SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Trojan spoofing: A threat to critical infrastructure

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 explores the phenomenon of location spoofing—where the spoofer is able to "teleport" systems in and out of defined locations, either for the purpose of infiltration into no-go zones or for the "teleportation" out of real, defined zones in the physical world. The research relied on a qualitative methodology, utilising academic research findings, media reports, hacker demonstrations, and secondary data from these sources, to situate the spoofing threat in the context of international security. This conceptual, argumentative essay finds that signal spoofing, the methods of which can be followed via online scripts, allows users the ability to overcome geographically defined territorial restrictions. This, as this article finds, allows violent actors to weaponise systems, such as unmanned aerial systems, potentially leading to the escalation of political tensions in extreme but unfortunately ever-frequent episodes. The article concludes that, while Trojan spoofing (in particular) poses a real and an existential threat to international security, it is only a sum-of-all parts in considering other threats to critical functions in society. If geofences are used as a single point of security to protect assets against hostile actors, managers need to be aware of the vulnerability of intrusion and the resulting geopolitical consequences.

Keywords:

global positioning system, military deception, information warfare, unmanned aerial systems

Article info
Received: 2 December 2022
Revised: 11 April 2023
Accepted: 27 April 2023
Available online: 21 May 2023

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

Introduction

Criminals and violent actors are increasingly finding ways to overcome the physical and digital security defences intended to limit their target choices. Increasingly, we see actors turning to the cyber domain to enable infiltration to obtain information and to enable physical access to secured locations. Whilst most cyber-enabled intrusions require a certain level of knowledge, sophistication, and motivation to carry out successfully, there are many seemingly "unsophisticated" ways in which cyber tools can complement physical crimes that are accessible, easy to use, and potentially damaging to societies.

Spoofing is one of many ways in which a criminal or, arguably worse, violent extremists, can expand their target choices for financial or political or ideological gains. Signal (Global Navigation Satellite System [GNSS]) spoofing is an attack using the electromagnetic spectrum to alter the time, trajectory, and/or positional data of the system with the intention to deceive the system, or a user of that system, to make a choice or action that might be favourable to the attacker.

From financial, aviation, maritime sectors, transportation, and energy infrastructures, many systems nowadays rely on precise positional and timing information from multiple orbiting satellites. The Global Positioning System (GPS) is one of a small number of satellite constellations, part of the GNSS, that provide free and accurate but insecure signals allowing civilian users, including businesses, critical infrastructures, and individual users, to enjoy its benefits. Beyond its military utility (the signals used with which are encrypted), it provides huge economic benefits, greater efficiency, and better use of resources in societies around the world.

Despite its vulnerability to manipulation, particularly from jamming, GNSS is used for a number of safety- and security-critical applications that are vulnerable to exploitation, some of which are wholly dependent on GNSS as well as others only partially aided by it. Whilst there are specific threats that might manifest as a result of time spoofing, the opportunities for malign actors to manipulate location or positional data are a concerning variable worthy of dedicated attention. What makes matters worse is that many online repositories, video demonstrations, step-by-step guides, and spoofing applications are available and accessible to anyone.

There has been an expanse of research dedicated to the weaponisation of autonomous and semi-autonomous systems by non-state actors and their cyber vulnerabilities (for example, Almohammad and Speckhard, 2017; Bhatti *et al.*, 2012; Hoenig, 2014; Huang and Yang, 2015; Jafarnia-Jahromi *et al.*, 2012; Kerns *et al.*, 2014; Sathyamoorthy *et al.*, 2020; Westbrook, 2023). Whilst many drone attacks have created serious causes for concern, cyberattacks *against* drones have been described as largely inconsequential geopolitically, beyond highlighting state and non-state actor cyber capability, and the consequences for that cyber manipulation, including eavesdropping, surveillance, and reverse engineering of secret military technology (Almohammad and Speckhard, 2017). Most cyberattacks against surface vehicles have been undertaken by grey or black hat hackers, without intentionally targeting individuals, but instead for financial reward and revealing vulnerabilities for the common good (see, for example, Bradbury, 2019; Greenberg, 2016; Help Net Security, 2019; Mu, 2014; Posky, 2019; pzdupe1 (Pseudonym), 2016; Regulus, 2018, 2019; Stokel-Walker, 2019).

There are very few examples of cyberattacks on drones that have led to military confrontations between adversaries (Almohammad and Speckhard, 2017; Westbrook, 2019). This is due to the fact that the impacts of cyberattacks have been seen as end in themselves,

that is, online-to-online attacks; not as means-to-ends, that is, understood from the perspective of the physical manifestations—destruction of property to huge geopolitical consequences—that may result following the specific tactical manipulation of cyber-physical systems. Where this article fills a gap in knowledge is drawing attention to such physical manifestations and geopolitical consequences that might arise, particularly considering Iran, Russia, and America's actions in recent years, and how Trojan spoofing, in particular, as a sum-of-parts in terms of many different threats, plays a part in this.

Research question, methodology, and article structure

The primary research questions that this article seeks to answer are as follows: (1) To what extent can the identified spoofing strategies be used to endanger life and target critical infrastructure? and (2) what could be the consequences for international security?

Focussing on the vulnerabilities of systems and locations, the research involved an analysis of mostly academic research on spoofing as well as white/grey/black hat demonstrations, media reports, and secondary sources from these texts. The objective was to define specific spoofing tactics and strategies, with Trojan and Exposure spoofing being identified as two similar threats requiring further analysis and contextualisation (Westbrook, 2023). The results are expressed by way of a review of real and hypothetical examples of where Trojan and Exposure spoofing have been used. The data were analysed from the perspective of identified vulnerabilities of GNSS-dependent or GNSS-reliant systems, and further hypothesising of the consequences in light of previous and contemporary geopolitical events.

