C4ADS
innovation for peace

ABOVE US ONLY STARS

Exposing GPS Spoofing in Russia and Syria

ABOUT C4ADS

C4ADS (www.c4ads.org) is a 501(c)(3) nonprofit organization dedicated to data-driven analysis and evidence-based reporting of conflict and security issues worldwide. We seek to alleviate the analytical burden carried by public sector institutions by applying manpower, depth, and rigor to questions of conflict and security. Our approach leverages nontraditional investigative techniques and emerging analytical technologies. We recognize the value of working on the ground in the field, capturing local knowledge, and collecting original data to inform our analysis. At the same time, we employ cutting edge technology to manage and analyze that data.

The result is an innovative analytical approach to conflict prevention and mitigation.

COVER IMAGE

The cover image was produced by Brian G. Payne.

LEGAL DISCLAIMER

The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed as such.

ACKNOWLEDGEMENTS

The author would like to sincerely thank the team of C4ADS analysts who happily gave their time and skills to assist with data structuring, graphic design, editing, layout, and investigative analysis. This report truly would not have been possible without their efforts.

The author would also like to thank Todd Humphreys, associate professor of aerospace engineering at The University of Texas at Austin, for his contributions to this report. Todd's assistance throughout the research process were integral to this report.

TEXAS
The University of Texas at Austin

Additionally, the author would like to thank Dana Goward from the RNT Foundation for his invaluable insight and continued efforts to raise awareness of PNT issues.

RESILIENT NAVIGATION and TIMING FOUNDATION

Finally, this report heavily relied on the technology partners of C4ADS, particularly Palantir, whose software and systems were integral to the project's success. Many geospatial and statistical visualizations included in this report are derived from analysis conducted in Palantir Foundry.

ANALYSIS POWERED BY

Palantir

Executive Summary

GPS and other Global Navigation Satellite Systems (GNSS) are used in everything from cellular communication networks, to basic consumer goods, high-end military systems, and stock trading inputs. But these systems are vulnerable: by attacking positioning, navigational, and timing (PNT) data through electronic warfare (EW) capabilities, state and non-state actors can cause significant damage to modern militaries, major economies, and everyday consumers alike.[1] [2] [3] With recent technological advances, the tools and methodologies for conducting this interference are now at a high risk for proliferation. ***GNSS attacks are emerging as a viable, disruptive strategic threat.***

In this report, we present findings from a year-long investigation ending in November 2018 on an emerging subset of EW activity: the ability to mimic, or "spoof," legitimate GNSS signals in order to manipulate PNT data. Using publicly available data and commercial technologies, we detect and analyze patterns of GNSS spoofing in the Russian Federation, Crimea, and Syria that demonstrate the Russian Federation is growing a comparative advantage in the targeted use and development of GNSS spoofing capabilities to achieve tactical and strategic objectives at home and abroad. We profile different use cases of current Russian state activity to trace the activity back to basing locations and systems in use.

- In **Section One**, we examine GNSS spoofing events across the entire Russian Federation, its occupied territories, and overseas military facilities. We identify 9,883 suspected instances across 10 locations that affected 1,311 civilian vessel navigation systems since February 2016. We demonstrate that these activities are much larger in scope, more diverse in geography, and longer in duration than any public reporting suggests to date.

- In **Section Two**, we examine the role of Russian GNSS spoofing for very important person (VIP) protection. We find a close correlation between movements of the Russian head of state and GNSS spoofing events. We believe the Russian Federal Protective Service (FSO) operates mobile systems to support this activity. Through a review of Russian procurement data, we identify one possible mobile system, manufactured by a company closely connected to the FSO.

- In **Section Three**, we profile the use of Russian GNSS spoofing for strategic facilities protection. We identify potential technology in use for facility protection in Moscow. We also highlight spoofing activities taking place in proximity to protected facilities on the coast of Russia and Crimea in the Black Sea. Through a line of sight analysis, we judge the most likely placement for a GNSS spoofing transmitter on the Black Sea to be at a multi-million dollar "palace," formerly owned by reported family members of senior FSO officers and previously reported to be built for President Putin.

- Finally, in **Section Four**, we expose the use of GPS spoofing in active Russian combat zones, particularly Syria, for airspace denial purposes. This is a capability scarcely reported in the public domain. Using data from a scientific sensor on the International Space Station (ISS), we are able to identify ongoing activity that poses significant threats to civilian airline GPS systems in the region. We pinpoint the most likely location for the system to the northwestern quadrant of Khmeimim airbase, and identify potential military-grade EW systems in use through publicly available information.

The Russian Federation has a comparative advantage in the targeted use and development of GNSS spoofing capabilities. However, the low cost, commercial availability, and ease of deployment of these technologies will empower not only states, but also insurgents, terrorists, and criminals in a wide range of destabilizing state-sponsored and non-state illicit networks. GNSS spoofing activities endanger everything from global navigational safety to civilian finance, logistics, and communication systems.

Table of Contents

Methodology

This report presents findings from a year-long investigation ending in November 2018 on Global Navigation Satellite System (GNSS) spoofing activities affecting civilian GNSS receivers in the Russian Federation, its occupied territories, and the Syrian Arab Republic. Through our reporting we seek to illustrate the effectiveness of using publicly available data and technologies to report on GNSS interference activities. The report presents case studies on three unique applications of GNSS spoofing, highlighting Russia's role in pioneering the use of these capabilities to protect and promote its strategic interests. In each case study, we relied on publicly available information such as: GNSS positioning data, official records, news and social media reporting, and satellite imagery. Following an examination of publicly available data, we collaborated with The University of Texas at Austin (UT). Using signal recordings from a GPS receiver based on the International Space Station (ISS) in low-Earth-orbit (LEO), we characterized, mapped, and identified potential basing locations and equipment involved in GNSS spoofing activities in Syria. We then examine the broader ramifications of these findings.

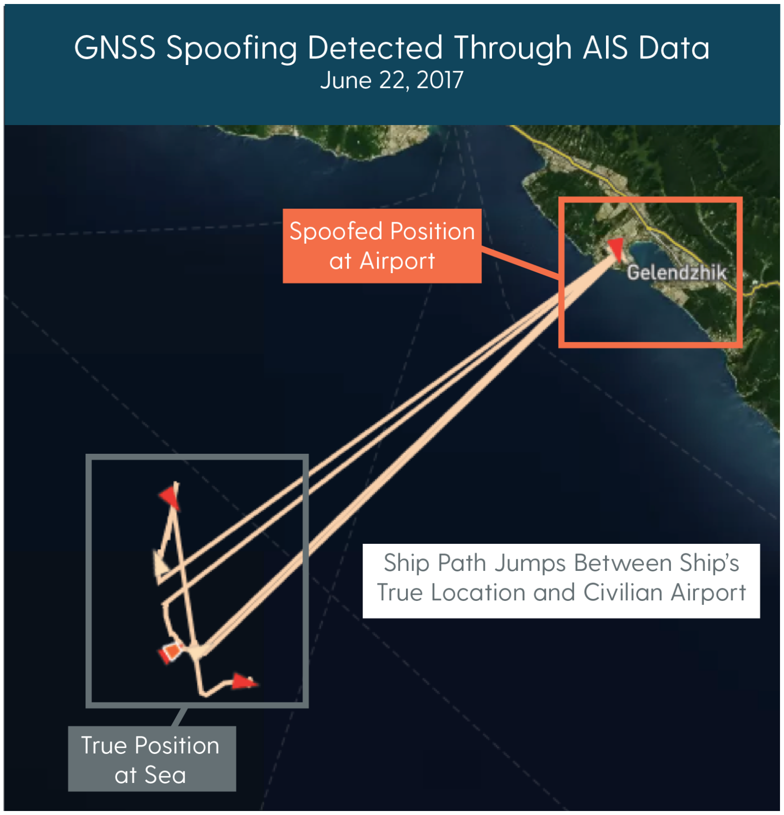
Any mention of GNSS refers to space-based navigation systems such as the US Global Positioning System (GPS/NAVSTAR), Russia's Global Navigation Satellite System (GLONASS), the European Union's Galileo System, China's Beidou Navigation Satellite System, India's Navigation Indian Constellation (NavIC), and Japan's Quazi-Zenith Satellite System (QZSS). Unless explicitly stated, the specific navigation systems targeted by the GNSS spoofing activities detailed in this report have not been confirmed. This report's investigations only detail activities that have affected civilian GNSS receivers. Civilian systems are more vulnerable to interference activities like GNSS jamming and spoofing than encrypted military GNSS receivers.

C4ADS used two distinct investigative methods to identify and map GNSS spoofing activities in Russia and Syria: (1) spoofing detection through marine vessel Automatic Identification System (AIS) path histories and (2) spoofing detection through a LEO satellite GNSS receiver. Each method presents ways in which publicly and commercially available data can be used to identify potential basing locations for devices used to conduct denial-of-service GNSS spoofing activities. The methodologies detailed in this report are highly replicable and scalable, and can be applied to other sources of GNSS positioning data, such as fitness tracking applications and aircraft positioning signals.

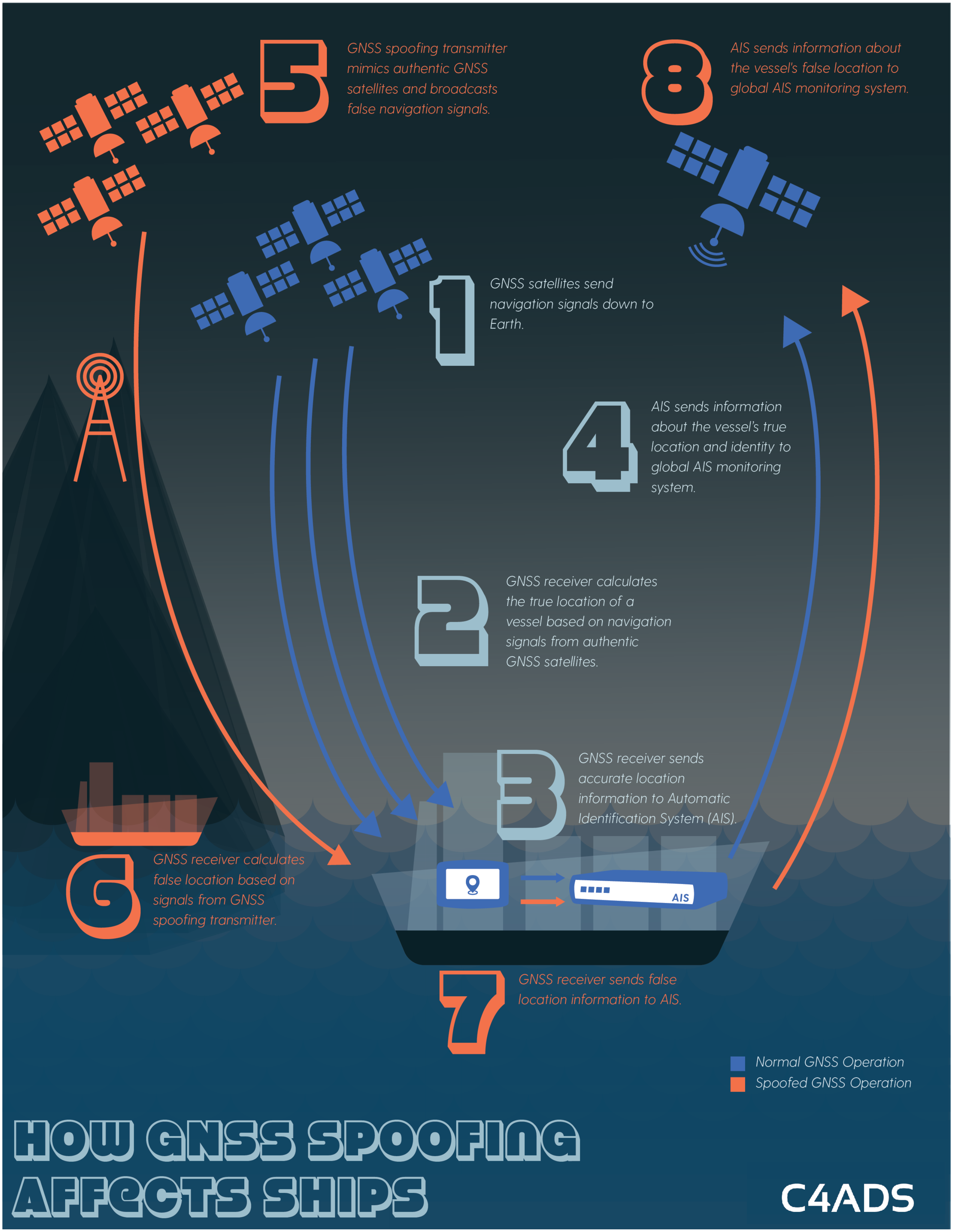
Vessel Detection Methodology

In order to find instances of denial-of-service GNSS spoofing affecting maritime navigation systems off the coast of the Russian Federation and Crimea, C4ADS, using technology from a maritime risk analytics company, used GNSS positioning information derived from maritime vessel AIS data consistent with known behaviors exhibited by victim receivers. In this case, C4ADS identified vessels that reported positioning information at civilian airports, mirroring public reports of GNSS spoofing in Russia. C4ADS manually verified and cross-referenced these path histories with thise of other vessels exhibiting similar patterns of behavior in order to help confirm that suspected victim vessel path histories are not the result of malfunctioning AIS equipment.

Then, using Palantir Foundry, C4ADS conducted both trends analysis and targeted investigations to identify where and when vessels fell victim to spoofing events.


GNSS Spoofing Detected Through AIS Data
June 22, 2017
Spoofed Position at Airport
Gelendzhik
Ship Path Jumps Between Ship's True Location and Civilian Airport
True Position at Sea

After C4ADS identified vessels affected by GNSS spoofing activities, we conducted investigations to determine actors present at each location at the time of the events. C4ADS collected information from records and reporting in English, Russian, and Ukrainian. Using line of sight analyses derived from the location information of ships affected by the spoofing activity, we identified potential land-based GNSS spoofing transmitter positions. We conducted further research on locations identified through this analysis using official property ownership and transfer records, official corporate records, and news and social media posts. Finally, we combined the above analysis with information contained in notice to airmen (NOTAM) alerts and satellite imagery to identify potential systems and motivations for this activity.



HOW GNSS SPOOFING AFFECTS SHIPS

1 GNSS satellites send navigation signals down to Earth.

2 GNSS receiver calculates the true location of a vessel based on navigation signals from authentic GNSS satellites.

3 GNSS receiver sends accurate location information to Automatic Identification System (AIS).

4 AIS sends information about the vessel's true location and identity to global AIS monitoring system.

5 GNSS spoofing transmitter mimics authentic GNSS satellites and broadcasts false navigation signals.

6 GNSS receiver calculates false location based on signals from GNSS spoofing transmitter.

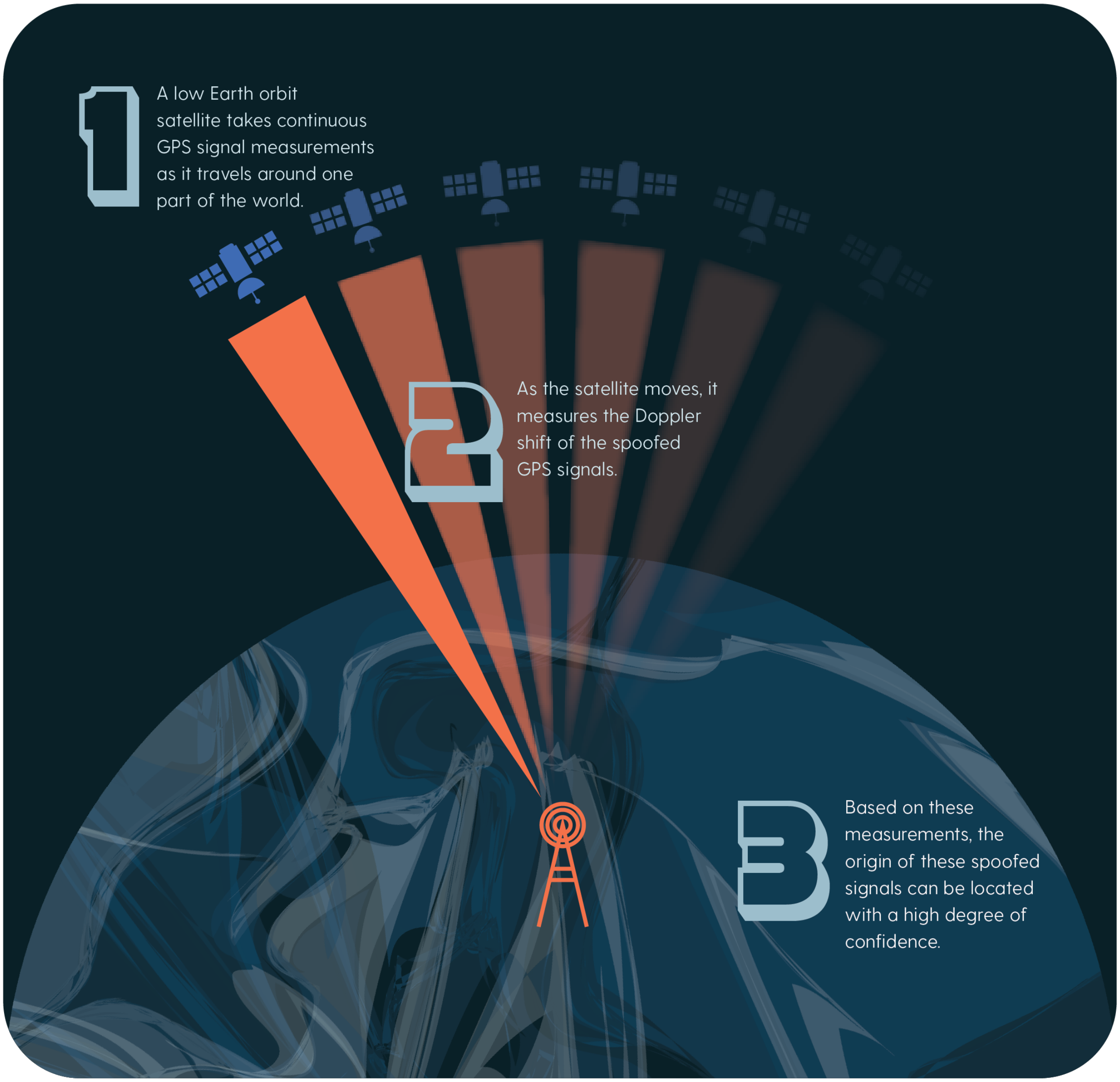
7 GNSS receiver sends false location information to AIS.

8 AIS sends information about the vessel's false location to global AIS monitoring system.

🟦 Normal GNSS Operation
🟧 Spoofed GNSS Operation

Transmitter Localization from Low-Earth Orbit Methodology

C4ADS, through close partnership with and technical expertise from researchers from UT Austin, collected, analyzed, and geolocated denial-of-service spoofing signals using a GPS receiver In low-Earth orbit (LEO) aboard the ISS.[4] In total, we collected three recordings on frequencies used by the GPS L1 and L2 frequency bands on three days in the spring of 2018. Researchers at UT Austin analyzed the raw signal data and used Doppler-based geolocation, illustrated below, to identify the origin point of the GPS spoofing transmissions.


1
A low Earth orbit satellite takes continuous GPS signal measurements as it travels around one part of the world.
2
As the satellite moves, it measures the Doppler shift of the spoofed GPS signals.
3
Based on these measurements, the origin of these spoofed signals can be located with a high degree of confidence.

Once UT Austin researchers analyzed and geolocated the interference signals, C4ADS used publicly available satellite imagery, official records, and imagery posted on social media to identify potential electronic warfare (EW) assets in use at the source location and their intended effects on target receivers.

This report is not designed to be an analysis of any country's laws or regulations, nor does it make conclusions about the intent or legality behind the GNSS spoofing activities detailed herein. We seek instead to profile and expose a critical issue of public interest. **The mention of any individual, company, organization, or other entity in this report does not imply the violation of any law or international agreement, and should not be construed as such**.

Technical Definitions

This report does not cover all existing forms of GNSS interference and thus, it relies on the following definitions to delineate between different variants of interference:

- **GNSS Jamming**, also referred to as brute force jamming, is when an attacker generates noise-like signals at frequencies used by a GNSS system in order to prevent GNSS receivers from tracking authentic signals.[5] [6]
- **Denial-of-Service GNSS Spoofing**, sometimes referred to as 'smart-jamming,' is when an attacker mimics authentic GNSS signals in order to hijack target GNSS receiver tracking loops and feed false or even blank navigational information to the vulnerable receiver. [7] In most cases, the effects of denial-of-service spoofing are readily apparent to the user. ***Unless explicitly stated, references to 'GNSS spoofing' in this report will refer only to denial-of-service spoofing attacks.***
- **Deception GNSS Spoofing** is when an attacker mimics authentic GNSS signals in order to hijack target GNSS receiver tracking loops, feed false positioning or timing information to the target receiver, and covertly misdirect the receiver and its platform to some desired location. Successful attacks will deceive both the target receiver and its user.[8]

Among GNSS interference experts, there are competing definitions on when spoofing can be categorized as either deception or denial-of-service.[9] For the purpose of this paper we use the above definitions. However, for more information about alternate definitions, see "Unmanned Aircraft Capture and Control via GPS Spoofing" by Kerns, Shepard, Bhatti, and Humphreys.

GNSS Spoofing: Overview and Applications

In the summer of 2013, a research team from The University of Texas at Austin (UT) successfully hijacked the GPS navigation systems onboard an $80 million superyacht using a $2,000 device the size of a small briefcase. The experimental attack forced the ship's navigation systems to relay false positioning information to the vessel's captain, who subsequently made slight course corrections to keep the ship seemingly on track. In reality, the falsified signals generated by UT Austin's device had successfully set the vessel off-course by several degrees, all without tripping a single alarm on the ship's navigational alert systems. While this was a controlled experiment, a malicious actor could use the same techniques to direct a vessel to stray into hostile waters.

The GNSS Family of Systems

GPS (United States)
GLONASS (Russia)
Galileo (European Union)
BeiDou (China)
QZSS (Japan)
NavIC (India)

The 2013 experiment demonstrated the use of one of the world's first openly acknowledged GNSS spoofing devices.[10] At its core, GNSS spoofing is the deliberate transmission of signals designed to emulate the authentic satellite systems that underpin much of the world's critical infrastructure. GNSS spoofing is distinct from other forms of navigation interference such as GNSS jamming, which simply drowns out satellite signals to prevent receivers from using them.[i] Instead, spoofed signals are able to force vulnerable GNSS receivers, like those installed on the superyacht, to lose their lock on authentic satellite signals and instead lock on to the signals generated by the spoofing device.[ii] Once a receiver locks on to the spoofed signals, the spoofing transmitter can relay false position or timing information to the victim receiver, thereby "taking control."[iii] UT Austin's successful experiment served to expose just one of the many systems vulnerable to GNSS spoofing attacks.

[i] GNSS Jamming is the deliberate transmission of signals on frequencies used by GNSS in an effort to prevent receivers from locking-on to authentic GNSS Signals. GNSS jamming requires relatively little technical knowledge and can be conducted by simply drowning out authentic signals with random or disruptive noise. For more information, see https://www.gps.gov/spectrum/jamming/

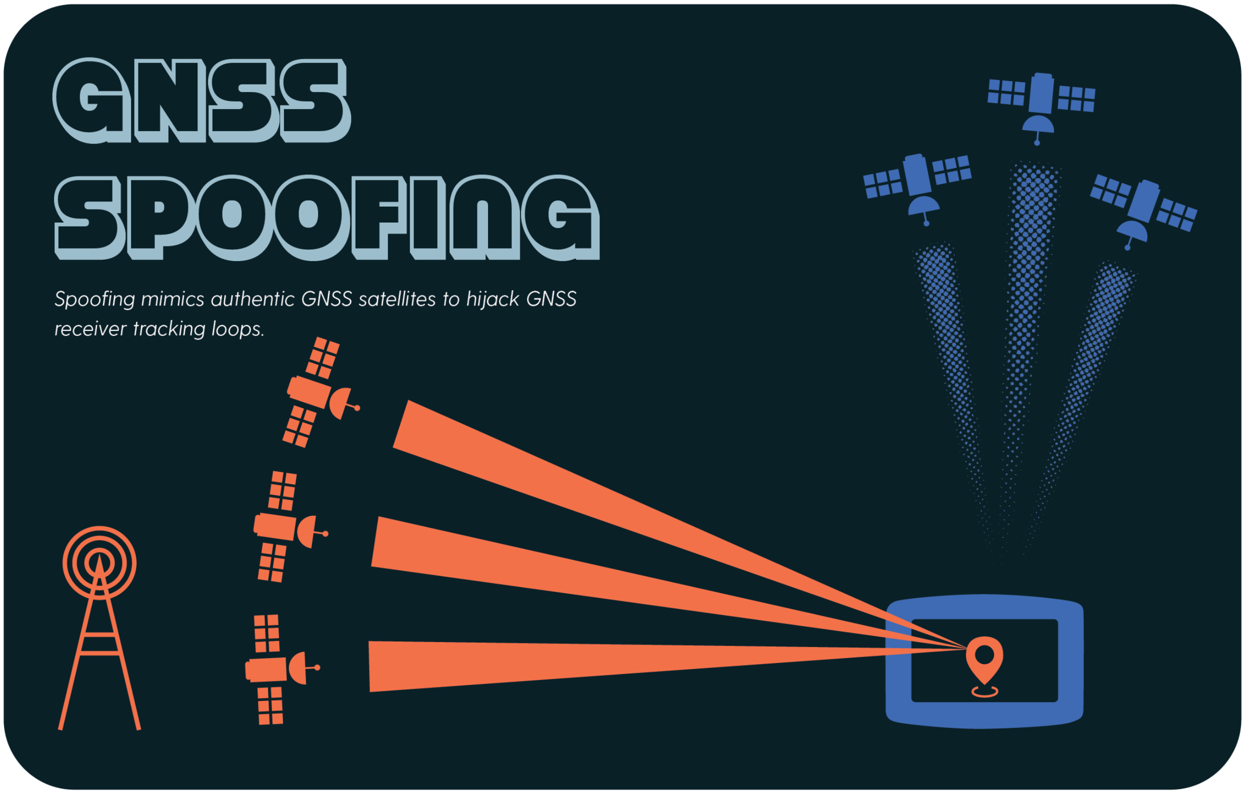
GNSS jamming is the deliberate transmission of signals on frequencies used by GNSS in an effort to prevent receivers from locking-on to authentic GNSS Signals. GNSS jamming requires relatively little technical knowledge and can be conducted by simply drowning out authentic signals with random or disruptive noise. For more information, see https://www.gps.gov/spectrum/jamming/

[ii] As previously mentioned, Denial-of-Service GNSS Spoofing, sometimes referred to as 'smart-jamming', is when an attacker mimics authentic GNSS signals in order to hijack target GNSS receiver tracking loops and feed false or even blank navigational information to the vulnerable receiver. In most cases, the effects of denial-of-service spoofing are readily apparent to the user. Deception GNSS Spoofing, on the other hand, is when an attacker mimics authentic GNSS signals in order to hijack target GNSS receiver tracking loops (through capture and drag-off techniques), feed false positioning or timing information to the target receiver, and covertly misdirect the receiver and its platform to some desired location. Successful attacks will deceive both the target receiver and its user. For more information, see http://www.au.af.mil/au/awc/space/au-18-2009/au-18_chap21.pdf and http://rnl.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf

[iii] In most public examples GNSS spoofing, the spoofing transmitter simulates false GNSS satellite ephemeris and timing information which coerces the victim receiver to calculate incorrect positioning and, in some cases, timing information.

GNSS Jamming

Jamming creates noise which prevents GNSS receivers from locking on to authentic GNSS satellites.



GNSS Spoofing

Spoofing mimics authentic GNSS satellites to hijack GNSS receiver tracking loops.

