Journal of Strategic Security

Volume 12 | Number 2 Article 1

The Global Positioning System and Military Jamming: The geographies of electronic warfare

Tegg Westbrook
University of Stavanger, teggwestbrook@gmail.com

Recommended Citation
Westbrook, Tegg. "The Global Positioning System and Military Jamming: The geographies of electronic warfare." *Journal of Strategic Security* 12, no. 2 (2019): : 1-16.
DOI: https://doi.org/10.5038/1944-0472.12.2.1720
Available at: https://scholarcommons.usf.edu/jss/vol12/iss2/1

The Global Positioning System and Military Jamming: The geographies of electronic warfare

Author Biography

Tegg Westbrook is Associate Professor at the University of Stavanger, Norway, at the Department of Safety, Economics, and Planning. His current research interests include geofencing as a counterterrorism measure, GPS jamming in urban areas,as well as the manufacture, trade in, and use of, military, security and police technologies.

Abstract

GPS supports infrastructure assets that are essential to the functioning of national and international banking operations, power grid, transportation, and communication systems, therefore its reliability and accuracy is critical. GPS boosts productivity around the world and has radically changed military operations. Despite the importance of GPS, the relative weakness of GPS signals are vulnerable to interference. This weakness provides a range of opportunities for criminals, terrorists and state actors using GPS jamming devices. Different types of jammers can cause varying degrees of interference, but the use of powerful military jammers are becoming more prevalent. This article provides an overview of the emergence, development, and scale of the GPS jamming phenomena. It argues, overall, that the use of jamming technologies creates new geographies of conflict when we think about the location and proximity of critical infrastructure. It identifies themes related to the impact of jamming to better understand present and possible geographical and geopolitical implications. It concludes that as GPS jamming is not confined to conflict zones. Interference is possible in a variety of geographical areas.

Introduction

The Global Positioning System (GPS) “is a satellite-based navigation system comprised of a network of orbiting satellites that provide location and time information, anywhere on or near the Earth.”[1] First launched in the 1980s, GPS satellites became fully operational in 1993, and were available for civilian use in 1995. These satellites were first used by the United States military for providing precision navigation and timing. Over recent decades, free-to-use GPS has improved considerably in accuracy and reliability, and now it is difficult to find any civilian or military infrastructure that is not in some way dependent on it.

Not only is GPS used to aid navigation in vehicles, it supports critical infrastructure by synchronizing a wide range of computer-based systems, including for law enforcement, emergency services, transportation, communications, electrical power grids, and financial transactions, amongst many others. It boosts productivity in many sectors, enabling precision timing for synchronization, algorithmic decision-making, and operational efficiency.[2] For all these reasons, it is important that GPS data is available and reliable.[3]

What is Jamming and Spoofing?

The U.S. Department of Homeland Security has called the GPS “a single point of failure for critical infrastructure.”[4] This is, in part, due to the fact that the vast majority of GPS receivers need to be very sensitive because of the weak signals coming from distant, orbiting satellites. This weakness creates many opportunities for criminals as well as state actors seeking military strategic gains.

Jamming is caused by “the transmission of a noise signal across one or more of the GPS frequencies to raise the noise level or overload the receiver circuitry and cause a loss of lock.”[5] Jammers vary in power and capability, and these are factors that play into end-user intentions. As this article highlights, jamming is used to block GPS-enabled tracking. It can also be used for harassment, or to disorientate navigation and positioning information. Jamming is often indiscriminate and causes both intentional and unintentional disruption that transcends borders and penetrates walls and systems.

There are various methods and intentions for interfering with GPS information. Spoofing 'is the act of producing a falsified version of the GPS signal with the goal of taking control of a target.[6] It could also include introducing a false time signal into electrical control systems and causing equipment malfunction and damage.[7] Counter-jamming technologies, usually built into systems and structures, are designed to identify when jamming occurs, identify the locations of jamming, trigger backup systems, or simply ignore or overcome interference. It is not within the scope of this article to explore counter-jamming technologies, however.

Interference of the GPS system is therefore an issue that is of concern to a range of actors, including the military, critical infrastructure owners, and aerial, maritime and road transport sectors, with potential economic and political consequences, and threat to life. It is a matter of importance not only in terms of international relations, but for national security.

