Journal of Strategic Security

Volume 16 | Number 2 Article 5

A Taxonomy of Radiofrequency Jamming and Spoofing Strategies and Criminal Motives

Tegg Westbrook
University of Stavanger, teggwestbrook@gmail.com

pp. 68-80

Recommended Citation
Westbrook, Tegg. "A Taxonomy of Radiofrequency Jamming and Spoofing Strategies and Criminal Motives." *Journal of Strategic Security* 16, no. 2 (2023) : 68-80.
DOI: https://doi.org/10.5038/1944-0472.16.2.2081
Available at: https://digitalcommons.usf.edu/jss/vol16/iss2/5

A Taxonomy of Radiofrequency Jamming and Spoofing Strategies and Criminal Motives

Abstract

This article provides a taxonomy of radiofrequency (RF) jamming and spoofing tactics and strategies associated with specific criminal objectives. This is based on the fact that the motivations and strategies of cyber-attackers – predominantly financial – is well-known, but the motivations behind specific electromagnetic interferences is lacking in the current literature. Previous research has also overlooked the motivations of other actors using jamming and spoofing devices.

The objective is to identify the most desirable spoofing and jamming strategies, likely targets, and likely motivations. The article finds that (a) previous literature on the subject overlooks a number of non-state actor motives, and therefore this research aims to fill this gap in knowledge; (b) out of 8 actors identified, denial of service attacks (7 out of 8), as well as so-called decoy spoofing (6), trojan spoofing (5), and jamming-enabled crime (5) are the most desirable strategies utilized; (c) out of 11 strategies identified, grey and black hat hackers (11 out of 11), terrorists (11) and activists (8), are likely to take advantage of most identified.

Acknowledgements

I would like to thank Dr Tim Wilson and colleagues from the Centre for the Study of Terrorism and Political Violence at the University of St. Andrews for their help and advice during this research.

Introduction

Cybercrime and cyberwar have been at the forefront of thinking in terms of understanding likely threat actors, not only against computer-based systems, but also against satellites and radio signals. 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 cyber-attackers, and their financial and political motivations are well documented. Whilst it is reasonable to be concerned about such threats, the focus on the opportunities for non-state actor crime using more accessible, easy to use, and disruptive technologies that are not cyberweapons or cyber tools, but electronic ones–such as jammers and spoofers–has been limited. Such systems, arguably cheaper and requiring comparatively low skill levels to use, can do as much if not more to affect computer-based cyber-physical systems.

Radio frequency jammers used by non-military actors, costing no more than 50 United States dollars (USD) at the least, can block weak signals emitting from satellites. Jammers will affect the receivers of a global positioning system (GPS)-reliant system depending on those signals–for navigation, tracking, and timing purposes. GPS spoofing devices, by comparison, can also affect a receivers' ability to receive satellite signals. These contraptions are assembled using off the shelf equipment available to buy online, or, if required, simply downloaded on a smart phone.

Unlike jamming, which blocks signals, spoofing will give a receiver, and a person or system relying on position, velocity, tracking, and timing information from those receivers, false information. Not only have spoofing devices become more accessible, but they have also become more affordable. A spoofing device that has been used to misdirect a ship that cost around 3000 USD in 2013 is now less than 250 USD to construct (in 2018).[1] Not only have these devices proved effective, they are also concealable; more or less the size of a cellphone.[2] They have also become increasingly easier to use over time after the introduction of the software-define radio, which means civilian users need not be engineers to use them nor comprehend its versatility.[3] The easiest are those which have online scripts with instructions about what equipment is needed and how to assemble, as well as those downloadable on cellphones. Even today, at the time of writing, there are numerous websites and repositories giving gamers precise

instructions as to how to spoof their location, and some spoofing apps exceed 10 million downloads.[4]

Whilst there have been cases of state actors affecting civilian users in maritime sectors and in aviation (using military-grade jammers and spoofers), there have also been a considerable number of civilian users of radiofrequency (RF) interference devices.[5] E.U.-funded STRIKE3, for example, deployed an international Global Navigation Satellite System (GNSS) interference monitoring network involving 23 countries around the world to understand the scale of the jamming and spoofing problem. 450,000 GNSS interference signals were captured and analysed, of which 73,000 interferences were classified as having a 'major impact on GNSS,' and 59,000 of these 'where identified as jammer signals.'[6] Overall, in theory, this means that over 10 percent all GNSS interference could be malicious or intentional.[7] Recent studies have noted continuing trends in the use of jammers, even identifying slight increases in some countries.[8]

For the limited focus on RF interference threats from non-state actors, there has been at least 22 threat vectors identified in the literature. These include privacy seekers, criminal jamming, criminal spoofing, terrorist jamming, and terrorist spoofing.[9] Missing in the literature is an acute focus on other, specific actors, including gamers, script kiddies; quiet seekers; activists; ethical or grey or black hackers; patriot hackers; corporations; and lone wolves. Literature in the past has thus not delved deeply enough into a variety of specific motivations. Such motivations include: Privacy, counter anti-social behavior, money, espionage, fame or status, damage reputation, entertainment, hacktivism, terrorism, and war, including information war, psychological war, and deception. The threats have evolved in part due to the extended use of location-based services in business, leisure, and critical infrastructures and systems reliant or aided by satellite-based systems which has created new opportunities crimes, from petty to serious.

By understanding the motivations of those targeting radio frequencies, there is a need to expand knowledge in the fields of criminology, political sciences, risk sciences, and engineering of the threat. There is a need to further understand why specific actors are motivated to do target GNSS systems, as indeed, the "threat is generally estimated as the likelihood that a hazard will manifest itself."[10] Unlike many cyber-attacks such as ransomware, phishing, RF interferences are nuisances

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

that have no obvious motives attributable to the actions since it could be caused by natural interferences, or because changes in time, position and velocity do not always immediately lead to physical, psychological or financial harm. To simply put RF interference into the same motivation-based boxes as cyber attackers would overlook the limits and opportunities that jamming and spoofing bring, and the unique targeting logics. Indeed, certain location-based systems would invite specific strategies depending on the goals of the actor, how exposed the systems are, how accessible the target is or how–in some cases–destructible the act may be. Such analyses thus require filtering unlikely targets from the likely targets to ensure proportional countermeasures.[11]

The article provides a short and basic introduction to the structure of the GPS and why non-state actors might want to target it. It then discusses the methodology used for acquiring and making sense of the data. The literature review identifies which actors are missing from previous threat assessments of RF interference. A taxonomy of spoofing and jamming strategies is listed, followed by a simple threat barometer differentiating between RF interference strategies and actor motivations. The results expand and contextualize those strategies and motives in the remaining sections, with the conclusions and recommendations exploring the significance of the findings.