The proven effectiveness of GNSS spoofing attacks on critical systems like maritime navigation equipment is increasingly recognized by US and other governments. A 2012 National Risk Estimate conducted by the US Department of Homeland Security found that "US critical infrastructure sectors are increasingly at risk from a growing dependency on the Global Positioning System (GPS) for space-based position, navigation, and timing (PNT)."[11] The report concluded that GNSS spoofing attack scenarios in particular presented the highest consequences to critical national infrastructure due to the potential lapse of time between when the interference begins and when it is detected.[12] A similar report commissioned by the United Kingdom Space Agency in 2017 asserted that "all critical national infrastructure" in the UK relies on GNSS to some extent, and that a five-day disruption to GNSS would result in an estimated £5.2 billion in economic loss.[13]

GNSS is embedded in a wide range of basic day-to-day economic and transport functions, but many civilian systems remain vulnerable. Attackers could use multiple techniques to disrupt and even profit off of these potential vulnerabilities, as summarized in the table below:

Sector	Systems Using GNSS	GNSS Spoofing Scenario
Transportation	• Maritime navigation systems • Road navigation / Advanced Driver Advisory Systems • Air transport infrastructure / Automatic Dependent Surveillance-Broadcast • Logistics monitoring and management • Automated navigation systems • Port container management systems • Vehicle-to-vehicle communications for connected and automated vehicle coordination	• Divert vessel into hostile or territorial waters • Disrupt port activities by targeting cranes using GNSS for automated container logistics • Hijack cargo in transit by disguising true location of container • Deny aircraft use of satellite navigation systems
Communication	• Cellular communication networks • Fixed-line communication networks	• Target time synchronization systems on cellular network systems to degrade and disrupt operations
Law Enforcement	• Search and rescue systems • GNSS positioning information as evidentiary material • Asset monitoring and tracking • Law enforcement equipment with time-based software licenses	• A vessel turning off its AIS transponder can alert regulators to possible illicit activity, spoofing location through vessel GNSS receiver can conceal vessels engaging in illicit trade, fishing, or sanctions evasion • Degrade the reliability of using GPS telemetry for legal action and proceedings • Force law enforcement equipment user licenses using GNSS for timing to prematurely expire

Sector	Systems Using GNSS	GNSS Spoofing Scenario
Defense	• Air-gapped NTP servers using GNSS for time synchronization • Precision Guided Munitions • Military GNSS receivers that have not been rekeyed with current encryption key. • Small unmanned aerial vehicles without spoofing countermeasure systems installed	• Spoof military GNSS receivers that have not been rekeyed due to human error. • Spoof GNSS timing signals on an air gapped NTP server to 'turn back time' on a time-based one-time password system • Target small military or monitoring drones to deny reconnaissance missions over sensitive locations
Financial	• Stock Exchange • Insurance telematics	• Target time synchronization systems for unsecured stock exchanges to drag off time and create artificial systems of arbitrage • Abuse marine delay in start up insurance on high value shipments to profit on insurance claims
Energy	• Power substation load transfer systems	• Degrade GPS-dependent time synchronization systems at power substations to cause widespread outage

Despite these vulnerabilities, leaders in the public and private sectors have paid little attention to the threat of GNSS spoofing. Until recently, this was for good reason. Signal generators capable of conducting a spoofing attack cost of tens of thousands of dollars and required expert knowledge to operate. But this all began to change over the past decade with the advent of cheap, commercially available, and portable "software defined radios" (SDR) and open-source code capable of transmitting spoofed GPS signals. SDRs are used for a variety of innocuous applications including amateur radio broadcast, aircraft tracking, and ship tracking. Today, these devices are capable of mimicking authentic, multimillion-dollar GPS satellite signals and can be produced for under $300—less than the price of a new television.[iv] Inexpensive systems have already been used to hijack vehicle navigation systems,[14] cheat at Pokémon GO,[15] and even "turn back time" on time-based authentication systems.[16] According to some US government officials, even drug cartels are beginning to use GNSS spoofing to mask their activities and target smaller US drones.[17]

The Russian Federation is a pioneer in the use of these techniques to further its strategic interests at home and abroad. In response to NATO's advantage in C4ISR[v] capabilities, Russia has prioritized the development of a comprehensive suite of asymmetrical EW systems designed to deceive, degrade, and deny military and civilian GNSS receivers.[18] [19] In effect, Russian forces now have the capability to create large GNSS denial-of-service spoofing environments, all without directly targeting a single GNSS satellite. These systems are widely believed to be in use across Russia's Western and Southern Military Districts at the border with NATO and reportedly have been forward deployed in conflict zones such as Ukraine[20] and Syria.[21]

[iv] The author was able to purchase all components for a homemade GPS spoofing device for less than $350.

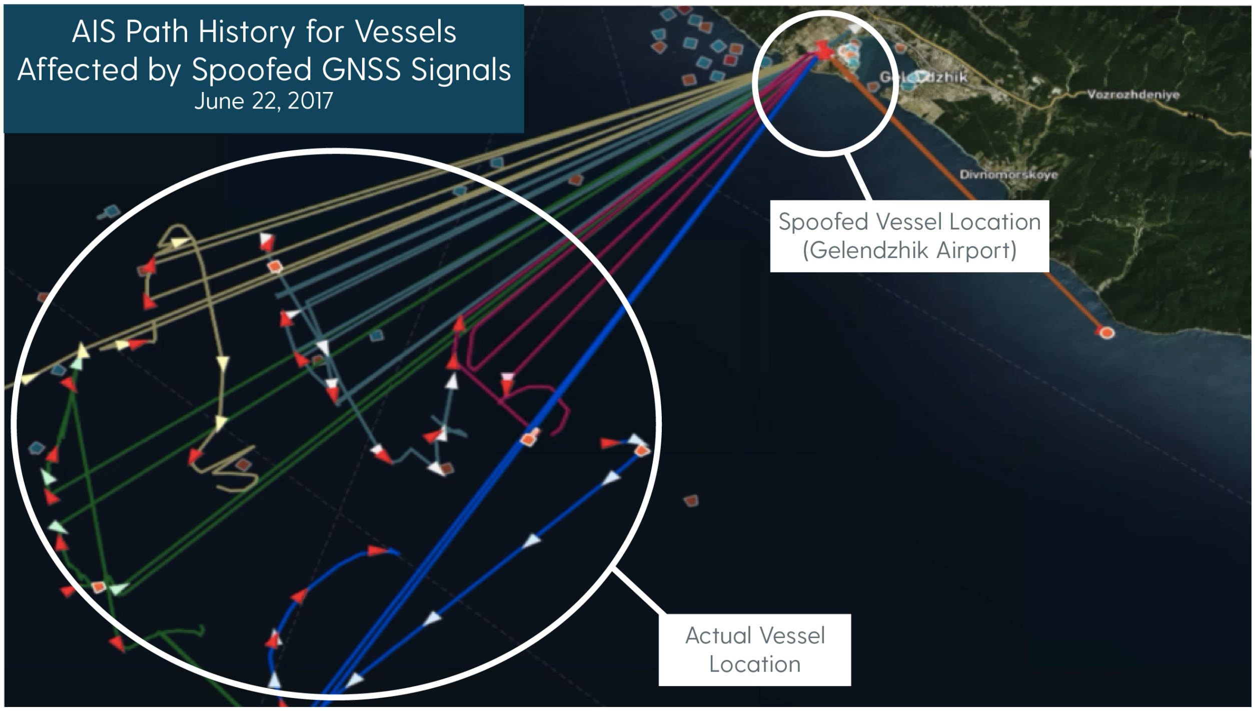
[v] Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) is a general term that refers to the systems and techniques used to collect and process information.

Increasing use of GNSS spoofing capabilities among the Russian military and security services has caused spillover effects on civilian systems. Public reports from Moscow began to surface in June 2016 claiming that mobile phone navigation systems often reported false positioning information when in proximity to the Kremlin.[22] [23] After similar activity was detected in Saint Petersburg, many were quick to hypothesize that this interference was tied to counter-drone activities of the Russian Federal Protective Service (FSO), the government entity charged with protecting Russia's president.[24] [25] These hypotheses, however, remained unconfirmed. In June 2017, the captain of the merchant vessel Atria provided direct evidence of GNSS spoofing activities off the coast of Gelendzhik, Russia, when the vessel's on-board navigation systems indicated it was located in the middle of the Gelendzhik Airport, about 20km away.[26] More than two dozen other vessels reported similar disruptions in the region on that day.[27] The US Maritime Administration subsequently issued a GPS interference advisory for vessels in the Black Sea, one of the first of its kind.[28] Activity was reported on a larger scale during military exercises, including Russia's Zapad 2017 and NATO's Trident Juncture 2018, when Norway and Finland reported severe GPS outages affecting commercial airliners and cell phone networks for several days.[29] [30]

To date, methods for detecting GNSS spoofing and other interference have been reserved for organizations with the ability to leverage advanced means for signals collection. As a result, the full scope of this activity has rarely been discussed in the public domain. With the democratization of technological capabilities and access to data, these advanced means are now available to a wider audience. **This report serves as one of the first systems-level demonstrations of how publicly available data can be used to identify, detect, and expose the deployment of denial-of-service GNSS spoofing capabilities.** In doing so, we demonstrate how the use of GNSS spoofing in the Russian Federation, its occupied territories, and its overseas military facilities is far more pervasive and advanced than previously thought.

SPOOFING ACTIVITY ACROSS RUSSIA, CRIMEA, AND SYRIA

C4ADS found that GNSS spoofing activities in the Russian Federation, its occupied territories, and its overseas military facilities are larger in scope, more geographically diverse, and started earlier than any public reporting has suggested to date. Reports by CNN[31] and the RNT Foundation[32] identify fewer than 450 vessels affected since late 2016.[i] Using Automatic Identification System (AIS) ship location data collected at scale, C4ADS identified 9,883 instances[ii] of GNSS spoofing that affected 1,311 commercial vessels beginning in February 2016.[iii] The disruptions appear to have originated from ten or more locations in Russia and Russian-controlled areas in Crimea and Syria.


AIS Path History for Vessels Affected by Spoofed GNSS Signals
June 22, 2017

C4ADS needed a proxy that would display patterns of disruption associated with spoofing. In principle, any device that relies on GNSS could be used to detect spoofing activity. In Moscow, for example, where GNSS spoofing disruptions have been observed near the Kremlin, public reporting has shown that location-based apps such as Uber often report false positioning data, mistakenly calculating fares for locations thousands of miles away.[33] It is also possible to detect this activity through other devices that report GNSS positioning information.

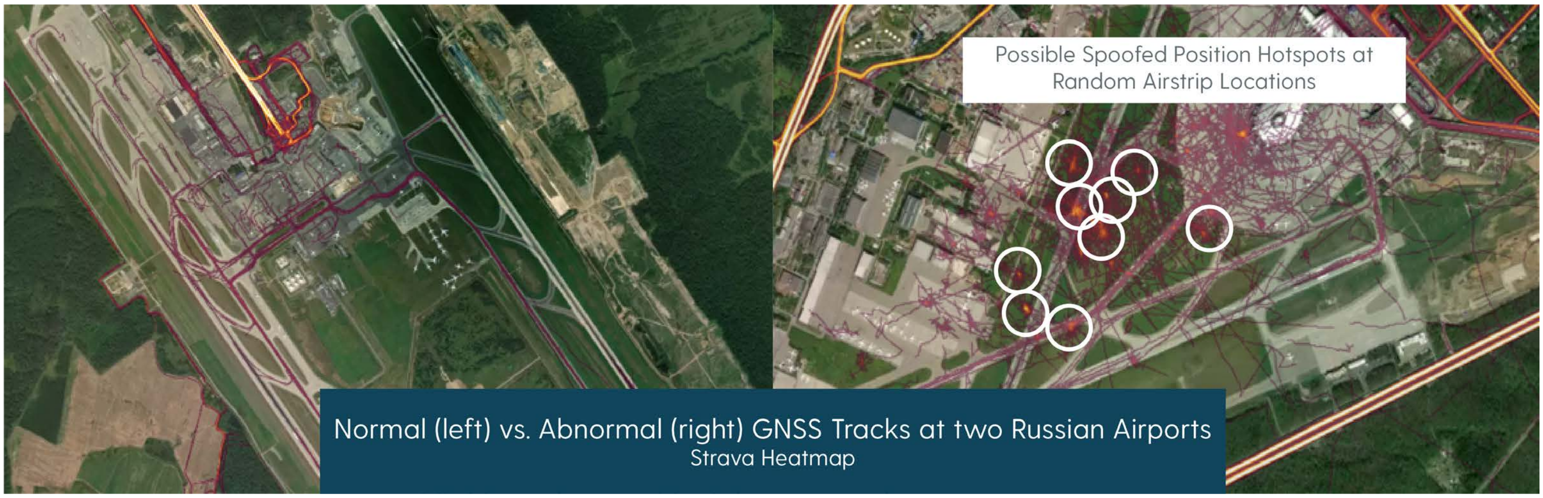
Publicly available position heatmaps derived from fitness tracker applications, such as Strava, can also be used to identify GNSS receiver path histories that exhibit unusual patterns.[34] Data from Strava shows a pattern of individuals in central Moscow suddenly

[i] Estimates of the number of victim vessels ranged from a few dozen to about 450. The first significant reporting of GPS spoofing in Moscow surfaced around October 2016.

[ii] C4ADS defined a spoofing 'instance' as every time we detected a vessel reporting a false position information at a civilian airport.

[iii] C4ADS examined AIS data between January 2013 and November 2018, but only detected spoofing activity beginning in February 2016. Activities may have taken place prior to this time frame, but could not be included in our sample set.

appearing at the Vnukovo and Sheremetyevo airport runways in Moscow. At normal airports throughout Russia and the rest of Europe, device position paths typically remain confined to aircraft taxiing paths and the terminal area, as seen below in the heatmap of Moscow's Domodedovo Airport, where activity is relatively normal. In contrast, victim receivers potentially located in central Moscow appear to be spoofed to discrete coordinates, which appear as hot spots on the Vnukovo Airport tarmac, about 20km outside Moscow. With the working assumption that the airport authorities do not allow passengers to run in circles on an active runway, these positions are highly suspect.


Possible Spoofed Position Hotspots at Random Airstrip Locations

Normal (left) vs. Abnormal (right) GNSS Tracks at two Russian Airports
Strava Heatmap

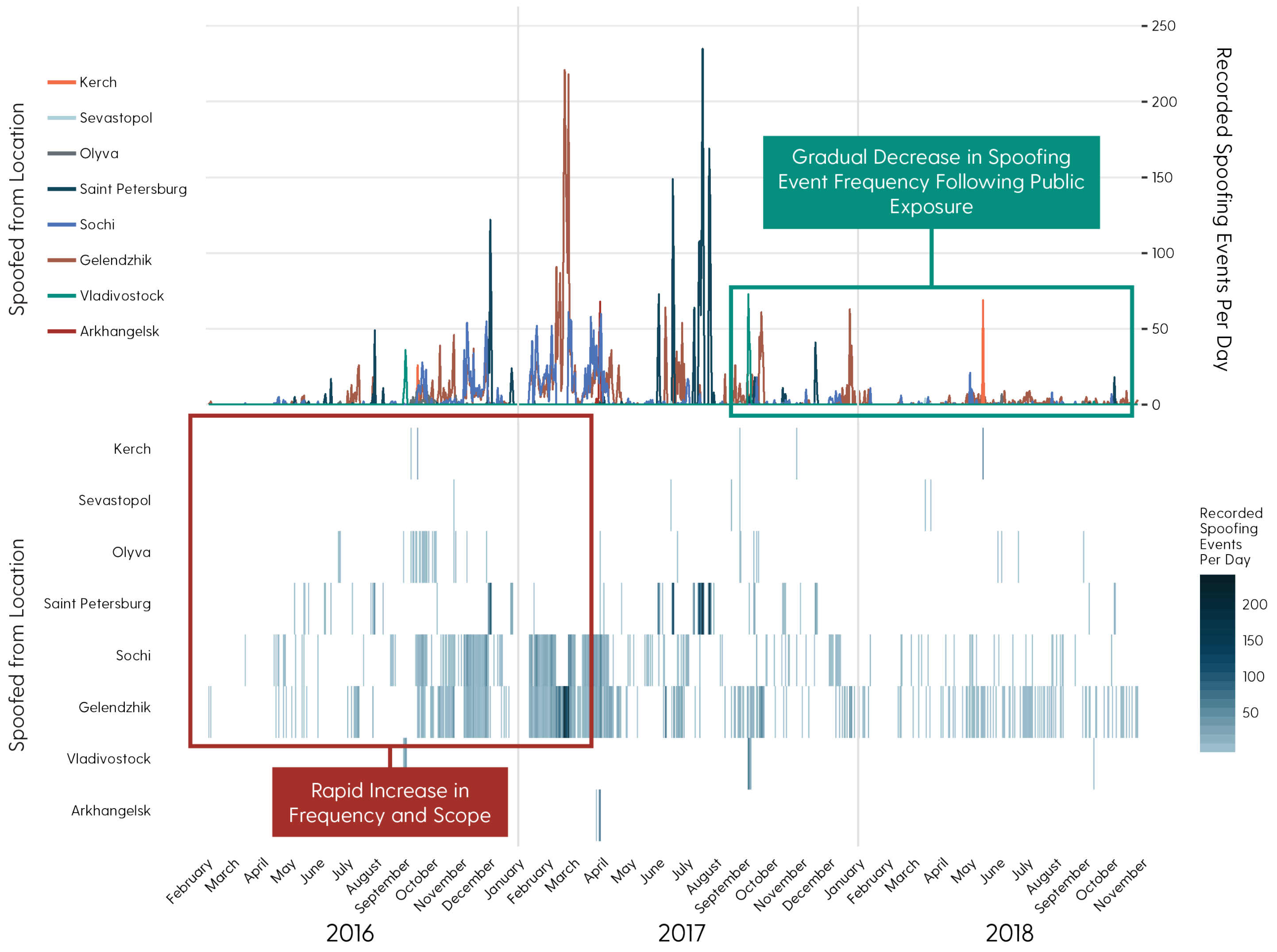
While Strava shows patterns of GNSS spoofing, AIS data present a more extensive, reliable, and easily studied source of location data. We found that AIS data served as a good proxy for identifying GNSS spoofing activity. GNSS spoofing activities that force maritime vessels to report positioning information at nearby airports create an easily recognizable and detectable pattern of activity where vessels that are clearly at sea report their positions on land. By building datasets of all vessels that exhibited these characteristics, C4ADS identified a number of additional vessels affected by GNSS spoofing activities in the waters around the Russian Federation.

We found that across all instances of GNSS spoofing detected in Russia and Crimea, receivers reported false positioning information at a local civilian airport, often dozens of kilometers away. Our findings support previous public reports that the GNSS spoofing activities detected in Russia are designed as a denial-of-service tool to activate firmware-level geofence locks on commercial drones. These locks prevent drones from flying in restricted airspace, such as the areas over airports.[35] If a commercial drone locks on to the spoofed signals, they would either return to what they perceive as 'non-restricted' airspace or land immediately.[36] Such a capability would have a wide range of both offensive and defensive applications but is likely to be relatively indiscriminate in nature, affecting both intended and unintended receivers in the vicinity.

Timeline of Detected Activity

GNSS spoofing in Russia and Crimea began long before public reporting on these disruptions emerged. This activity can be detected off the coast of Gelendzhik in early February 2016, more than a year before the June 2017 US Maritime Administration alert on Black Sea activity.[37]

Timeline and Frequency of Detected Spoofing Activity by Region



Gradual Decrease in Spoofing Event Frequency Following Public Exposure

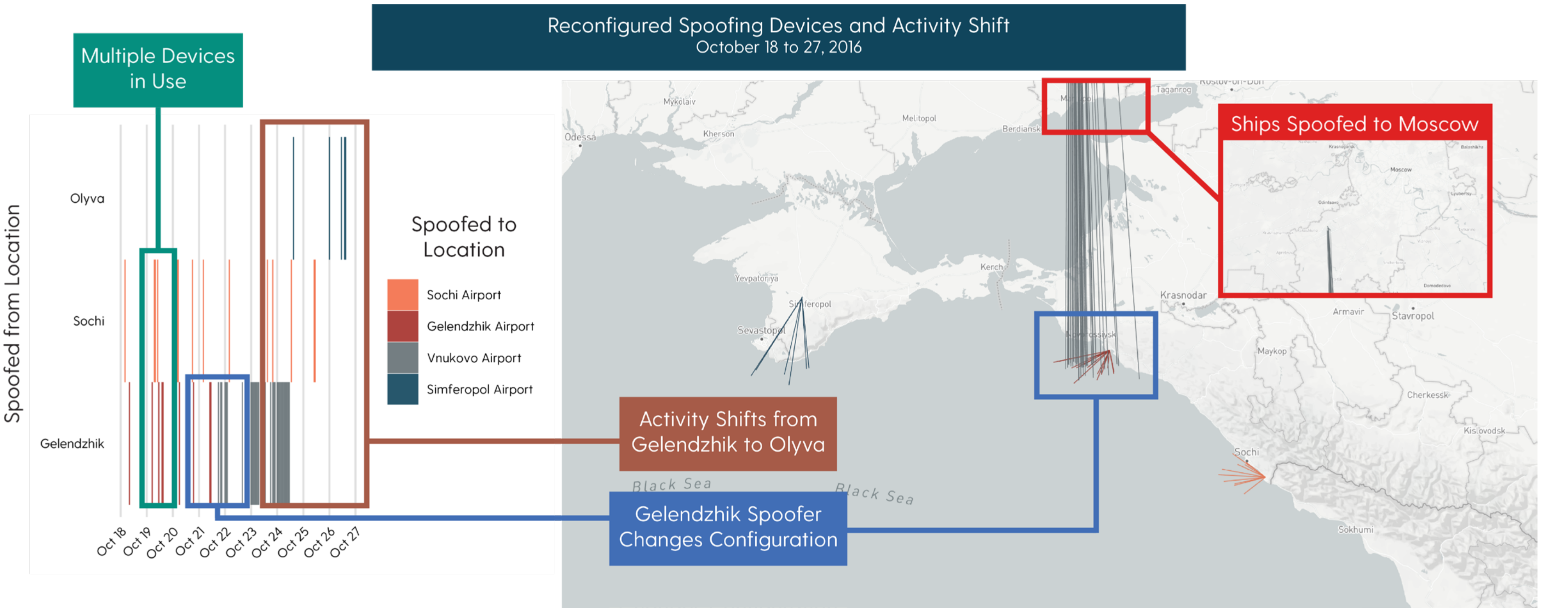
Rapid Increase in Frequency and Scope

In the timeline of spoofing events above, created from analysis in Palantir Foundry, we can view several key trends in how these disruptions evolved between February 2016 and November 2018. When the activity first began in the spring of 2016, fewer than a dozen vessels were affected. However, over the next year, these events increased rapidly in both frequency and scope, possibly as these spoofing transmitters proliferated to new locations and increased in strength. Following high-profile public exposure of these events in several Russian and Western news outlets in June and July 2017, the frequency of these events appeared to gradually decrease.[38] [39]

Through investigations into events at each location, we found that GNSS spoofing likely began in 2016 in at least eight of the nine locations in Russia and Crimea where we found evidence of spoofing. Spoofing events near Gelendzhik, Sochi, Saint Petersburg, and Olyva were among the most frequent in the data analyzed; activity was detected on 462 separate days between February 2016 and November 2018. Activity at these locations took place on 46 percent of all days examined. In almost all cases where brief GNSS spoofing events occurred in remote locations in Russia and Crimea, such as in Arkhangelsk, Vladivostok, and Kerch, we found that spoofing events directly coincided with visits by Russian president Vladimir Putin. In the case studies examined later in this report, we hypothesize that the short-lived and isolated nature of these one-off events suggests that at least some devices used to conduct this activity are mobile and can be temporarily deployed at a location to create local areas of effect.

C4ADS also found evidence suggesting that multiple GNSS spoofing devices were in use. Spoofed GNSS signals can generally only affect receivers that are within line of sight of the spoofing device.[40] Therefore, the range of these devices is typically limited to the surrounding area. In our sample, there were 593 instances where vessels located in areas too far for a single land-based transmitter to reach were affected within the same hour. Additionally, it appears that the spoofing devices may not be constantly active as vessels' locations were not consistently spoofed. In the timeline and frequency distribution graphs pictured above and the example shown below, spoofing activity appears to 'swap' between two or more locations over time. When spoofing activity at one location ends, it often resumes at a separate location shortly after, indicating that this activity is coordinated to some degree.

Focusing on activity in the Black Sea between October 18 and 27 of 2016, vessel GNSS receivers in proximity to both Gelendzhik and Sochi fell victim to spoofing events within less than an hour of one another on multiple occasions. About half-way through


Reconfigured Spoofing Devices and Activity Shift
October 18 to 27, 2016

Multiple Devices in Use

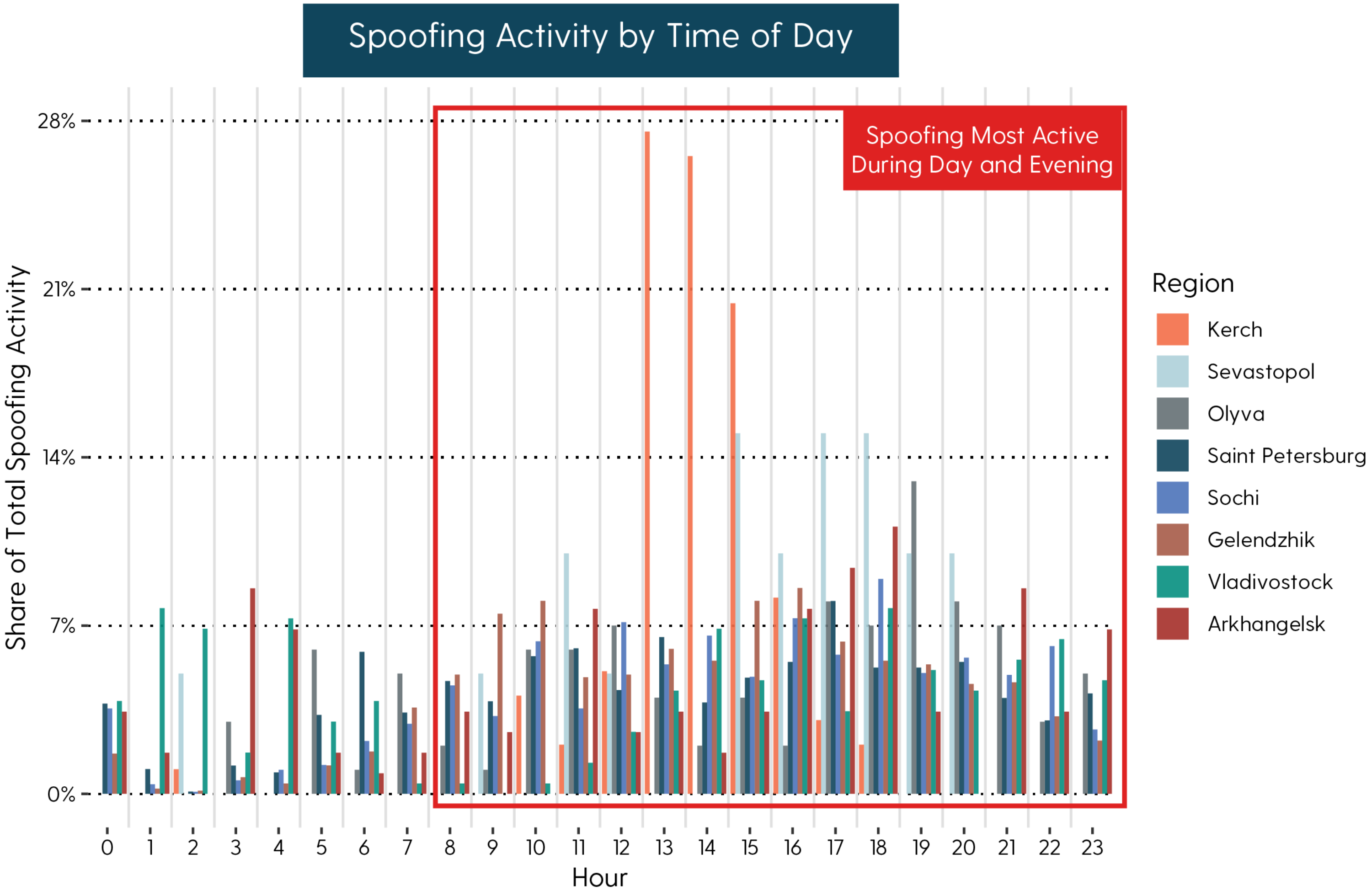
Activity Shifts from Gelendzhik to Olyva

Gelendzhik Spoofer Changes Configuration

Ships Spoofed to Moscow

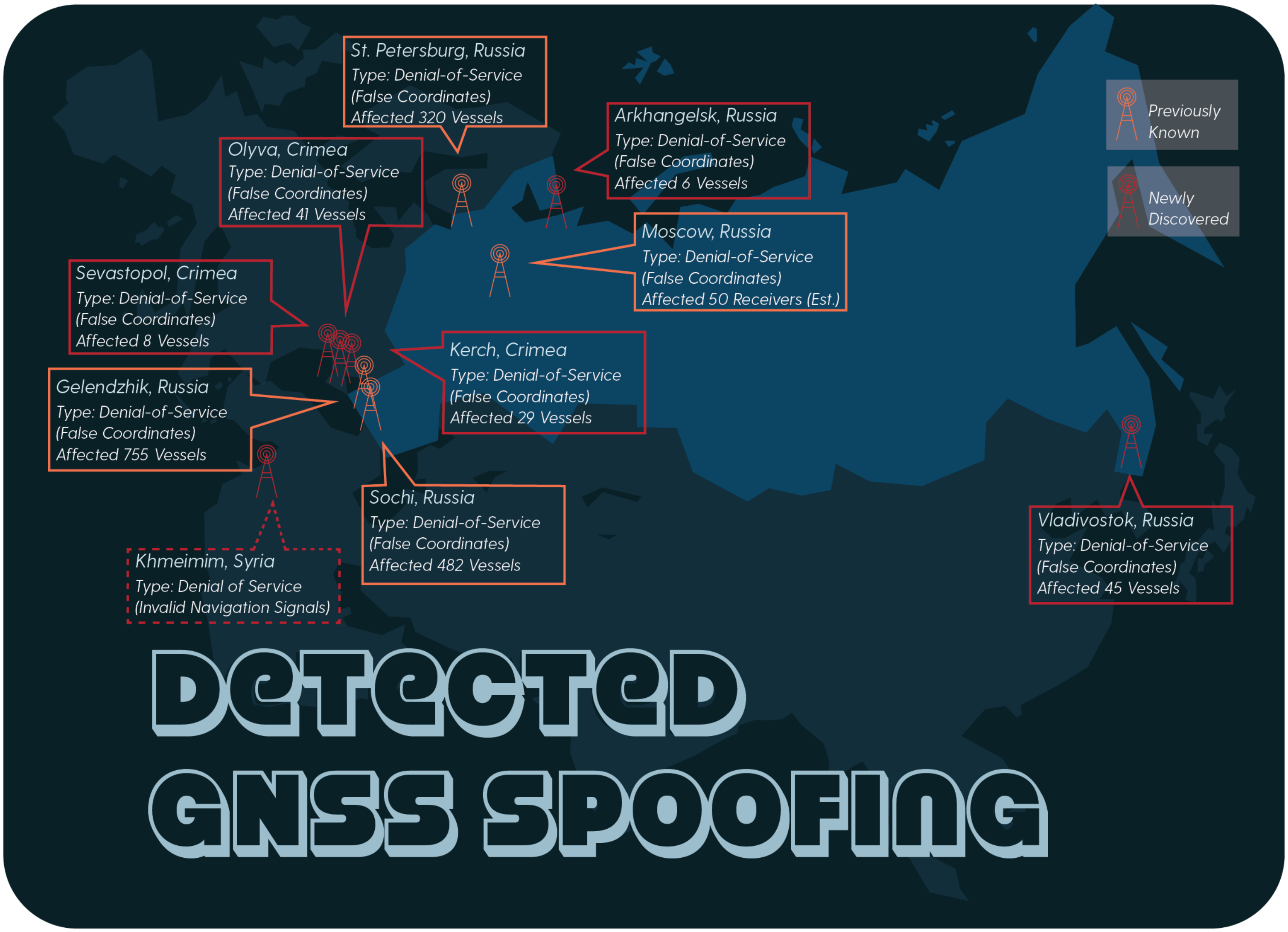
this period, the spoofing device located near Gelendzhik temporarily stopped directing receivers to the Gelendzhik Airport and, instead, began to direct them to Vnukovo Airport in Moscow, more than 1,000 kilometers away. As activity appeared to taper off near Gelendzhik, activity in waters near the Crimean city of Olyva began. This pattern of activity indicates that (1) at least two spoofing devices are in use in the Black Sea, (2) these devices can be reprogrammed to spoof vessel receivers to multiple locations, and (3) spoofing activity at certain locations is not constant, and may even shift between locations over time.