Ever since the implications of GPS interference became clear, academic studies have largely focussed on technical and situational aspects of jamming and counter-jamming technologies. These studies have focussed on the outcomes of specific methods which have been undertaken under careful testing conditions. Technical studies have provided valuable information for the practitioner/military community, especially in respect to risk and vulnerability assessments. There has also been interest in how technological changes have shaped the development of critical infrastructures and influenced their vulnerability over time.[8] Whilst some organizations such as the Resilient Navigation and Timing Foundation, C4ADS and members have explored various dimensions of GPS interference, a prime focus on its wider geographical and geopolitical implications requires more dedicated attention. There is an opportunity here to explore the geopolitical context of jamming to identify future challenges.

The aim of this article is to (1) identify the specific contexts jamming is typically used; (2) to identify the outcomes of the jammings, and; (3) based on these examples, it seeks to better comprehend the geographical and geopolitical implications based on likely users, their intentions, and the known ranges of jammers. It considers the proliferation of more oft-used low-power jamming devices and the use of high-powered military jammers (Table. 1).

Table 1. Likely Users and Distances of GPS Jammers

Likely End-users	Power	Approximate Distance
Privacy seekers; criminals	1 deciwatt	Few meters to 9.3 miles
Organised criminals; terrorists; state proxy actors; state/private security actors	1 kilowatt	31 miles
State-assisted terrorist groups; militaries	10 kilowatts	94 miles - 124 miles

Notes: Collected from open-access sources.[9]

The thesis of this article is based on the premise that, through time, the changing nature of war and military technology will consistently affect the "spatial organisation of nations and their resources."[10] It is argued here that end-user intentions accordant with current jamming distances means that the risk and vulnerability of assets, in relation to their proximity to those end-users, can be better comprehended. But this is complicated by the fact that small jamming devices are easily available and powerful jammers can be homemade or smuggled into territories as parts and components and then reassembled, or even projected from aircraft or via ships.

The article first locates the jamming phenomena from a historical perspective in order to build a contextual understanding of its contemporary implications. Drawing on examples, it also seeks to identify the likely end-users and their intentions based on the outcomes of their activities, whether intentional or unintentional. Finally, it explores future geopolitical challenges in relation to the examples explored, based on likely end-users and the locations of critical infrastructure that have been previously affected. The article concludes that as GPS jamming is not confined to conflict zones, interference is possible in a variety of geographical areas.

The findings were achieved by extensive literature review of online and offline media and governmental material. It is important to note that there is a bias with the material in this article, which relies almost entirely on English language and Western-sourced material.

Historical to Contemporary Context of the Effectiveness of Jamming

Brief History of Radio Jamming

The discovery and use of radio waves as a form of communication can be traced back to the late 19th century. The first recorded instance of intentional radio jamming (which was, interestingly, for commercial rather than military gains) was in 1901 during a yacht race in the USA.[11] During World War I, radio was used primarily for military and maritime communications, but became increasingly used for propaganda purposes.[12] It was not until the 1920s when radio was capable of distributing mass media to millions of listeners.[13]

During the war and interwar periods of the 20th century, radio transmissions enabled governments and movements to transmit prohibited information and ideas over national borders.[14] Government and military efforts to disrupt these transmissions evolved over time, progressively overcoming technical, financial and geographical hurdles. During the Cold War, for example, the Polish Communist regime undertook a relentless 39-year campaign of jamming transmissions from Radio Free Europe, placing transmitters on police stations and military bases. Such attempts replicated other jamming campaigns by other communist regimes and colonial Western powers.[15] Jamming, though limited in radius and only effective in certain frequencies, was a large part of controlling the movement of information for political and military reasons. Radio broadcasting for propaganda purposes and jamming continues in disputed territories to this day.

Effectiveness of Jamming Smart Weapons

The launching of communication satellites, the expanded use of radio waves, and resultant technologies has increased the opportunities for, and the implications of, jamming. A probable catalyst for new jamming developments came as a result of the instigation of GPS in the 1970s and the miniaturization of GPS receivers in the 1980s. Applying GPS guidance to munitions allows the U.S. to develop steerable smart weapons. These weapons were more precise resulting in greater

DOI: https://doi.org/10.5038/1944-0472.12.2.1720

efficiency and less collateral damage in military operations.