The article is structured as follows: It situates the concept of military deception in the context of location spoofing, considering location "teleportation" as a useful analogy in considering the possibilities of an attacker infiltrating digital zones—namely geofences—for the purpose of illegal or lethal activity. In defining what geofences are, it explores its importance for security despite its susceptibility to location spoofing. Having identified the vulnerability of geofences, it then explores the concept of Trojan spoofing, identifying real and hypothetical scenarios within which Trojan spoofing has been used or at least considered to infiltrate geofenced zones. Thereafter, the concept of Exposure spoofing is explored, considering how, based on evidence, it could put people (rather than critical infrastructure) in danger. A discussion of the underlying foundations determining the threat picture is explored, with the Persian Gulf Crisis (2019–2021) and the Russian invasion of Ukraine (2022–) being considered examples of the utility of weaponising drones, and politically incendiary consequences for international security. In the conclusion, I argue that whilst Trojan and Exposure spoofing are concerning threats that can be followed using online scripts, it still requires a certain degree of sophistication, planning, and motivation to use effectively. It is still questionable whether they would be a replacement for other seemingly "easier" ways of attacking critical infrastructure.

Military Deception

Distributed denial-of-service attacks, ransomware, and various means of deception and deceit are serious calamities for many different businesses and critical infrastructure managers from cyberattackers. Deception as a means of gaining access to information or misleading someone into taking an action that favours an attacker is one of the numerous problems encountered by many individuals, businesses, and critical sectors. As for military tactics, this is understood within the sphere of military deception, or information

warfare, using communicative deception to protect ourselves and endanger others for our own absolute or relative gains. Here, digitisation and commercialisation of the radio spectrum blurs the lines between (dis-)information warfare, political violence, and criminality. There is now in society a fusion between classical military tactics and new and emerging cyber-criminal activity.

When it comes to GNSS spoofing, it is difficult to conceive how, aside from its ability to deny service to users by degrading their ability to use locational/positional data, it can be used beyond a measure to merely inconvenience, rather than threaten lives, livelihoods, and international order.

Teleportation (or time travel) sounds like something out of a science fiction book that contradicts the laws of physics. But there are forms of "teleportation" that does not mean the transfer of matter or energy, but rather the transfer of "information" that digitally makes physical matter "disappear" from its factual place of being. Compatible with the philosophy of "mind-body dualism," the transfer of "conscious matter" whilst keeping the physical matter in its true location, or indeed deceiving digital systems to believe visible matter is *not there*, is comparable with this analogy. In engineering disciplines, this is often known as an "outlier."

There is something "science fiction" about spoofing and the digital world we live in. The metaphor of teleportation (the instant transportation across space and distance) or time travel (the movement between different points in time) is not perfect, but the spoofing of GNSS timestamps affects the position and velocity information in a physical system, ultimately making locational information falsified. One source describes the deceptive tactics of the West African Rubber Frog as "a form of spoofing, or false data, attack." The frog "secretes a pheromone that prevents the normally aggressive stinging ant *paltothyreus tarsatus* from attacking it. The frog then lives inside the ant colony during the dry season, reaping the benefits of the nest's humidity and protection from prey" (Scharre, 2015). The courageous "infiltration" of the West African Rubber Frog, the pheromone of which is representative of the falsified time-location information, is the closest analogy to what this research identifies, notably Trojan and Exposure spoofing, which I explain in detail in the following sections.

Achieving Trojan and Exposure spoofing, however, is more about infiltrating "invisible territories" than territories and boundaries that are physically, culturally, legally, or politically defined, like state borders. These visible, invisible, and "imagined" territories overlap, but it is the *invisible* ones that have not been fully explored from a security and safety perspective in academic scholarship. In order to explore this further, there is a need to explain precisely what geofences—as "invisible zones"—are, and how and why they might be evaded via spoofing.

Geofences

Geofences use global navigation satellite signals or Radio Frequency Identification technology to create virtual geographic boundaries that regulate anything from altitude, speed, and access for unmanned aerial systems (UAS) and land-based systems like connected or semi-automated road vehicles and e-scooters. With the proliferation of smartphones and telematics, we see sectors, such as retail, logistics, automotive, marketing, gaming, and other industries using geofences.

Many businesses, like logistics companies and banks, use geofencing to track their assets for the purpose of monitoring their cargo entering and leaving designated areas, for example. Many other companies use geofences to gather big data for proximity marketing and use

this data to interpret consumer behaviours. In the autonomous vehicle industries, geofences are already widely deployed to control and restrict access for UAS (near airports and power stations, for example). Likewise, controlling speed and access restrictions for e-scooter users swooshing around cities like Stockholm and Amsterdam would not be possible without geofencing. Some companies geofence their own fleets of hybrid vehicles by making them switch between fossil fuels (e.g. on highways) and cleaner fuels (e.g. in residential areas). Geofences are limited to the systems and frequencies that have been registered.

Geofencing has even been considered as a tool to protect high-risk areas from marauding terrorist attacks. Following a vehicle ramming attack in Stockholm in April 2017, during which a stolen van was used to mow down pedestrians on a busy shopping street, the Swedish government announced that it was exploring the introduction of geofence technology in urban areas in collaboration with vehicle manufacturers Scania and Volvo (Government Office of Sweden, Ministry of Enterprise and Innovation, 2017). One idea behind the initiative is to create "no-drive" zones or enforce mandatory speed limits for vehicles accessing certain areas, thus limiting their opportunities to gather speed. Similarly, following vehicle attacks in Westminster (in March 2017), London Bridge, and Finsbury Park (both in June 2017) in the United Kingdom, research was carried out by the UK Department for Transport to determine whether devices can shut down vehicles when they have been hijacked (Israel's Homeland Security (iHLS), 2020). Similar to Swedish tests, the UK-based Trak Global Group was looking at how telematics, or black box-style devices, can be linked with driver ID mechanisms, such as a smartphone, "disabling the vehicle if the phone is not present" and alerting "emergency services in the event of a hijacking or vehicle theft" (iHLS, 2020).