Finally, through an analysis of the hourly distribution of activity, we can demonstrate that spoofing events primarily take place during the day across all locations. In total, 90 percent of events took place between the hours of 6:00 and 22:00 local time. One explanation for the apparent dip in activity between midnight and the early hours of the morning could be that the spoofing devices are only turned on when the operators are awake. A second potential explanation, examined later in this paper, is that the spoofing transmitters are used to protect the movements of high-value individuals during the day.



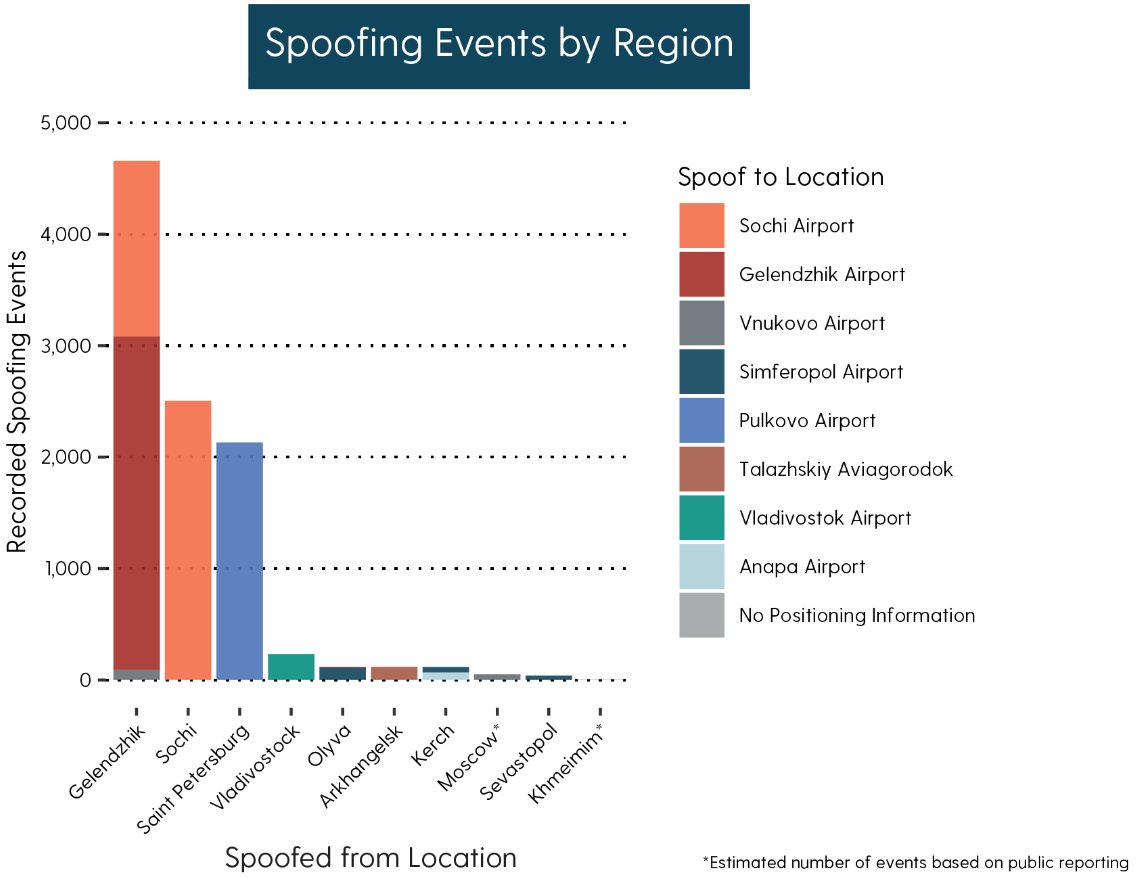
Geography of Detected Activity

The scope of GNSS spoofing events appears to be far more indiscriminate, persistent, and widespread than previous public reporting suggests. In total, C4ADS found 9,883 GNSS spoofing instances affecting 1,311 vessels across ten locations in Russia, Crimea, and Syria between February 2016 and November 2018. In addition to Moscow, Saint Petersburg, Sochi, and Gelendzhik, where GNSS spoofing activity was already known, C4ADS found evidence of newly discovered activities in Arkhangelsk in the Russian far north, Vladivostok in the far east, the Kerch Strait near the frontline with Ukraine, and Sevastopol and Olyva on the Crimean Peninsula. Finally, working with researchers from UT Austin, we detected GNSS spoofing originating from Russia's Khmeimim Airbase in Syria on three separate occasions.



Scope of Detected Activity

Previous public reporting by the Resilient Navigation and Timing Foundation and CNN suggests that only about 450 vessels fell victim to GNSS spoofing as of November 2018.[41] However, C4ADS found that the total number of vessels spoofed during this time may be closer to 1,311. Furthermore, we are able to demonstrate that events near Gelendzhik, Sochi, and Saint Petersburg comprise over 94 percent of all detected activity. However, this trend may be related to limitations associated with our use of AIS as a proxy. Gelendzhik and Sochi, which experienced the most GNSS disruption with 4,659 and 2,506 spoofing events, respectively, are both in close proximity to key maritime transit and port facilities with a high density of GNSS receivers available to detect the spoofed signals. Gelendzhik is located next to the Novorossiysk port, which is one of the largest deep-water ports in Russia and home to a large contingent of the Russian Black Sea Fleet[42] [43] while the Port of Sochi is a major destination and mooring location for passenger and luxury vessels.[44]



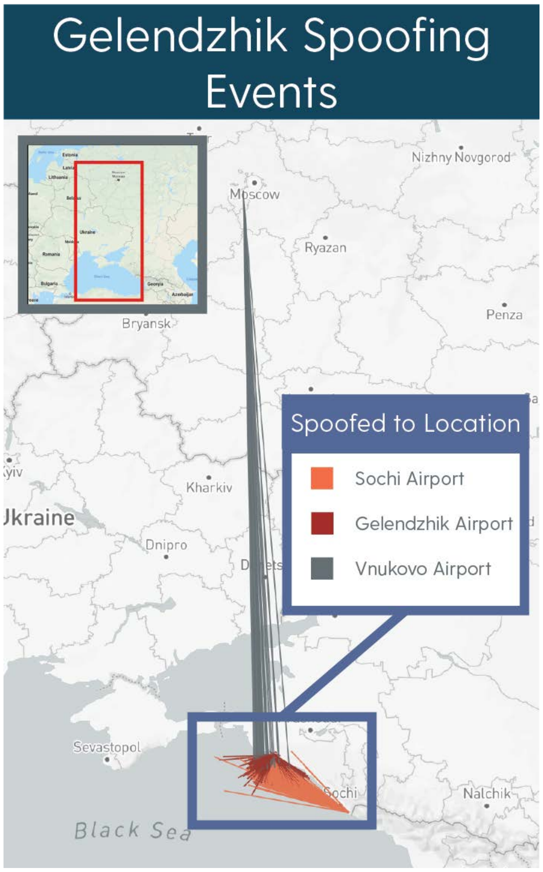
*Estimated number of events based on public reporting

In areas where there are fewer receivers to report irregular activity, spoofing may be much harder to detect using publicly available information, and is therefore not included in our dataset. However, based on the available data, we were able to observe some key trends that have significant impacts on navigational safety.

Trend I: GNSS Receivers are Spoofed to Multiple Locations

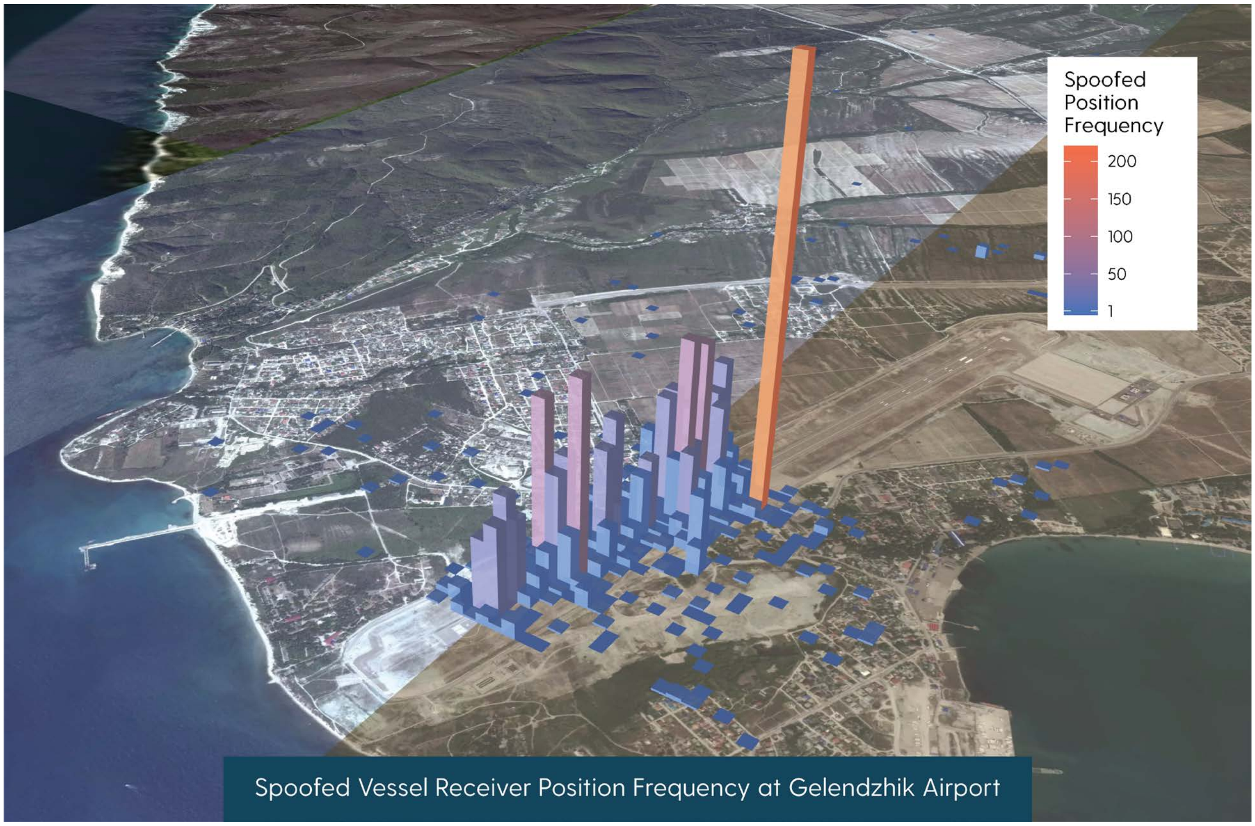
While most affected locations in Russia and Crimea saw vessels spoofed to only one nearby airport, vessels off the coast of Gelendzhik and Kerch were spoofed to two or more airports sequentially between 2016 and 2018. AIS data throughout this period indicate that vessels near Gelendzhik were spoofed to the Gelendzhik Airport, the Sochi-Adler Airport, and the Vnukovo Airport in Moscow, as shown in the image on the right. Additionally, vessels near Kerch reported spoofed positioning information at both the Simferopol Airport in Crimea and the Anapa Airport on the other side of the Kerch Strait.

This change in where vessels are spoofed to is an indication that the GNSS spoofing devices used in these regions can be reprogrammed to force victim receivers to different coordinates at will. By examining the approximate positions to which victim vessels had their positions spoofed, 'hot spots' at each airport can be observed. An example of 'hot spots' at Gelendzhik airport, visualized through the spoofed position frequency distribution below, indicates that destination coordinates may vary significantly across spoofing events over time. This variation within the confines of the airport could potentially be the result of either manual coordinate selection by the device operator or by victim receiver calculation errors.


Gelendzhik Spoofing Events

Spoofed to Location

- 🟧 Sochi Airport
- 🟥 Gelendzhik Airport
- ⬛ Vnukovo Airport



Spoofed Vessel Receiver Position Frequency at Gelendzhik Airport

Trend II: Activity Takes Place Near Sensitive Government Airspace

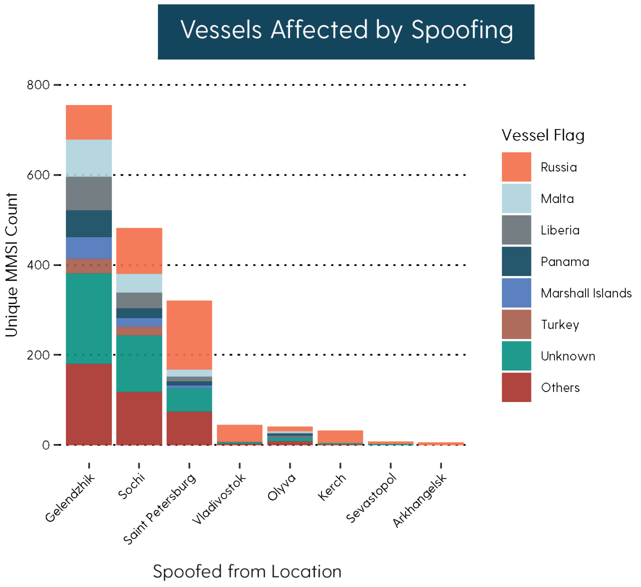
C4ADS found a high correlation between GNSS spoofing events and the presence of sensitive or prohibited airspace. In Russia and Crimea, we found at least 12 isolated and ongoing GNSS disruptions. These instances appear to be localized in areas within close proximity to the Russian head of state and Russian government facilities operated by the FSO, as detailed below. In Syria, spoofing events took place in proximity to Khmeimim Airbase, which is protected by advanced Russian military EW and anti-aircraft equipment.[45]

GNSS Spoofing Event Date	Location (Approx.)	GNSS Spoofing Type	Prohibited or Sensitive Airspace Present
February 2016 to Present	Gelendzhik, Russia	Denial-of-Service (False Coordinates)	**Yes**, prohibited airspace over residence allegedly tied to President Putin located near affected area.[46] [47]
March 2016 to Present	Sochi, Russia	Denial-of-Service (False Coordinates)	**Yes**,[48] Riviera-6 and Bocharov Ruchey Government residences operated by Russian FSO[49] are adjacent to Sochi Port and coast where highest levels of spoofing activity have been detected.
May 28, 2016	Novo-Ogaryovo, Moscow, Russia	Denial-of-Service (False Coordinates)	**Yes**,[50] took place within prohibited airspace with Russian presidential residence <1km away from affected receiver.[51]
July 10, 2016 to Present	Central Moscow, Russia	Denial-of-Service (False Coordinates)	**Yes**,[52] activity most prevalent near Kremlin.[53]
August 31 to September 3, 2016	Vladivostok, Russia	Denial-of-Service (False Coordinates)	**Likely**, Russian president arrived in area on August 31 for 2016 Eastern Economic Forum and departed on September 3. Spoofing activity localized to areas close to Forum.[54] [55]
c. September 2016 to Present	Olyva, Crimea	Denial-of-Service (False Coordinates)	**Yes**,[56] Government residences in Olyva transferred to FSO in 2014 and underwent significant security upgrades circa March 2018.[57]
September 15, 2016	Kerch, Crimea	Denial-of-Service (False Coordinates)	**Likely**, Russian president in Kerch to oversee progress on the construction of the Kerch Bridge. This is the first of two known instances of GNSS spoofing near Kerch.[58]
March 26 and March 29 to 30, 2017	Arkhangelsk, Russia	Denial-of-Service (False Coordinates)	**Likely**, Russian president arrived in area for Arctic Forum on March 29 and left on March 30. This is the first and only known case of GNSS spoofing in Arkhangelsk.[59] [60]
June 22 and 23, 2017	Gelendzhik, Russia	Denial-of-Service (False Coordinates)	**Likely**, Russian president aboard vessel in Novorossiysk bay to mark the symbolic launch of Turk Stream pipeline.[61]

GNSS Spoofing Event Date	Location (Approx.)	GNSS Spoofing Type	Prohibited or Sensitive Airspace Present
September 5 to 8, 2017	Vladivostok, Russia	Denial-of-Service (False Coordinates)	**Likely**, Russian president arrived in area on September 5 for 2017 Eastern Economic Forum and departed on September 8. Spoofing at remote Zvezda Shipyard detected within minutes of presidential speech at the location.[62] [63]
c. April 2018	Khmeimim Airbase, Syria	Denial-of-Service (Blank/ Invalid Navigation Signals)	**Yes**, Khmeimim Airbase was reportedly protected by Russian Pantsir-S1,[64] S-400,[65] and possibly Tor-M2U[66] anti-air systems as well as Krasukha-4[67] and likely other EW systems.
c. May 2018	Khmeimim Airbase, Syria	Denial-of-Service (Blank/ Invalid Navigation Signals)	**Yes**, See above.
May 15, 2018	Kerch, Crimea	Denial-of-Service (False Coordinates)	**Likely**, Russian president took part in unveiling of Kerch bridge during time of detected GNSS spoofing. This is the second of only two known instances of GNSS spoofing near Kerch.[68]
September 11, 2018	Vladivostok, Russia	Denial-of-Service (False Coordinates)	**Likely**, Russian president visit to remote Zvezda Shipyard coincided with nearby vessel reporting spoofed positioning information.[69]

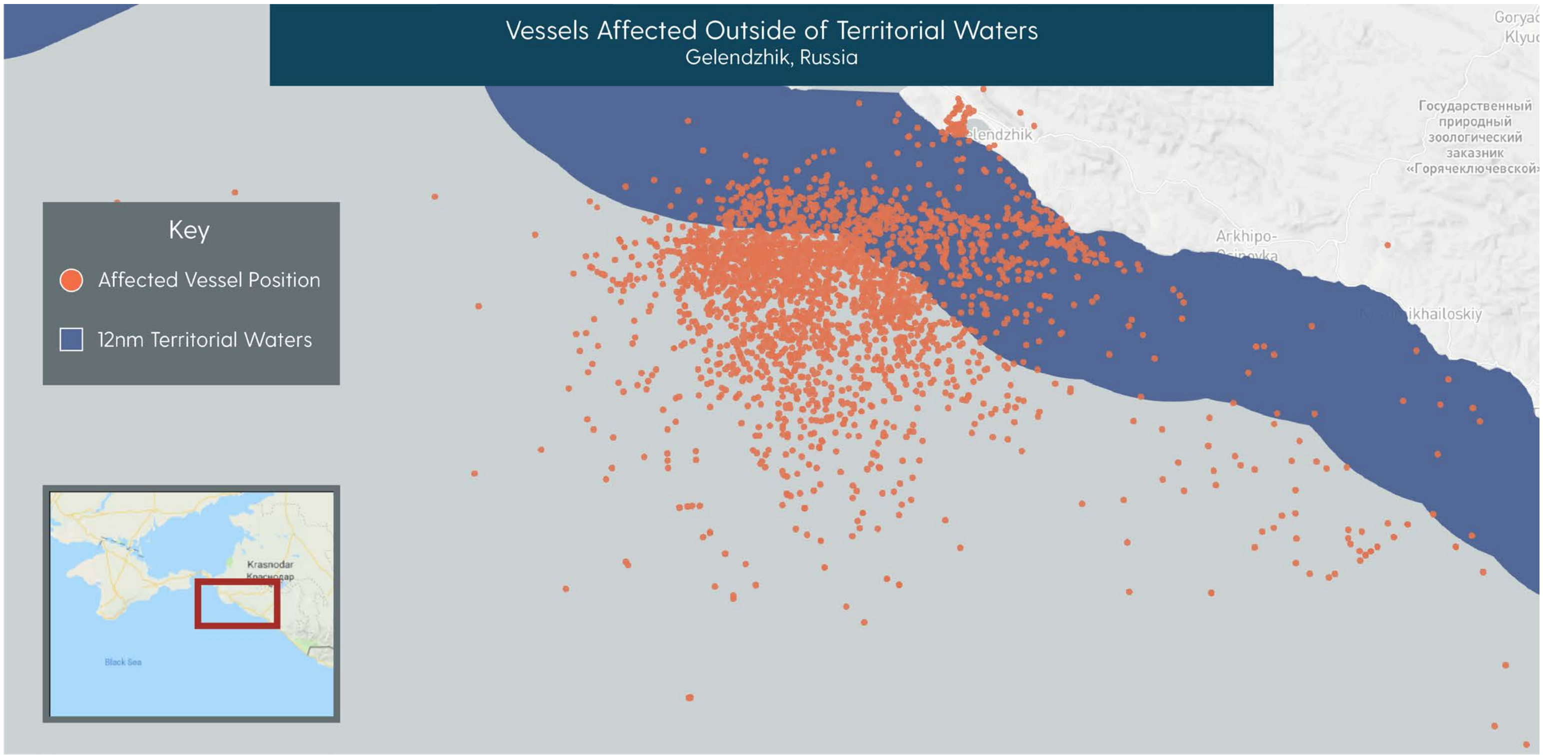
Trend III: Activity is Indiscriminate to Ownership and International Boundaries

Even though spoofing events appear to be localized to regions near sensitive and prohibited airspace, our research shows that these events are indiscriminate in nature and appear to affect vulnerable GNSS receivers in the vicinity regardless of vessel nationality. In fact, through an examination of the top vessel flags affected by these disruptions displayed in the chart below, we found that Russia-flagged ships were some of the most affected vessels across almost all locations.



*Approximate numbers based on March 2019 Vessel Ownership Data

While C4ADS did not find evidence confirming that GNSS spoofing at any of the ten locations is used to deliberately target specific receivers, it is clear that across all locations these disruptions may constitute a safety hazard for vessels and aircraft alike. We found that GPS spoofing signals originating from Khmeimim Airbase in Syria, for example, would be deafening for aircraft flying near the transmitter, subjecting them to spoofing signals 500 times stronger than authentic GPS signals.[70] Similarly, based on the geographic scope and nature of these GNSS spoofing events, at least some of these activities may be in contravention of the United Nation's International Telecommunications Union (ITU) Radio Regulations Articles, which prohibit harmful radio frequency interference.[iv] [71] C4ADS detected at least 7,910 instances where victim vessels located outside of Russian territorial waters fell victim to GNSS spoofing activity, potentially posing a risk to maritime navigational safety. A majority of these instances, for example, took place outside Russian territorial waters in the Black Sea, as seen in the image below.


Vessels Affected Outside of Territorial Waters
Gelendzhik, Russia
Key
● Affected Vessel Position
□ 12nm Territorial Waters
Gelendzhik
Arkhipo-Osipovka
Mikhailoskiy
Goryac Klyuc
Государственный природный зоологический заказник «Горячеключевской»
Krasnodar
Краснодар
Black Sea

These safety hazards are likely a spillover effect of actions taken in pursuit of Russian national security objectives. In the following case studies, we will explore three applications of GNSS spoofing and in each identify potential systems and basing locations.

[iv] According to Article 15 of the ITU's Radio Regulation Articles, of which the Russian Federation is a party, states agree to prohibit unrestricted signal transmissions that may interfere with safety systems.

- Section 1: All stations are forbidden to carry out unnecessary transmissions, or the transmission of superfluous signals, or the transmission of false or misleading signals, or the transmission of signals without identification (except as provided for in Article 19).
- Section 4: Special consideration shall be given to avoiding interference on distress and safety frequencies, those related to distress and safety identified in Article 31 and those related to safety and regularity of flight identified in Appendix 27.

PROTECTING VIPS

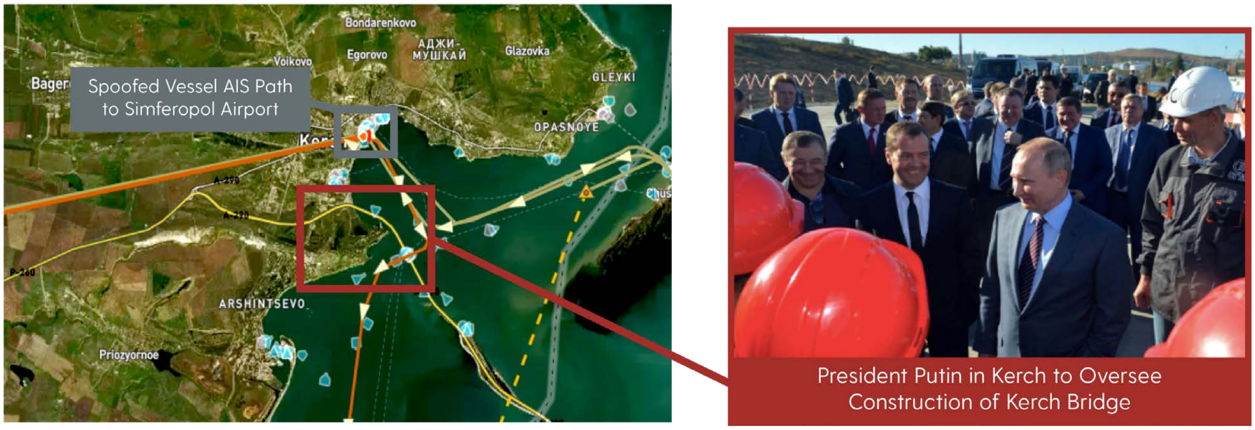
One of the clearest use cases for GNSS spoofing in the Russian Federation is for the protection of very important persons (VIP). C4ADS uncovered cases where GNSS spoofing in certain geographically isolated locations took place only in correlation with Russian leadership movements and FSO security activities. The purpose of this spoofing activity was likely to prevent unauthorized civilian drone activity as a VIP protection measure.[i] Because many of these activities took place over brief time periods in isolated locations, they support the working hypothesis that at least some of the devices used to conduct GNSS disruptions are mobile and can be temporarily deployed to create local areas of effect.

The Kerch Bridge Visit

The Kerch Bridge was built after the Russian annexation of Crimea to link the Crimean Peninsula to mainland Russia. The Kerch Strait, where the bridge is situated, has become a point of contention between Russia and Ukraine over the past several years, with Russia detaining three Ukrainian military vessels in November 2018 over accusations that the vessels had strayed into Russian territorial waters.[72] C4ADS identified GNSS spoofing activities in proximity to the Kerch Bridge on only two occasions – on September 15, 2016 and May 15, 2018. On both days, Russian President Vladimir Putin was present in the area to oversee the progress and completion of the Kerch Bridge. Vehicles suspected to belong to the Russian FSO could be seen following the Russian president during both events.

September 15, 2016

On September 15, 2016, the Russian President and Prime Minister made a single-day trip to Kerch to examine progress on the Kerch Bridge.[73] That same day, vessels moored at the nearby Kerch Port reported false positioning information at the Simferopol



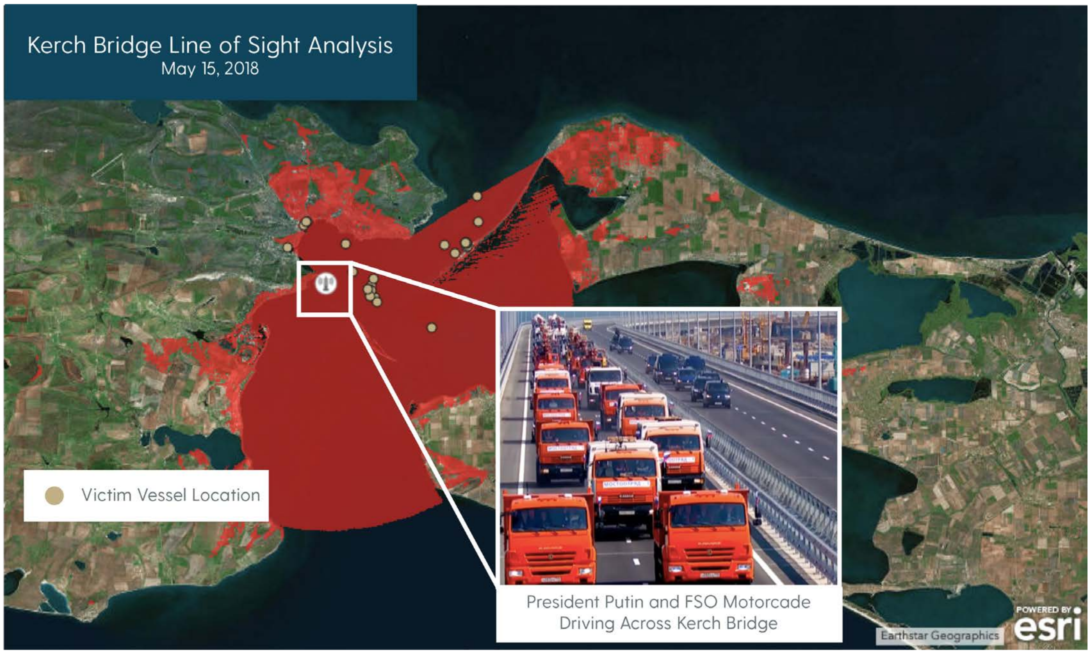
President Putin in Kerch to Oversee Construction of Kerch Bridge

[i] As previously mentioned, GNSS spoofing events detected in Russia are likely designed to deceive GNSS receivers on commercial drones to activate firmware-level geofence locks that prevent these drones from flying in restricted airspace such as an airport. If one of these commercial drones locks on to the spoofed signals, they would either return to what they perceive as 'non-restricted' airspace or disengage entirely before they reach the restricted airspace.