During the first Gulf War, many states recognized the importance and versatility of GPS in modern warfare (beyond its utility in smart weapons), and in later years the potential of GPS jammers was becoming more marketable. High-power military jammers were being openly marketed at various defense fairs by America's traditional adversaries.[16] During the second Gulf War, Iraqi forces placed Russian-sourced jamming devices on buildings on or near important strategic targets.[17] These jammers were intended to confuse cruise missile guidance systems, such as Boeing JDAM (Joint Direct Attack Munition), and Raytheon's BGM-109 Tomahawk land attack cruise missile and Enhanced Paveway.

There have been mixed messages with regards to the effectiveness of Iraq's jamming. The UK and US forces argued that the jammers proved ineffective.[18] In the short term, however, it prompted coalition forces to target the jammers with force and place more reliance on their laser-guided capabilities.[19]

In the long term, more investment went into anti-spoofing and anti-jamming capabilities in JDAM kits (even as recently as 2011, there had been speculation that North Korea were able to affect South Korea's JDAM arsenal with military jammers), as well as guided weapons specifically developed to locate and target jamming locations.[20] Furthermore, the U.S. Department of Defense sought more significant investment into counter-space capabilities as a consequence of Iraq's jammings.[21] Indeed, the method of placing jammers on key infrastructures remains a contemporary mode of defense. Russia's defense initiative *Pole-21*, for example, involves placing jammers on key domestic infrastructures as a precaution for possible conventional war.[22] Therefore, whilst the effectiveness of jamming smart weapons is not entirely clear from open-access sources, it certainly affected military strategy and had a political and financial impact in years that followed. For military strategists, precision bombings are simply more likely to be successful in locations where jammers are not situated, hence the geographical and geopolitical factors are influenced by strategic alliances, defense acquisitions, end-user intentions, and owners of jammers.

Military Jamming and Spoofing Civil and Military Aviation and Shipping

Apart from potentially disorienting smart weapons, jamming has been used to make surveillance and targeting methods more difficult. GPS jamming, for example, was used thwart the OSCE Special Monitoring Mission to Ukraine in 2018. The Mission reported severe jamming of its long-range UAV, which was observing compliance with the latest ceasefire agreed by fighting parties. The jamming "caused most of the control and communication links (including backup systems) between the Ground Control Station and the UAV to fail."[23] In 2016, the Mission had lost a long-range UAV in the same area, over Korsun.

Like in smart weapons, the miniaturization of lightweight antenna systems is useful for UAVs with low payload capacities. As well as affecting communication links, spoofing can impact their coordinates. In 2011, Iran spoofed and captured a U.S. RQ-170 Sentinel UAV by redirecting it to land inside Iranian borders.[24] Adding to the embarrassment of the Obama administration, Iran subsequently accused the U.S. of spying within Iranian airspace and have reportedly attempted to reverse-engineer the design of the UAV.

China has reportedly used GPS jamming against its neighbors and against U.S. forces in the Asia-Pacific region, in light of contentious issues over the its territorial disputes in the South China Sea. Amongst other coordinated cyber-attacks, there were also reports that China "attempted to interfere with U.S. military drones at least once in recent years…conducting surveillance missions in the Spratly Islands."[25]

In the ongoing civil war in Syria, where jamming is commonplace, U.S. surveillance UAVs and AC-130 gunships have been affected by jamming and spoofing.[26] Whilst it has not been disclosed how the gunships have been affected, it was stressed that the jamming of communication systems and data links between AC-130 crews, special forces and supporting conventional forces could affect the process of establishing the location and positive identification of targets. Even with electro-optically or infrared-enhanced visual aids, jamming GPS location information can make it harder for AC-130 crews to differentiate between friendly/hostile forces and civilians, especially in close combat situations.[27]

In the same region, Pyongyang has targeted military and civil air and naval

DOI: https://doi.org/10.5038/1944-0472.12.2.1720

traffic near the demilitarized zone with Russian-designed military jammers on more than 100 occasions. This jamming reportedly affected over 1000 civilian aircraft (as well as South Korean military aircraft), hundreds of fishing vessels, cell phone services, and car navigation systems, targeting infrastructure separately and systematically.[28]

What is unique about North Korea's military jamming is that it is done with full knowledge of the consequences to civilian operations, and therefore intended for harassment and possible economic damage. Indeed, in 2012, one jamming campaign aimed at the South Korean capital lasted more than two weeks.[29] This length of time is unparalleled elsewhere in civilian areas.