Thus, the opportunities for creating invisible zones to control autonomous systems, including weaponised UAS, for security and safety purposes are numerous, and the industry for it is steadily increasing (Market Watch, 2022). It is likely to accelerate further following the COVID-19 pandemic, which has highlighted the need for tracking and geolocation tools to limit the spread of infections and isolate those infected.

As for aerial systems, a drone flyer would be unable to fly in some geofenced zones (like airports or prisons) for obvious reasons. Altitude zones likewise restrict UAS to fly at heights that might endanger aircraft or infringe on people's privacy, for example, preventing UAS from flying over gardens. Other "no-drone zones" or less-restrictive "some-drone zones" (for inspection work or emergency situations) might be placed near schools, over electricity pylons, highways, and so forth. Some geofences can be requested, or removed, by site managers and drone operators at request. Many geofences around critical infrastructure are not removable.

Perhaps due to the implementation of geofences (as well as their relatively low levels of consumption and use), the number of deaths and injury caused by UAS is extremely minor compared with land vehicles. But there are no open-source data to tell us whether geofencing has improved overall safety and security in high-risk areas. We can postulate, however, that without geofencing, a "free-for-all" anarchic airspace would likely lead to some serious and undesirable problems, and if UAS can be easily spoofed so that they can fly in restricted areas (Trojan spoofing), this is similarly worrying.

Trojan Spoofing

Trojan spoofing allows manned or autonomous vehicles to enter restricted (geofenced) areas by making the autonomous system believe—based on false position information—it is in an unrestricted location, thus overcoming the *real* area restrictions.

Trojan spoofing is a tactic intended to trick a system (drone, car, or ship) to believe that it is somewhere else. Encroaching geofenced areas may not even require spoofing. The operator could make their own drone from scratch or remove the geofencing software (installed in most commercial unmanned aerial vehicles [UAVs]), or fly the UAS manually (albeit with some difficulty). "Insiders" with special access, for example, in airports, could also use UAS in "some-drone zones" without the usual restrictions to fly in hazardous areas, as might have been the case at Gatwick Airport, UK, in December 2018, leading to hundreds of cancelled flights (Rowlatt, 2019). Recently, Russian nationals have been banned from using drones in Norway following several incidents in which drones were flown around critical infrastructure in the country (Soni, 2022). The accusation of China using "spy balloons" over North America in 2023 also demonstrates the potential utility of aerial systems to surveil critical infrastructure.

There are numerous examples of hobbyists, activists, journalists, paparazzi, criminals, and violent organisations using UAS to enter "restricted zones"—zones that are defined in the legal, social, military, and political sense, but of which is not clear in the "invisible" sense (geofenced). The most serious examples being for reconnaissance and surveillance of nuclear facilities, smuggling contraband to prisoners, smuggling drugs over national borders, for propaganda purposes, or weaponising them with chemical, biological, radiological, and explosive materials (G4S, 2020). There is thus high interest for utilising UAS for political, financial, and strategic reasons. Indeed, in 2019, an "investigative report by the Russian independent media group 'The Project' into luxury dachas owned by high-ranking government officials revealed that almost all included [signal] jammers among their amenities. Attempts by the journalists to photograph the dachas from the air using drones were routinely foiled by jamming" (Goward, 2019; Zholobova, 2019). Prisons around the world use geofencing and jamming to stop contraband being smuggled in via the use of UAS (Link, 2022).

Whilst geofencing has made it more difficult for those with commercial UAS to enter restricted zones, it is still possible to do this easily and cheaply with spoofing equipment. In 2015, researchers from China's Qihoo demonstrated "Trojan spoofing" by "using the free and open source GNU radio, amongst other tools, to alter the GPS coordinates on a DJI Phantom 3" (Brewster, 2015). Researcher Qing Yang said that "any hackers wanting to land a DJI [a China-based manufacturer and distributor of UAS] or other drone on Obama's lawn, or into other no-fly zones, can send spoof signals that would make it seem the UAV was in a safe zone" (Huang and Yang, 2015). What was apparently concerning was that the researchers did not need physical access to the drone, and that the Phantom drone in question was of the upper-end of secure UAS for the period (Tucker, 2015).

Similar tricks are shown by enthusiasts on social media and video-sharing platforms, and the methods are openly shared in hobbyist chat rooms and websites for people annoyed with what they deem to be arbitrary and excessive zoning of anywhere that appears remotely hazardous or asocial. A green open space miles away from an airport might be geofenced because it is at the edge of a possible alternative landing approach zone (which is never used other than in exceptional circumstances)—information of which is not readily apparent to the hobbyist.

More serious examples can be found when we look at possible cases of Trojan spoofing in conflict zones, where terrorists/insurgents/rebels have either utilised civilian UAS, made their own, or been assisted in some way by a sympathetic state actor. Indeed, major manufacturers and distributors of civilian zones, like DJI, geofence their UAS so that they disable them from being used by assailants in conflict zones like Iraq and Syria. This, however, has not eliminated the consistent surveillance and weaponisation of UAS.

Indeed, UAS give terrorists—like their adversaries—the range the required to operate from great distances.