Airport nearly 200km away in Crimea. This event was the first GNSS spoofing event detected near Kerch, and the only one detected in 2016. According to official news releases posted on the Kremlin's website, the September 15 trip was the first and only official Presidential visit to Kerch in 2016.[74]

May 15, 2018

Less than two years later, President Putin returned to Kerch to take part in the official opening of the Kerch Bridge.[75] To celebrate the opening, Putin led a convoy of construction vehicles across the bridge from Russia to Crimea.[76] AIS records for vessels in the Kerch Strait at the time show that vessel passage through the straight was heavily restricted at the time of the event. It is during this time that at least 24 vessels anchored in waters in proximity to the bridge reported spoofed GNSS positioning information at the Anapa Airport more than 65km away. This was the only sustained spoofing disruption evidenced by AIS records in Kerch in 2018. Official news releases from the Kremlin indicate that the May 15 event was the only official Presidential visit to Kerch in 2018.[77]


Kerch Bridge Line of Sight Analysis
May 15, 2018
● Victim Vessel Location
President Putin and FSO Motorcade
Driving Across Kerch Bridge
Earthstar Geographics
POWERED BY esri

On the same day as the May 2018 GNSS disruptions, vehicles suspected to belong to the FSO drove alongside Putin's construction truck motorcade as it made its way across the Kerch Bridge. Using a line of sight analysis to estimate the potential range of a GNSS spoofing device, we can show that a spoofing transmitter based on one of the FSO vehicles at the Kerch bridge would likely be capable of targeting all vessels that reported spoofed location information on May 15, 2018.[ii]

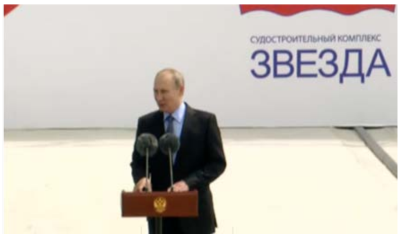
[ii] Due to the physical limitations of ultra-high frequency GNSS signals, spoofed signals would generally be unable to pass through physical obstructions such as mountains. To determine visibility from the Kerch bridge, C4ADS used ArcGIS to process a 3D terrain maps of the area surrounding the bridge and calculated what would be in view of a transmitter positioned on the bridge.

The Zvezda Shipyard Visit

The Zvezda Shipyard is located near the remote Russian Far East town of Bolshoy Kamen, 30km away from the port city of Vladivostok. For the past two years in early September, vessel GNSS receivers stationed at the shipyard have reported false location information at the Vladivostok International Airport. As in Crimea, these disruptions coincide directly with visits made by the Russian President to the shipyard, in this case for the Eastern Economic Forum hosted in Vladivostok in 2017 and 2018.

September 8, 2017

On his last day in Vladivostok for the 2017 Eastern Economic Forum, President Putin visited Bolshoy Kamen to inspect the newly constructed Zvezda Shipyard. The official Kremlin website reported the visit and the Russian President's speech at 1:30pm local time.[78] At approximately 1:24pm local time, the only vessel moored at the shipyard reported spoofed positioning information at the Vladivostok International Airport. This is the first and only detected instance of GNSS spoofing near Bolshoy Kamen in 2017.

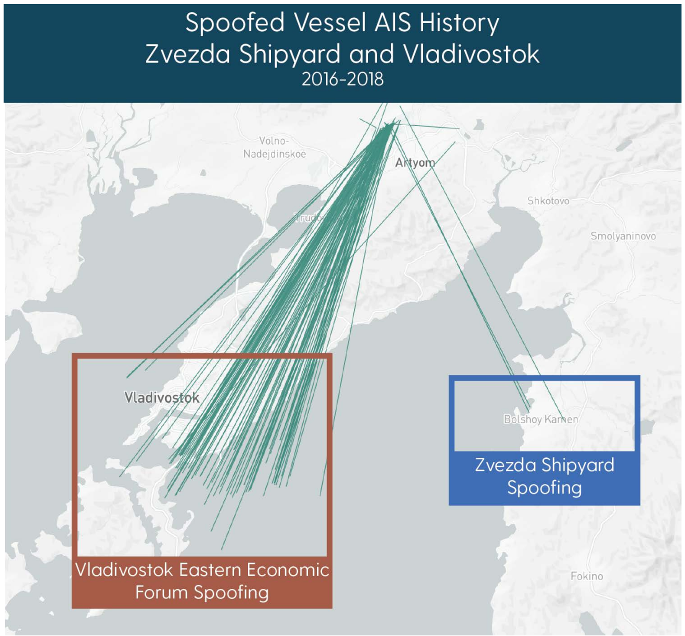


Putin's Speach at Zvezda Shipyard

September 11, 2018

Approximately one year after the first spoofing event detected at Zvezda Shipyard, Putin returned to the facility to oversee the implementation of the shipyard's production projects.[79] Once again, at least one vessel-based GNSS receiver located at the shipyard reported false positioning information at the Vladivostok Airport at the time of the president's afternoon visit.

The temporary and isolated nature of the GNSS spoofing detected near the Kerch Bridge and Zvezda Shipyard strongly suggests that the equipment used to create these disruptions could be based on a mobile platform, and that it is capable of creating localized zones of spoofing.

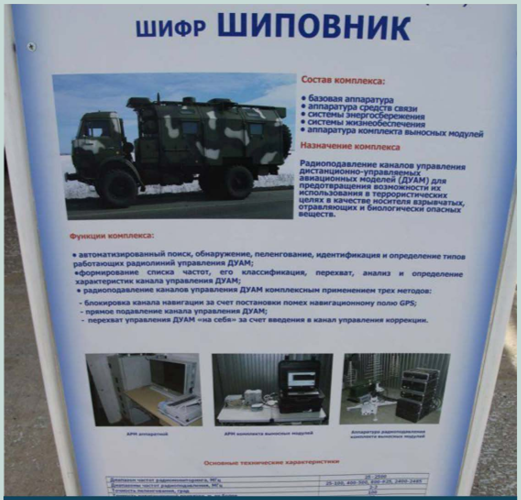

Spoofed Vessel AIS History
Zvezda Shipyard and Vladivostok
2016-2018

Potential Systems in Use (Mobile)

Based on the pattern of spoofing activity outlined above, it is reasonable to assume that the FSO likely possesses EW systems capable of producing the type of interference seen in our investigation. In 2016, an unnamed official who claimed to have direct knowledge of EW systems used by the FSO near the Kremlin told the Russian outlet Vedomosti that the FSO was likely using the “Shipovnik-Aero or some close analog to it.”[80] According to official documentation and the information sheet shown in the image on the right, the Shipovnik-Aero is a military-grade EW system based on a Kamaz vehicle frame that can be used to suppress unmanned aerial vehicle systems by creating a false navigation field, thereby forcing drones to land.[81] [82] However, a representative from the United Instrument-Making Corporation (UIMC), the company that produces the Shipovnik-Aero, denied that the system is in use by the special services at the Kremlin.[83] [84]

Based on our analysis of the use of GNSS spoofing for VIP protection, we believe that the GNSS spoofing device (or devices) used in Kerch and Vladivostok are likely mobile, able to be turned on and off to create local areas of effect, and are potentially operated by the FSO.

Using these specifications and the leads generated by Vedomosti in 2016 as guidance, C4ADS examined over a thousand contracts in the official Russian government contracts registry in search of equipment purchases potentially related to GNSS spoofing infrastructure.[85] In line with UIMC’s official stance that it did not supply Shipovnik-Aero systems to the FSO, C4ADS did not find any public contracts between UIMC and the FSO.



шифр ШИПОВНИК

Состав комплекса:

- базовая аппаратура
- аппаратура средств связи
- системы энергосбережения
- системы жизнеобеспечения
- аппаратура комплекта выносных модулей

Назначение комплекса

Радиоподавление каналов управления дистанционно-управляемых авиационных моделей (ДУАМ) для предотвращения возможности их использования в террористических целях в качестве носителя взрывчатых, отравляющих и биологически опасных веществ.

Функции комплекса:

- автоматизированный поиск, обнаружение, пеленгование, идентификация и определение типов работающих радиолиний управления ДУАМ;
- формирование списка частот, его классификация, перехват, анализ и определение характеристик канала управления ДУАМ;
- радиоподавление каналов управления ДУАМ комплексным применением трех методов:
  - блокировка канала навигации за счет постановки помех навигационному полю GPS;
  - прямое подавление канала управления ДУАМ;
  - перехват управления ДУАМ «на себя» за счет введения в канал управления коррекции.

АРМ аппаратный
АРМ комплекта выносных модулей
Аппаратура радиоподавления комплекта выносных модулей

Основные технические характеристики

Диапазон частот радиомониторинга, МГц	25–2500
Диапазоны частот радиоподавления, МГц	25-100, 400-500, 800-925, 2400-2485
Точность пеленгования, град	2-3
[illegible]	100

Shipovnik-Aero Information Sheet

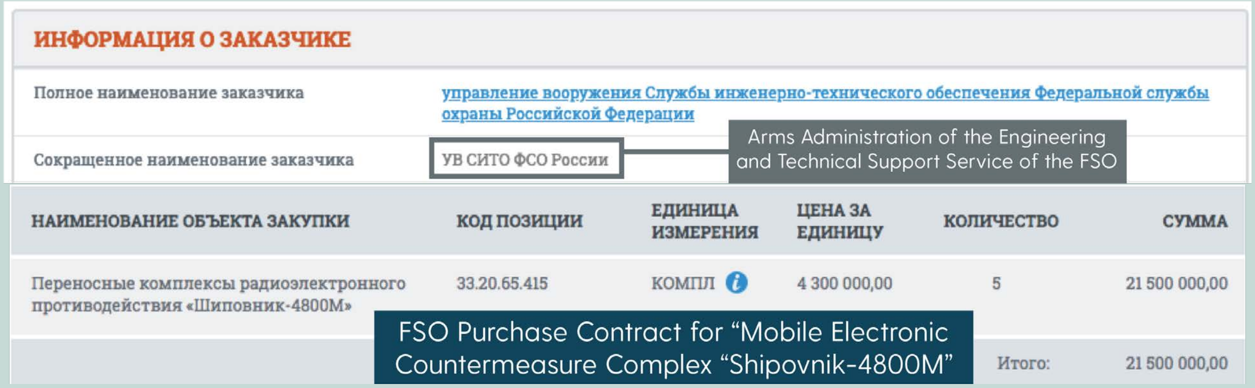
However, C4ADS did locate numerous FSO procurement contracts and repair agreements for several mobile electronic countermeasure systems, including the “Shipovnik-4800M” and the “Shipovnik-M.” These systems are produced not by UIMC, but rather by a joint stock company based in the town of Vladimir named JSC Design Skilled Office of Radio Equipment (JSC KOBRA).[86] [87]

According to a June 2009 issue of Mayak, a trade publication, JSC KOBRA was at one time the sole supplier of equipment used for radio-control and monitoring near the Kremlin and the Russian White House.[88] In its online catalogue, JSC KOBRA offers several electronic countermeasure systems, including ones designed to neutralize commercial drones by counteracting the communication channels of GLONASS, GPS, GALILEO, and COMPASS.[89]

No references to either the Shipovnik-4800M or the Shipovnik-M could be found in public media sources or on JSC KOBRA’s website. The 2009 issue of Mayak references both the Shipovnik-95 and the Shipovnik-98 as systems supplied to the FSO by JSC

KOBRA for radio signal suppression.[90] The article also claimed that the FSO has deployed the Shipovnik-95 on Russian presidential escort vehicles.[91] [92]

Official government records, shown below, indicate that in August 2014 the Arms Administration of the Engineering and Technical Support Service of the FSO with a listed address at the Kremlin purchased five Shipovnik-4800M portable electronic countermeasure complexes for about $120,400 each.[93] [94] [95]



ИНФОРМАЦИЯ О ЗАКАЗЧИКЕ

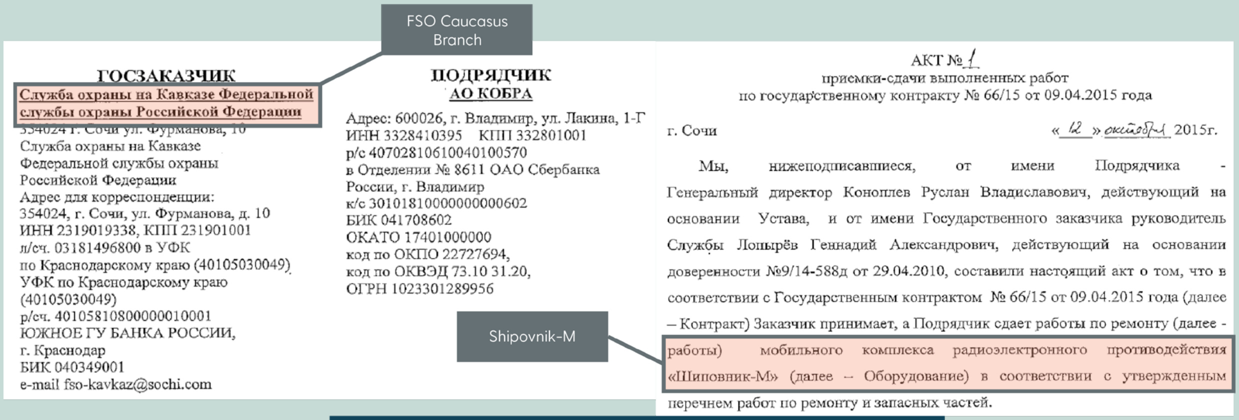
Полное наименование заказчика	управление вооружения Службы инженерно-технического обеспечения Федеральной службы охраны Российской Федерации
Сокращенное наименование заказчика	УВ СИТО ФСО России

Arms Administration of the Engineering and Technical Support Service of the FSO

НАИМЕНОВАНИЕ ОБЪЕКТА ЗАКУПКИ	КОД ПОЗИЦИИ	ЕДИНИЦА ИЗМЕРЕНИЯ	ЦЕНА ЗА ЕДИНИЦУ	КОЛИЧЕСТВО	СУММА
Переносные комплексы радиоэлектронного противодействия «Шиповник-4800М»	33.20.65.415	КОМПЛ	4 300 000,00	5	21 500 000,00
				Итого:	21 500 000,00

FSO Purchase Contract for "Mobile Electronic Countermeasure Complex "Shipovnik-4800M"

In October 2015, the Caucasus branch of the FSO, based in Sochi and responsible for security activities at government residences on the Black Sea coast, finalized a contract with JSC KOBRA for the repair of a "mobile radio-electronic countermeasure complex" named the Shipovnik-M.[96]



FSO Caucasus Branch

ГОСЗАКАЗЧИК
Служба охраны на Кавказе Федеральной службы охраны Российской Федерации
354024 г. Сочи ул. Фурманова, 10
Служба охраны на Кавказе
Федеральной службы охраны
Российской Федерации
Адрес для корреспонденции:
354024, г. Сочи, ул. Фурманова, д. 10
ИНН 2319019338, КПП 231901001
л/сч. 03181496800 в УФК
по Краснодарскому краю (40105030049)
УФК по Краснодарскому краю
(40105030049)
р/сч. 40105810800000010001
ЮЖНОЕ ГУ БАНКА РОССИИ,
г. Краснодар
БИК 040349001
e-mail fso-kavkaz@sochi.com

ПОДРЯДЧИК
АО КОБРА
Адрес: 600026, г. Владимир, ул. Лакина, 1-Г
ИНН 3328410395 КПП 332801001
р/с 40702810610040100570
в Отделении № 8611 ОАО Сбербанка
России, г. Владимир
к/с 30101810000000000602
БИК 041708602
ОКАТО 17401000000
код по ОКПО 22727694,
код по ОКВЭД 73.10 31.20,
ОГРН 1023301289956

Shipovnik-M

АКТ № 1
приемки-сдачи выполненных работ
по государственному контракту № 66/15 от 09.04.2015 года

г. Сочи «12» октября 2015г.

Мы, нижеподписавшиеся, от имени Подрядчика - Генеральный директор Коноплев Руслан Владиславович, действующий на основании Устава, и от имени Государственного заказчика руководитель Службы Лопырёв Геннадий Александрович, действующий на основании доверенности №9/14-588д от 29.04.2010, составили настоящий акт о том, что в соответствии с Государственным контрактом № 66/15 от 09.04.2015 года (далее – Контракт) Заказчик принимает, а Подрядчик сдает работы по ремонту (далее - работы) мобильного комплекса радиоэлектронного противодействия «Шиповник-М» (далее – Оборудование) в соответствии с утвержденным перечнем работ по ремонту и запасных частей.

Repair Agreement for Shipovnik-M Mobile Electronic Countermeasure Complex
Dated October 12, 2015

The specifications and potential capabilities of both the Shipovnik-4800M and Shipovnik-M could not be identified through official records. Records from the Russian Federal Accreditation Service, responsible for issuing regulatory certifications for equipment, describe the Shipovnik-4800M as "portable electronic countermeasure equipment" that is able to operate on battery power.[97] [98]

The FSO procured several mobile EW devices for its branches in Moscow and Sochi, which appear to belong to a family of systems used for presidential motorcade protection. While we cannot say for certain that these mobile systems are behind the isolated spoofing activity detected near the Russian president, learning more about them gives us a better understanding of potential systems in play.

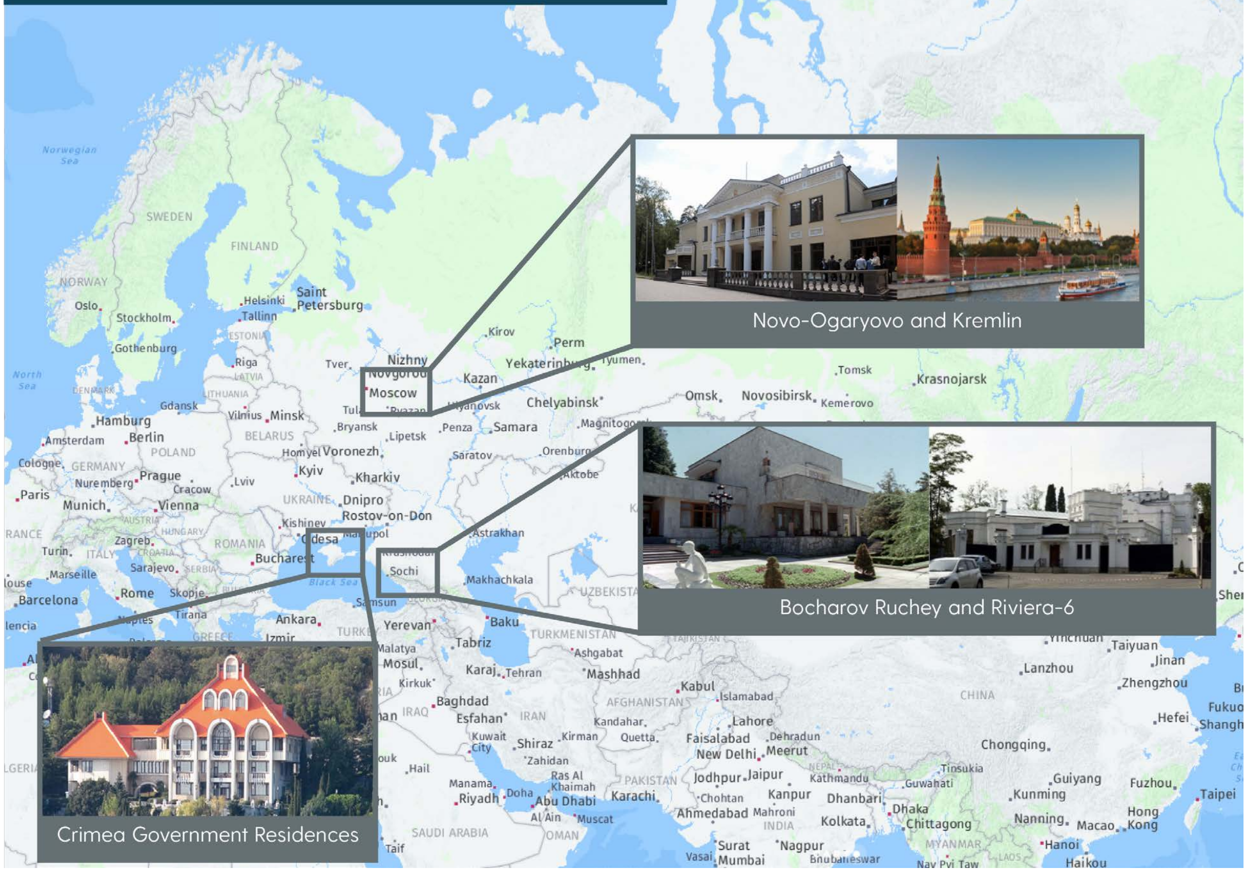
DEFENDING STRATEGIC FACILITIES

In addition to the protection of Russian leaders, C4ADS found evidence that GNSS spoofing is used to protect strategic Russian government residences and other highly-sensitive facilities near the Black Sea and in Moscow. Unlike the spoofing activity associated with VIP visits to remote locations, the activity seen in the vicinity of static government facilities is more frequent, affects a greater number of vessels, and appears to interfere with receivers over a greater distance.

Official Russian Government Facilities

C4ADS observed patterns of GNSS spoofing around official Russian buildings in both Moscow and on the Russian Black Sea coast. In Sochi and Olyva, GNSS spoofing interfered with vessel navigation systems off the coast of official government residences owned and operated by the FSO. Similarly, potential spoofing activity occurred near the Kremlin and the Presidential Residence in Moscow. These facilities are publicly acknowledged as belonging to the Russian government and are afforded special airspace protections reserved for strategic government and military facilities. In all cases, GNSS spoofing disruptions beginning in 2016 forced victim receivers to report positions at local civilian airports. These events have continued to affect receivers as of the time of this report's publication.

GNSS Spoofing Near Russian Government Facilities



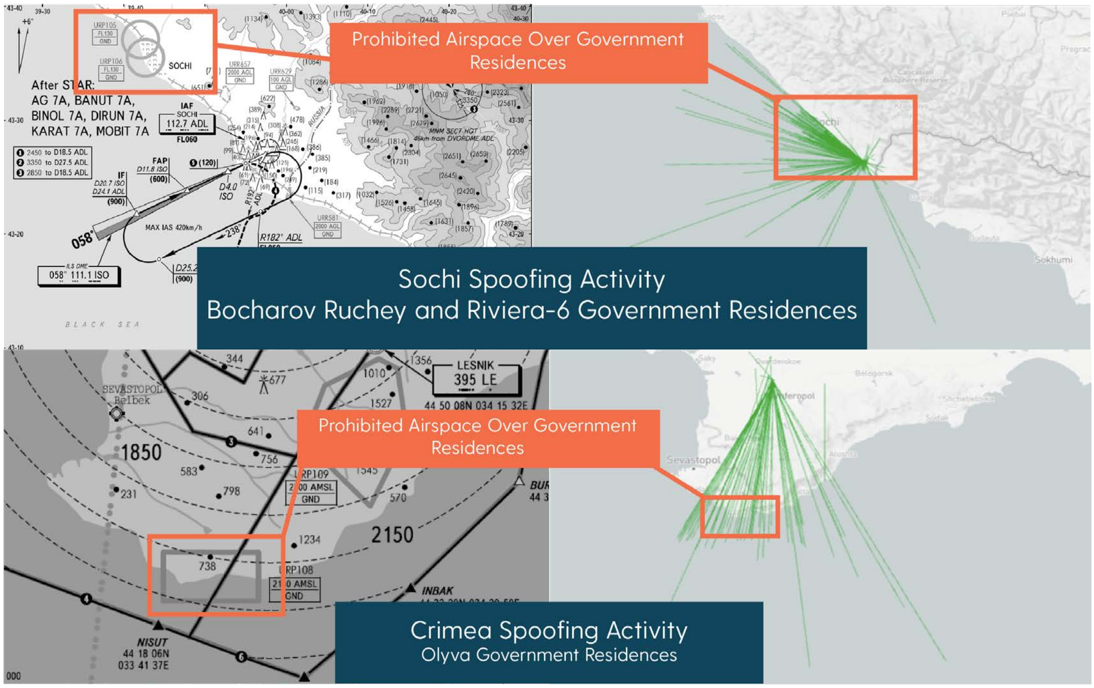
Novo-Ogaryovo and Kremlin

Bocharov Ruchey and Riviera-6

Crimea Government Residences

Black Sea Residences

Aeronavigation charts dated July 2017 and August 2018 from the Russian Center of Aeronavigation Information show that the airspaces above two facilities in Sochi and a large swath of the southern coast of Crimea near Olyva are classified as prohibited.[99] [100] Prohibited is the strictest classification for airspace in the Russian Federation and is typically used for airspace over highly sensitive government and military installations.[101] In Sochi, the Russian presidential and prime ministerial residences of Bocharov Ruchey and Riviera-6, respectively, are located in the center of two prohibited airspaces. Similarly, the prohibited airspace along the southern coast of Crimea is situated above a string of coastal residences that are now occupied by the Russian government.[102]

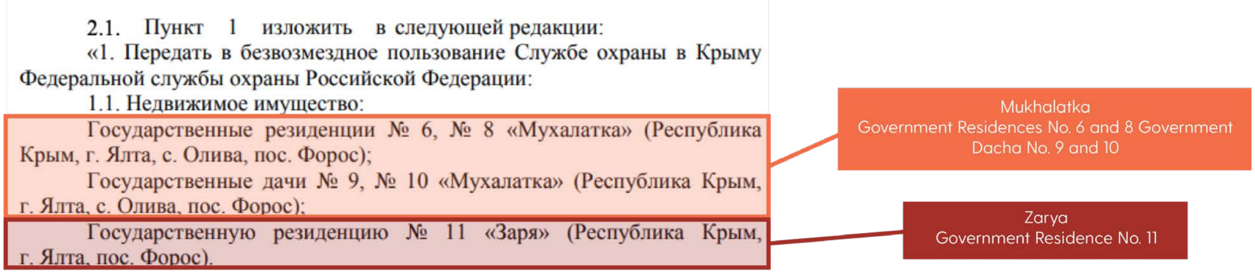

Prohibited Airspace Over Government Residences

Sochi Spoofing Activity
Bocharov Ruchey and Riviera-6 Government Residences

Prohibited Airspace Over Government Residences

Crimea Spoofing Activity
Olyva Government Residences

The Bocharov Ruchey and Riviera-6 residences in Sochi are widely reported to be overseen by the Caucasus branch of the FSO, which is responsible for the protection of all government residences in the south of the country.[103] [104] Similarly, in December 2016, following the Russian annexation of the Crimean Peninsula, Crimean authorities transferred control of five government residences located in Foros and Olyva to the Crimean branch of the Russian FSO.[105]


2.1. Пункт 1 изложить в следующей редакции:

«1. Передать в безвозмездное пользование Службе охраны в Крыму Федеральной службы охраны Российской Федерации:

1.1. Недвижимое имущество:

Государственные резиденции № 6, № 8 «Мухалатка» (Республика Крым, г. Ялта, с. Олива, пос. Форос);

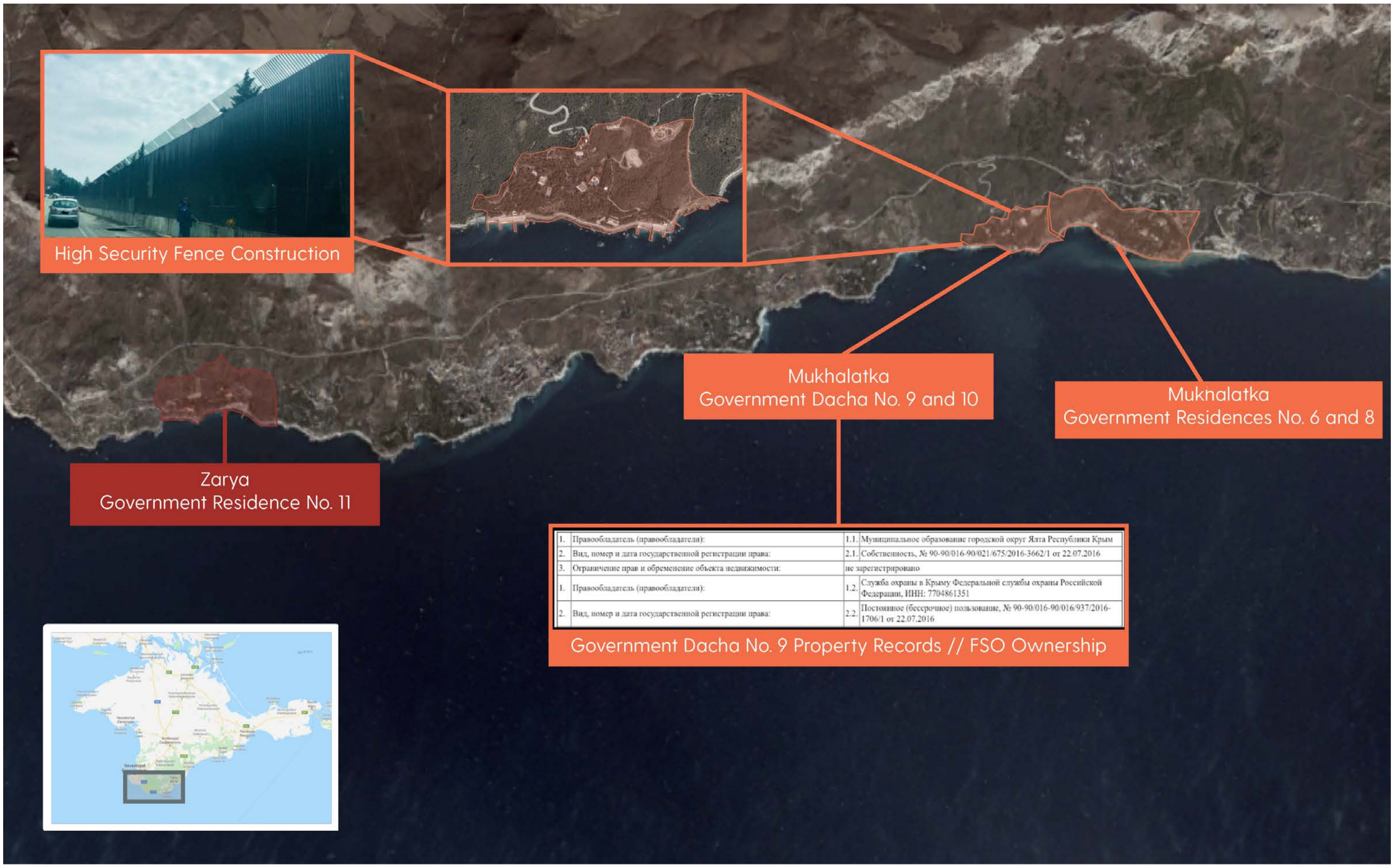
Государственные дачи № 9, № 10 «Мухалатка» (Республика Крым, г. Ялта, с. Олива, пос. Форос);

Государственную резиденцию № 11 «Заря» (Республика Крым, г. Ялта, пос. Форос).

