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

Aircraft vulnerability to politically motivated Radio Frequency Interference (RFI) in Eastern Europe

Tegg Westbrook

teggwestbrook@gmail.com

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

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

Abstract

Countries in Europe have experienced radio frequency interference from Russian electronic warfare units, affecting navigation systems without discrimination. Interference has been identified as coming from the Russian mainland, Kaliningrad, and in the areas where it is engaged in conflicts abroad, creating serious hazards for aircraft. Previous research has identified the technical vulnerabilities to aviation from radio frequency interference, but it has yet to be contextualised in light of the ongoing geopolitical tensions. Using literature review analysis, the aim of the article is to place the jamming and spoofing threat in the context of ongoing political tensions between Russia and the region and to establish worse-case scenarios based on the former's motives. Focusing on the threats to aircraft, it finds that the likely motivations are to (1) complement political narratives of Western aggression; (2) to deny service for intimidation, harassment, economic loss, and to portray a dominant Russian cyber influence; and (3) to use spoofing to enable hostage diplomacy via the seizure of people and assets. It argues that reporting mechanisms for aviation risks assumes geographical staticism, which does not correspond adequately to the threat. It also creates arbitrary "predictability" in otherwise unpredictable environments, which could ultimately affect vigilance and due diligence in the areas not considered problematic.

Keywords

electronic warfare, cyber security, geopolitics, satellite navigation systems

Article Info:
Received: 15 September 2023
Revised: 3 January 2024
Accepted: 4 January 2024
Available online: 9 February 2024

Citation: Westbrook, T. (2024) 'Aircraft vulnerability to politically motivated Radio Frequency Interference (RFI) in Eastern Europe', *Security and Defence Quarterly,* 46(2), pp. 104–117. doi: 10.35467/sdq/178249.

Introduction

Russia's invasion of Ukraine has pulled the world back to the early 20th century thinking about international relations, revitalising largely outdated notions of pure realism. The ongoing tensions between North Atlantic Treaty Organization (NATO) and Russia are dynamic and could change at a moment's notice as a result of miscalculating and misreading intentions. The electronic warfare (EW) technologies at states' disposal threaten both civilian and military systems, and the separation between critical civilian functions and their protection from military activity are becoming harder to achieve.

Russia possesses a range of EW equipment that includes jamming and spoofing technologies and has used them consistently and indiscriminately against civilian users of the Global Navigation Satellite System (GNSS) outside or within intra- and interstate conflicts. Navigational functions on aircraft have been consistently affected by Russian jamming. Radio frequency jamming denies service to users, including critical location information. Spoofing creates misleading location information, which poses a more serious problem for aviation, particularly in poor weather conditions, at night time, in busy skies, and when flying near precarious borders.

Radio frequency interference (RFI) has an impact on network efficiency, cost effectiveness, undermines trust in the GNSS, and adds additional financial burden for operators having to invest in security measures (Eurocrontrol, 2021). Challenges posed as a result of RFI are the possible misdirection of civilian users, which is especially precarious in the aviation sector. This could lead to major civilian casualties and also create potential escalation between Russia and the West. In aviation, where ground- and satellite-based signals are used for navigation purposes, it is important to consider the consequences resulting from RFI from a geopolitical perspective.

RFI is used defensively and offensively in different scenarios, affecting civilian and military aircraft, and often the interference can be attributed to intentional interference, collateral interference to civilian systems in conflict areas, or in non-combat situations (hereafter, conceptual clarifications are not always explicated). Since 2016, denial of service RFI has been used to conceal the true locations of key Russian officials and Russian military units, which has affected all constellations (even Russia's own GLONASS) (Westbrook, 2023a, p. 76). A massive rise in GNSS RFI incidents was identified in 2018, where 38.5% of European en-route air traffic operating through the region was regularly affected by RFI. In fact, 5% of this traffic in the designated "disruption zones" was considered needing special assistance due to the increase in potential pilot and controller workload (Mishra, 2022, slide 3). In 2021, it was cited that there had been a 2000% increase in GNSS RFI incidents since 2018, according to the voluntary incident reporting mechanism (Goward, 2023). In 2019 alone, there were up to 10,000 jamming and spoofing events, affecting aviation systems beyond Russia's borders (StrategyPage, 2019; Westbrook, 2023a). Since February 2022, indiscriminate jamming within and outside Russian territory has intensified. While its military utility is widely documented, it has yet to be known how the tactical use of RFI against aircraft could further Russia's political aims.

Taking inspiration from a taxonomy of jamming and spoofing tactics (Westbrook, 2023b), and considering previous incidents of RFI (not just relating to Russia), the aim of the article is to place the jamming and spoofing threat in the context of ongoing political tensions between Russia and the region, and to establish worse-case scenarios based on the former's motives. The article explores how intentional and collateral RFI could lead to catastrophic unintentional events. In extreme cases, RFI could accidentally prompt military responses from NATO or Russia, leading to potential escalation.

The article first explores how RFI has affected aircraft in Europe, drawing on previous military exercises and local RFI documented by the media and pilot reports. It considers patriot hackers, cyber mercenaries, and Russian military units as the main threats. It then critiques the suitability of the European Union Aviation Safety Agency's (EASA) Information Sharing and Cooperation Platform on Conflict Zones (2022d). It follows by exploring the specific vulnerability of aircraft, particularly the Automatic Dependent Surveillance–Broadcast (ADS-B) and the Instrument Landing System (ILS), and what the motives might be behind that interference. Following a thematic overview of political motivations, the conclusion argues that collateral or intentional RFI could purposely or indeed inadvertently escalate tensions between Russia and the West due to the potential of fabricating data, or opposing parties misinterpreting or miscalculating intentions based on those fabrications, putting lives and aviation safety at risk.