A similar theme is identified in Europe. The Norwegian Ministry of Foreign Affairs confronted Russian authorities over concerns that civilian aviation and communications systems had been repeatedly 'jammed in connection with nearby Russian military activities' near Norway's Eastern Finnmark region.[30] On one occasion, in September 2017, airliners SAS and Widerøe 'had to navigate with the help of radio signals due to loss of GPS when they entered the East Finnmark airspace.'[31] Similar instances have occurred in other European countries bordering Russia.

Impacts and Potential Repercussions

Based on the above examples, military GPS jamming is used as a combined attrition of an enemy's communications, target accuracy, surveillance capabilities, and navigational reliability. GPS jamming can significantly affect the efficiency and effectiveness of operations, and impact morale. It is also used offensively and politically for harassment and intimidation in disputed territories or near military training exercises. The impact of jamming and spoofing have different consequences, but the potential impacts and repercussions are here discussed in more detail.

In both the South Korea and Norway examples, whilst it was speculated that South Korea's JDAM capabilities were affected, the aircraft and ships in both countries were able to switch to their backup inertial navigation systems (INS) and other ground-based systems. In Seoul, much of the jamming signals were blocked by buildings and hills, and generally caused more of a 'nuisance more than a threat.'[32] In Norway, there were no reports of widespread problems in urban centres.

Nevertheless, whilst the impacts have been reported as relatively negligible, the consequences of jamming in metropolitan areas could be much more serious if the jamming persists over a number of days. North Korea's lengthy 2012 jamming campaign extended the period of inconvenience for civil users, magnifying the frustration of the population and therefore placing more pressure on the South to take action. Instead of taking military action (of which the outcome would be catastrophic), the South protested to the United Nations.

It can be assumed that Russia, North Korea, and China jam neighbouring countries knowing that lethal retaliation is extremely unlikely, making jamming a low-risk, high-reward option if provocation is the intention. Intentional jamming of civilian areas has so far not led to any significant issues beyond scoring relatively obscure political gains. But there is the potential for the escalation of conflict and of causing serious vehicle accidents.

On this point, one of the most concerning issues relating to jamming or spoofing aircraft or ships are in cases where users are not aware that they are receiving inaccurate navigation and location data. Reports of jamming in the Black Sea, which affected the situational awareness of some 20 ships (reporting that the location of the vessels were 20 miles inland), would present obvious inaccuracies that could be quickly rectified.[33] In situations where momentary disorientation is caused, this could prove catastrophic. Indiscriminate jammings of ships in the Korean Peninsula was largely negligible as ships had alternative navigation systems and methods. But momentary and targeted GPS jamming can affect systems such as automatic identification systems (AIS) which normally use GPS receivers. Research by the University of Nottingham and the Royal Norwegian Naval Academy confirmed that jammers could momentarily affect the positioning data of ships of up to 10 meters which, they stressed, could be very hazardous in narrow, busy straits.[34] Validating these tests, in one real-world example, momentary GPS interference was considered a likely cause of two large ships colliding in Germany's busy Kiel Firth waterway.[35]

In the case of Iran's spoofing of the US UAV, the act of misdirecting aircraft or ships into unauthorized airspaces and territories adds weight to the concern that spoofing or momentary disorientation of positioning data could escalate tensions much more than practice of indiscriminately jamming of civilian areas, ships and aircraft. Indeed, former U.S. Vice President Dick Cheney stated that he supported the option of targeting the captured UAV in Iran immediately with airstrikes (former President Barack Obama decided instead to request the return of the UAV).[36] It is highly unlikely that Iran's intentions was to provoke the U.S. into an armed response, but the outcome of their actions could have had major consequences.

It is a dark irony that Russia's downing of the Korean Airlines Flight 007 in 1983 after it accidentally flew into its territory led to Ronald Reagan's executive order allowing civilian access to GPS. But it is a reminder that loss of location could be exploited by a range of actors with malign intentions, and that reliance on GPS is not an answer but rather a useful but fragile invention that is exploitable.

The Use and Impact of Small Jamming Devices

There are rising concerns about the widespread acquisition and use of small pocket-sized 'privacy seeking' jamming devices, as well as the potential of home-made jamming devices. Privacy seeking jammers are typically used by drivers in the freight industry to stop their managers tracking their location, and can be bought for less than $100 online. These small jamming devices cover a jamming distance of a few meters to as far as 9 miles.[37] They are significantly more difficult to detect and locate than powerful military devices.