What is Jamming and Spoofing?

For millennia, adversaries have found creative ways of falsifying data and information to get an upper hand in warfare, something that is often defined as information warfare. In time, weapons and communications systems have incorporated some type of electromagnetic function as a necessity for modernizing in response to enemy offensive and defensive innovations and communications systems. Whilst such updates have improved the efficiency and effectiveness of military systems, it has also opened weaknesses that can be exploited. Indeed, the methods of spoofing and jamming has evolved considerably over time. During WWI, the British and French were using jamming and spoofing to affect the navigation capabilities of German Zeppelins.[12] The first specialized electronic warfare units began to appear during WWII.[13] After discovering that the Luftwaffe were using specific radiofrequency beams (in what is sometimes referred to as the Battle of the Beams) to determine the position of a target for its aerial bombers during night-time raids, the Royal Air

Force used its own beams to make the bombers believe the Luftwaffe were dropping their bombs on its targets. From WWI to the present Russian invasion of Ukraine, adversaries routinely degrade and block communications. Spoofing can affect the accuracy of smart weapons aided by GPS, degrade use of weaponized or surveillance drones, or simply deny reliable use for simple navigation in urban areas.

States may also purposely jam other countries for intimidation and harassment, or deny an adversaries' surveillance or eavesdropping or spying capabilities.[14] State actors may also use spoofing to bypass international sanctions on certain goods, or disrupt the operations of sanctions monitoring and ceasefire monitoring.[15] State militaries may also use spoofing to enable capture of goods for hostage diplomacy, as seen in Iran's seizure of the *Stena Impero*.[16] Several states will use spoofing techniques to harass their own citizens by means of gathering intelligence about the whereabouts of individuals of interest.[17]

While there have been recorded cases of civilians targeting radiofrequencies in the 20th century, and recently a lot of focus drawn on Russian, Iranian, Chinese and North Korean sanctions evasions using spoofing, the motivations of civilian actors has not been adequately analyzed, particularly in the context of GPS ubiquity.[18] After GPS opened to civilian users in the early 1990s, leading subsequently to greater reliance on the timing, position and velocity information provided, spoofing and jamming has evolved in the civilian domain. Timing is critical to the GPS, as without it, it would be impossible to derive one's position, velocity, and accurate transaction of information. Using atomic clocks, precise time stamps are delivered from satellite signals to receivers, which in turn calculates its position based on latitude, longitude, and altitude, from four satellites (out of 30+) in space.[19] Affecting the timing with jamming and spoofing is simply all that is needed to affect critical functions of cyber-physical systems for which societies increasingly depend.

The consequences of intentional RF interference can vary depending on the vulnerabilities of the target system and the capabilities of the threat actor. As per the examples, one could understand why militaries would want to jam enemy communications; the motives of non-state actors, however, are limited to targeting civilian systems in the so-called user segment, which consists mostly of civilian systems reliant on the open GPS codes (not the exclusive, encrypted military codes).

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

Methodology

The study involved a meta-data analysis to understand the scope and activity in the electromagnetic domain, specifically the radio spectrum, on GPS-aided and GPS-dependent cyber-physical systems. It involved a qualitative analysis into academic research mostly from the engineering domain, as well as government-initiated projects, non-governmental organizations, media reports, and secondary data from these sources. Embracing a grounded theory approach, the data collected was defined into separate categories relating to the means-ends goals and tactics of different types of non-state actors, motivations, and targeting choices. The outcome of the approach has led to the development of a taxonomy of spoofing and jamming strategies and tactics. Such strategies have not received a comprehensive overview before (or are of variations of the same tactics described differently in separate papers and reports).

Findings

Taxonomy of Jamming and Spoofing Strategies and Tactics

Below this section presents several petty and serious spoofing and jamming strategies. Some tactics could be distinguished into two types, as means to end attacks, for example attacks against the spectrum that complement physical crimes. Others are ends in themselves, where the interference itself achieves the desired criminal ends. Some of the tactics enable physical crimes, otherwise understood as jamming- or spoofing-enabled crimes:

- *Wolf in Sheep's Clothing* can trick unsuspecting users that another vehicle or another person is safe by mimicry and duping, otherwise defined as defensive or offensive mimicry. Pirates using false identification data to enable hijackings of container ships is one example of this tactic.[20]
- *Ghost Routing* is similar to Ghost Spoofing, a spoofing strategy intended to deceive a driver, for example, to follow the direction of a spoofed route. Such strategies can complement kidnap attempts but would require high sophistication and motivation.[21]
- *Following Crooked Paths* and *Correcting Crooked Paths* can also mislead a GPS user or system using GPS or ground-based navigation beacons to correct or follow a false velocity reading or direction, thus making the target go in the wrong

direction. A test undertaken by the University of Texas at Austin found, for example, that inducing a false trajectory reading into a yacht can lead a pilot or captain to correct a crooked trajectory, when in fact they are leading a vehicle in the wrong direction.[22] Similar issues have been identified when spoofing the Instrument Landing System used for landing aircraft.[23]