In January 2018, insurgents/terrorists attacked a Russian military base Khmeimim in Syria with 13 commerical, fixed-wing UAVs laden with "explosive fragmentation munitions" with pre-programmed [GNSS] flight path coordinates. The UAS were reportedly "all launched from the same location about 96 km away" (C4AS, 2019; Ministry of Defence of the Russian Federation, 2018). The insurgents/terrorists either removed the geofencing software for their "homemade drones" and/or spoofed their locations. The "swarm attack" largely failed, however. The UAS were jammed, captured, or shot down, with no known casualties. The Khmeimim airbase, built by Russia in 2015 near the port city of Latakia, is 85 km north of Tartus and 50 km from the Turkish border. Reportedly, but unconfirmed, the insurgents/terrorists were based near the Turkish border (Strategy Page, 2019).

It is disputable whether Houthi rebels or Iran attacked the Abqaiq–Khurais Saudi oil installations in 2019 this way, temporarily cutting Saudi Arabia's oil production by half and creating a knock-on effect on global markets (and coincidentally, triggering the Persian Gulf Crisis, of which the British-flagged vessel *Stena Impero* might have been spoofed and captured by Iran [BBC, 2019]). Indeed, after the attack, reportedly involving more or less a dozen UAS and missiles flying southwards from the direction of Iran, a Houthi leader boasted that they "built their drones in order to avoid [the Saudi defence system, and their] defense system failed to even spot our drones" (VoV News, 2019). Senior officials from affected countries, including the United States (whose homemade defence system was bypassed), pointed the finger at Iran. There are many different reasons suggested as to why the defences—including missile defence systems—were overcome. One suggestion is that the UAS flew low enough to avoid detection. Trojan spoofing is only one of many possibilities. Iran has proven to be capable of spoofing military drones to enable capture or for the justification for armed confrontation without provoking armed responses. In two known cases of Iran spoofing US drones, on both occasions an armed response was considered at higher levels in the United States (Adde, 2021; Kelley and Cenciotti, 2012; Westbrook, 2019).

What is worrying, though, is that such an attack can be easily replicated in geofenced areas with more accessible UAS without state assistance: targeting cities, sports stadiums, airports, and so forth. Indeed, Osama bin Laden allegedly considered attacking G8 Summit leaders in 2001 using UAS with explosives; another Al-Qaeda terrorist planned to attack the House of Commons with Anthrax (2002); Hamas and other groups have plotted and attempted to attack Israeli civilians with UAS; and the Islamic State, who have used commercial UAS at scale in Iraq and Syria (Warrick, 2017), encouraged its supporters to attack the Rio Olympics in 2016 this way; ten plotters were arrested (G4S, 2020).

Indeed, in 2010, in a classified report, the CIA noted "that al-Qaeda was placing special emphasis on the recruitment of technicians and that 'the skills most in demand' included expertise in drones and missile technology" (Whitlock and Gellman, 2013). Whilst focusing more on evasion than overcoming virtual fences, the eagerness to recruit technicians and computer scientists shows the potential in finding ways to overcome drone defences. Abandoned Al-Qaeda documents has indicated that the Russian SkyGrabber software, Russian "Rascal" devices, and self-tuning Wave Bubble jamming and spoofing technologies, among others, have been suggested to be used to target aerial systems (Associated Press, 2011).

For targeting individuals, current research shies away from proclaiming that groups will "take over" UAS and use them to target high-profile individuals. It is most likely that

they would use their own UAS laden with lethal materials, fly them "old school" without GNSS guidance, and/or remove the geofence software. Assuming that geofencing might not be used, where the risks are disproportionate to the threat or location, or likely where interferences would affect too many bystanders, they could simply fly them with planned GNSS coordinates, and manually take charge at the point of need.

Indeed, in 1994, Aum Shinrikyo attempted but failed to attack a rival spiritual leader using a remote-controlled helicopter, which was designed to spray sarin gas (Bunker, 2015). Unknown individuals were able to fly a drone with trace amounts of radiation on the roof of Japan's former Prime Minister Shinzo Abe's official residence in 2015. Activists from a rival political party were able to fly a drone within feet of Germany's former Chancellor Angela Merkel at a campaign rally event in September 2013 (Lee, 2013). In August 2018, two explosives-laded GNSS-guided UAS were used in a failed attempt to assassinate Venezuelan President Maduro during a military parade (Watson, 2018). Seven people were reportedly injured. Madura blamed it on the "Venezuelan ultra-right in alliance with the Colombian ultra-right" (Daniels, 2018). Russia blamed Ukraine for an 'attempted assassination' on Russian President Vladimir Putin using explosive-laden drones targeting the rigorously defended (including geofenced) Kremlin complex in May 2023 (BBC News, 2023). The attack, however, has been described as staged by some commentators (Gozzi, 2023).

These "successful" events are few among many foiled plots. In 2012, a man plotted to use a large remote-controlled model aircraft filled with plastic explosives to attack the Pentagon and Capitol Building (United States Government Accountability Office, 2012, p. 30). It is thus clearly more favourable to manually fly—rather than "take over"—UAS to target high-profile individuals. In the present conflict in Ukraine, the deployment of "kamikaze" or "tactical drones" intended to crash into their targets (Hambling, 2022), shows the fusion between military and insurgency thinking. The notorious US-made Switchblade is, for example, GNSS-guided.

Another worrying issue is intentionally spoofing a system—manned or unmanned—to expose people to certain dangers, rather than using spoofing to access restricted zones. The "dislocation" is where the concept Exposure spoofing comes into consideration.