The methodology involved a literature review mapping the EW activities in the region and how they have affected military and civilian use of the GNSS. Using existing primary and secondary data identifying both real and hypothetical risk to aviation (from other case examples not involving Russia), the data was arranged into themes relating to the possible means–ends objectives of Russian units and sympathetic non-state actors. The study also used taxonomy of spoofing and jamming tactics to inform new critical thinking about scenarios that might manifest themselves.

Background

The Russian invasion of Ukraine and cyber and RFI threats in Europe

Europe shares thousands of kilometres of borders and seaways with Russia and Belarus, and is facing threats of invasion. Billions of Euros in trade rely on secure land, sea, and air navigation. Some Eastern European states, with western allies, support Ukraine financially and with weapons, imposing sanctions and flight restrictions (European Commission, 2022). North, east, and southeast Europe, along with the Arctic, frequently experience Russian jamming and spoofing (US Department of Transportation Maritime Administration, 2022).

In response to Russian EW actions in Ukraine, Europe's aviation authority warns of GNSS issues affecting GPS and Galileo users (European Union Aviation Safety Agency [EASA], 2022a, p. 2). Russian RFI, spanning from Varanger to Kaliningrad and the Kola Peninsula, has disrupted aviation systems and airports, leading to cancelled flights (Nilsen, 2022b). These incidents are becoming more frequent and prolonged (Nilsen, 2022a) and even affectair ambulance services.

RFI has various criminal and military uses, including Russia supplying non-state actors in Ukraine (Patrick, 2015, 2016; Westbrook, 2019b, p. 6). Homemade jamming systems, including legacy Soviet technology, water pumps, copper pipes, and electromagnetic emitters, pose aviation risks (The Associated Press, 2011, p. 3). Off-the-shelf jamming and spoofing devices are accessible and concealable, from miniaturised versions to backpack-sized equipment (Westbrook 2019b, p. 9).

States may use ‘cyber mercenaries’ covertly for offensive or defensive purposes, targeting emergency responders, port operators, and airliners (Westbrook, 2023b). Patriot hackers and cyber mercenaries, often limited to civilian systems, are much less sophisticated than state militaries (Westbrook, 2023a, p. 86). Russian EW units possess advanced EW technologies and trade with other countries (Iran, possibly China).Coordination among aviation authorities is emerging to tackle the growing RFI problem, despite the challenges posed by diverse attack methods and attackers (Westbrook, 2023b).

What is Europe doing?

As a result of interference from civilian and military users, in recent years there has been a stronger international urge for action from the likes of the International Air Transport Association (IATA) and the U.N.’s International Civil Aviation Organisation (ICAO), among others (Goward, 2023). In terms of restrictions on trade, the European Union (EU) and United Kingdom have adopted a number of bans of exports on goods, technology, and technical assistance targeting the Russian aviation sector (EASA, 2022c; UK Government, 2023). Following a number of serious aviation incidents after Russia’s annexation of Crimea in 2014, the EU, for example, has developed common rules in reporting civil aviation safety hazards (although this was planned before the invasion happened; European Parliament, Council of the European Union, 2014). As a result of increase in interference since 2022, the EASA (2022b), using data from network of analysts and open sources, has issued information about affected regions and a European information sharing and cooperation platform on conflict zones. The aim of the platform is to enable domestic operators to carry out risk assessments based on events experienced by other operators. Safety information bulletin warnings communicating increased probability of issues with GNSS interference are shared. Unlike the equivalent US reporting systems (Aviation Safety Reporting System (ASRS), 2023), the reporting mechanism is not open access to independent observers, but only to commercial air operators within the EASA. The information is not distributed in real time based on current events, and has little context about the motivations for why RFI might be used.

The reporting mechanism also assumes that RFI is a static problem confined to geographical locations. This may lead to interference being shrugged off as blips in the areas considered safe. Indeed, it assumes a level of predictability in problem areas which may lead to lack of vigilance in non-problem areas. Due to the new “normality” of frequent and prolonged RFI, interference may be treated with less due diligence as “passive alarms” that are not serious enough to warrant more action. RFI can come from the ground, from other aircraft, people onboard aircraft, or from devices within or attached to aircraft. Finally, the inadequate sharing of data to other interested parties gives observers a narrow picture that produces conjecture and redundancy, rather than objective and evidence-based analysis and response to the full risk situation.

Why is RFI Specifically Dangerous for Aviation?

Many aircraft, including manned and unmanned aerial vehicles, rely on the position, timing, and navigation information provided by the GNSS and other navigations aids. While all aircraft are vulnerable to RFI, smaller aviation users are at the highest risk, because many of these aircraft use consumer-grade GPS receivers (Goward, 2023), and do not have the additional navigation aids that large commercial aircraft typically have.

There are many different navigation aids built into various aircraft, and many studies have demonstrated that a number of aviation systems are vulnerable to attacks (Sathaye *et al.*, 2019). The Automatic Dependent Surveillance–Broadcast (ADS-B), for example, enables pilots and other observers to identify where (most) other aircraft are at any given time. In some cases, ADS-B is used as a sole means of position information and surveillance of other aircraft when the level of service is low. In the current literature exploring technical vulnerabilities of navigation systems in aircraft and supporting infrastructure (e.g. Costin and Francillon, 2012; Kožović and Đurđević, 2019, 2021; Sathaye *et al.*, 2019; Khan *et al.*, 2021), there have been numerous problems identified with ADS-B. This includes injecting non-existing aircraft by spoofing ADS-B messages, and modifying the route of an aircraft by jamming and replacing the ADS-B signals. ADS-B has been criticised for lacking the minimal and necessary mechanisms, including entity authentication, message encryption, and vulnerability to tampering (Costin and Francillon, 2012, p. 1), among other things (Alohali, 2019).