- *Trojan Spoofing* allows vehicles to enter restricted (geofenced) areas by making the vehicle believe–based on false position information–it is in a location which it presently is not, thus overcoming the area restrictions.[24] Trojan spoofing can also digitally displace devices, like mobile phones, to overcome area restrictions. Researchers have shown, for example, that a spoofed drone can encroach geofenced no-drone zones.[25]
- *Exposure Spoofing*, on the contrary, is the reverse of trojan spoofing, but is used to, for example, intentionally expose the victim to risks by putting users in geographically defined areas that would trigger an automatic system to adjust itself to its (false) surroundings, or fool a driver or pilot to believe they are in safe passage.[26] An Israeli company Regulus, for example, spoofed a Tesla 3 vehicle in 2019, demonstrating that the height of the vehicle could change to suit the terrain and adjust according to the required aerodynamics.[27]
- *Decoy Jamming and Spoofing* is deceiving the location information of a user as a means of distracting attention away from another nefarious operation. Police, border patrol may follow GPS coordinates to find perpetrators but could in fact be deceived.[28] Prior to the HMS Defenders' voyage through Russian-controlled Ukrainian waters in 2021, exercising its right to 'innocent passage […] in accordance with international law,' this prompted an aggressive response from the Russian Airforce and Navy. Among many hypotheses, the British, American, Dutch, and Swedish Navy ships may have spoofed their Automatic Identification Systems (AIS) to Russian-controlled waters as a 'feint' to test what reaction it would spark.[29] Reports of other suspicious AIS manipulations include illegal fishing, environmental violations, and sanctions evasions.[30]
- *Shame Spoofing* is spoofing an adversary or commercial competitor to draw attention to their vulnerabilities and security failures and procedures, causing reputational

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

damage or worse. It can give businesses a competitive advantage by demonstrating the inadequacies of others' security controls or systems. There has been many media stories of bloggers, white-hat hackers and scientists targeting surface vehicles to draw attention to their vulnerabilities. Examples include a 2014 model Jeep Cherokee, a Build Your Dreams vehicle, and Tesla, among others.[31]

- *Back-Seat Driver* is the attacker taking control of a vehicle that they are already in, as opposed to doing it from a distance, thus overcoming specific security controls and geographical inhibitors. This is because many experiments on manned and semi-autonomous systems have been done within the vehicle or in controlled conditions favorable to the back-seat driver attacker.[32]
- *Denial of Service* (DoS) degrades and denies confident use of GPS and other navigation beacons, and potentially destroys the victim's receivers with strong, overpowering signals. Such attacks can be achieved using cheap jamming devices to enable physical crimes, or with specialized ones attainable via black markets or stealing or misuse from licensed users.[33] In July 2014, according to the National Insurance Crime Bureau in the United States, auto thieves reportedly placed GPS jammers inside over 40 shipping containers destined to arrive in China.[34] Thieves have been known also to jam vehicles to prevent prosecutors using tracking evidence that could lead to prosecutions.[35]
- *Momentary Spoofing* is the spoofing or jamming of a vehicle during a critical time of its maneuverability–whether it is approaching a runway or passing other ships, for example. The University of Nottingham and Royal Norwegian Naval Academy found in its research that momentary jamming of ships for up to 10 seconds could lead to dangerous situations, especially in narrow straits. The jamming 'gave false readings in the on-board navigation system with positional data moving more than 10 meters.'[36]

GPS Jamming and Spoofing Threat Matrix

After defining spoofing and jamming strategies from various sources, the following non-state actors displayed in Table 1 are considered likely users of these strategies. For ease of reading, many of the sources in the endnotes provide evidence and elaboration on the connections made.

Table 1. Jamming and Spoofing Actors and Associated Tactics

	Gamers	Privacy Seekers	Quiet seekers	Grey / Black hats	Activists	Financial criminal	Businesses	Terrorists
DoS		X	X	X	X	X	X	X
Decoys		X		X	X	X	X	X
Trojan	X			X	X	X		X
Jamming / spoofing-assisted crime				X	X	X	X	X
Shame				X	X		X	X
Crooked paths				X	X			X
Wolf in sheep's clothing				X	X			X
Ghost routing				X	X			X
Backseat driver				X	X			X
Momentary				X				X
Exposure				X				X

Notes. The researcher reviewed all literature in this table. The endnotes contain only sources cited in the text. Source: Author.

Explanation of the results

Gamers or Script Kiddies

Gamers and script kiddies may follow online instructions or download ready-developed codes or apps to bypass location restrictions for video games.[37] Drone enthusiasts will also use online codes and manuals to enter geofenced no-drone zones.[38] Since the gaming market is so dynamic, demand for cheat codes can surge unexpectedly, and even lead to new market innovations. Script kiddies may also try to overcome other geofences–virtual zones which might restrict drone access or slow down e-scooters–for entertainment, curiosity, and mild forms of protest.[39]

Overall, their intentions are usually neither financially nor criminally motivated, but entertainment reasons as the primary motivator. The risk of capture is relatively low, although anti-spoofing algorithms can pick up suspect location jumping for some games and give temporary bans to gamers. Some gamers may go to some lengths to overcome the anti-spoofing algorithms, following other online instructions.[40]

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

Privacy Seekers

Privacy seekers seek privacy from non-consensual, unwanted (untrustworthy or abusive partners, police etc.) and compulsory tracking (work management, Covid contagion). Privacy seekers most likely use low cost and low power jammers as well as spoofing apps similar to those used by script kiddies, if they want to mislead the tracker about their whereabouts.[41] Regarding the latter point, Gig workers may use spoofing apps as a way of resisting or mitigating demanding algorithmic timestamps on deliveries, or who feel unsafe meeting deadlines to deliver goods on time.[42] Such spoofing apps can be detected. For those using jammers, the risk of punishment has increased in recent years, due to greater awareness of RF interference sources and devices, the distribution of jamming detectors, and even the use of portable detectors in some countries. While the user might try to use a jammer with a limited radius, it can indiscriminately affect other users up to and beyond 9km in some locations.[43]

Privacy seekers may also use jamming systems to avoid eavesdropping. In the legitimate, licensed use of jammers, they have uses for private diplomatic, government, and military meetings, and to protect certain individuals or properties from journalists or paparazzi, for example. Unlicensed users replicate such motives.

It is possible to foresee a subculture that rebels against new technologies and societal changes that challenges rights to privacy. For example, drone deliveries may be subject to interference from privacy seekers. Minority groups and individuals or groups of certain dispositions may seek privacy from government spying, or from those deemed a threat to that minority or subculture. Minorities such as homosexuals have been tracked and subsequently punished in countries that outlaws their sexuality.[44]

Quiet Seekers

Quiet seekers usually use low cost or low power jammers of many varieties, including ones advertised as cell phone or Wi-Fi jammers, in response to what quiet seekers deem to be anti-social behavior.[45] In some circumstances, there is greater impetus to be directional or discriminatory than privacy seekers. Targets might include people talking on the phone on public transport, in theatres, cinemas, or in religious institutions.[46] The quiet seeker may be indiscriminately

denying other bystanders who are not being anti-social. The motivation to use a jammer for such purposes would be due to the perceived risks or problems of confrontation with the babbler, or a group of babblers.