Whilst more "determined" groups, such as organized criminal gangs and terrorists, may have the means to produce and acquire more powerful jamming devices than those used by privacy seekers, it is still argued by some critics that it would take significant mastery of GPS technology to bring "apocalyptic visions of a cyber-hell" to life, as argued by cyber specialist Martyn Thomas.[38] However, the widespread use of jamming devices that are intended for privacy indiscriminately and unintentionally affect other services that rely on GPS.

Unintentional jamming with low-power devices has disrupted air travel and financial transactions on frequent occasions in the U.K. and the United States. For example, the London Stock Exchange, which relies on precision timing for financial transactions, has been subject to repeated GPS outages, and many users have not been identified or prosecuted.[39] In July 27, 2013, it was recorded that time stamps on the financial trade in the London Stock Exchange were affected and navigation systems in cars 'stopped working.' It was determined that the offender was a delivery driver hiding from his management.[40]

Such events have arguably opened Pandora's box in terms of potentially inviting criminals and state actors to exploit this weakness, recognizing not only that time manipulation can disrupt a nation's economy (by scaring away market participants or putting domestic traders at significant disadvantages), but this can be achieved with small devices without being quickly detected. Indeed, it has been argued by one specialist that spoofing could create 'opportunities for ill-gotten gains and disruptions like the 2010 'flash crash.'[41]

It is also feared that these deliberate disruptions could be combined with other types of electronic and cyber-attacks.[42] For example, if jamming alone is undertaken by numerous individuals in one urban location, the time it would take to locate and stop them could be considerable. Likewise, there have been many raised concerns about how devices—whether single powerful device or multiple devices used systematically—could cause a serious shipping accident in areas like the English Channel, the world's busiest seaway.[43]

Theoretically, in the event of conflict between two or more adversaries, the combined use of military and low-power 'civilian' devices could cause significant disruption. China—a country where small jamming devices are mass-produced—has the industrial-base to produce and distribute high quantities of such devices. Socio-technical changes may also increase the incentive to buy jamming devices by civilian users; for example, GPS-enabled tracking, toll collection (notably in Germany), and even gaming trends (Pokémon Go), has seen increased use of small jamming devices.

Geographies of Jamming

Unlike cyber-crime which has no limitations in terms of ranges, GPS jamming and spoofing can only be achieved within a minimum of a few meters to a maximum of over 100 miles. In practice, this puts critical infrastructures and other assets in certain geographical locations in more danger than others. Indeed, during World War II, the westernmost and northernmost industries in

DOI: https://doi.org/10.5038/1944-0472.12.2.1720

Germany and the southernmost and easternmost industries in England were targeted significantly more than industries at opposite ends. This was based on capable distances and payload capacities of aerial bombers. In hindsight, should infrastructure managers and military planners consider proactively the geographical locations of assets in relation to known military jamming capabilities and likely end-users? Should GPS reliance be reduced and should more investment into counter-jamming technologies be invested in these locations?

There are, of course, predictable instances where jamming is a possibility. GPS-reliant military systems such as UAVs used in conflict zones or near borders of 'enemy' states are vulnerable to jamming and spoofing. The interference of civilian systems will likely be affected if within similar proximities of military jammers. North Korea's jamming in 2012, for example, was traced to the town of Kaesong, just over the border.[44] South Korea's Incheon International Airport, one of the busiest airports in the world, which serves the greater Seoul metropolitan area, is only 23 miles from the demilitarized zone. The metropolitan area of Seoul is approximately 60 miles from the demilitarized zone. Counter-jamming technologies should therefore be refined to these areas in practice. Governments of countries whose populations are likely to be affected by electronic warfare methods will have sufficiently more pressure weighed on them to take action.

Understanding a states' strategic calculus of using electronic warfare as means of harassment and intimidation over borders will also inform risk and vulnerability assessments. Russia's *Zapad* military drills, involving thousands of soldiers, are carried out as far as 10km from Norway.[62] Finland have also experienced jamming from Russian military exercises. This could be tied to Norway's hosting of NATO Exercise Trident Juncture 2018 and the latter's involvement. Only diplomatic approaches to persuade Russia to practice its jamming capabilities out of reach of bordering infrastructures is the least aggravating approach.

There is, however, the issue of complacency if vulnerability assessments are confined to critical infrastructures near adjacent borders. There is always the possibility that military jammers target locations from ships or aircraft or smuggled into territories as parts and components and reassembled. The use of privacy seeking devices further complicates this matter. It is unrealistic for critical infrastructure managers, particularly in dense urban locations (such as the financial district of London) to create physical stand-off distances sufficient to mitigate against interference.