Mukhalatka
Government Residences No. 6 and 8 Government Dacha No. 9 and 10

Zarya
Government Residence No. 11

December 2016 Transfer Agreement


High Security Fence Construction
Mukhalatka
Government Dacha No. 9 and 10
Muknalatka
Government Residences No. 6 and 8
Zarya
Government Residence No. 11

1.	Правообладатель (правообладатели):	1.1.	Муниципальное образование городской округ Ялта Республики Крым
2.	Вид, номер и дата государственной регистрации права:	2.1.	Собственность, № 90-90/016-90/021/675/2016-3662/1 от 22.07.2016
3.	Ограничение прав и обременение объекта недвижимости:	не зарегистрировано	
1.	Правообладатель (правообладатели):	1.2.	Служба охраны в Крыму Федеральной службы охраны Российской Федерации, ИНН: 7704861351
2.	Вид, номер и дата государственной регистрации права:	2.2.	Постоянное (бессрочное) пользование, № 90-90/016-90/016/937/2016-1706/1 от 22.07.2016

Government Dacha No. 9 Property Records // FSO Ownership

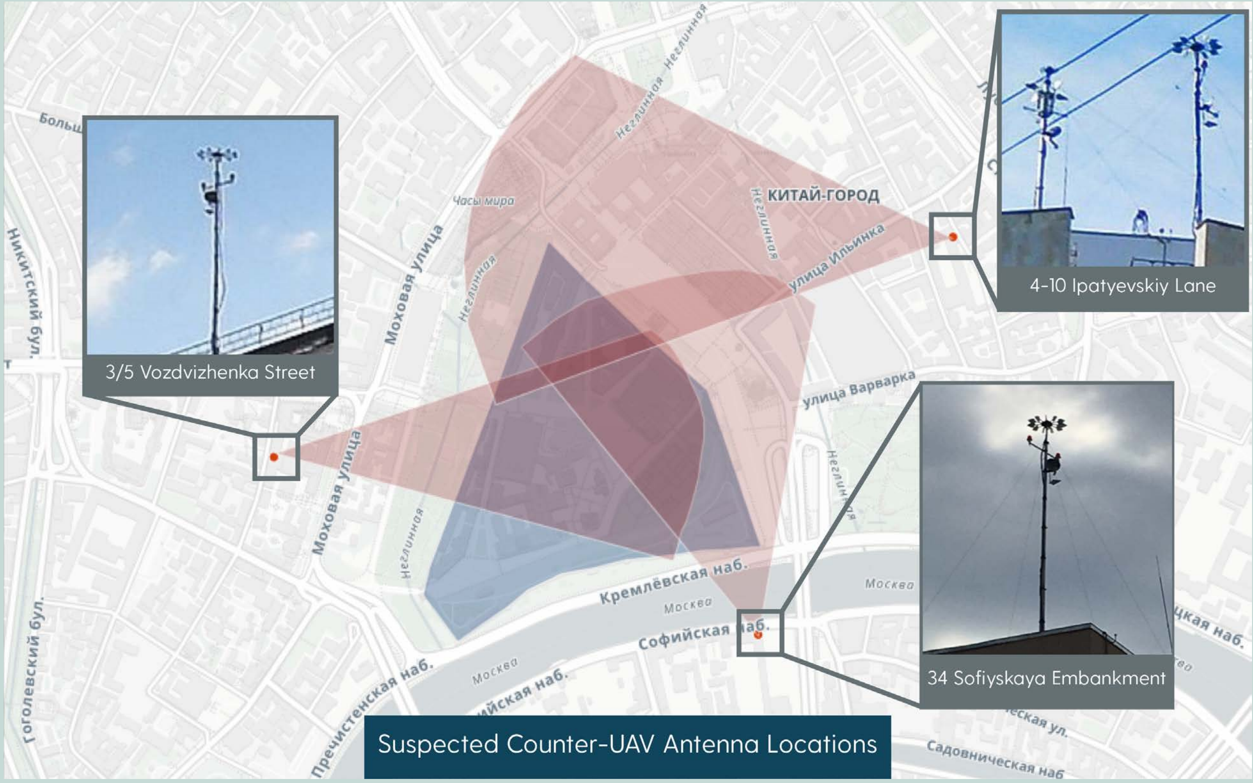
According to Crimean news and social media reports, significant FSO security activities began at the government dachas and residences around March 2016, several months before the first detection of GNSS spoofing in the region.[106] In addition to FSO checkpoints and brick walls now surrounding the complexes, images of large security fences bordering the highway to the north have emerged on social media accounts.[107] [108]

Potential Systems in Use (Stationary)

Due to heightened security around the Black Sea dachas and residences, C4ADS was unable to collect data on the systems potentially in use at these facilities. However, the area around the Kremlin in central Moscow is more prone to analysis using public data. Already, Russian researchers have recorded possible spoofing activity near the Kremlin. In October 2016, a researcher driving around central Moscow on a Segway reportedly used a collection of receivers to detect GPS and GLONASS interference signals near the Kremlin.[109] Similarly, in September 2017, a researcher searching for the source of Moscow's GPS spoofing found that the spoofed signals likely originate from a position outside, rather than inside, the Kremlin.[110]

Suspected Kremlin Counter-Drone Systems

Based on leads generated by Russian journalists and hobbyists searching for the source of Moscow's GNSS spoofing,[111] [112] C4ADS identified possible GNSS spoofing equipment based on at least three buildings in central Moscow. All three buildings host what appear to be identical antennas and transmission equipment on their rooftops. According to publicly available imagery, the antennas appear to face the Kremlin. Two of the buildings are openly owned by the Russian government, the third inexplicably lacks official ownership information in local property records.[113] The equipment at all three locations first appeared between June 2015 and September 2016 on street mapping websites, or within the time frame that GNSS spoofing activity was first reported near the Kremlin.[114]



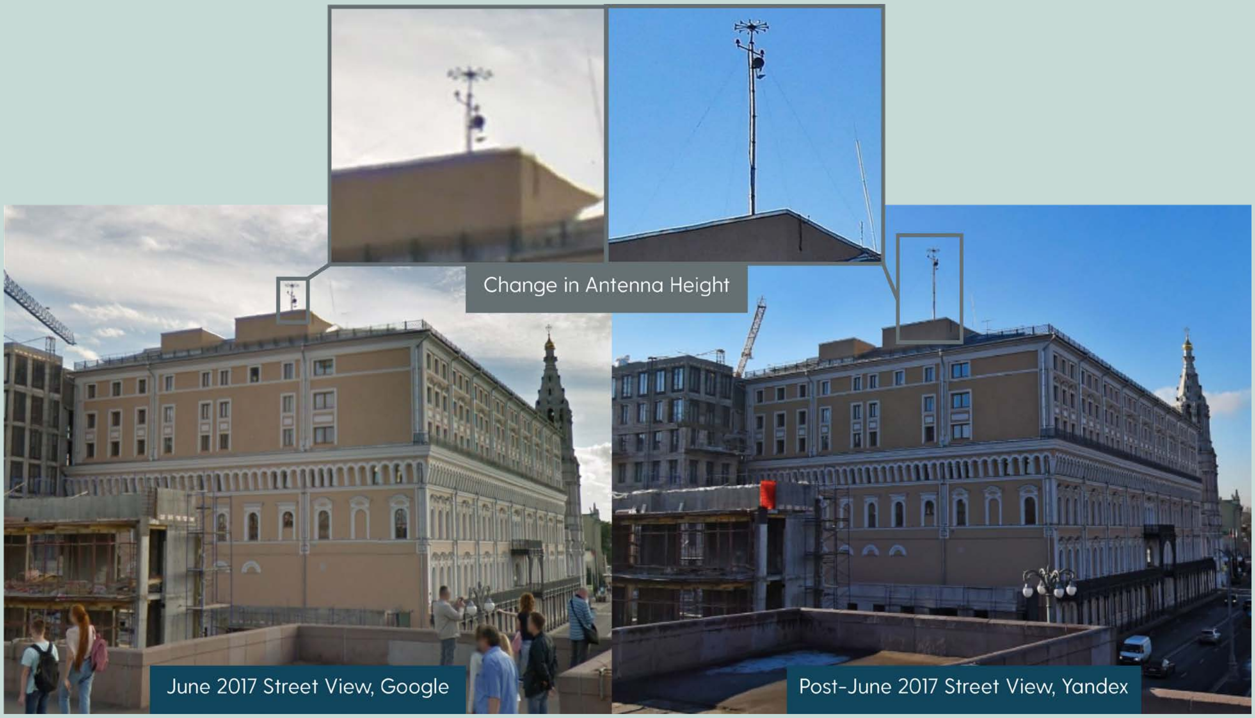
Suspected Counter-UAV Antenna Locations

Based on a review of the images of the equipment by individuals with electronic warfare experience and familiarity with electronic warfare systems, the equipment located at all three locations appears to include an 11-element direction-finding antenna array likely able to operate on ultra-high frequency (UHF) bands.[115] This would include the GPS L1, L2, and L5 bands, as well as bands used by many civilian drone controllers.[116] [117] It is also possible that the direction-finding antennas are designed to geolocate civilian drone control systems operating at locations close to the Kremlin. Alternatively, the direction-finding antennas could be used to direct GNSS spoofing signals in a desired direction. The equipment may also include a small cylindrical microwave antenna, which could potentially be used to create a cone of GNSS spoofing or jamming signals in the direction it is facing.[118] [119]

The antennas facing the Kremlin appear to be undergoing upgrades. On one of the buildings, the eastern side of the rooftop at 34 Sofiyskaya Embankment, a direction-finding antenna array can be seen. Sometime between June and December 2017, it appears that the mast used for the array increased in height.[120] This height increase may have been an effort to enhance the effectiveness of the direction-finding antenna array in locating the source of ground-based signal transmissions, such as those used by civilian drone controllers.

Potential Spoofing Method in Use?

Reports from one Moscow-based journalist who claimed to have recorded the spoofed signals indicate that the spoofing transmitter(s) in Moscow conduct GPS jamming on the L2 and L5 bands in order to force receivers onto GPS L1, which is subsequently spoofed. This effective method of spoofing is well-known among navigation warfare experts. (Source: http://addmeto.cc/828.html)

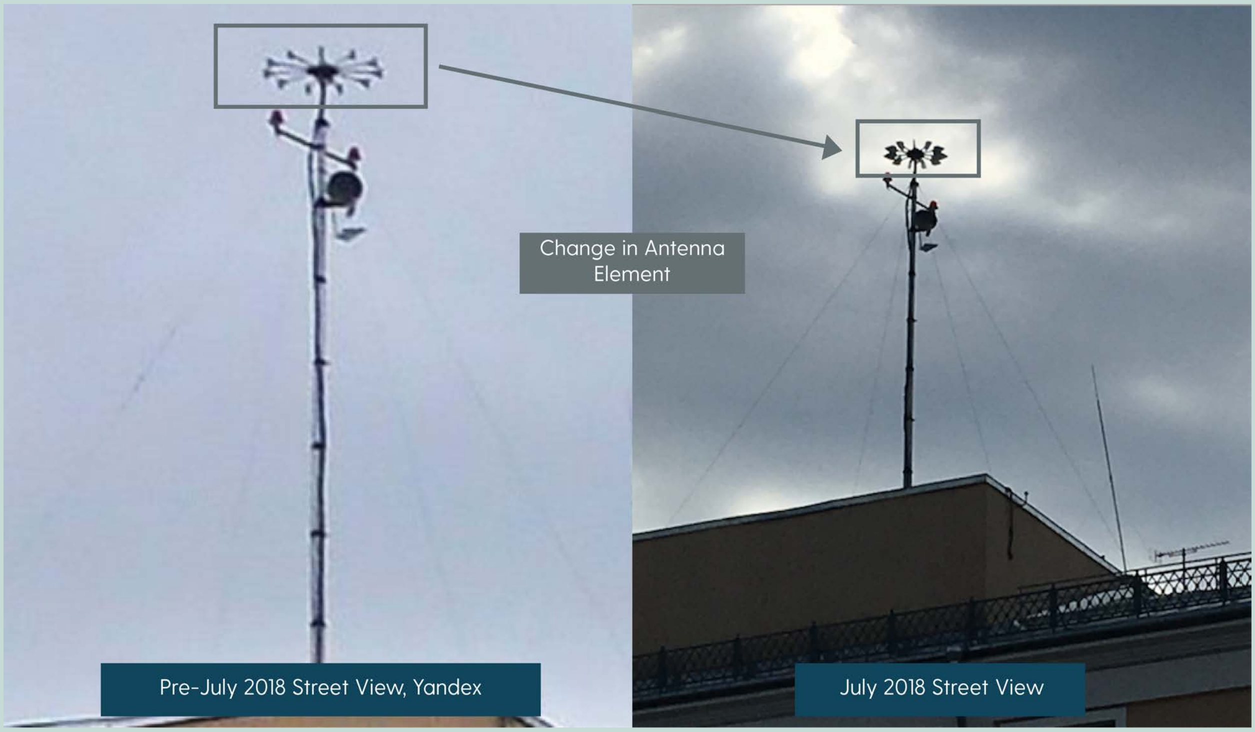


Change in Antenna Height

June 2017 Street View, Google

Post-June 2017 Street View, Yandex

In June 2018, photographs of the direction-finding antennas showed additional changes implemented sometime between January and June 2018. These changes appear to include a switch from a standard dipole element to a more broadband-type antenna such as a Vivaldi element, which would allow for a wider range of frequencies to be potentially monitored and located.[i] [121]



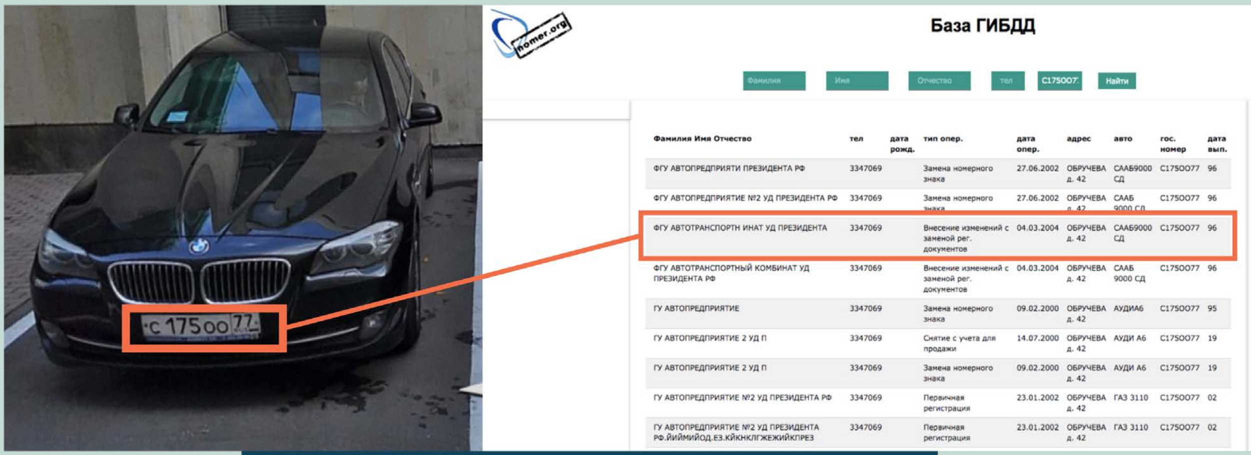
Unidentified Building with Counter Drone Equipment

Of the three buildings that C4ADS identified in Moscow hosting possible counter-drone systems, at least two are directly associated with the Russian Government, as evidenced in official Russian property records from August 2018.[122] The third, located at D 4-10 Ipatyevskiy Lane, Building 1, has no associated ownership information listed in official government databases. However, this building hosts an antenna array that appears identical to the equipment seen at the government-owned facilities elsewhere in Moscow. Based on a review of publicly available imagery on sites such as Yandex and Google Street View, the equipment appears to have been deployed sometime between 2015 and September 2016. Like the other two buildings, the equipment at Ipatyevskiy Lane faces the Kremlin.

Official documentation from the Russian Land Registry for D 4-10 Ipatyevskiy Lane, Building 1, indicates that the ownership information has either been censored, removed, or never recorded in the official registry, although the available records show that the property was assigned a cadastral number on May 22, 2012.[123] While property records do not provide ownership information for the complex, street view imagery from 2013,

[i] At this time, updated 2018 Yandex Street view imagery of the direction-finding antenna positioned at 4-10 Ipatyevskiy Lane suggests that these upgraded antennas are now in use at multiple identified locations.

before the road was shut to the public, shows at least 10 vehicles with serialized license plate numbers ending in OO77 parked outside the building.[124] [125] According to several publicly available Russian DMV databases reviewed by C4ADS, this serialization pattern has been previously associated with vehicles belonging to the Office of the President of the Russian Federation.[126]



База ГИБДД

Фамилия Имя Отчество	тел	дата рожд.	тип опер.	дата опер.	адрес	авто	гос. номер	дата вып.
ФГУ АВТОПРЕДПРИЯТИ ПРЕЗИДЕНТА РФ	3347069		Замена номерного знака	27.06.2002	ОБРУЧЕВА д. 42	СААБ9000 СД	С175ОО77	96
ФГУ АВТОПРЕДПРИЯТИЕ №2 УД ПРЕЗИДЕНТА РФ	3347069		Замена номерного знака	27.06.2002	ОБРУЧЕВА д. 42	СААБ 9000 СД	С175ОО77	96
ФГУ АВТОТРАНСПОРТН ИНАТ УД ПРЕЗИДЕНТА	3347069		Внесение изменений с заменой рег. документов	04.03.2004	ОБРУЧЕВА д. 42	СААБ9000 СД	С175ОО77	96
ФГУ АВТОТРАНСПОРТНЫЙ КОМБИНАТ УД ПРЕЗИДЕНТА РФ	3347069		Внесение изменений с заменой рег. документов	04.03.2004	ОБРУЧЕВА д. 42	СААБ 9000 СД	С175ОО77	96
ГУ АВТОПРЕДПРИЯТИЕ	3347069		Замена номерного знака	09.02.2000	ОБРУЧЕВА д. 42	АУДИА6	С175ОО77	95
ГУ АВТОПРЕДПРИЯТИЕ 2 УД П	3347069		Снятие с учета для продажи	14.07.2000	ОБРУЧЕВА д. 42	АУДИ А6	С175ОО77	19
ГУ АВТОПРЕДПРИЯТИЕ 2 УД П	3347069		Замена номерного знака	09.02.2000	ОБРУЧЕВА д. 42	АУДИ А6	С175ОО77	19
ГУ АВТОПРЕДПРИЯТИЕ №2 УД ПРЕЗИДЕНТА РФ	3347069		Первичная регистрация	23.01.2002	ОБРУЧЕВА д. 42	ГАЗ 3110	С175ОО77	02
ГУ АВТОПРЕДПРИЯТИЕ №2 УД ПРЕЗИДЕНТА РФ.ЙИЙМИЙОД.ЕЗ.КЙКНКЛГЖЕЖИЙКПРЕЗ	3347069		Первичная регистрация	23.01.2002	ОБРУЧЕВА д. 42	ГАЗ 3110	С175ОО77	02

Vehicle Historically Registered to Office of the President

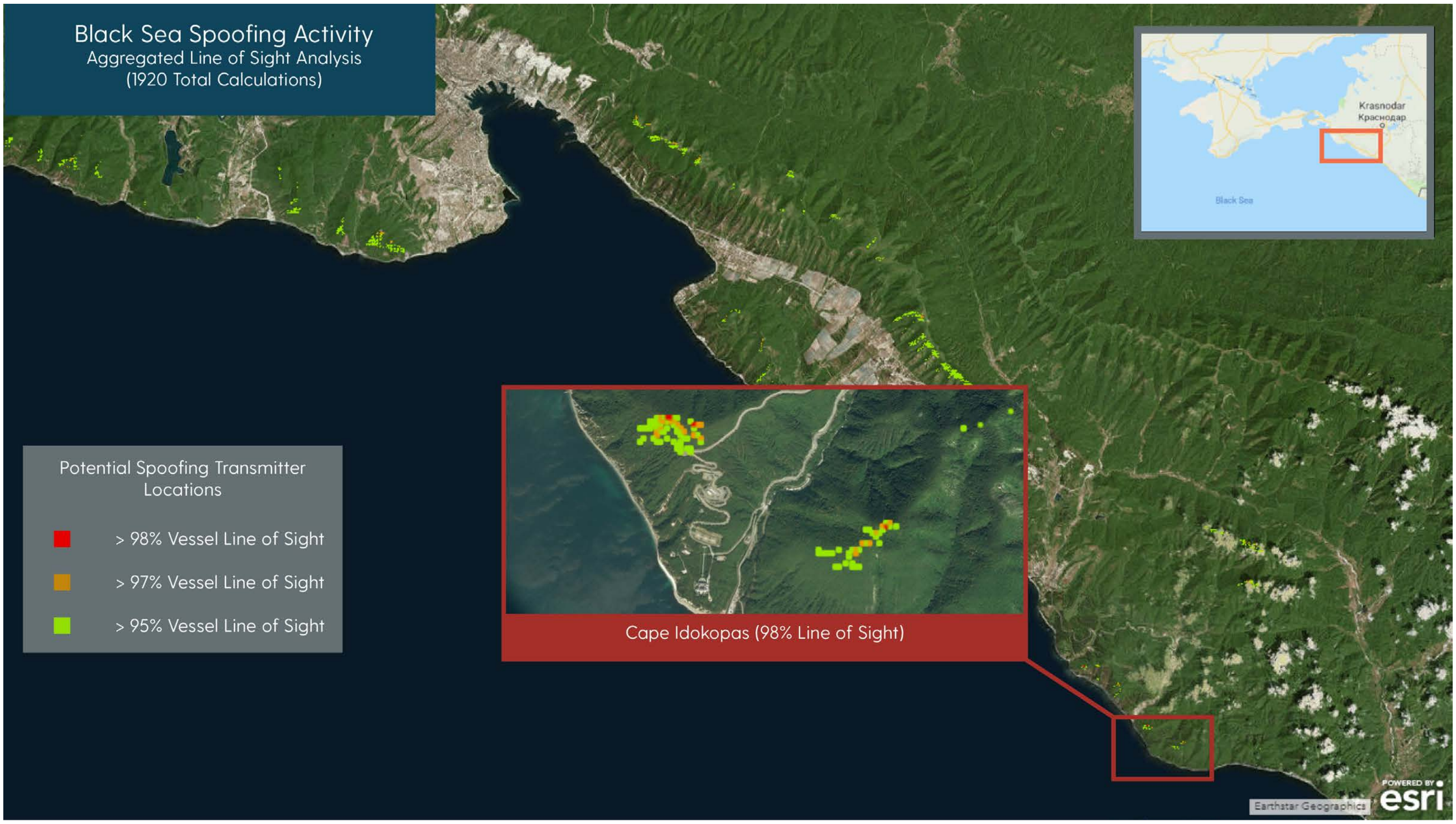
Unofficial Government Facilities

In contrast to areas where an official government presence made the placement of a GNSS spoofing device a logical protective measure, spoofing activity off the coast off Gelendzhik did not appear to have an obvious explanation. The coast near Gelendzhik does not have any declared government residences. Despite this, spoofing events off the Gelendzhik coast were the most frequent in our sample. We wanted to find the likely source of this activity, and so we turned to local media reports and an abundance of spoofed vessel position data to narrow our search.

Gelendzhik is frequented by security service officials, which is in line with popular but unconfirmed reports that President Vladimir Putin maintains a private residence in the outskirts of the town.[127] [128] [129] Following an examination of several hypotheses, we believe that the GNSS spoofing system in use near Gelendzhik is land-based.[130] Given the frequent nature of GNSS spoofing activity near Gelendzhik and its wide-reaching effects on vessels in the area, we posited that the device has access to a reliable and sustained source of electricity.

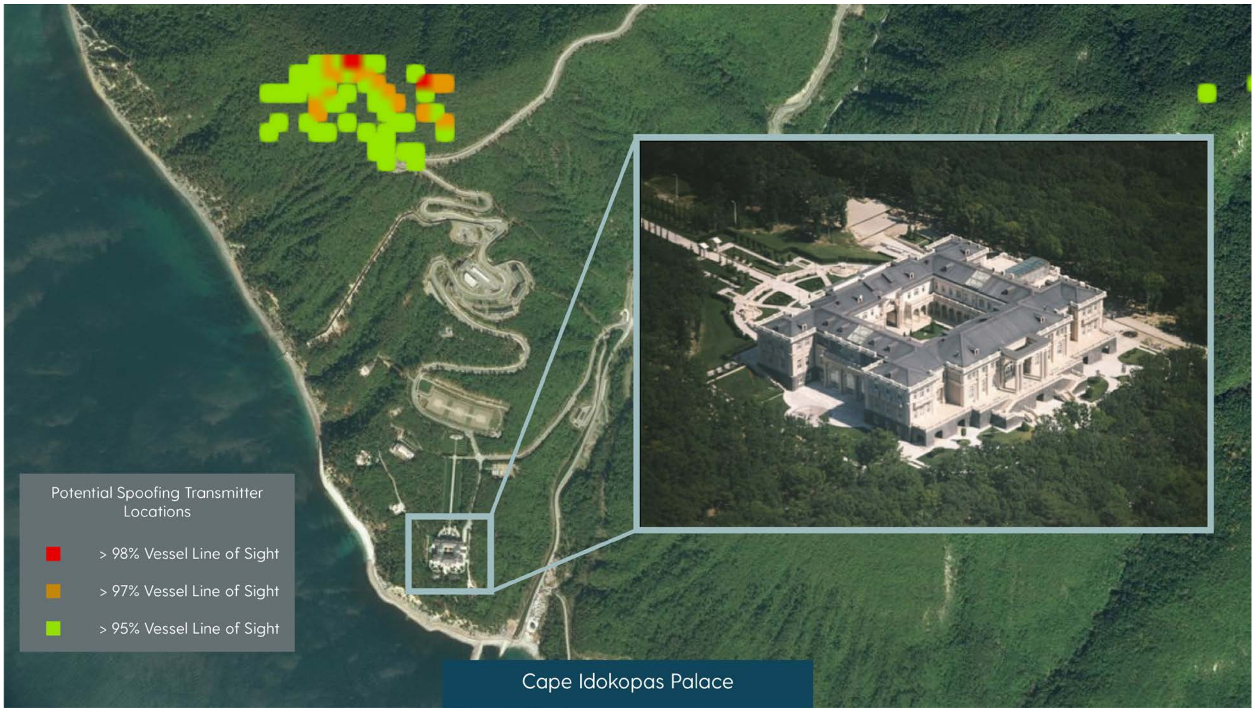
Aggregated Line of Sight Analysis

To trace back to high-probability basing locations for spoofing devices in use near Gelendzhik, C4ADS conducted an aggregated line of sight analysis. Due to the physical limitations of ultra-high frequency GNSS signals, spoofed signals would generally be unable to pass through physical obstructions such as mountains.[131] To determine visibility from a given location, C4ADS used ArcGIS to process 3D terrain maps of the area around Gelendzhik. Using AIS positioning data from 1,920 spoofing instances, we calculated the areas along the coastline that would be able to “see” all or nearly all of the vessels in our dataset. Based on these line of sight calculations for affected vessel receiver positions, we were able to narrow down potential basing areas to just a few land-based locations. The results indicated that only one facility located at Cape Idokopas appeared to have line of sight with more than 98% of the affected vessel-based receivers.