Quiet seekers may target non-human things to satisfy their desires. Like privacy seekers, quiet seekers may conceivably use RF interference against GNSS-aided systems that make a noise, such as commercial or private drones. In a similar niche market, there are low-cost and easy-to-install ultrasonic repellent devices to deter noisy children, teens, pets, and other animals from property.[47] Though not jammers, such systems emit certain frequencies that affect unfortunate ears.

Grey Hats and Black Hats

Ethical hackers will use legitimate or illegitimate means to identify security flaws in systems for the purpose of exposing those weaknesses for the public good, broadly defined. This might be contractual work, or, most closely under the term grey hat, done without permission for publicity and financial reasons, offering services that will help rectify the problems identified.[48] Black hats, by comparison, are often considered malicious actors seeking personal gains (see criminal jamming and spoofing). Grey and Black hats may do such deeds under a pseudonym to avoid punishment.[49]

Grey and black hats usually have good-advanced technical skills, with relatively low risk of punishment (given that they usually operate in a grey legal area), and potentially high financial and reputational rewards. Some hackers are more transparent about their capabilities than others–delivering online and in-person presentations and demonstrations at yearly conferences.[50] Some hacker conventions and testing arenas come with prizes.[51] Depending on the intention, the equipment hackers use may be either targeted or indiscriminate. Targets that might attract high publicity–such as safety or security-critical systems–or targets that may be inclined to pay for repair, are particularly vulnerable. Recent spoofing events have happened during expeditions, demonstrations (to increase the damage and embarrassment to a company), and hacking events (shame spoofing).[52] Further hardening measures may lead to further grey or black hat hacks for testing.

Notwithstanding, jamming and spoofing only provide limited options for grey and black hats. Other cyber tools will probably provide much

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

more variety of targets and rewards. In this context, whilst spoofing would score high points within subcultural circles, jamming may be considered too easy to be called a serious hacker operation, probably without the reward of recognition or money. All told, easy targets that could provide headline-grabbing consequences. What if a popular and widely used drone crashes due to the actions of an (anonymous) grey hat using online spoofing codes, or worse - a low-cost, easily accessible pocket jammer?

Activists

Not a lot of data is available on how activists have used RF interference, therefore much of this analysis is hypothetical. Activists may use jamming or spoofing with no violent intentions to complement and amplify political objectives, using RF interference to enable physical forms of protest, or deny service to those deemed counter to their political interests. If their political or religious motivations are extreme, activists may use jamming and spoofing for intimidation or harassment, for instance religious vigilantism, pro-life (anti-abortion) activism, or extreme forms of animal rights activism.[53] Their skill levels are mixed, and the element of self-sacrifice is usually high. Activists and hacktivists may have special access as insiders, and thus may be well-organized and assisted.[54] Many activists and hacktivists may want to avoid being labelled terrorists, so might be careful about what targets to select–in other words, ones that avoid putting people in physical danger.

Financial Criminal Jamming and Spoofing

Whilst previous literature has acknowledged the role of jamming and spoofing to complement financial criminal motives, there is a need for expansion of elaboration. Financially motivated criminals use RF interference to enable theft of tracked goods, defraud taxi or ride-hailing companies and customers, to enter restricted areas, avoid toll payment, prevent eavesdropping, avoid insurance-related tracking in cars, and avert tracking and location finding for first responders.[55] Motivations and capabilities vary considerably. It could be difficult to prove what a criminals' intentions are if caught with a jammer or computer equipment. In some countries, possession is not illegal, and evidence of use is difficult to verify (but is increasingly getting easier to verify.)[56] Organized criminals will likely invest in more quality-assured jammers and spoofers. Organized criminal gangs may seek specialist

assistance to identify the specific vulnerabilities of the systems they wish to target. Like cyber-criminals, jamming and spoofing helps some criminals avoid physical or geographical obstacles, albeit to a lesser degree than cybercrime.

In some parts of the world the jammer or spoofer might be a more favorable instrument than the proverbial crowbar or lockpick, due to higher tracking and surveillance practices, or because of specific favorable and facilitating conditions, for example, in areas where bribery is expected, pirated waters, or where ransoms are usually paid with limited effort, or even where corrupt government or police have a stake in the crimes committed.

Corporations or Businesses

Many businesses routinely hire white and grey hackers to identify vulnerabilities in their own systems, but they may hire black hats to target rivals to damage their reputation or seek to make profits by other nefarious means. To avoid severe punishment, businesses might hire cyber mercenaries with no direct connection to the company on a need-to-know basis to operate on their behalf. The rewards could be significant in highly competitive markets, but the punishment would be severe if caught and attributed to the company. For these reasons, some businesses may operate in the 'semi-legal' area that might disincentivize the victim to take legal action. Therefore, attacks will likely be discriminatory, difficult to detect, and carried out by specialists and adequate equipment. Businesses, like privacy seekers, may also use jammers legitimately or illegitimately to avoid eavesdropping and drone surveillance.

Some unscrupulous businesses, or individuals within those businesses, might use spoofing to overcome location-restrictive protection measures, for example by spoofing AIS to access restricted fishing grounds, or to bypass sanctions (flag hopping) and protected areas (for raw materials).[57] Some legitimate businesses such as prisons restrict workers or visitors from using cell phones (similar to quiet seekers). It has been documented that unscrupulous actors have used spoofing to locate persons of interest for financial gains, for example lawyers targeting potential clients via spoofed geofences.[58]

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

Terrorist Jamming and Spoofing

Terrorists may use jamming or spoofing in a variety of ways to coerce governments, generate fear in society, and draw media and public attention to extreme political, ideological, or religious goals, with 'impact' and media exposure as the essence of many of their operations. The tactics, targets, and broader objectives, of course, depend on factors such as ideology, dynamics of the struggle, targeting logic, the targets' likely countermeasures, and many other factors.[59] Some targets are, under the acronym EVIL DONE, 'Exposed,' 'Occupied' and 'Destructible,' including both GPS-dependent or GPS-aided systems, such as drones, aircraft, ships, and individual users.[60]

As well as enabling aversion from surveillance, it can be hypothesized that jamming and spoofing can act as force-multipliers by enabling more extreme modes of violence via cyber-physical attacks and cyber-enabled stealing, hijacking, or kidnap.[61] Due to the ease-of-use of jammers and spoofers by comparison to other cyber or electronic means, it is especially attractive to such actors with limited technical expertise, and could even be construed as technologically advanced by outside lay observers (certainly for spoofing). Some GPS users are more vulnerable than others, for example those with outdated receivers, relying on a single signal, in situations where redundancy or complementary navigation cues are not available, in black swan situations, and those generally ignorant of the threat.