For landing purposes, aircraft may use the Instrument Landing System (ILS) to navigate a plane's position in relation to the runway. It has been identified that ILS is vulnerable to so-called overshadow attacks, which is where an attacker can transmit signals that overpower the ILS signals (Sathaye *et al.*, 2019, p. 361). Other types of attacks, such as those against signal generation, can "cause deflections in the course deviation indicator needle" (Sathaye *et al.*, 2019, p. 359). The seriousness of the problem can depend on the location, the duration, the phase of the flight, and environmental conditions. If such systems are affected, pilots usually resort to other navigational cues and detection systems, but when such alternatives are not available, or degraded, it could lead to serious hazards.

Some instances of accidental military jamming gives us an idea of the potential harm it can do to civilian systems if/when used in an indiscriminatory manner (Harris, 2021), and the impacts are not just felt by aviation systems. Numerous hazards have been reported from anonymous pilots in the United States, ranging from airspace violations and near collisions to landing at the wrong airport as a result of jamming and spoofing (National Aeronautics and Space Administration [NASA], 2022). The Institute of Electrical and Electronics Engineers (IEEE) spectrum has also documented "173 instances of lost or intermittent GPS during a six-month period of 2017 and another 60 over two months in early 2018" because of accidental military jamming. The data they found

> show aircraft flying off-course, accidentally entering military airspace, being unable to manoeuvre, and losing their ability to navigate when close to other aircraft. Many pilots required the assistance of air traffic control to continue their flights. The affected aircrafts included a pet rescue shuttle, a hot-air balloon, multiple medical flights, and many private planes and passenger jets (Harris, 2021).

Flight deviations and airspace violations as a result of suspected GPS jamming and spoofing have been reported frequently from anonymous pilots, some of which have been tied to military training activities (NASA, 2022). Reports from 2022 alone indicate altitude deviations, track heading deviations, the GPS going into dead reckoning mode without the pilot noticing, and very near airspace violations due to incorrect GPS readings (NASA, 2022). Some reports indicate how GPS interference distracts pilots, some already fatigued after long flights, and leads them to inadvertently violating airspace. In 2019, a commercial passenger aircraft, having relied on GPS through the mountainous approach in the Sun Valley in Idaho, deviated off course due to low-level inference. The aircraft was reportedly saved by an attentive radar controller, saving the lives of all on board (Goward, 2023).

In extreme circumstances, distractions and deviations could mean relying on limited fuel reserves, and for sleep-deprived pilots on long-haul flights with limited resting periods, it could lead to more serious mistakes. Deviations into countries experiencing conflict, such as Russia, Belarus, and Ukraine, could result in the plane being misidentified, as indicated by the EASA (2022b).

There has been a speculation about spoofing, leading to the tragic Malaysia Airlines Flight MH370 disaster in 2014 (Wise, 2019; Rietjens, 2019) which probably deviated from its North-East flight path from Kuala Lumpur to Beijing and was last picked up by military radar heading North-West towards the Indian Ocean. It has been suggested by some national authorities that the flight path could have been altered by an employee, but there has been no conclusive evidence.

All in all, these examples demonstrate how indiscriminate or targeted attacks against aircraft are worthy of specific analysis in political sciences. Hereafter, drawing on various related and unrelated incidents, the tactical and politically motivated attacks are arranged into hypothetical categories.

Results

RFI to complement political narratives of Western aggression

One main concern about RFI is the potential that actors could spoof aircraft into Russian airspace in real terms but also via pilot's and observer's digital interfaces. Russia has consistently used alternative media narratives to justify its unprovoked invasion of Ukraine. These narratives are targeted towards its own population and populations of sympathetic states. Where spoofing of aircraft could aid such narratives, in the taxonomy of RFI tactics (Westbrook, 2023b, p. 73), one such strategy of decoy spoofing could fit into such motives. Used primarily to trick other users into an action desirable to the attacker, the same strategy could be used to give the impression that NATO aircraft have been intruding into Russian or Belarussian airspace.

Concerns about the vulnerability of ADS-B bare similar risks in terms of "digital intrusions" into territories. Following 9/11, it was found that hackers could easily introduce as many as 50 false targets onto controllers' radar screens (McCallie, 2011, p. 17). Two researchers spoofed "faked aircraft into the simulated busy airspace over San Francisco." They found that "[s]poofing a target into the real ADS-B system would be a simple matter of transmitting the signal on the ADS-B frequencies (978 and 1090 MHz)" (Thurber, 2012). While such studies indicate a more maligned and destructive motivation, similar strategies could be used to give the impression of airspace violation, or inadvertently influence a pilot to enter airspace to avoid falsified, impending collisions.