Since the manufacture, trade and use of privacy seeking jammers has increased, the geographical and geopolitical implications of critical infrastructure protection have become more complex. Not only does jamming occur in conflict zones and over territories, it already takes place in domestic locations. GPS interference is, therefore, no longer confined to conflict zones or adjacent territories, but prevails as an issue possible in all locations.

Conclusion

Since radio waves were utilized to relay information, so has the incentive of those to disrupt that process. Since the introduction of GPS, jamming methods and intentions have evolved at pace with developments in military technologies and systems. Jamming has adapted from obstructing communications to affecting target accuracy, surveillance capabilities, and navigational reliability. As an offensive measure, it has been used almost entirely for harassment and intimidation, affecting GPS-reliant systems in both military and civilian realms. Overall, the practice of jamming has become potentially deadlier as reliance on GPS has increased.

Whilst technical studies are extremely useful, they often do not explore the geographical and geopolitical implications of jamming and spoofing in sufficient depth. Based on the findings, it is unclear if jamming and disorientating smart weapons by placing jammers on targeted buildings is effective, but Russia's *Pole-21* initiative demonstrates that it is a mode of defense that is considered to this day. For military strategists, precision bombings are simply more likely to be successful in locations where jammers are not situated, hence the geographical and geopolitical factors are influenced by strategic alliances, defense acquisitions, end-user intentions, and owners of jammers.

States have targeted UAVs and military aircraft with some success in Ukraine, Syria, and Afghanistan. North Korea and Russia are using electronic warfare frequently as a mode of harassment into civilian areas. If jamming occurs in

DOI: https://doi.org/10.5038/1944-0472.12.2.1720

civilian areas for extended periods, this could place more pressure on countries to respond with force (at the extreme end of the scale) but so far, such incidents have been pursued diplomatically. Governments of countries whose populations are likely to be affected by electronic warfare methods will have sufficiently more pressure weighed on them to take action.

The impact of indiscriminate jamming of ships and planes has been largely negligible, as they typically have backup navigation systems. But momentary disruption has proven to be extremely hazardous in situations where collisions could occur. Not only is this a threat to life but can provoke conflict. In the case of Iran's spoofing of the US UAV, the act of misdirecting aircraft or ships into unauthorized airspaces and territories adds weight to the concern that spoofing or momentary disorientation of positioning data could escalate tensions much more than practice of indiscriminately jamming civilian areas, including ships and aircraft.

The proliferation of small privacy seeking devices has grown considerably since tracking, toll collection, gaming trends and other GPS-reliant systems have emerged. Frequent interruptions to aircraft and the financial sector could be further exploited by criminal, terrorists, proxy state actors in numerous ways. GPS jamming is therefore no longer confined to conflict zones, it is a present threat to domestic infrastructures.

Overall, the geographical position of a national territory and of its key infrastructures in relation to likely end-users should influence the perception of a countries' defense needs.[44] But this is further complicated by the fact that the proliferation of jamming devices - which can be made at home or acquired online, or projected from aircraft or ships - means that jamming ranges should form only part of risk and vulnerability assessments.

There are, however, predictable instances where jamming is always a possibility: In disputed territories, conflicts, and close to unfriendly borders. Likewise, indiscriminate jammings in civilian areas may occur if military jamming is used in self-defense in neighbouring countries. But military drills, like in Russia, which could be practically undertaken away from adjacent territories, are intentionally provocative. Overall, the vulnerability and proximity of infrastructure should be considered in relation to the strategic intentions of neighbouring states.

In the near future, military jamming will continue to be used as a form of harassment in civilian areas, mostly in relatively short bursts that are less likely to provoke an armed response. In distant future, as long as military systems rely on GPS, electronic warfare will continue to be used in conflict to affect communications, target accuracy, surveillance capabilities, and navigational reliability. The success and efficiency of military operations will depend on the enduring capability race between those involved in the research, development, manufacture, trade in and use of jamming and counter-jamming technologies.

In order to develop our understanding of the possibilities and implications of jamming, further research is required into the geographical implications of the manufacture, trade in, and use of jamming devices as well as the possibilities of their parts and components being smuggled and assembled in countries. More research also is required into the socio-technical forces driving the demand for different types of jammers, in particular the relationships between GPS reliance and the forces that want to exploit that reliance.