Mass casualty attacks via unsophisticated or semi-sophisticated spoofing and jamming are unlikely to succeed, but possible in some situations. Traditional targets such as aircraft could generate significant media attention, sympathy, and support, even if the impact is minimal.[62] It is nevertheless hard to attribute success to the action without prior published intentions or livestreaming (high-value targets such as passenger planes are usually hardened targets).

Terrorists, like financial criminals, will likely use jamming and spoofing to an end, not an end itself. An example might be enabling hijacking of a large vehicle (say, with chemicals), or denying first responders navigational and communication abilities in the event of a mass casualty attack.[63] In such cases, the chances of success are heightened, rewards high, and risk of capture is lessened.

Terrorists are more likely to succeed when targeting civilian systems since they do not have the robust protections that military receivers have. Groups assisted by state actors could, and likely have, targeted military systems. Other terrorist intentions might include using trojan spoofing to overcome drone defenses to attack critical infrastructure targets.[64] Terrorists, like pirates, may use spoofing to misdirect ships for seizure, or even misdirect persons of interest if highly motivated.[65]

Conclusion

The article has primarily focused on what motivates non-state actors to use jamming and spoofing to enable them to meet their goals, and what strategies they might utilize. The findings show that not only should equal consideration of the vulnerabilities of the radio spectrum correspond with many cyber vulnerabilities, but societies' increasing reliance on location-based services diversifies the vulnerabilities and threats in many ways.

There are some limitations to the research. For example, other performance metrics, such as the sophistication of the actor and the sophistication of equipment required for certain tactics, could provide a more detailed comparison. Such questions require further expansion. Furthermore, there are other non-state actors that would be able and willing to deploy certain tactics against civilian systems that have not been explored. Patriot hackers might undertake RF interference unofficially and autonomously on behalf of the state, its ideology, and its struggles with other states. During Russia's invasion of Ukraine, a huge rise in vigilante hacking targeting Russia was something not predicted by most analysts.[66] Whilst most of these attacks took place in the cyber realm, such actors could theoretically target systems and critical infrastructure reliant on the electromagnetic spectrum. Self-radicalized lone wolves similarly might amplify the goals of a certain group, representing but essentially acting independent from those groups. These actors could have insider access, stationed abroad in the location of the desired target.

Overall, regardless of the limitations, whilst most minds focus on Russia's unprovoked invasion of Ukraine (and the electronic warfare activities there), there is a plethora of civilian uses for jamming and spoofing that are both criminally and geographically diverse. The greater reliance on location-based services will lead to different actors

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

with different motivations and tactics in the near future, and thus requires careful monitoring.

Endnotes

[1] Jahshan Bhatti and Todd E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection Navigation." *Journal of the Institute of Navigation* 64, no. 1 (2017): 51-66. https://doi.org/10.1002/navi.183 ; Kexiong (Curtis) Zeng, Shinan Liu, Yuanchao Shu, Dong Wang, Haoyu Li, Yanzhi Dou, Gang Wang, and Yaling Yang, "All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems." *Proceedings of the 27th USENIX Conference on Security Symposium*, *Baltimore, MD, USA,* August 15-17, 2018: 1527–1544. https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-zeng.pdf.

[2] Stephen Lawson, "GPS Spoofing Fooled Drivers Into Taking Wrong Way," *Automotive*, July 18, 2018, www.tu-auto.com/gps-spoofing-fooled-drivers-into-taking-wrong-way/.

[3] Hackers Arise, "Software Defined Radio for Hacker: How to Spoof your Global Position (GPS) to Hide Your Location," January 28, 2023, www.hackers-arise.com/post/software-defined-radio-for-hacker-how-to-spoof-your-global-position-gps-to-hide-your-location.

[4] David Robinson, "Using GPS Spoofing to control time." *DEFCON 25 Presentation, July 27-30, 2017, Caesars Palace, Las Vegas*, available on YouTube at: www.youtube.com/watch?v=isiuTNh5P34; Google Play, "Fake GPS location." August 16, 2022. https://play.google.com/store/apps/details?id=com.lexa.fakegps&hl=en&gl=US&pli=1.

[5] Maritime Link, "From Mines to AIS Spoofing, Assessing the Risks to Shipping in the Black Sea," March 03, 2022, www.marinelink.com/news/mines-ais-spoofing-assessing-risks-494729; C4ADS, "Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria." (2019): 1 – 66, 9. https://www.c4reports.org/aboveusonlystars; NASA, "Aviation Safety Reporting System: Global Positioning (GPS) Reports." January 29, 2020. https://data.nasa.gov/Aerospace/Aviation-Safety-Reporting-System-Global-Positionin/mi9x-dvtp.

[6] STRIKE3, "STRIKE3 Project." European Global Navigation Satellite Systems Agency, Horizon Europe. Accessed February 16, 2023. https://aric-aachen.de/strike3/S3-work/.

[7] Interview with Dana Goward, in: Anusuya Datta, "Vulnerabilities of GPS is a big concern: Dana Goward," *Geospatial World*, September 05, 2020, https://www.geospatialworld.net/blogs/vulnerabilities-of-gps-is-a-big-concern-dana-goward/.

[8] Nicolai Gerrard, Anders, Rødningsby, Aiden Morrison, Nadezda Sokolova, Christian Rost, "GNSS RFI Monitoring and Classification on Norwegian Highways – An Authority Perspective." *Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021) Union Station Hotel St. Louis, Missouri*, *September 20 - 24, 2021.* https://www.ion.org/publications/abstract.cfm?articleID=17952.

[9] RNT Foundation, "Prioritizing Dangers To The United States From Threats To GPS." 2016: 5. rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf.