While spoofing can be used to demonstrate western aggression in the digital domain, it can, and has been, used to justify the shooting down of aircraft. In proxy conflicts, such interference is intended for the purpose of testing military systems while not instigating a direct military confrontation. While there are no known instances of military actors targeting civilian aircraft for such purposes, it is worth considering military systems as being ample targets for such political tactics. In the taxonomy, the strategy of *correcting* or *following crooked* paths (Westbrook, 2023b, pp. 72–73) could provide both explanations for why two US drones were misdirected into Iranian skies. Dana Goward, a commentator on RFI events, noted that the flight was on a routine trip from two different ports off the coast of Saudi Arabia in international airspace. “Somehow [the drone] ended up way to the left, where the Iranian navy just happened to be waiting for them. All of a sudden it’s taking a right-hand turn toward Iran, and getting shot down while it was in their territorial airspace” (Adde, 2021). In 2019, then President Donald Trump reportedly “came close to calling for an airstrike against Iran in retaliation” (Adde, 2021). Former US Vice President Dick Cheney similarly stated that he supported the option of targeting a captured US *unmanned* aerial vehicle (UAV) that Iran claimed to have captured (expanded later) (Westbrook, 2019b, p. 9).

While correcting or following crooked path attacks could inadvertently lead to military confrontations, indiscriminate jamming and spoofing attacks, such as these, could likewise lead to civilians being accidentally targeted due to incorrect or degraded navigation information. During the Cold War era, passenger flights, such as the London to Tel Aviv El Al Flight 402, strayed into and was subsequently shot down in Bulgarian airspace. The Libyan Arab Airlines Tripoli to Cairo flight LN 114 experienced equipment failure and got lost in the disputed Sinai Peninsular in bad weather. It was shot down. And two Korean Airlines passenger aircraft in 1978 (KAL 902) and 1983 (KAL 007) strayed into Soviet airspace and were shot down. Ironically, such examples were prior to accurate GNSS was a utility available to commercial airliners, but even with GNSS ubiquity, incidents of misidentification occur. In January 2020, Ukraine International Airlines flight PS752 was tragically shot down in Tehran because it was misidentified as a US missile during heightened tensions between the two countries, according to Iran’s armed forces (which previously blamed it as a technical fault; Gritten, 2023).

Indeed, we do not need to look hard for an example of high-grade military equipment being used by non-state actors where a catastrophic incident happened. Although not related to RFI, a notable example includes the downing of Malaysia Airlines Flight 17 in 2014 by pro-Russian separatists in Ukraine using a Russian-supplied Buk surface-to-air missile, resulting in 298 deaths. The aircraft was misinterpreted as a military aircraft. Russia and its media changed their narrative many times but initially insisted that a NATO plane was shot down, then insisting a Ukrainian jet shot at the aircraft. Russian nationals Igor Girkin, Sergey Dubinsky, and Oleg Pulatov, and Ukrainian national Leonid Kharchenko were tried in absentia. Girkin, Dubinsky, and Kharchenko were sentenced to life imprisonment (Netherlands Prosecution Service, 2021).

Denial of service (DoS) for intimidation, harassment, economic loss, and to portray a dominant Russian cyber influence

Denial of service is intended to degrade and deny confident use of GPS and other navigation beacons, and potentially destroy the victim’s receivers with strong overpowering signals (Westbrook, 2023b, p. 74). Recent papers have focused on the political motives of DoS attacks on the radio spectrum and the state level (Westbrook, 2019a, 2023b) and DoS has been linked to the potential indirect loss of life as a result of degrading the ability of emergency services to operate safely (Harris, 2021). Some events have been attributed to civilian users using cheap jammers to avert toll payments in Norway and elsewhere (Gangeskar and Laagstein, 2022; Westbrook, 2019a). It has also been linked to causing economic damage to airports, particularly for civilian users (Woodrow, 2017). In all likelihood, there are possibly thousands of such incidents each year worldwide that are not reported openly. Thus, if this can all happen accidentally or unintentionally, what can be done intentionally?

Russian military DoS has recently been described as “smart jamming” by some commentators (Center for Advanced Defense Studies (C4ADS), 2019, p. 9; Milner, 2020 citing Todd Humphreys), specifying that such jamming can morph into spoofing, giving the pilot hazardously misleading information, instead of direct loss of position information. This smart jamming could 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 them go in the wrong direction because of crooked path attacks (Westbrook, 2023b, p. 72). A test undertaken by the University of Texas at Austin found, for example, that inducing a false trajectory reading into a drone could make it try to correct its position, and potentially crash as a result (Kerns *et al.*, 2014).

Similar issues have been identified when spoofing the Instrument Landing System (ILS) used for landing planes. Evidently, the RFI at the landing stage could be imposed by (suspected) cell phone towers, or other electromagnetic interference, as was considered in cases in South Korea, the Philippines, Indonesia, and Thailand (International Civil Aviation Organization, 2018). In South Korea, of the hundreds of aircraft affected, four missed their approach due to a GPS warning (International Civil Aviation Organization, 2012). Such attacks could easily be imposed by low-sophisticated political actors, such as patriot hackers, and thus also potentially by indiscriminate military-grade spoofing.

It is certainly important to consider the possibility of attacks on the ILS based on other previous operational failures of the system, including the Singapore Airlines flight SQ327 (143 passengers and 15 crew) in 2011, which “unexpectedly banked to the left […] about 30 feet above a runway,” and then “veered to the right, crossed the centreline” at Munich airport in Germany (Goodwin, 2019; German Federal Bureau of Aircraft Accident Investigation status report, no date). According to an incident report, “the jet missed its intended touch down point by about 1,600 feet. Investigators said one contributor to the accident was localiser signals that had been distorted by a departing aircraft” (Goodwin, 2019). Goodwin (2019) also notes other “near-catastrophic accidents involving ILS failures”, including “Air New Zealand flight NZ 60 in 2000 and a Ryanair flight FR3531 in 2013 (Dutch Safety Board, 2014). DoS smart jamming could hypothetically replicate what was found with a low-cost spoofing device. Spoofing ILS could “generate what is sometimes called a ‘fly down’ signal that instructs the pilot to steepen the angle of descent, possibly causing the aircraft to touch the ground before reaching the start of the runway.” A pilot could “react by guiding the plane to the right and inadvertently steer over the centreline” (Goodwin, 2019; see also Sathaye *et al.*, 2019).