Exposure Spoofing

As many systems are dependent on geographical triggers like geofences, Exposure spoofing is something that is also worthy of attention. Exposure spoofing is intentionally exposing a victim to hazards by falsely positioning them in geographically defined areas that would trigger an automatic system to adjust itself to its (false) surroundings. Examples include making a motor vehicle automatically adjust to a higher suspension on a highway (as tests on older models of Tesla and Jeep models have shown) or, more seriously, making a commercial airplane adjust its wing dynamics too late off a runway (based on known instances of malfunctions). Referring to the former, tests on modern road vehicles have confirmed that this could be achieved, but the means-ends outcomes for today's violent organisations are not obvious. It is more likely that Exposure spoofing will be used for "nonviolent" means, including unlocking doors to valuable cargo in faked zones (spoofing-enabled crime), as demonstrated by organised criminal gangs in South America. But this does not mean that "spoof-to-kill" intentions are eliminated. As mentioned, geofencing is a growing and versatile industry that is used for many applications, providing security, convenience, and efficiency for many users. There is a difference to be drawn between the act of spoofing to draw someone into a false sense of security (a form

of deception) and spoofing that exploits automatic systems to adjust to a false location (Exposure spoofing).

Geofencing in some land vehicles is used for speed adaptation purposes. A vehicle using a mandatory intelligent speed adaptation system might use GNSS to regulate its speed between, say, a 30-mph road and 70-mph road. This presents a serious problem if we imagine that a system can be manipulated to believe that it is in the latter zone when actually it is in the former (or indeed the reverse.) Other onboard systems may also be manipulated to put the driver and passengers at risk. For example, systems, such as hands-free lane guidance, lane centring, or automatic lane changing, currently use cameras to detect road lines and other markings and, in 2019, researchers showed that it was possible to deceive these systems using fake road stickers (Stokel-Walker, 2019). While GNSS spoofing has not been tested in this way, it is not difficult to imagine a scenario where road users are put at risk by a car made to believe that it is driving on the wrong side of the road.

For further context, the Israeli company Regulus undertook tests on a Tesla 3 vehicle in 2019, and revealed "a link between the car's navigation and air suspension systems." Their spoofing test demonstrated that height of the car could change "unexpectedly while moving because the suspension system 'thought' it was driving through various locations during the test, either on smooth roadways, when the car was lowered for greater aerodynamics, or 'off-road' streets, which would activate the car elevating its undercarriage to avoid any obstacles on the road" (HelpNet Security, 2019). At face value, this does not appear to be too hazardous a situation (as Tesla stated in response, among other rebuttals [HelpNet Security, 2019]), but if there are any other links between navigation systems and other systems there is reason to be concerned, according to Regulus. This includes the possibility of a vehicle failing to slow down before intersections, braking on main road thinking an intersection is close, to reporting a wrong SOS location in the event of accidents/collisions (Zangvil, 2019). Given these examples, perhaps the proposed no-drive zones used for counterterrorism purposes by Swedish and UK authorities, could be overcome via GNSS spoofing. It really depends whether access/speed restrictions are dependent on GNSS or not.

On the other hand, whilst you can spoof the location of a drone to enter restricted geofenced zones (Trojan spoofing), you can do the reverse—to spoof to make a drone believe it is in a no-fly zone—as a denial of service (DoS) attack. The aforementioned Qihoo researchers demonstrated in a video how you can force a drone to crash land via "Exposure spoofing." The researchers made the drone crash land when it reached the spoofed zone. Russia has consistently used spoofing as a form of DoS as an anti-drone measure for such purposes (C4ADS, 2019).

Indeed, this kind of DoS spoofing can be used for defensive reasons. In and around the Kremlin in Russia, GNSS users—cab drivers, tourists, and the like—find that their digital maps show them at the nearest (geofenced) airport, and not strolling around the cobbled streets of Red Square. The spoofing used at the Kremlin complex is thought to be an anti-drone measure, but the illicit use of this method could be especially dangerous if people are underneath flying UAS, or if the UAS are directed into flight paths or instructed to land in hazardous areas (a motorway, for example).

Whilst Exposure spoofing can put those *in* (semi-)autonomous land vehicles and *underneath* UAVs in danger, what about other vehicles? Exposure spoofing can similarly be targeted at a vessel's control systems and to trick the pilots and crew, or indeed the autopilot. Exposure spoofing could, for example, cause a ship to deviate from its desired trajectory and make the (auto)pilot believe it has plenty of clearance under the keel due to the spoofed location (Farivar, 2013).

Whilst minor incidents daily occur in aerial and maritime industries, many of which are quickly resolved without any issue, a combination of other factors could increase the risks and hazards. Mild sickness, tiredness, boredom, inattention, inexperience, intoxication, the "map must be wrong" disbelief, and many other factors can make the issue worse. A combination of trickery and naivety, much like a pickpocketer's magic show, could lead to serious consequences.

A Threat to International Security?

The two primary research questions that this article sought to answer are as follows: (1) To what extent can the identified spoofing strategies be used to endanger life and target critical infrastructure? and (2) what might be the consequences for international security?

Although the present research was confined to a literature review of academic findings, media, and secondary sources, the concept of Trojan spoofing, in particular, should be taken seriously in light of the present and possible future conflicts. The threat of Trojan spoofing relies upon some underlying foundations determining the threat picture. Firstly, the more physical and hardened defences we have in place, the more actors will increasingly turn to the cyber domain to overcome such barriers. Using drones and cyberattacks lessens the risk of capture or killing of the attacker. Secondly, systems or assets dependent upon, or primarily aided by, GNSS are especially vulnerable to exploitation, and infrastructure managers using geofencing as a single source of security to control drones (or indeed any other aerial, land, or marine system), without additional detection, deterrence, and response controls, are neglecting this possibility and the range of potential "threat actors"—including hobbyists, activists, criminals, terrorists, or indeed rogue states. Thirdly, for purposes, such as hostile vehicle mitigation for surface vehicles, there are many other scenarios with which Trojan spoofing could apply. Fourthly, and importantly, the overriding assumption in contemporary literature is that the impact of cyberattacks, analysed as ends-in-themselves, not means-to-ends, leans on the side of an "inconvenience" measure of impact. This overlooks the potential cyber-physical manifestations resulting from the cyber event, and the intangible, often immeasurable, geopolitical consequences that might arise. Although the resulting consequences of Trojan and Exposure spoofing will probably cause inconvenience as well as financial impact, it could hypothetically do much worse.