[10] United States Government Accountability Office, *GPS DISRUPTIONS: Efforts to Assess Risks to Critical Infrastructure and Coordinate Agency Actions Should Be Enhanced*, Mark Goldstein, Joseph Kirschbaum, Sally Moino, Glenn Davis, Eli Albagli, Melissa Bodeau, Katherine Davis, Richard Hung, Bert Japikse, Sara Ann Moessbauer, Josh Ormond, Nalylee Padilla, and Daniel Rodriguez. GAO-14-15, Washington: 2013: 15. https://www.gao.gov/assets/gao-14-15.pdf.

[11] Ronald V. Clarke and Graeme R. Newman, *Outsmarting the Terrorists*. Westport, CT: Praeger Security International, 2006.
[12] Commander Malte von Spreckelsen, "Electronic Warfare – The Forgotten Discipline Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict?" *JAPCC*, December 2018, https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/.
[13] Government of Sweden, Försvarsdepartementet/Ministry of Defence, *Russian Electronic Warfare – The Role of Electronic Warfare in the Russian Armed Forces,* Jonas Kjellén, FOI-R--4625--SE, 2018.
[14] Tegg Westbrook, "Will GPS Jammers Proliferate in the smart city?" *Salus Journal* 7, no. 2, (2019): 45–67. https://search.informit.org/doi/10.3316/informit.674593796248459.
[15] Anatoly Kurmanaev, "How Fake GPS Coordinates Are Leading to Lawlessness on the High Seas," *New York Times*, September 03, 2022, https://www.nytimes.com/2022/09/03/world/americas/ships-gps-international-law.html; Tegg Westbrook, "The Global Positioning System and Military Jamming: The geographies of electronic warfare." *Journal of Strategic Security* 12, no. 2 (2019). https://doi.org/10.5038/1944-0472.12.2.1720.
[16] Insurance Maritime News, "Seized Stena Impero was probably GPS spoofed," August 21, 2019, https://insurancemarinenews.com/insurance-marine-news/seized-stena-impero-was-probably-gps-spoofed/
[17] Paul Wagenseil, "Grindr Worst of Many Apps Leaking User Location, Researchers Say," *Tom's Guide*, January 18, 2015, https://www.tomsguide.com/us/geoleaky-apps-grindr,news-20323.html.
[18] Tegg Westbrook, "The Global Positioning System and Military Jamming: The geographies of electronic warfare." *Journal of Strategic Security* 12, no. 2 (2019): 4. https://doi.org/10.5038/1944-0472.12.2.1720.
[19] Jill Stuart, "Exploring the Relationship Between Outer Space and World Politics: English School and Regime Theory Perspectives." (PhD diss., London School of Economics, 2007?), 126.
[20] Chris Lo, "GPS spoofing: what's the risk for ship navigation?" *Ship Technology*, April 15, 2019, https://www.ship-technology.com/features/ship-navigation-risks/
[21] Zeng et al, "All Your GPS Are Belong To Us…"
[22] UT News, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea," July 29, 2013, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/.
[23] Sathaye, Harshad, Schepers, Domien, Ranganathan, Aanjhan, and Noubir, Guevara. "Wireless Attacks on Aircraft Instrument Landing Systems," *Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, August 14–16, 2019*, 375 – 372. https://www.usenix.org/system/files/sec19-sathaye.pdf.
[24] Tegg Westbrook, "Trojan spoofing: A threat to critical infrastructure." *Security and Defence Quarterly*, 42 no.2 (2022): 1-14. 10.35467/sdq/164760.
[25] Thomas Brewster, "Watch GPS Attacks That Can Kill DJI Drones Or Bypass White House Ban," *Forbes*, August 8, 2015, https://www.forbes.com/sites/thomasbrewster/2015/08/08/qihoo-hacks-drone-gps/#7f6c16cf2bf5; Lin Huang and Qing Yang, "GPS Spoofing: Low-Cost GPS Simulator." *Presented at DEF CON 23, Las Vegas, NV, USA, August 2015.* https://www.researchgate.net/publication/286330869_Low-cost_GPS_simulator_-_GPS_spoofing_by_SDR.
[26] Tegg Westbrook, "Trojan spoofing: A threat to critical infrastructure." *Security and Defence Quarterly*, 42 no.2 (2022): 1-14, doi: 10.35467/sdq/164760.
[27] Help Net Security, "Research shows Tesla Model 3 and Model S are vulnerable to GPS spoofing attacks," June 19, 2019, https://www.helpnetsecurity.com/2019/06/19/tesla-gps-spoofing-attacks/; Regulus, "TESLA MODEL 3 SPOOFED OFF THE HIGHWAY – REGULUS NAVIGATION SYSTEM HACK CAUSES CAR TO TURN ON ITS OWN," August 04, 2019, https://www.regulus.com/blog/tesla-model-3-spoofed-off-the-highway-regulus-navigation-system-hack-causes-car-to-turn-on-its-own.

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

[28] Patrick Tucker, "DHS: Drug Traffickers Are Spoofing Border Drones," *Defense One,* December 17, 2015, https://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/.

[29] Dana Goward, "Who "Moved" the Position of a U.S. Navy Ship From Odessa to Crimea?" *The Maritime Executive*, July 6, 2021, https://www.maritime-executive.com/editorials/who-moved-the-position-of-a-u-s-navy-ship-from-odessa-to-crimea.

[30] Neal Ungerleider, "Spoofed Satellite Feeds Trouble Google's Global Fishing Watch," *Fast Company*, November 20, 2014, https://www.fastcompany.com/3038863/spoofed-satellite-feeds-trouble-googles-global-fishing-watch; Michael Hoffmann, "Roving bandits and looted coastlines: How the global appetite for sand is fuelling a crisis," *The Conversation*, May 3, 2020, https://theconversation.com/roving-bandits-and-looted-coastlines-how-the-global-appetite-for-sand-is-fuelling-a-crisis-132412; Bjorn Bergman, "Systematic data analysis reveals false vessel tracks," *SkyTruth,* July 29, 2021, https://skytruth.org/2021/07/systematic-data-analysis-reveals-false-vessel-tracks/.