[1] PR Newswire, "Study Shows Interference with GPS Poses Major Threat to U.S. Economy," June 22, 2011, in: Jeff Coffed, "The Threat of GPS Jamming: The Risk to an Information Utility," Harris Corporation (2016): 3-12, https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf (all following websites accessed February 28, 2019).
[2] Coffed, "The Threat of GPS Jamming." 3.
[3] Ibid, 3.
[4] Resilient Navigation and Timing Foundation (RNTF), "Prioritizing Dangers to the United States from Threats to GPS: Ranking Risks and Proposed Mitigations," 2016, White Paper, 2, https://rntfnd.org/wp-content/uploads/12-7-Prioritizing-Dangers-to-US-fm-Threats-to-GPS-RNTFoundation.pdf.
[5] Coffed, "The Threat of GPS Jamming." 3.
[6] Aaron A. Fansler, Daniel P. Shepherd, Jahshan A. Bhatti, and Todd E. Humphreys, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," Conference Paper: ION GNSS Conference (January 2012): 2, https://www.xdrones.es/wp-content/uploads/2016/07/PMUAndUAVSpoofingION2012.pdf.
[7] RNTF, "Prioritizing Danger." 15.

[8] For example, see: Thomas Hellström, “Critical infrastructure and systemic vulnerability: Towards a planning framework,” Elsevier, Safety Science, 45, 3 (March 2007): Abstract, https://doi.org/10.1016/j.ssci.2006.07.007.

[9] Logan Scott, George Shaw, Sherman Lo, “GNSS-Denied Environments: Living in a vulnerable world,” Presentation webinar, Inside GNSS, May 12, 2013, www.insidegnss.com/pdf/GNSS_in_Denied_Environment_Webinar_slides_5_2_13.pdf; Christopher Mims, “How Cruise Missiles Would Beat GPS Jammers in Libya,” *MIT Technology Review*, March 20, 2011, https://www.technologyreview.com/s/423363/how-cruise-missiles-would-beat-gps-jammers-in-libya/; Dianna Lynne, “GPS-jammer contractor plays both sides of war, “ *WND*, March 29, 2003, https://www.wnd.com/2003/03/17996/.

[10] Roy E. H. Mellor, *National Defence - The Military Aspects of Political Geography: A Reconnaissance Study* (O’Dell Memorial monograph: University of Aberdeen, 1987) no 19, 2.

[11] Alfred W. Price, *The Evolution of Electronic Warfare Equipment and Techniques in the USA, 1901 to 1945* (Doctoral thesis, 1985), 17, University of Loughborough Institutional Repository.

[12] Pawel Machcewicz, *Poland’s War on Radio Free Europe, 1950-1989* (Washington: Woodrow Wilson Center Press, 1994), 13.

[13] Rebecca P. Scales, *Radio and the Politics of Sound in Interwar France*, 1921-1939 (Cambridge: Cambridge University Press, 2016), 1.

[14] Richard H, Cummings, *The Dangerous History of American Broadcasting in Europe*, 1950-1989 (Jefferson: MacFarland & Company, Inc., 2009).

[15] Donald R. Browne, *International Radio Broadcasting: The limits of the Limitless Medium* (USA: Praeger Publishers, 2014), 18; Pawel Machcewicz, *Poland’s War on Radio Free Europe, 1950-1989* (Washington: Woodrow Wilson Center Press, 1994), 1.

[16] Lynne, “GPS-jammer contractor plays both sides of war.”

[17] Russia and the company in question denied these claims.

[18] Flight International, “Conflict see first use of GPS jamming,” April 1, 2003, https://www.flightglobal.com/news/articles/conflict-sees-first-use-of-gps-jamming-163587/.

[19] Larry Greenemeier, “GPS and the World's First “Space War”,” *Scientific American*, February 8, 2016, https://www.scientificamerican.com/article/gps-and-the-world-s-first-space-war/.

[20] James Hasik, *Arms and Innovation: Entrepreneurship and Alliances in the Twenty-First Century Defense Industry* (Chicago: University of Chicago Press, 2008), 70; Joe Gould, “Guided-Bombs Makers Anticipate GPS Jammers,” Defense News, May 31, 2015, https://www.defensenews.com/air/2015/05/31/guided-bomb-makers-anticipate-gps-jammers/.

[21] Jeffrey Lewis, “Iraq and GPS Jamming,” Arms Control Wonk, September 15, 2004, https://www.armscontrolwonk.com/archive/200039/iraq-and-gps-jamming/.

