), pp. 1–15. doi: [10.35467/sdq/164760](https://doi.org/10.35467/sdq/164760).

Westbrook, T. (2024) 'Aircraft vulnerability to politically motivated radiofrequency interference (RFI) in Eastern Europe', *Security and Defence Quarterly*, 46(2), pp. 104–117. doi: [10.35467/sdq/178249](https://doi.org/10.35467/sdq/178249).

Zeng, K., Liu, S., Shu, Y., Wang, D., Li, H., Dou, Y., Wang, G. and Yang, Y. (2018) 'All your GPS are belong to us: Towards stealthy manipulation of road navigation systems', *Proceedings of the 27th USENIX Conference on Security Symposium*, August, pp. 1527–1544. doi: [10.5555/3277203.3277318](https://doi.org/10.5555/3277203.3277318).