The seriousness of such scenarios is heightened in bad weather conditions, in darkness, and at airports where there are high volumes of entering and departing aircraft. For example, the augmented depictions of the vertical path (the glide path) that a plane follows cannot always be visually verified in poor weather. In summary, smart jamming used intentionally to target the ILS could lead to serious hazards in drone operations and for aircraft landings.

RFI to enable hostage diplomacy via the seizure of people and assets

Prolonged and intermittent jamming of civilian areas may bring governments to the negotiation table if the jamming is affecting a nation’s society and the economy, as in the case of North Korea targeting South Korea for an extended number of days in 2012 and thereafter (Westbrook, 2019b, p. 5). Jamming could be so severe that commercial aircraft users are forced to land. Such events alone demonstrate how jamming could coerce opposing governments to negotiate matters and enable seizure of assets. Sophisticated and tactical use of GNSS spoofing, particularly crooked path attacks, can also be used as a hybrid warfare tactic by mixing fake news, plausible deniability, and "hostage diplomacy" via the seizure of people and assets.

Iran has been known to coerce merchant shipping into its territorial waters to justify seizures for hostage diplomacy strategies (Bockmann, 2019; Dudley, 2021; Hughes and Selby, 2019; Westbrook, 2023a). With incorrect position and velocity readings, a plane could unknowingly stray a few miles between invisible borders, from one airspace, which is peaceful, to one at war or which is hostile. Provided that there are very limited physical navigation aids to cross-check, or a well-caffeinated co-pilot to check every other instrument on board, even slow and subtle increase in *speed* and changes in *direction* over relatively long periods could create eye-watering slip-ups. Researchers have found that they can purposely deviate the speeds of aircraft targeting onboard FLARM transceiver devices by implementing faked target positions and reported positions of other aircraft (Jansen *et al.*, 2018, p. 1021). This could also inadvertently influence a pilot to intrude into airspace.

No open-source account exists of these methods of attacks happening to manned aircraft. The lengths at which governments and non-state actors will go to leverage concessions, however, leave the question of worse-case scenarios open to conjecture. The Belarussian government deliberately falsified a bomb threat on an Athens to Vilnius Ryanair flight (4978) to arrest 27-year-old journalist Roman Protasevich during its brutal crackdown on dissidents in the country (Eccles and Sheftalovich, 2022). The United Kingdom and EU, among other states, banned flights from using Belarussian airspace.

Spoofing-enabled hijacking or stealing can also be done to obtain intellectual property. Indeed, in 2012, it was speculated that Iran's military spoofed an American RQ-170 spy drone operating on the Afghan–Iran border. Having boasted of successfully spoofing the drone to land, and showcasing the drone to international media, the Iranians subsequently reverse-engineered the machine in design, material (which was "stealth-coated"), and possibly components (including flight controls, communications, video equipment, and self-destruct holding pattern or return-to-base mechanisms). There has been concern expressed by the US intelligence officials that the design has been shared with Chinese and Russian scientists, perhaps to assist in reverse-engineering the machine (Kelley and Cenciotti, 2012). Five years after capture, the Iranian Revolutionary Guard Corps aerospace division revealed a new "attack drone" called *Saegheh* (or "Thunderbolt" in English), which looked markedly similar to the RQ-170 (Cenciotti, 2016). While there are no known instances of civilian aircraft having been targeted, it is worth considering military systems as being ample targets for such political tactics. The Russian government has reportedly shared western technologies found on the battlefield with its allies in exchange for material assistance (Haynes, 2022).

Conclusions and Discussion

The invasion of Ukraine has led to a precarious situation of military RFI affecting commercial aircraft in Europe, and the results of this research can be applied anywhere in the world. From a broader geopolitical perspective, it is clear that jamming and spoofing could escalate tensions between states as a result of misinterpretation or miscalculations of intentions, or as a result of non-state actions. Evidently, spoofing—the turning of lies into truths—can complement alternative news and feed false narratives, something that Iran may have done over recent years to marine and aviation systems with falsified location data. This form of "sub-threshold warfare," operating in a grey zone below the threshold of war without direct conflict, now goes part and parcel with modern digital life.

For non-state actors, although limited in terms of targets and equipment, state support would widen the targets and tactical options, and therefore it is important that such potentialities are avoided. We see in contemporary conflicts, such as in Syria and Ukraine or between the United States and Iran, that states have flagrantly different interpretations about who is a terrorist, a state actor, or a freedom fighter. Their skewed interpretations and moral dividends allow them to choose who to train, who to arm, who to finance, and who to target without impunity. It is therefore not speculative to claim that Russia will transfer military-grade spoofing technologies to non-state actors if a situation arises beyond rational control.

Although many pilots will revert to other navigation references if their GPS is degraded, the likelihood of attack success will be in situations where people are less engaged with their surroundings (e.g. in autopilot), distracted due to interference, in poor weather conditions, or over-reliant on their GPS interfaces (Westbrook, 2023a, p. 74). While most cases of RFI will not manifest into something catastrophic, for malign intentions it is still important to stay within the logic of "they only need to be successful once." That is why, pilot training, anti-spoofing and anti-jamming systems, and training for identifying inconsistencies in navigation and positional data via various instruments will ensure safe air travel in Europe. Research into the criminal and political objectives of specific RFI must also keep pace with contemporary events. This article has identified tactics of decoy spoofing and following/correcting crooked paths as the main tactics supplementing political objectives by cyber–physical means.