Black Sea Spoofing Activity
Aggregated Line of Sight Analysis
(1920 Total Calculations)
Potential Spoofing Transmitter Locations
🟥 > 98% Vessel Line of Sight
🟧 > 97% Vessel Line of Sight
🟩 > 95% Vessel Line of Sight
Cape Idokopas (98% Line of Sight)
Krasnodar
Краснодар
Black Sea
Earthstar Geographics
POWERED BY esri

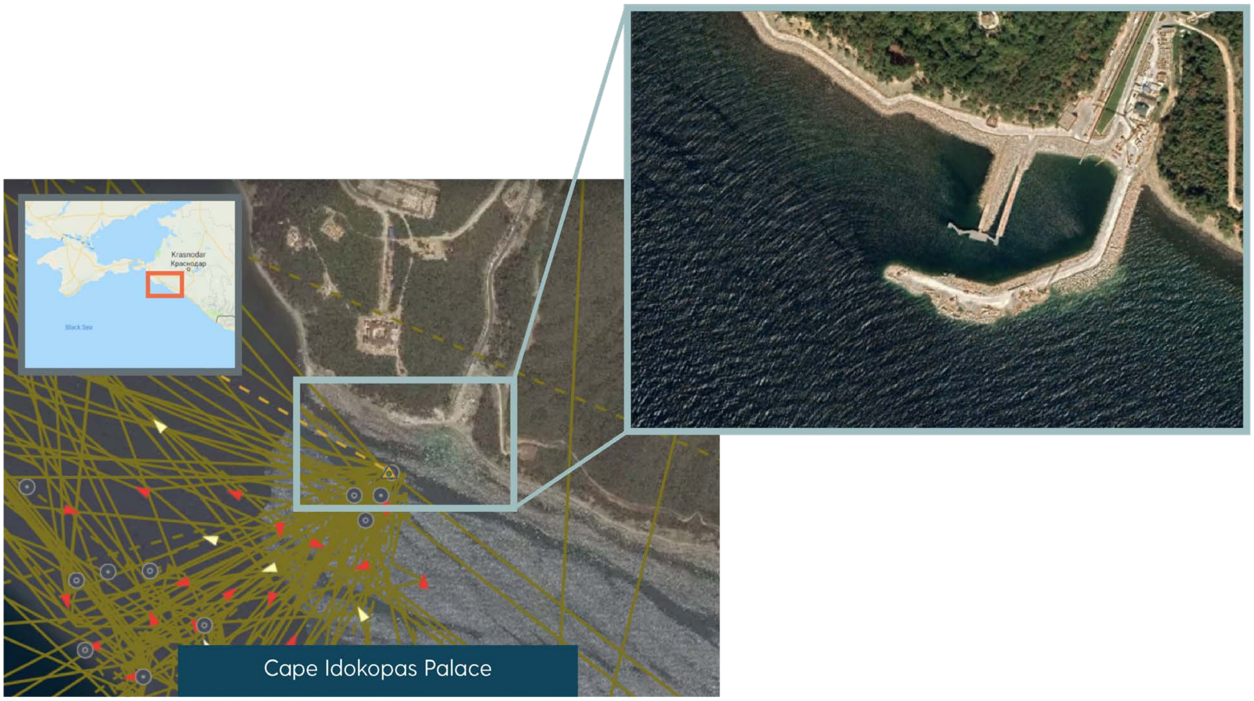
Cape Idokopas Residence

Cape Idokopas, located about 20km to the southeast of Gelendzhik, Russia, appears to be the most likely location for a terrestrial GNSS spoofing transmitter. The analysis indicates that it is located in proximity to several positions that have line of sight with at least 98 percent of affected vessels off the coast of Gelendzhik. The Cape is home to a sprawling facility containing a large Italianate palace, several helicopter pads, an amphitheater, and a small port. The complex was the subject of extensive international investigative reporting that alleged the property was built at the direction of then-Prime Minister Vladimir Putin under the auspices of an investment scheme referred to as “Project South,” allegedly for use as his private dacha.[132] [133] [134] The Russian government continues to deny that President Putin has any involvement with the facility.[135] [136] Regardless, high profile allegations of corruption have long dogged the project. Investigative reporting by Reuters in 2014 indicated that funds from a $1 billion program ordered by then-President Putin in 2005 to improve Russian healthcare were used to finance the construction of the facility.[137]


Potential Spoofing Transmitter Locations
🟥 > 98% Vessel Line of Sight
🟧 > 97% Vessel Line of Sight
🟩 > 95% Vessel Line of Sight
Cape Idokopas Palace

Aeronavigation charts dated July 2017 from the Russian Center of Aeronavigation Information show that the airspace above the Idokopas facility is classified as Prohibited.[138] [139] The facility maintains the same level of flight restriction that exists over the presidential and prime ministerial residences in Sochi.[140] However, unlike the official government residences and protected military facilities in Russia and Crimea, the prohibited airspace over Cape Idokopas appears to only protect a private residence. As discussed below, extensive property and corporate records along with previous investigative reporting outlined below suggest that the facility has an opaque history of involvement with elements of the FSO and Federal Security Service (FSB).[141]

For example, facility construction activities appear to have some associations with the FSO. In 2017, a newly constructed port appeared to the south of the Cape Idokopas palace. AIS records and satellite imagery indicate that a vessel called the Chernomorets-35 was present during, and may have assisted in, the development of the port.[142] Official records from the Russian contract registry show that 70 percent of the ship owner's contracts were with elements of the Russian state security services including the FSO, FSB, and the Presidential Administration.[143] This is supported by AIS records for the Chernomorets-35, which suggest that the vessel is one of a relatively small number permitted to operate at the FSO-operated government residences at Bocharov Ruchey, Riviera-6, and Olyva.[144] In fact, the majority of areas visited by Chernomorets-35 appear to be officially owned or operated by elements of the FSO.[145]

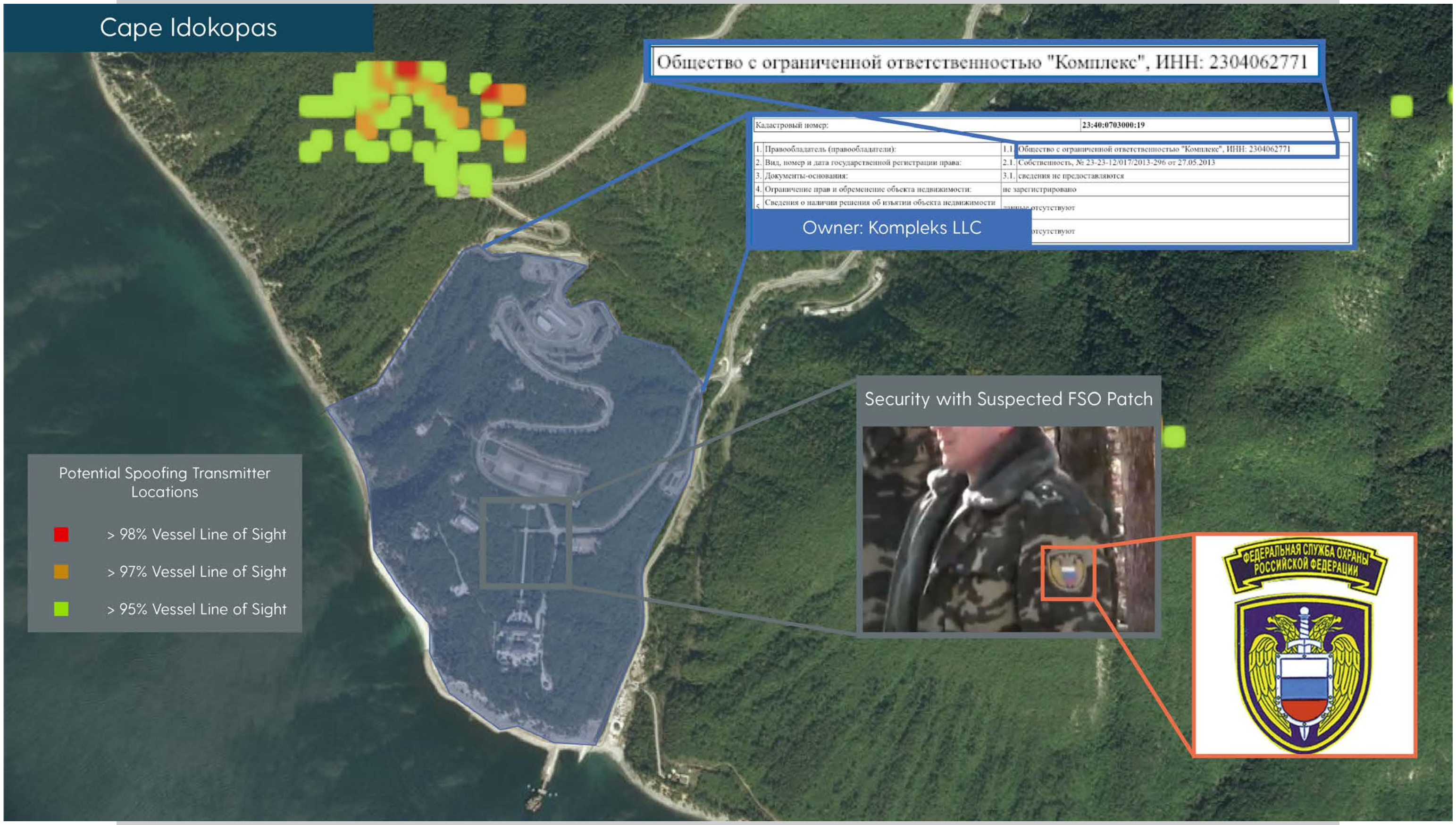


The Chernomorets-35 is the only vessel that fell victim to GNSS spoofing in proximity to Sochi, Gelendzhik, and Olyva while reportedly conducting construction activities at the government and private residences located nearby. The vessel's close position to the coast and proximity to sensitive facilities when it was affected by spoofed signals are additional indications that the spoofing devices may be positioned near the facilities themselves.

Idokopas Palace Ownership

C4ADS conducted an extensive property and corporate records analysis of the Cape Idokopas residence, matching it with previous investigative reporting. We found an opaque history of involvement with elements of the FSO and FSB.

According to official property records from the Russian cadastral registry last accessed by C4ADS in July 2018, the Gelendzhik-based company Kompleks LLC[146] is the sole owner of the Idokopas facility.[147] These same records indicated that Kompleks LLC became the owner of the facility on or before May 27, 2013. Official property records also show that the road and land bordering the main entrance to the facility is owned by the FSB's Border Directorate.[148] These records indicate that the FSB acquired the land on May 19, 2008.[149] It is currently unknown whether the FSB maintains an active presence at the facility. On at least one occasion in February 2011, environmentalists from the Russian organization Ecological Watch visiting the Cape Idokopas palace were confronted by facility security. This incident involved guards allegedly belonging to the border force, as well as an officer bearing patches and epaulets resembling those of a Senior Lieutenant in the FSO.[150] [151]


Cape Idokopas
Potential Spoofing Transmitter Locations
🟥 > 98% Vessel Line of Sight
🟧 > 97% Vessel Line of Sight
🟩 > 95% Vessel Line of Sight
Owner: Kompleks LLC
Security with Suspected FSO Patch
ФЕДЕРАЛЬНАЯ СЛУЖБА ОХРАНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Общество с ограниченной ответственностью "Комплекс", ИНН: 2304062771

Кадастровый номер:	23:40:0703000:19

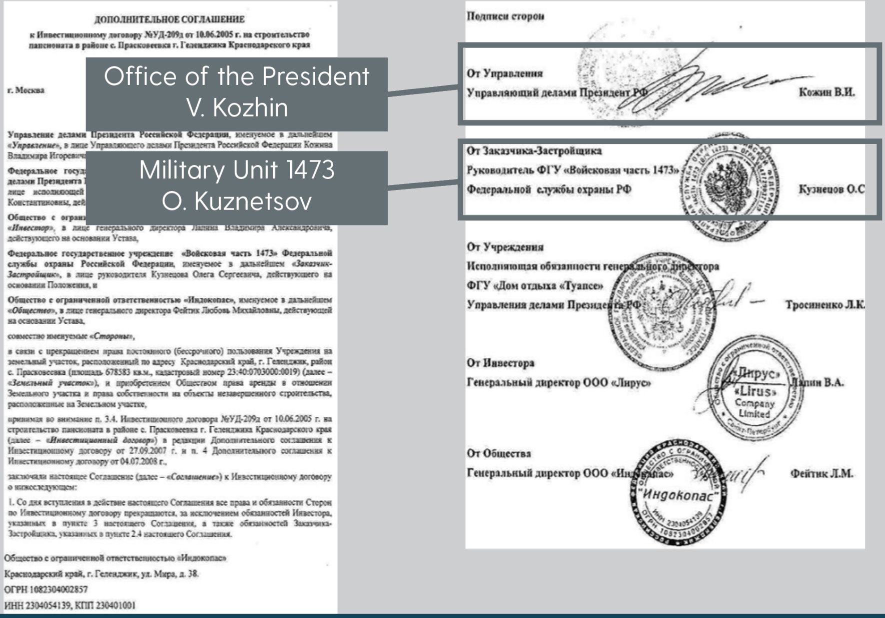
1.	Правообладатель (правообладатели):	1.1.	Общество с ограниченной ответственностью "Комплекс", ИНН: 2304062771
2.	Вид, номер и дата государственной регистрации права:	2.1.	Собственность, № 23-23-12/017/2013-296 от 27.05.2013
3.	Документы-основания:	3.1.	сведения не предоставляются
4.	Ограничение прав и обременение объекта недвижимости:		не зарегистрировано
5.	Сведения о наличии решения об изъятии объекта недвижимости		данные отсутствуют
			отсутствуют

Historical ownership records for Kompleks LLC appear to show that at the time of the property's purchase in May 2013, 100 percent of Kompleks LLC's shares belonged to Moscow-based Investstroy LLC.[152] [153] [154] According to Russian corporate records, at the time that Kompleks LLC purchased the property, two Russian individuals named

Tatyana Arnoldovna Kuznetsova and Inna Yuryevna Kolpakova were the sole equal shareholders of Investstroy LLC.[155] According to reporting from several Russian news agencies, both Tatyana Kuznetsova and Inna Kolpakova are married to former high-ranking officers in the FSO.[156] [157] [158]

Tatyana Kuznetsova is reportedly the wife of Oleg Sergeyevich Kuznetsov, who is reported to have previously served as the head of Military Unit 1473 of the FSO.[159] [160] Unit 1473, based in Moscow, is responsible for the management and operation of real estate belonging to the Russian state security services.[161] Inna Kolpakova is reportedly the wife of Alexandr Sergeyevich Koplakov who reportedly formerly served as the head of Directorate 'V' of the FSO Presidential Security Service until 2013.[162] [163] The FSO Presidential Security Service is directly tasked with protecting the Russian Head of State.[164]

A contract signed pursuant to a 2005 investment agreement, published by the Russian newspaper Novaya Gazeta, indicates that Oleg Kuznetsov and Unit 1473 maintained involvement in the initial stages of development of the Cape Idokopas facility.[165] [166] [167] These same documents also appear to show the involvement of Vladimir Kozhin in the development of the property at the same time that he was working as an aide to the Russian president.[168] The US Department of the Treasury sanctioned Kozhin under Executive Order 13661 in 2014 in response to the Russian annexation of Crimea.[169] In an April 2011 interview with Kommersant, Kozhin confirmed his involvement in the initial stages of the property's development, but claimed that it was only to encourage real estate development among investors.[170]


Office of the President
V. Kozhin
Military Unit 1473
O. Kuznetsov

ДОПОЛНИТЕЛЬНОЕ СОГЛАШЕНИЕ

к Инвестиционному договору №УД-209д от 10.06.2005 г. на строительство пансионата в районе с. Прасковеевка г. Геленджика Краснодарского края

г. Москва

Управление делами Президента Российской Федерации, именуемое в дальнейшем «*Управление*», в лице Управляющего делами Президента Российской Федерации Кожина Владимира Игоревич

Федеральное госуд **делами Президента** лице исполняющей Константиновны, дей

Общество с огран «*Инвестор*», в лице генерального директора Лапина Владимира Александровича, действующего на основании Устава,

Федеральное государственное учреждение «Войсковая часть 1473» Федеральной службы охраны Российской Федерации, именуемое в дальнейшем «*Заказчик-Застройщик*», в лице руководителя Кузнецова Олега Сергеевича, действующего на основании Положения, и

Общество с ограниченной ответственностью «Индокопас», именуемое в дальнейшем «*Общество*», в лице генерального директора Фейтик Любовь Михайловны, действующей на основании Устава,

совместно именуемые «*Стороны*»,

в связи с прекращением права постоянного (бессрочного) пользования Учреждения на земельный участок, расположенный по адресу Краснодарский край, г. Геленджик, район с. Прасковеевка (площадь 678583 кв.м., кадастровый номер 23:40:0703000:0019) (далее – «*Земельный участок*»), и приобретением Обществом права аренды в отношении Земельного участка и права собственности на объекты незавершенного строительства, расположенные на Земельном участке,

принимая во внимание п. 3.4. Инвестиционного договора №УД-209д от 10.06.2005 г. на строительство пансионата в районе с. Прасковеевка г. Геленджика Краснодарского края (далее – «*Инвестиционный договор*») в редакции Дополнительного соглашения к Инвестиционному договору от 27.09.2007 г. и п. 4 Дополнительного соглашения к Инвестиционному договору от 04.07.2008 г.,

заключили настоящее Соглашение (далее – «*Соглашение*») к Инвестиционному договору о нижеследующем:

1. Со дня вступления в действие настоящего Соглашения все права и обязанности Сторон по Инвестиционному договору прекращаются, за исключением обязанностей Инвестора, указанных в пункте 3 настоящего Соглашения, а также обязанностей Заказчика-Застройщика, указанных в пункте 2.4 настоящего Соглашения.

Общество с ограниченной ответственностью «Индокопас»
Краснодарский край, г. Геленджик, ул. Мира, д. 38.
ОГРН 1082304002857
ИНН 2304054139, КПП 230401001

Подписи сторон

От Управления
Управляющий делами Президент РФ **Кожин В.И.**

От Заказчика-Застройщика
Руководитель ФГУ «Войсковая часть 1473»
Федеральной службы охраны РФ **Кузнецов О.С**

От Учреждения
Исполняющая обязанности генерального директора
ФГУ «Дом отдыха «Туапсе»
Управления делами Президента РФ **Тросиненко Л.К.**

От Инвестора
Генеральный директор ООО «Лирус» **Лапин В.А.**

«Лирус» «Lirus» Company Limited

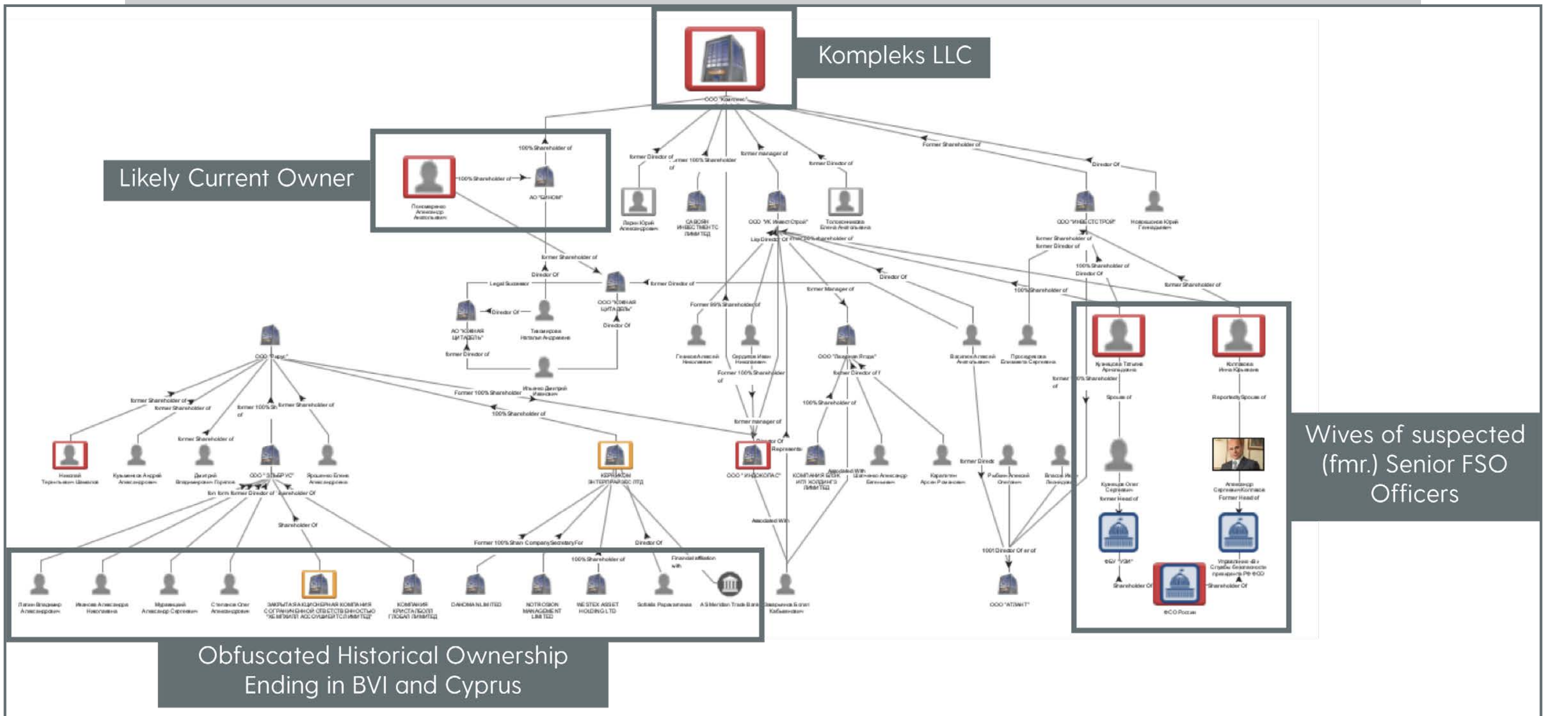
От Общества
Генеральный директор ООО «Индокопас» **Фейтик Л.М.**

"Индокопас"

Document Detailing Investment Agreement No. UD-209D (June 10, 2005) Obtained and Published by Novaya Gazeta in 2011

Novaya Gazeta reported that, in 2010, a Russian whistleblower who claimed to have been involved in the financing of the Cape Idokopas palace, alleged that construction of the Palace was personally directed by Nikolai Shamolov at the behest of then-Prime Minister Putin.[171] Shamolov, widely reported to be a close associate of Putin, has been sanctioned by the European Union since 2014.[172]

Prior to December 2016, the ultimate beneficial owner of Kompleks LLC and the Cape Idokopas residence remained hidden behind layers of holding companies based in secrecy jurisdictions, primarily in the British Virgin Islands.[173] In December 2016, a change in the shareholding structure revealed that the only natural person to own shares in Kompleks LLC, is Alexandr Anatolyevich Ponomarenko.[174] Ponomarenko is a high-profile Russian billionaire and apparent former owner of the nearby Novorossiysk Port.[175] [176] It is unclear when exactly Ponomarenko acquired the Idokopas facility, although he claims to have purchased the property from Nikolai Shamalov as early as March 2011.[177] [178]


Kompleks LLC
Likely Current Owner
Wives of suspected (fmr.) Senior FSO Officers
Obfuscated Historical Ownership Ending in BVI and Cyprus

Kompleks LLC Ownership History Network Graph

ANALYSIS POWERED BY Palantir

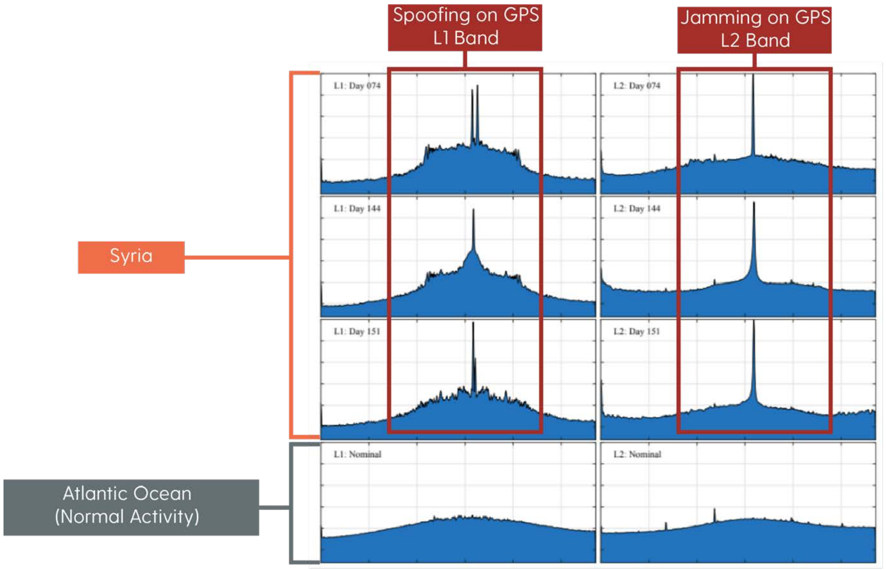
MILITARY PROTECTION ABROAD

While much of the previous reporting on GNSS spoofing has focused on where these activities appear within Russia, less attention has been paid to how these capabilities may be integrated into expeditionary force protection abroad. Using publicly available satellite data, we were able to uncover evidence that systems used to spoof GNSS signals are also being deployed on the ground in Syria. This work builds on previous public reporting on GPS interference activity reported in the Eastern Mediterranean,[179] Syria,[180] [181] Norway,[182] and Finland.[183]

From Jamming to Spoofing in Syria

Syria is a testbed for a range of Russian military equipment, including new EW assets. In April 2018, the head of US SOCOM Gen. Tony Thomas referred to Syria as, "the most aggressive electronic warfare environment in the world."[184] By some reports, GPS interference activities in Syria have been on the cutting edge, and Russia's deployment of EW capabilities has successfully targeted smaller US military drones.[185]

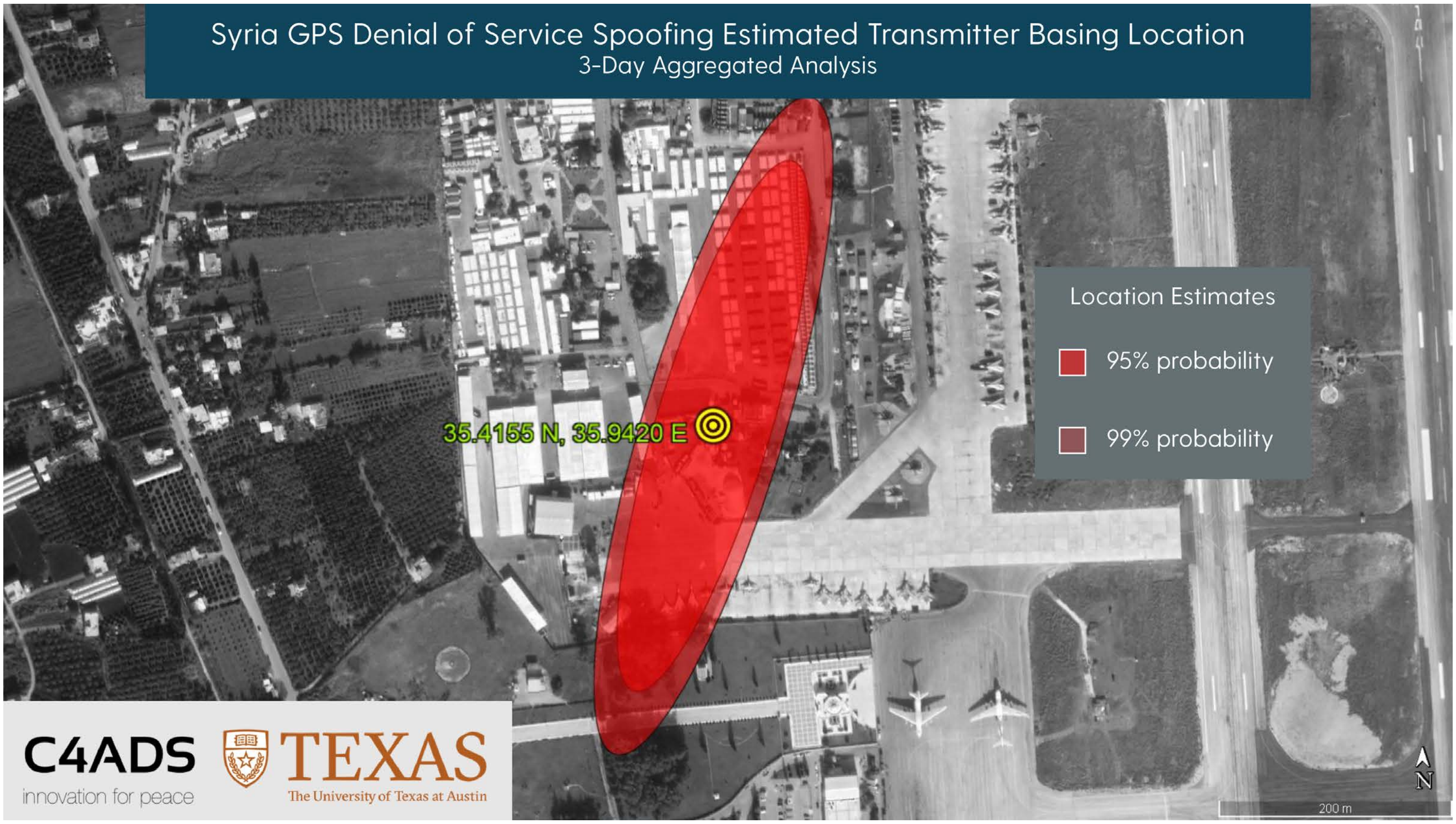
C4ADS and UT Austin used a GPS receiver onboard the International Space Station (ISS) to record, characterize, and ultimately geolocate a denial-of-service GPS spoofing transmitter to the Khmeimim Airbase in Syria. The research began in March 2018 when researchers from UT Austin detected evidence of GPS interference when examining historical GPS signal recordings collected from the ISS. In an effort to further characterize the GPS interference, C4ADS and UT Austin collaborated to conduct three independent GPS signal recordings over several months in the spring of 2018. On all three days of collection, researchers from UT Austin found clear evidence of GPS spoofing in the recorded signal data. Moreover, UT Austin researchers successfully geolocated the source of the signals in all three samples to Khmeimim Airbase, the nerve center of the Russian military campaign in Syria.