[31] Lisa Vaas, "US state police cars hacked," *Naked Security*, October 02, 2015, https://nakedsecurity.sophos.com/2015/10/02/us-state-police-cars-hacked/; Thomas Brewster, "Watch GPS Attacks That Can Kill DJI Drones Or Bypass White House Ban," *Forbes*, August 08, 2015, https://www.forbes.com/sites/thomasbrewster/2015/08/08/qihoo-hacks-drone-gps/#624ba6002bf5; Eric Mu, "China's Qihoo Hacks A Tesla Model S," *Forbes*, July 15, 2014, https://www.forbes.com/sites/ericxlmu/2014/07/15/chinas-qihoo-hacks-a-tesla-model-s/#3e3cdaee3ead; Roi Mit, "GPS Spoofing Mystery Affirms Need for Protection," *Wards Auto*, April 23, 2019, https://www.wardsauto.com/industry-voices/gps-spoofing-mystery-affirms-need-protection.

[32] Zeng et al, "All Your GPS Are Belong To Us…"; UT News, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea," July 29, 2013, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/.

[33] STRIKE3, "STRIKE3 Project." European Global Navigation Satellite Systems Agency, Horizon Europe, gnss-strike3.eu. Accessed July 13, 2021.

[34] FBI Cyber Division, "Cargo Thieves use GPS Jammers to Mask GPS Trackers." October 02, 2014: 1-4, 1. info.publicintelligence.net/FBI-CargoThievesGPS.pdf.

[35] G4S, *Supply Chain: Defeating the Security Watchdog, Corporate Risk Services*, Intelligence Bulletin, 2017: 1, 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.

[36] University of Nottingham, "GPS jamming: keeping ships on the 'strait' and narrow." Last modified July 21, 2016. https://www.nottingham.ac.uk/news/pressreleases/2016/july/gps-jamming-keeping-ships-on-the-strait-and-narrow.aspx.

[37] Chew Hui Min, "First Singaporean to catch all 145 Pokemon admits getting help from overseas friends," *The Straits Times*, August 18, 2016, https://www.straitstimes.com/singapore/first-singaporean-to-catch-all-145-pokemon-admits-getting-help-from-overseas-friends; https://www.executivetraveller.com/news/smart-selfies-the-key-to-home-isolation.

[38] Geoawesonware, "Wanna hack a drone? Possible with geo-location spoofing!" July 26, 2012, https://geoawesomeness.com/geo-location-spoofing/.

[39] Ahmet Saim Yılmaz; Haydar Çukurtepe; Emin Kuğu, "Analysis of Location Spoofing Threats on E-Scooter Sharing." *2022 30th Signal Processing and Communications Applications Conference (SIU), 2022:* 1-4. 10.1109/SIU55565.2022.9864946.

[40] Evelyn Hutton, "How to Avoid And Remove Pokemon Go Soft Ban Time?" *iToolLab*, December 07, 2021, https://itoolab.com/location/how-to-avoid-and-remove-pokemon-go-soft-ban-time/.

[41] Medha Basu and Tian Jiao Lim, "How Singapore is cutting time to isolate Covid patients," *GovInsider,* June 12, 2020, https://govinsider.asia/digital-gov/bruce-liang-ihis-how-singapore-is-cutting-time-to-isolate-covid-patients/; David Flynn, "'Smart selfies' the key to home isolation," *Executive Traveller*, September 30 2021, https://www.executivetraveller.com/news/smart-selfies-the-key-to-home-isolation.

[42] Karen Hao and Nadine Freischlad, "The gig workers fighting back against the algorithms," *MIT Technology Review*, April 21, 2022, https://www.technologyreview.com/2022/04/21/1050381/the-gig-workers-fighting-back-against-the-algorithms/; also personal correspondence with Nicolás Palacios Crisóstomo, doctoral candidate at D-BAUG, ETH Zürich.

[43] Tegg Westbrook, "Will GPS Jammers Proliferate in the Smart City?" *Salus Journal* 7, no.2 (2019): 45-67.

[44] Steve Ragan, "Grindr vulnerability places men in harm's way," *CSO*, September 10, 2014, https://www.csoonline.com/article/2604777/grindr-vulnerability-places-men-in-harms-way.html.

[45] "Phone jammer." https://www.phonejammer.com. Accessed November 11, 2022.

[46] Ben Grubb, "Popularity of mobile jamming in Australia revealed by regulator," *The Sydney Morning Herald*, March 29, 2012, https://www.smh.com.au/technology/popularity-of-mobile-jamming-in-australia-revealed-by-regulator-20120327-1vwvr.html; Heather McCracken, "Blockers break ban," *NZHerald*, March 20, 2010, https://www.nzherald.co.nz/nz/blockers-break-ban/DSXQ7LAQZJKSHER5GOYEWWYLZY/.

[47] "Stop the problem before it starts." https://mosquitoloiteringsolutions.com. Accessed November 11, 2022.

[48] It is also useful, without prejudice to grey hats, to consider whether some academics who identify security flaws in GPS systems should also be considered ethical hackers with sometimes a light tint of grey (at least on an unofficial capacity, before asking permission). The motivations to do this are also career oriented. Indeed, there are bachelor's degrees in ethical hacking in some areas of the world, and with standardised certification.

[49] Shech [pseudonym], "Fake apps and GPS spoofing used by fraudulent Grab drivers to cheat passengers and fellow drivers," *The Independent*, May 19, 2019, https://theindependent.sg/fake-apps-and-gps-spoofing-used-by-fraudulent-grab-drivers-to-cheat-passengers-and-fellow-drivers/.

[50] Brad Haines, "DEFCON 20: Hacker + Airplanes = No Good Can Come Of This." *Presentation at DEF CON Hacking conference 20, July 26 - 29* (2012). Presentation available via YouTube: https://www.youtube.com/watch?v=CXv1j3GbgLk.

[51] Eric Mu, "China's Qihoo Hacks A Tesla Model S," *Forbes*, July 15, 2014, https://www.forbes.com/sites/ericxlmu/2014/07/15/chinas-qihoo-hacks-a-tesla-model-s/#3e3cdaee3ead.

[52] Dark Reading, "GPS Spoof Hits Geneva Motor Show," March 13, 2019, https://www.darkreading.com/iot/gps-spoof-hits-geneva-motor-show/d/d-id/1334147.