The threat to aircraft is evidently not confined to geographical zones. Indeed, the threat is widespread, irregular, and intermittent and can happen any time. Improving detection and mitigating, and communicating the threat requires real-time notifications. This is something that Eurocontrol (2021, p. 7) is currently working on in light of the opportunities presented with big data, AI, and business intelligence. Evidently, in-flight RFI identification needs to be enhanced, as reportedly 36% of flight inspection aircraft possess a basic ability to detect GNSS RFI, and even fewer have geo-location capabilities (Eurocontrol, 2021, p. 7). Such reports need outside independent scrutiny, as without it, they will not receive alternative observances from different perspectives, and thus provides a limited threat and risk picture. Its relevance to wider and broader perspectives on political motivations alone could greatly contribute to security studies' literature.

Expanding on this point, while the article contributes to discussions about RFI within a confined geopolitical conflict, the analysis could further benefit from contextualising EW in alignment with geopolitical perspectives in the cyber domain (Westbrook, 2023a, 2023b). Further analysis into key theories in security studies, such as conflict escalation pathways, could add further richness to the findings.

Funding

This research received no external funding.

Data Availability Statement

All data used in this article has come from open access sources.

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*. Available at: www.nationaldefensemagazine.org/articles/2021/2/11/calls-grow-to-find-back-up-systems-for-gps (Accessed: 3 January 2024).

Alohali, B. (2019) *Cyber security threat to air navigation service provider (ANSP)*. PowerPoint slides. Available at: https://www.icao.int/Meetings/MIDCyberSec/PublishingImages/Pages/Presentations/2_Cyber%20Security.pdf#search=spoofing (Accessed: 3 January 2024).

Aviation Safety Reporting System (ASRS) (2023) *Aviation Safety Reporting System*. NASA ASRS. Available at: https://asrs.arc.nasa.gov (Accessed: 10 May 2023).

Cenciotti, D. (2016) 'Iran unveils new UCAV modelled on a captured US RQ-170 stealth drone', *The Aviationist.* Available at: https://theaviationist.com/2016/10/02/iran-unveils-new-ucav-modelled-on-captured-u-s-rq-170-stealth-drone/ (Accessed: 3 January 2024).

Center for Advanced Defense Studies (C4ADS) (2019) *Above us only stars: exposing GPS spoofing in Russia and Syria*. Resilient Navigation and Timing Foundation, University of Texas at Austin, pp. 1–66. Available at: https://www.c4reports.org/aboveusonlystars (Accessed: 3 January 2024).

Costin, A. and Francillon, A. (2012) 'Ghost in the air (traffic): on insecurity of ADS-B protocol and practical attacks on ADS-B devices', EURECOM. BLACKHAT, 21–26 July, Las Vegas, NV, pp. 1–10. Available at: https://www.s3.eurecom.fr/docs/bh12us_costin.pdf (Accessed: 3 January 2024).

Dudley, D. (2021) 'South Korea agrees to unfreeze $1 billion in Iranian assets, following tanker seizure by Tehran', *Forbes*. Available at: https://www.forbes.com/sites/dominicdudley/2021/02/24/south-korea-agrees-to-unfreeze-1-billion-in-iranian-assets-following-tanker-seizure-by-tehran/?sh=66ea285c1386 (Accessed: 3 January 2024).

Dutch Safety Board (2014) *Stick shaker warning on ILS final, Eindhoven Airport.* Available at: www.onderzoeksraad.nl/en/page/3003/stick-shaker-warning-on-ils-final-eindhoven-airport (Accessed: 3 January 2024).

Eccles, M. and Sheftalovich, Z. (2022) 'Inside the control room of Belarus' hijacked Ryanair flight', *Politco*. Available at: www.politico.eu/article/belarus-hijack-minsk-ryanair-athens-to-vilnius-control-room/ (Accessed: 3 January 2024).

Eurocontrol (2021) *Does radio frequency interference to satellite navigation pose an increasing threat to network efficiency, cost-effectiveness and ultimately safety*? Aviation Intelligence Unit Think Paper #9, 1 March 2021. Available at: https://www.eurocontrol.int/sites/default/files/2021-03/eurocontrol-think-paper-9-radio-frequency-intereference-satellite-navigation.pdf (Accessed: 3 January 2024).

European Commission (2022) *Statement by President von der Leyen on further measures to respond to the Russian invasion of Ukraine*. Available at: https://ec.europa.eu/commission/presscorner/detail/en/statement_22_1441 (Accessed: 3 January 2024).

European Parliament, Council of the European Union (2014) *Regulation (EU) No 376/2014 of the European Parliament and of the Council of 3 April 2014 on the reporting, analysis and follow-up of occurrences in civil aviation, amending Regulation (EU) No 996/2010 of the European Parliament and of the council and repealing Directive 2003/42/EC of the European Parliament and of the council and Commission Regulations (EC) No. 1321/2007 and (EC) No 1330/2007 Text with EEA relevance*. Document 32014R0376. Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32014R0376 (Accessed: 3 January 2024).

European Union Aviation Safety Agency (EASA) (2022a) 'Review of aviation safety issues arising from the war in Ukraine version 1', Available at: www.easa.europa.eu/downloads/136453/en (Accessed: 3 January 2024).