Indeed, the consequences from the previous, mostly hypothetical, events are to an extent "measurable" based on the observable geopolitical impacts. The knock-on effects of the Persian Gulf Crisis, including the escalation, and actual military confrontation, notably between the United States and Iran during Donald Trump's presidency, and the resulting increased militarisation in the Middle East, and threat of seizure and attacks against merchant shipping in the Gulf of Oman and Strait of Hormuz, show that one single event could exacerbate tensions in already precarious and globally vital regions. In light of Russia's unprovoked invasion of Ukraine, and its activities surveilling, and possibly targeting, critical infrastructure in Europe, UAS provide the reach needed to get access to critical infrastructures.

Conclusions

The world is increasingly being defined by invisible zones and digital leashes that distort the normative perceptions of location, territory, and (in)accessible space.

Satellite navigation systems and those territorial cartographers of polygons—corporations, government institutions, and critical infrastructure managers—lay the laws of access in the invisible space for obvious safety and security reasons. That invisible space only becomes visible to those who look hard enough and want to overcome it. The examples in this article have focused on non-military GNSS-dependent and GNSS-aided systems that could be directly *displaced* by spoofing device, but also means by which this displacement enables encroachments into these invisible spaces via means-to-end spoofing. This, worryingly, means that "hardened" areas are not safe, particularly from a drone threat. Both Trojan and Exposure spoofing gives undesirable actors a plethora of—sometimes "near" and "easy"—target choices that might otherwise be unreachable without deploying cyber or electronic tools.

But the reality is that neither is equally attractive as a weapon of choice. The weaponisation of UAS is something that is significantly growing in both modern warfare and terrorist operations. Trojan spoofing UAS has the potential to do the dirty deeds of death and physical destruction on targets that have significant economic, political, iconic, and symbolic attractiveness, with the potential of creating crises (as the Persian Gulf crisis has highlighted) and inviting significant global media attention. Key individuals (such as political leaders), innocent bystanders, and critical infrastructure are at risk. But Trojan spoofing is only a sum-of-parts of the possibilities of weaponising drones; they will perhaps only be considered in exceptional circumstances where seemingly "easier" ways are discounted. Whilst the research findings of Qihoo's research is 8 years old at the time of writing, the potential of exploitation still applies now, and will for the foreseeable future.

The examples of Exposure spoofing in this article, by comparison, are much more limited in terms of meeting certain political goals. Treated as an indiscriminate wide-area denial-of-service attack, and for aversion, it has potential utility. As a targeted attack against a person using a GNSS-aided system (such as a road vehicle), however, the media spectre of the threat supersedes the likelihood of it actually meeting violent group's objectives and motives. The relative difficulty and need for favourable conditions means that "primitive" attacks against specific individuals might supersede the cyber approach. All told, the identification of the security flaw means that companies using GNSS for safety/security-critical systems, some of which have not been identified here, must consider even the possibility of accidental or natural interference that could put people at risk.

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

Adde, N. (2021) 'Calls grow to find back up systems for GPS', *National Defense*, 11 February. Available at: www.nationaldefensemagazine.org/articles/2021/2/11/calls-grow-to-find-back-up-systems-for-gps (Accessed: 11 April 2023).

Almohammad, A. and Speckhard, A. (2017) *ISIS drones: evolution, leadership, bases, operations and logistics.* United States: International Centre for the Study of Violent Extremism. Available at: www.icsve.org/isis-drones-evolution-leadership-bases-operations-and-logistics/ (Accessed: 3 May, 2023).

Associated Press (2011) *The Al-Qaida papers – Drones*. Available at: https://cryptome.org/2013/02/al-qaida-drones.pdf (Accessed: 6 July 2022).

BBC News (2019) *Saudi oil attacks: US blames Iran for drone strikes on two sites*. Available at: www.bbc.co.uk/news/world-middle-east-49705197 (Accessed: 2 December 2022).

BBC News (2023) *Kremlin drone attack: Russia accuses Ukraine of trying to assassinate Putin*. Available at: https://www.bbc.com/news/world-europe-65471904 (Accessed: 3 May 2023).

Bhatti, J.A., Shepard, D.P. and Humphreys, T.E. (2012) 'Drone hack: spoofing attack demonstration on a civilian unmanned aerial vehicle', *GPS World*, 23, pp. 30–33. Available at: https://radionavlab.ae.utexas.edu/images/stories/files/papers/drone_hack_shepard.pdf (Accessed: 3 May, 2023).

Brewster, T. (2015) 'Watch GPS attacks that can kill DJI drones or bypass White House ban', *Forbes*, 8 August. Available at: www.forbes.com/sites/thomasbrewster/2015/08/08/qihoo-hacks-drone-gps/#7f6c16cf2bf5 (Accessed: 3 May, 2023).

Bradbury, D. (2019) 'Tesla 3 navigation system fooled with GPS spoofing', *Naked Security* (SOPHOS). Available at: https://nakedsecurity.sophos.com/2019/06/27/researchers-fool-tesla-3-navigation-system-with-gps-spoofing/ (Accessed: 11 April 2023).

Bunker, R.J. (2015, August) *Terrorist and insurgent unmanned aerial vehicles: Use, potentials, and military implications*. Carlisle, PA: Strategic Studies Institute, US Army War College. Available at: https://www.ausa.org/publications/role-drones-future-terrorist-attacks (Accessed: 2 December 2022).