[53] Identifying and locating individuals committing what might be considered 'immoral' acts within certain subcultures or religions (for example homosexuality in Islam or the Catholic church), by for example using 'hookup apps,' could be used for both persecution or even blackmail (a form of religious vigilantism, if you like); Matthew P. Schneider, "Electronic Privacy and Fidelity," *Through Catholic Lenses*, August 4, 2021, https://www.patheos.com/blogs/throughcatholiclenses/2021/08/electronic-privacy-and-fidelity/; Sharona Coutts, "Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits," *Rewire*, May 25, 2016, rewirenewsgroup.com/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/;

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081

Activists may try to overcome drone defences to enable surveillance (of farms, abattoirs, protests at airport etc,) (Trojan Spoofing).

[54] Justin Rowlatt, "Gatwick drone attack possible inside job, say police," *BBC News*, April 14, 2019, https://www.bbc.co.uk/news/uk-47919680.

[55] G4S, *Supply Chain: Defeating the Security Watchdog, Corporate Risk Services*, Intelligence Bulletin, 2017: 1, 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; New Strait Times, "Singapore ride-hailing drivers using fake apps, GPS spoofing to cheat Grab," May 18, 2019, https://www.nst.com.my/world/2019/05/489591/singapore-ride-hailing-drivers-using-fake-apps-gps-spoofing-cheat-grab; Naval Surface Warfare Center, *The Threat of radio frequency weapons to critical infrastructure facilities*, TSWG & DETO Publication, 17320 Dahlgren Road,Dahlgren,VA,22448, August 2005: 1-13, 7, https://apps.dtic.mil/sti/pdfs/ADA593293.pdf. Accessed 04 May, 2023.

[56] Tegg Westbrook, "Will GPS Jammers Proliferate in the Smart City?" *Salus Journal* 7, no.2 (2019): 45-67.

[57] Dan Goward, "The History of GPS Spoofing." *Presentation at John Hopkins University Applied Physics Laboratory*, available via You Tube: https://www.youtube.com/watch?v=L2fZGVVH5lg&t=3109s.; Neal Ungerleider, "Spoofed Satellite Feeds Trouble Google's Global Fishing Watch," *Fast Company*, November 20, 2014, https://www.fastcompany.com/3038863/spoofed-satellite-feeds-trouble-googles-global-fishing-watch; Jake Ryan, "Revealed: Iran's 'ghost armada' of 123 sanction-busting tankers is selling black market oil to China to bankroll its secret nuclear programme," *The Daily Mail*, June 20, 2021, https://www.dailymail.co.uk/news/article-9704151/Irans-ghost-armada-tankers-selling-black-market-oil-China-bankroll-nuclear-programme.html?ns_mchannel=rss&ns_campaign=1490&ito=1490; Michael Hoffmann, "Roving bandits and looted coastlines: How the global appetite for sand is fuelling a crisis," *The Conversation*, May 3, 2020, https://theconversation.com/roving-bandits-and-looted-coastlines-how-the-global-appetite-for-sand-is-fuelling-a-crisis-132412.

[58] Bobby Allyn, "Digital Ambulance Chasers? Law Firms Send Ads To Patients' Phones Inside ERs," *NPR*, May 25, 2018, https://www.npr.org/sections/health-shots/2018/05/25/613127311/digital-ambulance-chasers-law-firms-send-ads-to-patients-phones-inside-ers?t=1604415668217&t=1605714336526.

[59] Adam Dolnik, *Understanding Terrorist Innovation: Technology, Tactics and Global Trends,* Abington: Routledge, 2007.

[60] Ronald V. Clarke and Graeme R. Newman, *Outsmarting the Terrorists*, London: Praeger Security International, 2006.

[61] The Associated Press, "The Al-Qaida Papers – Drones." 2011?, https://cryptome.org/2013/02/al-qaida-drones.pdf, 2.

[62] Dan Goodwin, "The radio navigation planes use…"; Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir, "Wireless Attacks on Aircraft Instrument Landing Systems." *Proceedings of the 28th USENIX Security Symposium, Santa Clara, CA, USA, August 14–16, 2019*: 375 – 372. https://www.usenix.org/system/files/sec19-sathaye.pdf.

[63] Naval Surface Warfare Center, *The Threat of radio frequency weapons to critical infrastructure facilities*, TSWG & DETO Publication, 17320 Dahlgren Road,Dahlgren,VA,22448, August 2005: 1-13, 7, https://apps.dtic.mil/sti/pdfs/ADA593293.pdf. Accessed 04 May 2023.

[64] Tegg Westbrook, "Trojan spoofing: A threat to critical infrastructure." *Security and Defence Quarterly*, 42 no.2 (2022): 1-14.10.35467/sdq/164760; BBC News, "Saudi oil attacks: US blames Iran for drone strikes on two sites," September 15, 2019, https://www.bbc.co.uk/news/world-middle-east-49705197; VoV News media report, untitled ["…the Saudi Defense System failed to spot our drones"]. https://www.voanews.com/media/2394681/embed. Accessed October 16, 2020.

[64] Joby Warrick, “Use of Weaponized Drones by Isis Spurs Terrorism Fears,” *Washington Post*, February 21, 2017 in https://www.ausa.org/publications/role-drones-future-terrorist-attacks.

[65] Chris Lo, "GPS spoofing: what’s the risk for ship navigation?" *Ship Technology*, April 15, 2019, https://www.ship-technology.com/features/ship-navigation-risks/; Tanya Blake, "Hackers took ‘full control’ of container ship’s navigation systems for 10 hours," *Resilient Navigation and Timing Foundation*, November 22, 2017, https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/. The blog is referring to a report released by IHS Markit, "Navigating Maritime Risks in a sea of New and Emerging Challenges: An Insurers’ Perspective," no date, https://ihsmarkit.com/events/navigating-maritime-risks-in-a-sea-of-new-and-emerging-risks-an-insurers-perspective/overview.html. Accessed July 06, 2022.

[66] Gordon Corera, “Ukraine War: Don’t Underestimate Russia Cyber-threat, Warns US,” *BBC News*, May 11, 2022, https://www.bbc.com/news/technology-61416320.

https://digitalcommons.usf.edu/jss/vol16/iss2/5
DOI: https://doi.org/10.5038/1944-0472.16.2.2081