TEXAS The University of Texas at Austin

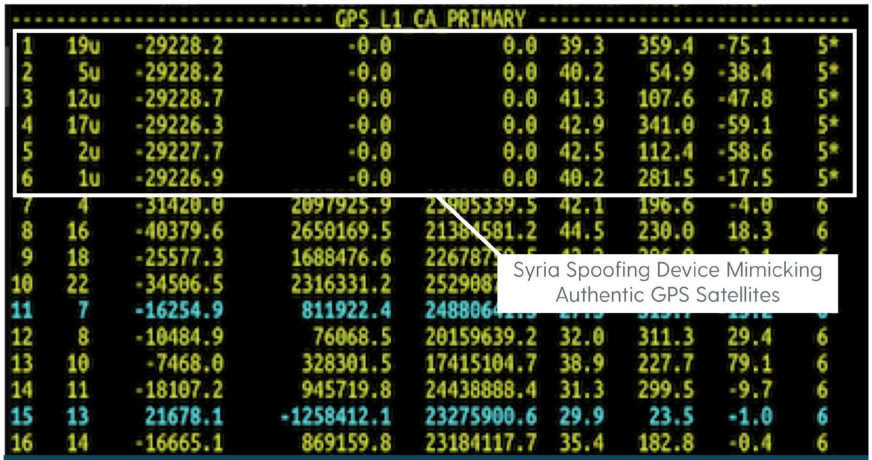
GPS Spoofing Detected from LEO Satellite

Based on an analysis of the Doppler signatures in the tracked data, we assess that the interference signals captured on all three days were likely generated by the same transmitter. This analysis has broader implications, specifically on how emerging civilian capabilities, such as cheap LEO satellites, combined with technical expertise, can be used to identify and track disruptions to GNSS worldwide.


Syria GPS Denial of Service Spoofing Estimated Transmitter Basing Location
3-Day Aggregated Analysis
35.4155 N, 35.9420 E
Location Estimates
🟥 95% probability
🟥 99% probability
C4ADS
innovation for peace
TEXAS
The University of Texas at Austin
N
200 m

UT Austin researchers found that while the signals successfully mimicked authentic GPS satellites, they carried no valid navigation information. In essence, GPS receivers targeted by these spoofed signals would report live GPS satellite connections but would be unable to calculate any valid positioning or timing information, which would effectively render the receivers inoperable. Furthermore, UT Austin researchers determined that the spoofing signals would be upwards of 500 times stronger than authentic GNSS signals for aircraft flying within line of sight of the transmitter, presenting a direct safety threat to commercial aviation in range of the transmissions.

Because denial-of-service spoofing would prevent receivers from calculating any navigation information, this activity may appear to be jamming, which has been widely reported in the Eastern Mediterranean in recent years. In late 2018, for example, Eurocontrol reported GNSS jamming activity originating from Syrian territory and identified high probability locations in the Eastern Mediterranean from which the interference appeared to originate.[186] [187]

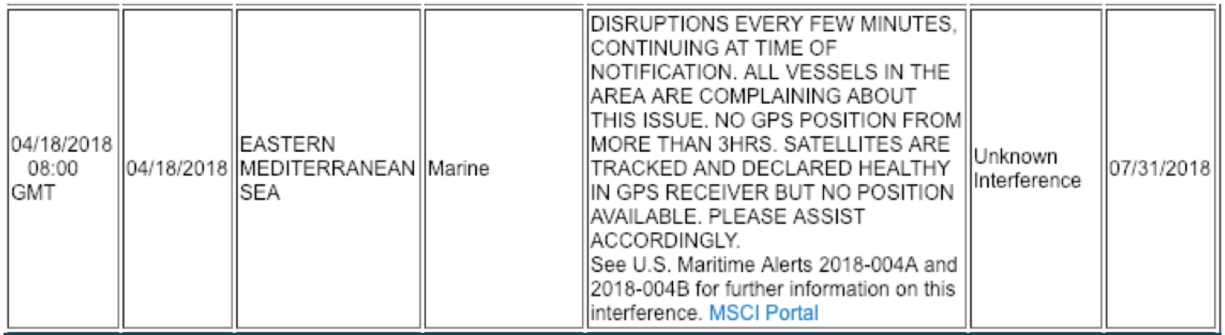


```
............................. GPS_L1_CA_PRIMARY .............................
1   19u  -29228.2          -0.0           0.0  39.3  359.4  -75.1    5*
2    5u  -29228.2          -0.0           0.0  40.2   54.9  -38.4    5*
3   12u  -29228.7          -0.0           0.0  41.3  107.6  -47.8    5*
4   17u  -29226.3          -0.0           0.0  42.9  341.0  -59.1    5*
5    2u  -29227.7          -0.0           0.0  42.5  112.4  -58.6    5*
6    1u  -29226.9          -0.0           0.0  40.2  281.5  -17.5    5*
7    4   -31420.0     2097925.9    2 905339.5  42.1  196.6   -4.0    6
8   16   -40379.6     2650169.5    21384581.2  44.5  230.0   18.3    6
9   18   -25577.3     1688476.6    226787
10  22   -34506.5     2316331.2    2529087
11   7   -16254.9      811922.4    248806
12   8   -10484.9       76068.5    20159639.2  32.0  311.3   29.4    6
13  10    -7468.0      328301.5    17415104.7  38.9  227.7   79.1    6
14  11   -18107.2      945719.8    24438888.4  31.3  299.5   -9.7    6
15  13    21678.1    -1258412.1    23275900.6  29.9   23.5   -1.0    6
16  14   -16665.1      869159.8    23184117.7  35.4  182.8   -0.4    6
```

Syria Spoofing Device Mimicking Authentic GPS Satellites

GPS Spoofing Detected from LEO Satellite

This interference, however, may well be the product of spoofing, and not just jamming. GPS interference reports posted on the US Coast Guard Navigation Center's website from ships based in the Eastern Mediterranean Sea, for example, mirror the pattern of activity that would be expected of a receiver affected by the spoofed GPS signals detected at Khmeimim. In these reports, several vessel GPS receivers in proximity to one another reported satellite signal locks but could not calculate any valid positioning information.



04/18/2018 08:00 GMT	04/18/2018	EASTERN MEDITERRANEAN SEA	Marine	DISRUPTIONS EVERY FEW MINUTES, CONTINUING AT TIME OF NOTIFICATION. ALL VESSELS IN THE AREA ARE COMPLAINING ABOUT THIS ISSUE. NO GPS POSITION FROM MORE THAN 3HRS. SATELLITES ARE TRACKED AND DECLARED HEALTHY IN GPS RECEIVER BUT NO POSITION AVAILABLE. PLEASE ASSIST ACCORDINGLY. See U.S. Maritime Alerts 2018-004A and 2018-004B for further information on this interference. MSCI Portal	Unknown Interference	07/31/2018

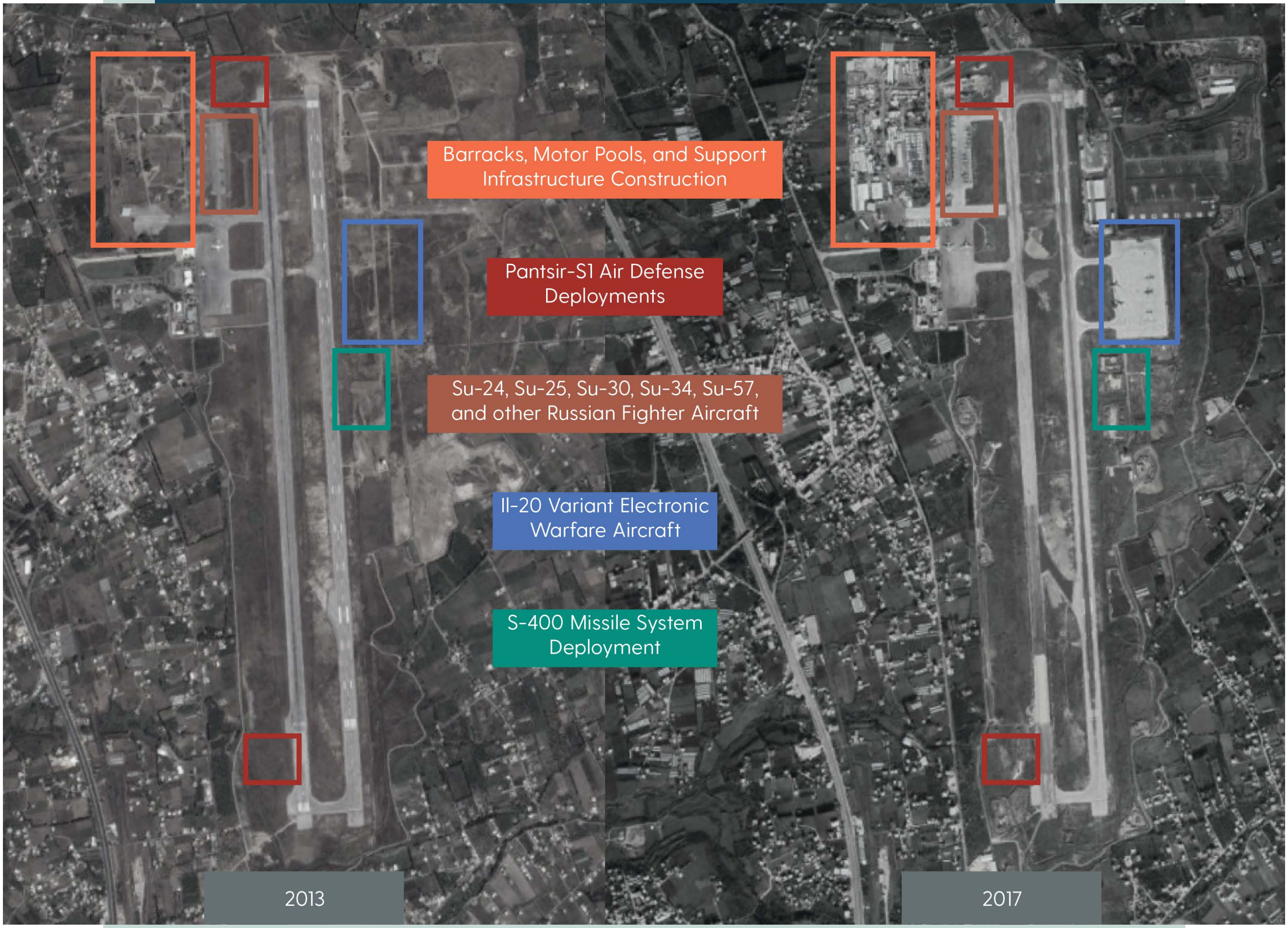
NAVCEN GPS Interference Report for Eastern Mediterranean Sea

In the context of these reports, C4ADS and UT Austin's findings bring to light the possibility that at least some of the GPS interference taking place in Syria and the Eastern Mediterranean may, in fact, be denial-of-service GPS spoofing.

Potential Systems in Use (Military)

Khmeimim Airbase, where the spoofed GPS signals appear to originate, serves as one of the primary staging locations for Russian military sorties in Syria. Since 2013, Kheimim has undergone heavy reconstruction and now supports and protects the most advanced Russian military assets deployed in Syria. According to a series of agreements signed between Russia and Syria in 2016 and 2017, Russian forces maintain full authority over air defense and rule of law within the territory of the facility.[188] [189] The airbase houses Russia's latest military assets, including S-400 surface-to-air missile batteries, the Pantsir-S1 anti-aircraft system, and Su-57 stealth fighters.[190] While the Russian military regularly displays these systems publicly on Russian media outlets, EW systems deployed at the airbase have generally avoided the limelight.[191] Many videos allegedly revealing the basing location for these systems are no longer online.[192]

Russian Military Build-Up of Khmeimim Airbase between 2013 and 2017


Barracks, Motor Pools, and Support Infrastructure Construction
Pantsir-S1 Air Defense Deployments
Su-24, Su-25, Su-30, Su-34, Su-57, and other Russian Fighter Aircraft
Il-20 Variant Electronic Warfare Aircraft
S-400 Missile System Deployment
2013
2017

Khmeimim has been a target of air attacks in the past. On January 5, 2018, a drone swarm consisting of 13 drones carrying explosive fragmentation munitions reportedly attacked from the east.[193] The drones, reportedly all launched from the same location about 96km from Khmeimim, came pre-programmed with flight path coordinates, suggesting that the drones likely used GNSS for navigation assistance.[194] According to the Russian Ministry of Defense, Russian EW systems based at Khmeimim forced at least six of the drones to land at "assigned coordinates" while Pantsir S1 anti-aircraft systems neutralized the remaining seven drones.[195] Based on this official description, it is possible that Russian EW systems targeted GNSS receivers onboard the drones in order to force them to land.

Commercial drones deployed by non-state combatants in warzones like Syria often have their geofencing restrictions removed to bypass flight restrictions over much of Syria and Iraq.[196] This means that GNSS spoofing designed to trigger typical drone geofence locks, as seen in Russia, cannot be used to disable these modified drones. Drones are now used consistently by combatants for reconnaissance purposes and to deliver low-yield payloads to protected targets such as ammo depots and airports.[197] In a militarized environment where geofences are not an effective tool, Russia has to rely on more other methods such as this unique form of denial of service spoofing to target and bring down homemade drones.

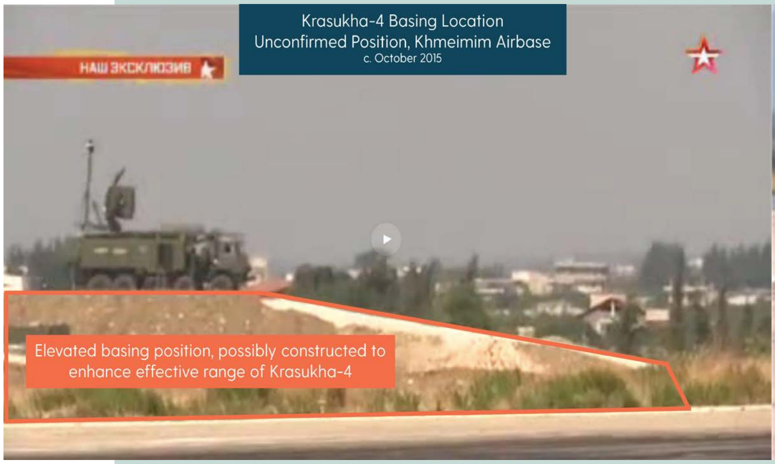
The Russian Ministry of Defense has not detailed the specific EW systems deployed in Syria, but at least two systems potentially capable of performing counter-drone missions by targeting GNSS are now confirmed or likely to be present in Syria.

Electronic Warfare System	Reported Capabilities	Spotted in Syria
Krasukha-4	Conflicting reports on capabilities, believed to be a multifunctional jammer capable of jamming radars on aircraft and LEO reconnaissance satellites.[198] [199]	c. October 2015 and June 2017 at Khmeimim Airbase (See Below)
R-330Zh 'Zhitel'	"SATCOM/GPS/GSM jamming station (detection, direction-finding, analysis and suppression of UHF radio signals). Part of R-330M1P Diabazol automated jamming system."[200]	c. December 2016 possibly spotted at Aleppo Airport.[201]
Samarkand	Allegedly capable of GPS jamming and spoofing in addition to interference with C4ISR systems.[202] [203] Possibly a stationary system.[204]	No confirmed sightings.
Shipovnik-Aero	UAV control signal jamming, GNSS jamming, possibly GNSS spoofing.[205] [206]	No confirmed sightings.

Krasukha-4

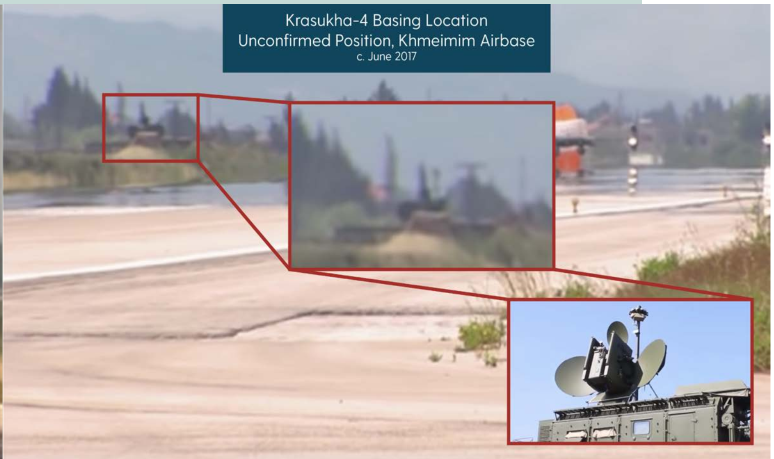
In 2015 and 2017, videos posted by several Russian news outlets appeared to corroborate satellite imagery analysis by IHS showing the deployment of the Krasukha-4 EW system at the northern portion of the Khmeimim Airfield.[207] [208] [209] There are many conflicting reports about the full breadth of the Krasukha-4's EW capabilities, with some sources claiming that the system is capable of "blocking GPS" in addition to radar systems over a large area.[210] [211] Satellite imagery from dates closest to the days where C4ADS and UT

Austin detected GPS interference shows a known Krasukha-4 basing location located within roughly 350 meters from the estimated signal origin.[212] It is currently unknown whether this system is responsible for the GPS interference signals detected coming from the facility.



Krasukha-4 Basing Location
Unconfirmed Position, Khmeimim Airbase
c. October 2015

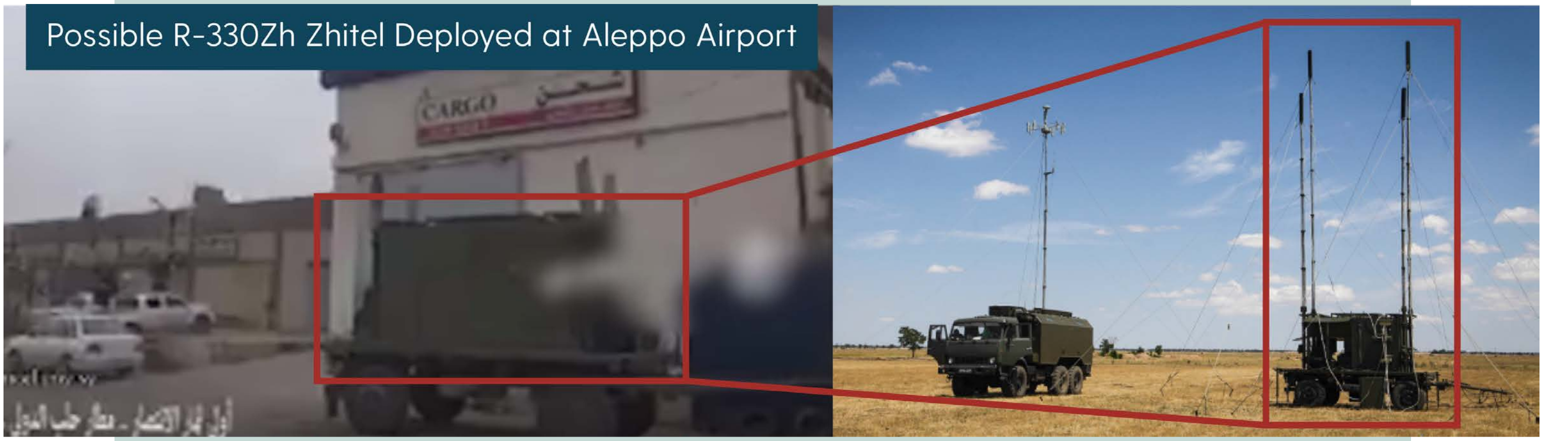
Elevated basing position, possibly constructed to enhance effective range of Krasukha-4



Krasukha-4 Basing Location
Unconfirmed Position, Khmeimim Airbase
c. June 2017

R-330Zh Zhitel

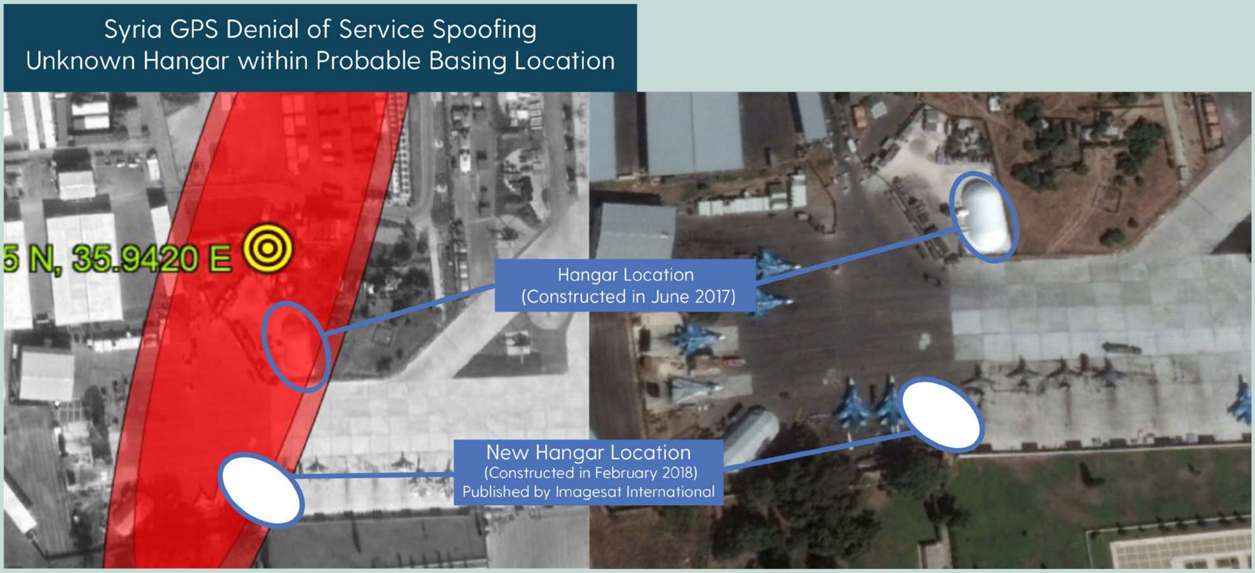
In addition to the Krasukha-4, the advanced Russian R-330Zh Zhitel EW system is also reportedly present in Syria. A video of Aleppo Airport posted around December 2016 show what appears to be a towable phased antenna array assembly belonging to the R-330Zh.[213] As opposed to the Krasukha-4, the R-330Zh's ability to jam and manipulate GPS systems is officially recognized by the Russian government.[214] C4ADS conducted an analysis of satellite imagery available for Khmeimim Airbase for dates near when we detected GPS spoofing. However, C4ADS could not confirm, with confidence, the presence of the R-330Zh at the Khmeimim Airbase due to limitations in the resolution of the imagery.



Possible R-330Zh Zhitel Deployed at Aleppo Airport

Unknown Hangars

In June 2017 and February 2018, two closed-off elliptic hangar-like structures, reportedly used to house delicate equipment including UAV components and other sensors, appeared within the high-probability transmitter basing area identified by UT Austin researchers.[215] According to the researchers' estimates, these hangars are located within the 99 percent probability basing area.



Syria GPS Denial of Service Spoofing
Unknown Hangar within Probable Basing Location

5 N, 35.9420 E
Hangar Location
(Constructed in June 2017)
New Hangar Location
(Constructed in February 2018)
Published by Imagesat International

Based on available imagery, it is believed that the hangar constructed in June 2017 is not directly connected to the tarmac and would therefore be an unlikely basing location for aircraft. Additionally, the hangar appears to include an elevated arm that could potentially be used to mask an antenna. The hangars themselves appear to be designed to prevent satellites or individuals stationed at the facility from photographing the hardware positioned inside the hangars. It is currently unconfirmed whether these structures are directly tied to the detected GPS spoofing activities.

CONCLUSION

Through C4ADS' investigation into GNSS spoofing activities taking place in the Russian Federation, Crimea, and Syria, we are able to demonstrate the effectiveness of leveraging publicly available signals, official records, social and news media, and technology to develop an enhanced awareness of the potential actors, systems, and locations used to conduct these activities. The systems-level analyses and case studies detailed in this report expose just a fraction of the GNSS interference activities taking place worldwide. However, our research indicates that Russia continues to act as a pioneer in this space, exposing its willingness to not only deploy these capabilities in protection of VIPs and strategically-important facilities, but also to leverage these techniques to promote its ventures at frontiers in Syria and Russia's European borders. Russia's continued development and deployment of systems designed to spoof GNSS and counteract NATO's decisive advantage in C4ISR capabilities at forward-operating locations in Syria and Kaliningrad presents a unique challenge to the security of critical national infrastructure.

While the GNSS spoofing activities against civilian GNSS systems detailed in this report identify capabilities used by state-level actors, the tools and methodologies for conducting similar activities are readily available to non-state actors. State and non-state actors engaged in illicit activity continue to show the lengths to which they are willing to go in order to both conduct and conceal their operations.[216] While the commercial availability and concealability of these do-it-yourself devices present a unique set of challenges for deterring both lone-wolf and coordinated spoofing activities, state-sponsored activities against civilian GNSS receivers continue to show how impactful these activities can be against vulnerable systems. Whether for profit, protection, or disruption, illicit actors, writ large, stand to gain from the proliferation of these capabilities.

The tools used to conduct this activity may be openly available, but so too are the technologies and methodologies for detecting, tracking, and geolocating these activities. This report aims to demonstrate the utility of combining subject matter expertise, like that from the University of Texas at Austin, with data-driven analysis to develop unique approaches for collecting, analyzing, and ultimately addressing GNSS spoofing activities. The techniques for finding GNSS spoofing detailed in this report are both replicable and highly extensible. Any system that reports GNSS-derived location information, like aircraft or mobile devices, can potentially be exploited to identify GNSS spoofing events affecting aircraft or ground-based GNSS receivers. Moreover, the collaboration between C4ADS and UT Austin researchers shows how GNSS receivers based on low-Earth-orbit satellites can be used to detect and geolocate interference signals worldwide. As private satellite firms continue to launch small and relatively inexpensive payloads into low-Earth-orbit, the commercial availability of GNSS receiver data that can be used to detect this interference will continue to proliferate.

Significant opportunities exist for both public and private sector organizations to get ahead of the curve and address these challenges head-on. Increased public awareness of GNSS interference threats can lead to not only a more measured and proportional response by private sector organizations, but also a more open discussion on how these threats can be successfully mitigated. Public efforts to protect, toughen, and augment existing PNT systems, such as those promoted by the RNT Foundation, combined with evidence-based reporting on these issues, can serve to enhance this dialogue.

Endnotes

[1] North Korean GPS jamming reportedly disrupted over 1,000 commercial airliners and military systems in 2016, see https://www.popularmechanics.com/military/weapons/a20289/north-korea-jamming-gps-signals/

[2] Chinese military journals discuss how to use anti-satellite weapons and EW to degrade American C4ISR systems, see http://caod.oriprobe.com/articles/39227089/Research_on_interference_effectiveness_analysis_of_high_altitude_UAV_airborne_GPS_INS_system.htm

[3] Jane's International Defence reports that the Russian Federation is actively refining its ability to detect electromagnetic signatures to guide artillery barrages against Ukrainian soldiers in the disputed regions of the Donbass, see https://www.janes.com/images/assets/111/80111/The_Czar_of_battle_Russian_artillery_use_in_Ukraine_portends_advances.pdf

[4] Data similar to that used by C4ADS and UT Austin in this study can be obtained through commercial vendors specializing in LEO satellite data. Potential vendors include Spire (https://www.spire.com/en) and HawkEye360 (https://www.he360.com/)

[5] Jeff Coffed, "The Threat of GPS Jamming: The Risk to an Information Utility," Harris Corporation, Last modified January 2016, https://www.harris.com/sites/default/files/downloads/solutions/d0783-0063_threatofgpsjamming_v2_mv.pdf.

[6] Major Brian Granio and Major Jane Gibson, "Space Systems Threats," In AU-18 Space Primer, Air University Press, 2009, http://www.au.af.mil/au/awc/space/au-18-2009/au-18_chap21.pdf.

[7] Major Brian Granio and Major Jane Gibson, "Space Systems Threats," In AU-18 Space Primer, Air University Press, 2009, http://www.au.af.mil/au/awc/space/au-18-2009/au-18_chap21.pdf.

[8] Mark L. Psiaki and Todd E. Humphreys, "GNSS Spoofing and Detection," Proc IEEE 104, no. 6 (2016): 1259-127, http://rnl.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf.

[9] A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys, "Unmanned Aircraft Capture and Control via GPS Spoofing," Journal of Field Robotics 31, no. 4 (2014): 617–636, https://radionavlab.ae.utexas.edu/images/stories/files/papers/unmannedCapture.pdf.

[10] The University of Texas at Austin, "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea," Last modified July 29, 2013, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/.

[11] "National Risk Estimate: Risks to U.S. Critical Infrastructure From Global Positioning System Disruptions," Department of Homeland Security, 2011, https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf.

[12] "National Risk Estimate: Risks to U.S. Critical Infrastructure From Global Positioning System Disruptions," Department of Homeland Security, 2011, https://rntfnd.org/wp-content/uploads/DHS-National-Risk-Estimate-GPS-Disruptions.pdf.

[13] "Economic Impact to the UK of a disruption to GNSS," London Economics, Last modified June 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/619545/17.3254_Economic_impact_to_UK_of_a_disruption_to_GNSS_-_Showcase_Report.pdf

[14] 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," Paper presented at the 27th USENIX Security Symposium, Baltimore, MD, United States, August 15-17 2018, https://people.cs.vt.edu/gangwang/sec18-gps.pdf.