European Union Aviation Safety Agency (EASA) (2022b) *ASA publishes SIB to warn of intermittent GNSS outages near Ukraine conflict areas*. Available at: www.easa.europa.eu/en/newsroom-and-events/news/easa-publishes-sib-warn-intermittent-gnss-outages-near-ukraine-conflict (Accessed: 3 January 2024).

European Union Aviation Safety Agency (EASA) (2022c) *Restrictive measures – Russia's military attack on Ukraine*. Available at: https://www.easa.europa.eu/en/the-agency/restrictive-measures-russia (Accessed: 10 May 2023).

European Union Aviation Safety Agency (EASA) (2022d) *EASA launches European information sharing and cooperation platform on conflict zones* 3 March. Available at: https://www.easa.europa.eu/en/newsroom-and-events/press-releases/easa-launches-european-information-sharing-and-cooperation (Accessed: 3 January 2024).

Gangeskar, D. and Laagstein, K. (2022) 'Denne lille gjenstanden kan føre til at liv går tapt', *2 Nyheter*. Available at: www.tv2.no/nyheter/innenriks/denne-lille-gjenstanden-kan-fore-til-at-liv-gar-tapt/15121495/ (Accessed: 3 January 2024).

Goodwin, D. (2019) 'The radio navigation planes use to land safely is insecure and can be hacked', *ArsTechnica*. German Federal Bureau of Aircraft Accident Investigation, Status Report (BFU EX010-11). Available at: arstechnica.com/information-technology/2019/05/the-radio-navigation-planes-use-to-land-safely-is-insecure-and-can-be-hacked/ (Accessed: 3 January 2024).

Goward, D. (2023) 'Increasing GNSS interference: UK and EU warn aviation', *GPS World*. Available at: https://www.gpsworld.com/increasing-gnss-interference-uk-and-eu-warn-aviation/ (Accessed: 3 January 2024).

Gritten, D. (2023) 'Ukraine plane: Iran court jails 10 over downing of flight PS752', *BBC News*. Available at: https://www.bbc.com/news/world-middle-east-65298216 (Accessed: 3 January 2024).

Harris, M. (2021) 'FFA files reveal a surprising threat to airline safety: the US military's GPS test', *IEEE Spectrum*. Available at: https://spectrum.ieee.org/faa-files-reveal-a-surprising-threat-to-airline-safety-the-us-militarys-gps-tests (Accessed: 3 January 2024).

Haynes, D. (2022) 'Russia flew €140 m in cash and captured Western weapons to Iran in return for deadly drones, source claims', *Sky News*. Available at: https://news.sky.com/story/russia-gave-eur140m-and-captured-western-weapons-to-iran-in-return-for-deadly-drones-source-claims-12741742 (Accessed: 3 January 2024).

Hughes, C. and Selby, A. (2019) 'Iran tanker crisis: MI6 probe link to Putin after British ship is seized', *The Mirror*. Available at: www.mirror.co.uk/news/world-news/iran-tanker-crisis-mi6-probe-18458279 (Accessed: 3 January 2024).

International Civil Aviation Organization (2012) *High-level conference on aviation security (HLCAS)*. Available at: www.icao.int/Meetings/avsecconf/Documents/WP%2039/WP.39.Korea.pdf#search=spoofing (Accessed: 3 January 2024).

International Civil Aviation Organization (2018) *Update of the GNSS signal protection issue*. Available at: www.icao.int/APAC/Meetings/2018%20PBN%20WS%20%20PBNICG5/IP08_AI06_Update%20of%20GNSS%20signal%20protection%20issue_final.pdf#search=jamming (Accessed: 3 January 2024).

Jansen, K., Schafer, M., Moser, D., Lenders, V., Popper, C. and Schmitt, J. (2018) 'Crowd-GPS-Sec: leveraging crowdsourcing to detect and localize GPS spoofing attacks', *IEEE Symposium on Security and Privacy (SP)*, San Francisco, CA, pp. 1018–1031. doi: 10.1109/SP.2018.00012.

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*. Available at: www.businessinsider.com/report-chinese-experts-to-inspect-and-collect-parts-of-drone-captured-in-iran-2012-8?r=USandIR=T (Accessed: 3 January 2024).

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.

Khan, S.Z, Mohsin, M. and Iqbal, W. (2021). 'On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions', *Peer J Computer Science,* 7, p. e507. doi: 10.7717/peerj-cs.507.

Kožović, D. and Đurđević, D. (2019) 'Cyber security in aviation', *Megatrend Revija*, 16(2), pp. 39–56 (in Serbian). doi: 10.5937/MegRev1902039K.

Kožović, D. and Đurđević, D. (2021) 'Spoofing in aviation: security threats on GPS and ADS-B systems', *Vojnotehnicki Glasnik* (*Military Technical Courier*), 69(2), pp. 461–485. doi: 10.5937/vojtehg69-30119.

McCallie, D.L. (2011) *Exploring potential ADS-B vulnerabilites in the FAA's nextgen air transportation system*, Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. New York, NY: Homeland Security Digital Library. Available at: https://apps.dtic.mil/sti/pdfs/ADA545599.pdf (Accessed: 3 January 2024).

Milner. G. (2020) 'How vulnerable is G.P.S.?', *New Yorker*. Available at: www.newyorker.com/tech/annals-of-technology/how-vulnerable-is-gps (Accessed: 3 January 2024).

Mishra, V.K. (2022) *Agenda item 2 – radio frequency interference on GNSS signal - an Eurocontrol study* (PowerPoint slides). Available at: www.icao.int/APAC/Meetings/2022%20PBNICG%209/WP06%20-%20Radio%20Frequency%20Interference%20of%20GNSS%20Signal.pdf#search=jamming (Accessed: 3 January 2024).