C4ADS (2019) *Above us only stars: Exposing GPS spoofing in Russia and Syria*, pp. 1–66. Available at: https://www.c4reports.org/aboveusonlystars (Accessed: 2 December 2022).

Daniels, J.P. (2018) 'Venezuela's Nicolás Maduro survives apparent assassination attempt', *The Guardian*, 5 August. Available at: www.theguardian.com/world/2018/aug/04/nicolas-maduros-speech-cut-short-while-soldiers-scatter (Accessed: 2 December 2022).

Farivar, C. (2013) 'Professor fools $80M superyacht's GPS receiver on the high seas', *ArsTechnica*, 30 July. Available at: arstechnica.com/information-technology/2013/07/professor-spoofs-80m-superyachts-gps-receiver-on-the-high-seas/ (Accessed: 2 December 2022).

G4S (2022) *Drones: Threat from above*. Available at: https://www.g4s.com/en-ca/-/media/g4s/canada/files/whitepapers/usa/drones_threat_from_above.ashx?la=en&hash=A5EE00E0402E0CB50FDA127500636B53 (Accessed: 16 October 2020).

Government Office of Sweden, Ministry of Enterprise and Innovation (2017) *Handshake on digitalisation and geofencing*. Available at: www.government.se/articles/2017/05/handshake-on-digitalisation-and-geofencing/ (Accessed: 2 December 2022).

Goward, D. (2019) 'Jammers at dachas add to Russia's ability to silence GPS', *GPS World*, 20 June. Available at: www.gpsworld.com/jammers-at-dachas-add-to-russias-ability-to-silence-gps/ (Accessed: 2 December 2022).

Gozzi, L. (2023) 'Ukraine war: Zelensky visits The Hague as fresh blasts rock Kyiv', BBC News, 4 May. Available at: www.bbc.com/news/world-europe-65478242 (Accessed: 4 May 2023).

Greenberg, A. (2016) 'Hackers fool Tesla S's autopilot to hide and spoof obstacles', *Wired*, 4 August. Available at: www.wired.com/2016/08/hackers-fool-tesla-ss-autopilot-hide-spoof-obstacles/ (Accessed: 11 April 2023).

Hambling, D. (2022) 'Ukrainian Kamikaze drone strike sets Russian oil facility ablaze (updated — Attack drone may have been made in China)', *Forbes*, 22 June. Available at: www.forbes.com/sites/davidhambling/2022/06/22/ukrainian-kamikaze-drone-strike-sets-russian-oil-facility-ablaze/?sh=768cea4b7a99 (Accessed: 2 December 2022).

HelpNet Security (2019) *Research shows Tesla Model 3 and Model S are vulnerable to GPS spoofing attacks*. Available at: www.helpnetsecurity.com/2019/06/19/tesla-gps-spoofing-attacks/ (Accessed: 3 May, 2023).

Hoenig, M. (2014) 'Hezbollah and the use of drones as a weapon of terrorism', *Public Interest Report*, 67(2), pp. 1–5. Available at: https://fas.org/pir-pubs/hezbollah-use-drones-weapon-terrorism/ (Accessed: 3 May, 2023).

Huang, L. and Yang, Q. (2015) *GPS spoofing: Low-cost GPS simulator*. Presented at DEF CON 23, Las Vegas, NV, USA. Available at: https://www.researchgate.net/publication/286330869_Low-cost_GPS_simulator_-_GPS_spoofing_by_SDR (Accessed: 2 December 2022).

Israel's Homeland Security (iHLS) (2020) *Would geo-fencing tech stop terrorist vehicle attacks?* Available at: https://i-hls.com/archives/77355 (Accessed: 2 December 2022).

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*, 2012 (article ID 127072), pp. 1–16. doi: 10.1155/2012/127072.

Kelley, M.B. and Cenciotti, D. (2012) 'REPORT: Chinese experts could be in Iran right now collecting parts from the captured RQ-170 drone', *Business Insider*, 17 August. Available at: www.businessinsider.com/report-chinese-experts-to-inspect-and-collect-parts-of-drone-captured-in-iran-2012-8?r=US&IR=T (Accessed: 11 April 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.

Lee, T.B. (2013) 'Watch the pirate party fly a drone in front of Germany's chancellor', *The Washington Post*, 18 September. Available at: www.washingtonpost.com/news/the-switch/wp/2013/09/18/watch-the-pirate-party-fly-a-drone-in-front-of-germanys-chancellor/ (Accessed: 2 December 2022).

Link. J. (2022) 'Drone contraband deliveries are rampant at US prisons', *Wired*, 29 July. Available at: www.wired.co.uk/article/drone-contraband-deliveries-prisons-united-states (Accessed: 11 April 2023).

Market Watch (2022) *Global active geofencing market size 2022 industry share, growth, business challenges, investment opportunities, demand, key manufacturers and 2026 forecast research report*. Available at: https://www.marketwatch.com/press-release/active-geofencing-market---growth-insights-and-trends-development-by-regions-2020-key-driven-factors-cagr-status-with-revenue-covid-19-impact-on-industry-size-forecast-to-2026-2020-10-14 (Accessed: 2 December 2022).

Ministry of Defence of the Russian Federation (2018) *Head of the Russian General Staff's office for UAV Development Major General Alexander Novikov holds briefing for domestic and foreign reporters*. Available at: http://eng.mil.ru/en/news_page/country/more.htm?id=12157872@egNews (Accessed: 2 December 2022).

Mu, E. (2014) 'China's Qihoo hacks a Tesla model S', *Forbes Asia*, 15 July. Available at: www.forbes.com/sites/ericxlmu/2014/07/15/chinas-qihoo-hacks-a-tesla-model-s/#3e3cdaee3ead (Accessed: 11 April 2023).