[22] Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the electromagnetic spectrum* (Tallinn: International Centre for Defence and Security. ISSN 2228-0529, September 2017), 39, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

[23] Organization for Security and Co-operation in Europe, “Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19:30,” Reliefweb, 9 November 2018, https://reliefweb.int/report/ukraine/latest-osce-special-monitoring-mission-ukraine-smm-based-information-received-584.

[24] Joe Gould, “Guided-Bombs Makers Anticipate GPS Jammers.”

[25] Paul Martini, “China Jamming US Forces' GPS,” *Resilient Navigation and Timing Foundation*, September 26, 2016, https://rntfnd.org/2016/09/26/china-jamming-us-forces-gps/.

[26] Adam Gorski, “When GPS jammers interfere with military operations,” *AGI*, April 10, 2018, https://www.agi.com/news/blog/april-2018/when-gps-jammers-interfere-with-military-operation.

[27] Joseph Trevithick, “American General Says 'Adversaries' Are Jamming AC-130 Gunships in Syria,” The Drive, April 25. 2018, https://www.thedrive.com/the-war-zone/20404/american-general-says-adversaries-are-jamming-ac-130-gunships-in-syria.

[28] Kyle Mizokami, "North Korea Is Jamming GPS Signals," *Popular Mechanics*, April 5, 2016, https://www.popularmechanics.com/military/weapons/a20289/north-korea-jamming-gps-signals/.

[29] James Dunnigan, "A Solution For The Jammer Threat."; Strategy Page, November 21, 2013, https://www.strategypage.com/dls/articles/A-Solution-For-The-GPS-Jammer-Threat-11-21-2013.asp.

[30] Alte Staalesen, "Norway requests Russia to halt GPS jamming in borderland," *The Barents Observer*, April 27, 2018, https://thebarentsobserver.com/en/security/2018/04/norway-requests-russia-halt-gps-jamming-borderland.

[31] Ibid.

[32] Dunnigan, "A Solution For The Jammer Threat."

[33] Dana Goward, "Mass GPS Spoofing Attack in Black Sea?," The Maritime Executive, November 7, 2017, https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea.

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

[35] Bundesstelle fur Seeunfalluntersuchung, *Collision in the Kiel Firth at Friedrichsort between the MV FRANCISCA and MV RMS BREMEN on 5 September 2014*, Federal Bureau of Maritime Casualty Investigation, Investigation Report 276/14, www.bsu-bund.de/SharedDocs/pdf/EN/Investigation_Report/2015/Investigation_Report_276_14.pdf?__blob=publicationFile

[36] CNN, "Obama says U.S. has asked Iran to return drone aircraft," December 13, 2011, https://edition.cnn.com/2011/12/12/world/meast/iran-us-drone/.

[37] Ryan H. Mitch et al, "Signal Characteristics of Civil GPS Jammers," Abstract only, 2011, Texas ScholarWorks, University of Texas Libraries, http://hdl.handle.net/2152/63304.

[38] Ben Rooney, "Terrorist Threat to GPS "Fanciful," *The Wall Street Journal*, March 8, 2011, https://blogs.wsj.com/tech-europe/2011/03/08/terrorist-threat-to-gps-fanciful/.

[39] CRFS, "How to deal with GPS jamming and spoofing," no date, accessed February 21, 2019, https://www.crfs.com/blog/how-to-deal-with-gps-jamming-and-spoofing/.

[40] The Economist, "GPS jamming: Out of sight," July 27, 2013, https://www.economist.com/international/2013/07/27/out-of-sight.

[41] Tim Fernholz, "The entire global financial system depends on GPS, and it's shockingly vulnerable to attack," *Quartz*, October 22, 2017, https://qz.com/1106064/the-entire-global-financial-system-depends-on-gps-and-its-shockingly-vulnerable-to-attack/.

[42] RNTF, "Prioritizing Dangers."

[43] Financial Times, "GPS Jammers Threaten Ships in Channel," February 21, 2012, https://www.ft.com/content/281ccca6-5bff-11e1-bbc4-00144feabdc0.

[44] Roy E. H. Mellor, *National Defence - The Military Aspects of Political Geography: A Reconnaissance Study* (O'Dell Memorial monograph, University of Aberdeen, 1987) no 19, 2.

DOI: https://doi.org/10.5038/1944-0472.12.2.1720