National Aeronautics and Space Administration (NASA) (2022) 'Aviation safety reporting system (ASRS) data, database report set, global positioning system (GPS) reports', Ames Research Center, Moffett Field. Available at: https://asrs.arc.nasa.gov/docs/rpsts/gps.pdf (Accessed: 3 January 2024). See: ACN: 1747135 reported 'lost GPS contact, got off track while reviewing the sectional chart'; ACN: 1775414 reported that 'they inadvertently entered Class B airspace without clearance due to distraction from having to troubleshoot the GPS system on the aircraft'; ACN: 1775414 reported 'pilot errors in communication and GPS interference as distractions'; ACN: 1747135 reported 'got off track while reviewing the sectional chart'.

Netherlands Prosecution Service (2021) *Prosecution recommends life imprisonment for downing of MH17*. Available at: https://www.prosecutionservice.nl/topics/mh17-plane-crash/news/2021/12/22/prosecution-recommends-life-imprisonment-for-downing-of-mh17 (Accessed: 3 January 2024).

Nilsen, T. (2022a) 'Pro-Russian hacker group says it attacked Norway', *The Barents Observer*. Available at: https://thebarentsobserver.com/en/security/2022/06/pro-russian-hacker-group-says-it-attacked-norway (Accessed: 3 January 2024).

Nilsen, T. (2022b) 'More Russian GPS jamming than ever across border to Norway', *The Barents Observer*. Available at: https://thebarentsobserver.com/en/security/2022/07/more-russian-gps-jamming-ever-across-border-norway (Accessed: 3 January 2024).

Norwegian Government Security and Service Organisation (2020) Report from the working group on GNSS/GPS-disruptions in aviation. Norway: Group of State Secretaries (Ministry of Transport [Chair]; Ministry of Justice and Public Security; Ministry of Local Government and Modernisation; Ministry of Defence;

Ministry of Foreign Affairs); The Norwegian Communications Authority (Nkom); The Civil Aviation Authority of Norway (CAA Norway)). Available at: https://www.regjeringen.no/contentassets/ea62b7ef5071439a-99390c77a54f2bc4/disruptions-in-aviation.pdf (Accessed 28 January 2024).

Patrick, T. (2015) 'Drone war in Ukraine forces big tech changes', *The Fiscal Times.* Available at: www.thefiscaltimes.com/2015/03/10/Drone-War-Ukraine-Forces-Big-Tech-Changes (Accessed: 3 January 2024).

Patrick, T. (2016) 'To counter Russia's cyber prowess, US army launches rapid-tech office', *Defense One*. Available at: www.defenseone.com/technology/2016/08/russia-cyber-army-rapid-technology-office/131185/ (Accessed: 3 January 2024).

Rietjens, S. (2019) 'Unraveling disinformation: the case of Malaysia Airlines Flight MH17', *The International Journal of Intelligence, Security, and Public Affairs,* 21(3), pp. 195–218. doi: 10.1080/23800992.2019.1695666.

Sathaye, H., Schepers, D., Ranganathan, A. and Noubir, G. (2019) 'Wireless attacks on aircraft instrument landing systems', *Proceedings of the 28th USENIX Security Symposium*, 14–16 August 2019, Santa Clara, CA, pp. 375–372. Available at: https://www.usenix.org/system/files/sec19-sathaye.pdf (Accessed: 3 January 2024).

StrategyPage (2019) *Electronic weapons: Russia takes a victory lap*. Available at: www.strategypage.com/htmw/htecm/articles/20191103.aspx (Accessed: 3 January 2024).

The Associated Press (2011?) *The Al-Qaida papers – drones*. Available at: https://www.academia.edu/5185403/The_Al_Qaida_Papers_Drone (Accessed: 6 July 2022).

Thurber, M. (2012) 'ADS-B is insecure and easily spoofed, say hackers', *AIN Online.* Available at: www.ainonline.com/aviation-news/aviation-international-news/2012-09-03/ads-b-insecure-and-easily-spoofed-say-hackers (Accessed: 3 January 2024).

UK Government (2023) *Sanctions against Russia*. Available at: https://researchbriefings.files.parliament.uk/documents/CBP-9481/CBP-9481.pdf (Accessed: 3 January 2024).

US Department of Transportation Maritime Administration (2022) *2022-005-various-GPS interference and AIS spoofing*. Available at: https://maritime.dot.gov/msci/2022-005-various-gps-interference-ais-spoofing (Accessed: 3 January 2024).

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

Westbrook, T. (2019b) 'Will GPS jammers proliferate in the smart city?', *Salus Journal*, 7(2), pp. 45–67. https://view.salusjournal.com/article/view/102/96.

Westbrook, T. (2023a) 'A taxonomy of radiofrequency jamming and spoofing strategies and criminal motives', *Journal of Strategic Security* (JSS), 16(1), pp. 68–80. doi: 10.5038/1944-0472.16.2.2081.

Westbrook, T. (2023b) 'Radiofrequency interference strategies targeting marine navigation systems: political motives and consequences', *Journal on Baltic Security*, 9(1), pp. 69–97. doi: 10.57767/jobs_2023_003.

Wise, J. (2019) *The taking of MH370.* New York, NY: The Yellow Cabin Press (Published independently).

Woodrow, B. (2017) 'Are GPS jamming incidents a growing problem for aviation?', *Aviation Today*. Available at: www.aviationtoday.com/2017/01/31/are-gps-jamming-incidents-a-growing-problem-for-aviation/ (Accessed: 3 January 2024).