Posky, M. (2019) 'Hackers do the dirty to another Tesla model 3', *The Truth About Cars* (*TTAC*), 28 June. Available at: www.thetruthaboutcars.com/2019/06/hackers-do-the-dirty-to-another-tesla-model-3/ (Accessed: 11 April 2023).

pzdupe1 (Pseudonym) (2016) 'Hackers show how they tricked a Tesla into hitting objects in its path', *Business Insider India*, 9 August. Available at: www.businessinsider.com/defcon-tesla-jamming-spoofing-autopilot-2016-8?r=US&IR=T (Accessed: 11 April 2023).

Regulus (2018) *Defending against spoofing and jamming GPS*. Available at: www.regulus.com/blog/defending-against-spoofing-and-jamming-gps (Accessed: 11 April 2023).

Regulus (2019) *Tesla model 3 spoofed off the highway – Regulus navigation system hack causes car to turn on its own*. Available at: www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-navigation-system-hack-causes-car-to-turn-on-its-own. (Accessed: 2 December 2022).

Rowlatt, J. (2019) 'Gatwick drone attack possible inside job, say police', *BBC News*, 14 April. Available at: www.bbc.co.uk/news/uk-47919680 (Accessed: 2 December 2022).

Scharre, P. (2015) 'Counter-swarm: A guide to defeating robotic swarms', *War on the Rocks*, 31 March. Available at: warontherocks.com/2015/03/counter-swarm-a-guide-to-defeating-robotic-swarms/ (Accessed: 2 December 2022).

Stokel-Walker, C. (2019) 'Tesla's autopilot tricked into driving on the wrong side of the road', *New Scientist*, 1 April. Available at: www.newscientist.com/article/2198325-teslas-autopilot-tricked-into-driving-on-the-wrong-side-of-the-road/ (Accessed: 2 December 2022).

Sathyamoorthy, D., Amin, Z.F.M., Selamat, E., Hassan, S.A., Firdaus, A., Kazmar, A., and Zaimy, Z. (2020) 'Evaluation Of The Vulnerabilities Of Unmanned Aerial Vehicles (UAVS) to global positioning system (GPS) jamming and spoofing', *Defence S and T Technical Bulletin*, November 2020. Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia. Available via ResearchGate at: https://www.researchgate.net/profile/Dinesh-Sathyamoorthy/publication/345150887_EVALUATION_OF_THE_VULNERABILITIES_OF_UNMANNED_AERIAL_VEHICLES_UAVS_TO_GLOBAL_POSITIONING_SYSTEM_GPS_JAMMING_AND_SPOOFING (Accessed: 3 May 2023).

Strategy Page (2019) *Electronic weapons: Russia takes a victory lap*. Available at: www.strategypage.com/htmw/htecm/articles/20191103.aspx (Accessed: 2 December 2022).

Soni, B. (2022) '*Norway's ban on Russians flying drones faces test in court*', *Financial Times*, 28 November. Available at: www.ft.com/content/1688a960-64a0-43ee-a3b4-243c5f1ccdfe (Accessed: 11 April 2023).

Tucker, T. (2015) 'Chuck Schumer's no-fly-zone rule for drones won't work', *Defense One*, 24 August. Available at: www.defenseone.com/technology/2015/08/chuck-schumer-no-fly-zone-drones/119389/ (Accessed: 2 December 2022).

United States Government Accountability Office (2012) 'Unmanned aircraft systems: Measuring progress and addressing potential privacy concerns would facilitate integration into the national airspace system', *GAO-12-981*, 14 September, pp. 1–45. Available at: https://www.gao.gov/assets/gao-12-981.pdf (Accessed: 3 May 2023).

VoA News (2020) Untitled media report, … *The Saudi Defense system failed to spot our drones*. Available at: www.voanews.com/media/2394681/embed (Accessed: 2 December 2022).

Warrick, J. (2017) 'Use of weaponized drones by ISIS spurs terrorism fears', *Washington Post*, 21 February. Available at: https://www.ausa.org/publications/role-drones-future-terrorist-attacks (Accessed: 2 December 2022).

Watson, K. (2018) 'Venezuela President Maduro Survives drone assassination attempt', *BBC News*, 5 August. Available at: https://www.bbc.com/news/world-latin-america-45073385 (Accessed: 2 December 2022).

Westbrook, T. (2019) 'The Global Positioning System and Military Jamming: The geographies of electronic warfare', *Journal of Strategic Security* (JSS). 12(2), pp. 1–18. doi: 10.5038/1944-0472.12.2.1720.

Westbrook, T. (2023) 'A Taxonomy of Radiofrequency Jamming and Spoofing Strategies and Criminal Motives', *Journal of Strategic Security* (JSS). 16(1), pp. 1–14. In press.

Whitlock, C. and Gellman, B. (2013) 'US documents detail al-Qaeda's efforts to fight back against drones', *The Washington Post*, 3 September. Available at: www.washingtonpost.com/world/national-security/us-documents-detail-al-qaedas-efforts-to-fight-back-against-drones/2013/09/03/b83e7654-11c0-11e3-b630-36617ca6640f_story.html (Accessed: 2 December 2022).

Zangvil, Y. (n.d.) *Research on GPS resiliency & spoofing mitigation techniques across applications*. Regulus, presentation slides accessible via: GPS.gov, "GPS: […] A global public service brought to you by the U.S. government." Available at: https://www.gps.gov/governance/advisory/meetings/2019-06/zangvil.pdf (Accessed: 2 December 2022).

Zholobova, M. (2019) *Investigation into how the Russian leadership acquired unofficial residences*. The Project Dacha partnership. Available at: www.proekt.media/investigation/dacha-putina-gorki10/ (Accessed: 2 December 2022). Translated from Russian using Google Translate.