15 "Using a Hackrf to Spoof GPS Navigation in Cars and Divert Drivers," RTL-SDR, Last modified July 19, 2018, https://www.rtl-sdr.com/using-a-hackrf-to-spoof-gps-navigation-in-cars-and-divert-drivers/.

16 DEFCONConference, "DEF CON 25 – David Robinson – Using GPS Spoofing to Control Time," YouTube, Video File, October 27, 2017, https://www.youtube.com/watch?v=isiuTNh5P34.

17 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/.

18 Roger N McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum," International Centre for Defence and Security, Last modified September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

19 The precise capabilities of Russian electronic warfare systems are often a closely held secret to prevent the development of countermeasures to the techniques these systems use. Publicly available information on these capabilities suggests that the following systems may target or disrupt the use of GNSS: R-330Zh Zhitel, Shipovnik-Aero, Samarkand

20 "Latest from the OSCE Special Monitoring Mission to Ukraine (SMM), based on information received as of 19:30, 19 January 2017," OSCE Special Monitoring Mission to Ukraine, Last modified January 20 2017, https://www.osce.org/ukraine-smm/294856.

21 Roger N McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum," International Centre for Defence and Security, Last modified September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

22 Constantine (@CKonovalov on Twitter), "Короче, сегодня глушат gps от Большого театра вниз до Садового кольца. Охренеть глушилка у них!" July 10, 2016, https://twitter.com/CKonovalov/status/752111666196803585.

23 Clare Sebatstian, "Getting lost near the Kremlin? Russia could be 'GPS spoofing,'" CNN Business, Last modified December 2, 2016, https://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/.

24 Дмитрий Крылов, "Кремль продложит искажать," gazeta.ru, Last modified December 19, 2016, https://www.gazeta.ru/auto/2016/12/16_a_10430909.shtml#page2.

25 "St. Petersburg Drivers Report Strange GPS Problems in City Center," The Moscow Times, Last modified December 27, 2016, https://themoscowtimes.com/news/drivers-in-st-petersburg-report-gps-problems-in-city-center-56653.

26 Matt Burgess, "When a tanker vanishes, all the evidence points to Russia," Wired, Last Modified September 21, 2017, https://www.wired.co.uk/article/black-sea-ship-hacking-russia.

27 Matt Burgess, "When a tanker vanishes, all the evidence points to Russia," Wired, Last Modified September 21, 2017, https://www.wired.co.uk/article/black-sea-ship-hacking-russia.

28 "2017-005A-Black Sea-GPS Interference," Maritime Administration, Accessed March 20, 2019, https://www.maritime.dot.gov/content/2017-005a-black-sea-gps-interference.

29 Elisabeth Braw, "The GPS Wars Are Here," Foreign Policy, Last Modified December 17, 2018, https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/.

30 Knut-Sverre Horn, “Støy fra Russland slo ut GPS-signaler for norske fly,” NRK, Last Modified October 5, 2017, https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305.

31 Muhammad Darwish, “Did Russia make this ship disappear?” CNN Business, Last modified November 3, 2017, https://money.cnn.com/2017/11/03/technology/gps-spoofing-russia/index.html.

32 "GPS Spoofing Patterns Discovered," Resilient Navigation and Timing Foundation, September 25, 2017, https://rntfnd.org/wp-content/uploads/GPS-Spoofing-Patterns-Press-Release.1-26-Sep-17-RNT-Foundation.pdf.

33 “Moscow taxi users confusion amid GPS meddling claims,” BBC, Last Modified January 10, 2018, https://www.bbc.com/news/technology-42633024.

34 “The Global Heatmap,” Strava, Accessed March 20, 2019, https://www.strava.com/heatmap#14.45/37.26274/55.59919/hot/all.

35 Michael Jones, “Spoofing in the Black Sea: What really happened?” GPS World, Last Modified October 11, 2017, https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/.

36 John Patterson, “Heliguy’s Guide to Geofencing,” Heliguy, Last Modified February 16, 2017, https://www.heliguy.com/blog/2017/02/16/heliguys-guide-to-geofencing/.

37 “MSCI Advisory,” United States Department of Transportation Maritime Administration, Last modified September 1, 2017, https://www.maritime.dot.gov/content/2017-006-global-gps-disruption.

38 Matt Burgess, “When a tanker vanishes, all the evidence points to Russia,” Wired, Last Modified September 21, 2017, https://www.wired.co.uk/article/black-sea-ship-hacking-russia.

39 Иван Щварц, “Россия отключает на Черном море спутниковую навигацию,” Независимая Газета, Last modified September 25, 2017, http://www.ng.ru/armies/2017-09-25/100_gps250917.html.

40 For more information on the physical limitations of GNSS signals, see Paul Groves, Lei Wang, and Marek Ziebart, “Shadow Matching: Improved GNSS Accuracy in Urban Canyons,” GPS World, Last Modified February 1, 2012, https://www.gpsworld.com/wirelesspersonal-navigationshadow-matching-12550/.

41 Muhammad Darwish, “Did Russia make this ship disappear?” CNN Business, Last modified November 3, 2017, https://money.cnn.com/2017/11/03/technology/gps-spoofing-russia/index.html.

42 Robert Wallack, “Russia’s Port of Novorossiysk expanding to handle larger volumes of grains,” Ajot, Last modified November 27, 2018, https://www.ajot.com/premium/ajot-russias-port-of-novorossiysk-expanding-to-handle-larger-volumes-of-grains.

43 Damien Sharkove, “Russia to unveil new $1.4 billion black sea fleet base near Crimea,” Newsweek, Last modified July 28, 2016, https://www.newsweek.com/russia-unveil-new-14-bn-black-sea-fleet-base-four-years-484974.

44 “Port of Sochi,” JSC Commercial Seaport of Sochi, . http://www.morport-sochi.ru/index-eng.php.

45 “Часовой - Сирия. Авиабаза Хмеймим. Фильм 1-й. Выпуск от 18.02.2018,” YouTube, Video File, February 18, 2018, https://www.youtube.com/watch?v=a4RZpc5Vt1g.

46 “Standard Departure Chart Instrument, Krasnodar, Russia,” Federal Air Transport Agency, Last modified July 20, 2017, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/urkk/1-ad2-rus-urkk-142.pdf.

47 Stephen Grey, Jason Bush, and Roman Anin, “Billion-dollar medical project helped fund ‘Putin’s palace’ on the Black Sea,” Reuters, Last modified May 21, 2014, https://www.reuters.com/investigates/special-report/comrade-capitalism-putins-palace/.

48 “Visual Approach Chart – ICAO: Sochi, Russia,” Federal Air Transport Agency, Last modified August 16, 2018, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/urss/1-ad2-rus-urss-113.pdf.

49 Пьер Сидибе, "ПОЛИТИКА Резиденцию для Медведева перестраивают после отъезда Путина," Известия, July 26, 2012, https://iz.ru/news/531337.

50 “Standard Departure Chart Instrument (SID) – ICAO,” Federal Air Transport Agency, November 9, 2017, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/uuww/1-ad2-rus-uuww-139.pdf.

51 Alexey (@Alekezzzzz on Twitter), “GPS у дачи Путина дал ошибку и заслал меня во Внуково, охрана что ли сигнал глушит, на самом деле только 103 км,” May 28, 2016, https://twitter.com/Alekzzzzz/status/736686021371383808.

52 “Standard Departure Chart Instrument (SID) – ICAO,” Federal Air Transport Agency, November 9, 2017, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/uuww/1-ad2-rus-uuww-139.pdf.

53 Constantine (@CKonovalov on Twitter), “Короче, сегодня глушат gps от Большого театра вниз до Садового кольца. Охренеть глушилка у них!” July 10, 2016, https://twitter.com/CKonovalov/status/752111666196803585.

54 "Visit to Vladivostok branch of the Nakhimov Naval Academy," President of Russia, August 31, 2016, http://en.kremlin.ru/events/president/news/52782.

55 “Vladimir Putin arrived in China,” President of Russia, September 3, 2016, http://en.kremlin.ru/events/president/news/52815.

56 “ATC Surveillance Minimum Altitude Chart – ICAO,” Federal Air Transport Agency, November 9, 2017, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/urff/1-ad2-rus-urff-059.pdf.

57 Крымский канал, “#нампишут Вот такой теперь вид на море вдоль трассы Ялта-Севастополь в районе Кастрополя и Оливы. Госдачи становятся Крымом Их собственного заточения. Кстати, 4 года до этого обходились без заборов,” March 13, 2018, https://t.me/fcpeshka/454.

58 “Осмотр участка строительства Крымского моста,” President of Russia, September 15, 2016, http://kremlin.ru/events/president/news/52900.

59 “Meeting with employees of Russian Arctic National Park,” President of Russia, March 29, 2017, http://en.kremlin.ru/events/president/news/54155.

60 “Meeting with President of Iceland Gudni Johannesson,” President of Russia, Last Modified March 30, 2017, http://en.kremlin.ru/events/president/news/54152.

61 “Владимир Путин дал старт стыковке мелководной и глубоководной частей «Турецкого потока»,” President of Russia, Last modified June 23, 2017, www.kremlin.ru/events/president/news/54859.

62 “Vladimir Putin arrived in Vladivostok,” President of Russia, Last Modified September 5, 2017, http://en.kremlin.ru/events/president/news/55537.

63 “Visit to Zvezda shipyard,” President of Russia, Last Modified September 8, 2017, http://en.kremlin.ru/events/president/news/55560.

64 See 16:43, Телеканал Звезда, “Военная приемка в Сирии. База Хмеймим. Часть 2," Youtube, Video File, Posted June 11, 2017, https://www.youtube.com/watch?v=JDM2Vl0Qp8o.

65 See 20:25, Телеканал Звезда, “Военная приемка в Сирии. База Хмеймим. Часть 2,“ Youtube, Video File, Posted June 11, 2017, https://www.youtube.com/watch?v=JDM2Vl0Qp8o.

66 Joseph Trevithick, “Russia Releases First Official Video of Its Su-57s On Their Absurdly Short Trip to Syria,” The Drive, Last Modified November 19, 2018, http://www.thedrive.com/the-war-zone/24997/russia-releases-first-official-video-of-its-su-57s-on-their-absurdly-short-trip-to-syria.

67 Krasukha-4 spotted behind Su-25 aircraft at 06:22, Телеканал Звезда, “Военная приемка в Сирии, База Хмеймим, Часть 2,“ Youtube, Video File, Posted June 11, 2017, https://www.youtube.com/watch?v=JDM2Vl0Qp8o.

68 “Открытие автодорожной части Крымского моста,” President of Russia, Last Modified May 15, 2018, www.kremlin.ru/events/president/news/57472.

69 “Посещение судостроительного комплекса «Звезда»,” President of Russia, Last Modified September 11, 2018, www.kremlin.ru/events/president/news/58521.

70 Confidential Source.

71 “Radio Regulations,” International Telecommunications Union, Last Modified November 2016, https://www.itu.int/pub/R-REG-RR-2016.

72 “Russia-Ukraine tensions rise after Kerch Strait ship capture,” BBC, Last Modified November 26, 2018, https://www.bbc.com/news/world-europe-46340283.

73 “Осмотр участка строительства Крымского моста,” President of Russia, Last Modified September 15, 2016, http://kremlin.ru/events/president/news/52900.

74 “Новосты,” President of Russia, Accessed March 20, 2019, http://kremlin.ru/events/president/news/page/119.

75 “Открытие автодорожной части Крымского моста,” President of Russia, Last Modified May 15, 2018, www.kremlin.ru/events/president/news/57472.

76 “Открытие автодорожной части Крымского моста,” President of Russia, Last Modified May 15, 2018, www.kremlin.ru/events/president/news/57472.

77 “Новосты,” President of Russia, Accessed March 20, 2019, http://kremlin.ru/events/president/news/page/45

78 “Visit to Zvezda Shipyards,” President of Russia, September 8, 2017, http://en.kremlin.ru/events/president/news/55560.

79 “Посещение судостроительного комплекса «Звезда»,” President of Russia, September 11, 2018, http://kremlin.ru/events/president/news/58521.

80 Elizaveta Sergina, “Телепортация из Кремля во «Внуково»,” Vedomosti, October 21, 2016, https://www.vedomosti.ru/technology/articles/2016/10/21/661873-kremlya-vnukovo.

81 Vidal Sorokin, “Russian SHIPOVNIK-Aero Jamming Station Presumably Spotted in

the Center of Donetsk," InformNapalm, July 31, 2016, https://informnapalm.org/en/russian-shipovnik-aero-jamming-station-donetsk/.

82 "Interception System Suppresses UAV Control in Less than Minute," iHLS, September 22, 2016, https://i-hls.com/archives/71825.

83 Elizaveta Sergina, "Телепортация из Кремля во «Внуково»," Vedomosti, October 21, 2016, https://www.vedomosti.ru/technology/articles/2016/10/21/661873-kremlya-vnukovo.

84 "Interception System Suppresses UAV Control in Less than Minute," iHLS, September 22, 2016, https://i-hls.com/archives/71825.

85 In recent years, the Russian government enabled Russian State companies to hide public contracts in order to prevent these commercial suppliers from being targeted by US sanctions. We were therefore only able to review records listed on the Official government procurement website and third-party aggregator services. For more information, see https://www.themoscowtimes.com/2017/11/30/with-new-sanctions-looming-russian-state-firms-allowed-to-hide-public-contracts-a59762.

86 "ИНФОРМАЦИЯ О КОНТРАКТЕ № 0173100004813000801," zakupki.gov.ru, March 19, 2014, http://zakupki.gov.ru/epz/contract/contractCard/common-info.html?reestrNumber=0173100004813000801.

87 Official JSC Kobra catalogues list the English name as 'Design Skilled Office of Radio Equipment', however, the firm may also be referred to as 'JSC Experimental Design Bureau of Radio Equipment'. See JSC Kobra "Catalog: Science, Skill, Protection," http://kobra.su/include/documents/Catalog%20EN%202018.pdf.

88 "Корпоративная Газета ОАО "ВПО "ТОЧМАШ," vpotochmash.ru, Last modified June 1, 2009, http://vpotochmash.ru/catalog0007/2009_06_01.pdf.

89 "ШТОРА - 2 (НОВИНКА),"JSC KOBRA, http://kobra.su/catalog/statcionarnye/item/shtora-2/.

90 "Корпоративная Газета ОАО "ВПО "ТОЧМАШ," vpotochmash.ru, Last modified June 1, 2009, http://vpotochmash.ru/catalog0007/2009_06_01.pdf.

91 "Корпоративная Газета ОАО "ВПО "ТОЧМАШ," vpotochmash.ru, Last modified June 1, 2009, http://vpotochmash.ru/catalog0007/2009_06_01.pdf.

92 A video posted on the official JSC Kobra Youtube channel titled "Top Level Security" exclusively shows clips of the Russian head of state motorcade. See "Безопасность на высшем уровне," Youtube, Video File, Posted September 24, 2018, https://www.youtube.com/watch?v=kOU98VIaq9E.

93 RUB 4,300,000 per unit converted at July 18, 2014 exchange rate of USD .028/ 1 RUB, see https://www.bloomberg.com/quote/USDRUB:CUR for more information.

94 Единая информационная система, "ИНФОРМАЦИЯ О КОНТРАКТЕ № 0173100004813000801," zakupki.gov.ru, Last Modified March 19, 2014, http://zakupki.gov.ru/epz/contract/contractCard/common-info.html?reestrNumber=0173100004813000801.

95 Единая информационная система, "УПРАВЛЕНИЕ ВООРУЖЕНИЯ СЛУЖБЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ОХРАНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ (ОБОСОБЛЕННОЕ СТРУКТУРНОЕ ПОДРАЗДЕЛЕНИЕ)," zakupki.gov.ru, http://zakupki.gov.ru/epz/organization/view/info.html?organizationCode=03731000442.

96 Единая информационная система, "ИНФОРМАЦИЯ О КОНТРАКТЕ № 1231901933815000059," zakupki.gov.ru, Last Modified June 3, 2015, http://zakupki.gov.ru/epz/

contract/contractCard/document-info.html?reestrNumber=1231901933815000059.

[97] “Декларации о соответствии: ТС N RU Д-RU.МЛ66.В.00974 от 26.10.2016 действует до 25.10.2021,” Росаккредитации, https://pub.fsa.gov.ru/rds/declaration/view/6120395/historical-data.

[98] “Декларации о соответствии: ТС N RU Д-RU.МЛ66.В.00978 от 26.10.2016 действует до 25.10.2021,” Росаккредитации, https://pub.fsa.gov.ru/rds/declaration/view/5882324/historical-data.

[99] “ATC Surveillance Minimum Altitude Chart – ICAO”. Federal Air Transport Agency. November 9, 2017. http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/urff/1-ad2-rus-urff-059.pdf.

[100] “Instrument Approach Chart: Sochi, Russia,” Last Modified August 16, 2018, https://vatrus.info/files/caiga/1-ad2-rus-urss-104.pdf.

[101] Prohibited airspace in the Russian Federation is typically used over sensitive military and government locations to prevent civilian aircraft from flying near these facilities. For more information, see http://www.caiga.ru/common/AirInter/validaip/html/eng.htm.

[102] “ПРЕЗИДЕНТСКИЕ ДАЧИ В КРЫМУ,” RussianGate, Last modified June 2, 2017, http://russiangate.com/regiony/prezidentskie-dachi-v-krymu-/.

[103] “Резиденцию для Медведева перестраивают после отъезда Путина,” Izvestia. Last modified July 26, 2012, https://iz.ru/news/531337.

[104] “Новая охрана для Кавказа,” РБК, Last modified February 6, 2017, https://www.rbc.ru/newspaper/2017/02/07/589839d39a79472ff16eae15.

[105] “РАСПОРЯЖЕНИЕ СОВЕТА МИНИСТРОВ РЕСПУБЛИКИ КРЫМ,” Правительства Республики Крым, Last modified December 16, 2014, https://rk.gov.ru/rus/file/pub/pub_236639.pdf.

[106] “Из-за закрытого пляжа в Кацивели не едут туристы, местные - в отчаянии,” НОВОСТИ 24, Last modified June 21, 2016, https://www.crimea.kp.ru/daily/26544/3561422/.

[107] “ПРЕЗИДЕНТСКИЕ ДАЧИ В КРЫМУ,” RussianGate, Last modified June 2, 2017, http://russiangate.com/regiony/prezidentskie-dachi-v-krymu-/.

[108] Крымский канал, Telegram, March 13, 2018 05:29, https://t.me/fcpeshka/454.

[109] Grigoriy Bakunov, who investigated Moscow GNSS Spoofing activities in October 2016, concluded that the transmission infrastructure near the Kremlin simulates GPS and GLONASS signals at the L1 band and creates “noise” at the L2 and L5 bands. At the time, Bakunov believed that the spoofed signals originated from within the Kremlin. For more information, see Grigoriy Bakunov, “Почему Кремль во Внуково,” Telegram, October 19, 12:48, http://addmeto.cc/828.html.

[110] In September 2017, Amungo Navigation claimed to have used a directional antenna to show that the “GPS spoofer” is not in the Kremlin, as Bakunov had concluded, but is likely situated outside the Kremlin. In the investigation video, an individual operating what is believed to be Amungo Navigation’s XNZR Augmented Reality Direction Finder appears to record directional signal strength at 1572.72 MHz at various points along Kremlevskaya Embankment bordering the southern wall of the Kremlin. At several points in the video, the operator records interference signals originating from the northeastern corner of 34 Sofiyskaya Embankment, Building 1. For more information, see https://www.youtube.com/watch?v=yiy2Mt79M1c.

[111] See Bakunov, Grigoriy, Grigoriy Bakunov, “Почему Кремль во Внуково,” Telegram,

October 19, 12:48, http://addmeto.cc/828.html.

112 For more information, see Amungo Navigation, "XNZR is searching for Moscow GPS Spoofing Anomaly," Youtube, Video File, https://www.youtube.com/watch?v=yiy2Mt79M1c.

113 Rosreestr records for D. 3/5 Vozdvizhenka Street, Building 5; 34 Sofiyskaya Embankment, Building 1; D 4-10 Ipatyevskiy Lane, Building 1, Documents Held by Author.

114 Google Street View, Yandex Street View, Documents Held by Author.

115 Based on reporting from multiple confidential sources who reviewed the imagery and have experience in electronic warfare systems.

116 "New Civil Signals," GPS.gov, Accessed March 21, 2019, https://www.gps.gov/systems/gps/modernization/civilsignals/.

117 "Basics of Radio Frequencies for Quadcopter Drones," Droneflyers.com, Last modified November 17, 2014, https://www.droneflyers.com/basics-radio-frequencies-fpv-quadcopter-drones/.

118 Confidential Source.

119 Confidential Source.

120 Google Street View, Yandex Street View, Documents Held by Author.

121 Confidential Source.

122 Rosreestr for D. 3/5 Vozdvizhenka Street, Building 5 and 34 Sofiyskaya Embankment in Moscow. Documents Held by Author.

123 Rosreestr for D 4-10 Ipatyevskiy Lane, Building 1 in Moscow. Documents Held by Author.

124 "База ГИБДД," Nomber.org, Accessed January 25, 2019, http://nomer-org.me/mosgibdd/.

125 Yandex Street View, Documents Held by Author.

126 C4ADS cross-referenced ownership information listed on number-org.me with several publicly available Russian GIBDD databases.

127 Stephen Grey, Jason Bush and Roman Anin, "Billion-dollar medical project helped fund 'Putin's palace' on the Black Sea," Reuters, Last modified May 21, 2014, https://www.reuters.com/investigates/special-report/comrade-capitalism-putins-palace/.

128 Egor Skorbenko, "I went to the South of Russia: And it was controversial," Medium (blog), July 20, 2017, https://medium.com/@egorskorbenko/i-went-to-the-south-of-russia-dc02bd5bbb5c.

129 "Призрак дворца Путина охраняют призраки из ФСО: Сергей Колесников о том, что происходило в истории с дворцом премьер-министра после его открытого письма президенту," Novaya Gazeta, Last modified August 11, 2011, https://www.novayagazeta.ru/articles/2011/08/12/45422-prizrak-dvortsa-putina-ohranyayut-prizraki-iz-fso.

130 C4ADS also examined the possibility that the spoofing device used near Gelendzhik could be based on an air platform, as posited by others who have examined this subject (See http://www.thedrive.com/the-war-zone/13549/russia-may-be-testing-its-gps-spoofing-capabilities-around-the-black-sea). Using historical flight path data collected through ADS-B Exchange (https://www.adsbexchange.com/), we found that aircraft operated by the Russian Special Flight Detachment, tasked with providing transportation and communications support for the Russian head of state and government delegations, conduct regular support missions

over Gelendzhik, Sochi, Kerch, and Crimea. While we found that these aircraft, namely the Tu-214SR, conducted support missions over affected areas when we detected GNSS spoofing, we also found that spoofing took place independent of these aircraft being on-station. This could be the result of gaps in data or that these aircraft do not consistently broadcast ADS-B or Mode-S signals when conducting these missions. At this time, C4ADS has not found evidence to suggest that civilian or governmental aircraft are conducting GNSS spoofing activities near Gelendzhik.

[131] Paul D. Groves, Lei Wang, and Marek K Ziebart, “Shadow Matching: Improved GNSS Acuracy in Urban Canyons,” GPS World, Last modified February 1, 2012, https://www.gpsworld.com/wirelesspersonal-navigationshadow-matching-12550/.

[132] Stephen Grey, Jason Bush and Roman Anin, “Billion-dollar medical project helped fund ‘Putin’s palace’ on the Black Sea,” Reuters, Last modified May 21, 2014, https://www.reuters.com/investigates/special-report/comrade-capitalism-putins-palace/.

[133] Sergey Kolesnikov, “Open Letter,” Sergey Kolesnikov: Russia, Honor, Freedom (blog), December 21, 2010, http://skolesnikov.org/en/?page_id=73.

[134] Tim Whewell, “Putin’s palace? A mystery Black Sea mansion fit for a tsar,” BBC, Last modified May 4, 2012, https://www.bbc.com/news/magazine-17730959.

[135] Tim Whewell, “Putin’s palace? A mystery Black Sea mansion fit for a tsar,” BBC, Last modified May 4, 2012, https://www.bbc.com/news/magazine-17730959.

[136] “Призрак дворца Путина охраняют призраки из ФСО: Сергей Колесников о том, что происходило в истории с дворцом премьер-министра после его открытого письма президенту,” Novaya Gazeta, Last modified August 11, 2001, https://www.novayagazeta.ru/articles/2011/08/12/45422-prizrak-dvortsa-putina-ohranyayut-prizraki-iz-fso.

[137] Stephen Grey, Jason Bush and Roman Anin, “Billion-dollar medical project helped fund ‘Putin’s palace’ on the Black Sea,” Reuters, Last modified May 21, 2014, https://www.reuters.com/investigates/special-report/comrade-capitalism-putins-palace/.

[138] “Standard Departure Chart Instrument, Krasnodar, Russia,” Federal Air Transport Agency, Last modified July 20, 2017, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/urkk/1-ad2-rus-urkk-142.pdf.

[139] “Standard Departure Chart Instrument (SID)—ICAO: Krasnodar, Russia,” Federal Air Transport Agency, Last Modified July 20, 2017, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/urkk/1-ad2-rus-urkk-142.pdf.

[140] “Visual Approach Chart–ICAO: Sochi, Russia,” Federal Air Transport Agency, Last modified August 16, 2018, http://www.caiga.ru/common/AirInter/validaip/aip/ad/ad2/rus/urss/1-ad2-rus-urss-113.pdf.

[141] “Управляющие дворца Путина получают госдолжности, дома, гражданство и банки,” Navalny (blog), Last modified April 23, 2015, https://navalny.com/p/4214/.

[142] AIS data from a maritime risk analytics company.

[143] Clearspending, last accessed on March 21, 2019, https://clearspending.ru/supplier/inn=2317010308&kpp=231701001.

[144] AIS data from a maritime risk analytics company.

[145] AIS data from a maritime risk analytics company.

[146] Tax Identification Number: 2304062771.

147 Rosreestr Cadastral Number: 23:40:0703000:19, Documents Held by Author.

148 Rosreestr Cadastral Number: 23:40:0703000:18, Documents Held by Author.

149 Rosreestr Cadastral Number: 23:40:0703000:18, Documents Held by Author.

150 Экологическая Вахта, "(2011.02.11) СОБЫТИЯ НА "ДАЧЕ ПУТИНА" (полная версия)," YouTube, Video File, February 14, 2011, https://www.youtube.com/watch?v=BEfUcxOiBYE.

151 "Федеральная Служба Охраны: Президентский оркестр (офицеры и прапорщики)," Major-jim.narod.ru, Accessed March 21, 2019, http://major-jim.narod.ru/uniform_insignia/UniformEurope/Russia/Minestry/FsO/FsO/InsigniaFSO/InsigniaFSO-COO2.htm.

152 Tax Identification Number: 7709773660.

153 "ООО 'Комплекс,'" Коммерсантъ КАРТОТЕКА, Accessed March 21. 2019, https://www.kartoteka.ru/card/36daac35ab1a60b54075a5272cc95e46/214c2e9ab8199a70fa447448227bb427/.

154 "ООО 'КОМПЛЕКС,'" СПАРК-Профиль, Accessed March 21, 2019, https://www.dropbox.com/s/6r978teji5gxw8b/%D0%9E%D0%9E%D0%9E%20_%D0%9A%D0%9E%D0%9C%D0%9F%D0%9B%D0%95%D0%9A%D0%A1_%20-%20%D0%A1%D0%9F%D0%90%D0%A0%D0%9A-%D0%9F%D1%80%D0%BE%D1%84%D0%B8%D0%BB%D1%8C.pdf?dl=0.

155 "ООО 'ИнвестСтрой,''" Коммерсантъ КАРТОТЕКА, Accessed March 21, 2019, https://www.kartoteka.ru/card/eecedbb657035cc321cf2d7ff135422c/.

156 Алиса Кустикова and Роман Анин, "Дорога к храму привела к ФСО: Кто стоит за избиением экозащитника Андрея Рудомахи," Новая газета, April 1, 2018, https://www.novayagazeta.ru/articles/2018/04/02/76011-kto-stoit-za-izbieniem-ekozaschitnika-andreya-rudomahi-rassledovanie-novoy.

157 Александр Колпаков, "Хорошо живет на свете Колпаков," Руспрес, May 16, 2016, Accessed March 21, 2019, https://www.rospres.com/government/18245/.

158 Олег Ролдугин, "Тайны биографии нового главы Управделами президента Александра Колпакова," Собеседник, June 11, 2014, https://sobesednik.ru/rassledovanie/20140611-tayny-biografii-novogo-glavy-upravdelami-prezidenta-aleksand.

159 Алиса Кустикова and Роман Анин, "Дорога к храму привела к ФСО: Кто стоит за избиением экозащитника Андрея Рудомахи," Новая газета, April 1, 2018, https://www.novayagazeta.ru/articles/2018/04/02/76011-kto-stoit-za-izbieniem-ekozaschitnika-andreya-rudomahi-rassledovanie-novoy.

160 Military Unit 1473 (В/Ч 1473) is now referred to as Federal Budgetary Institution "UEI" (ФБУ УЭИ).

161 "УПРАВЛЕНИЕ ЭКСПЛУАТАЦИИ ИМУЩЕСТВА ОРГАНОВ ГОСУДАРСТВЕННОЙ ОХРАНЫ," Федеральное бюджетное учреждение, http://fbu-uei.ru/.

162 Олег Ролдугин, "Тайны биографии нового главы Управделами президента Александра Колпакова," Собеседник, June 11, 2014, https://sobesednik.ru/rassledovanie/20140611-tayny-biografii-novogo-glavy-upravdelami-prezidenta-aleksand.

163 "Колпаков Александр Сергеевич – Биография," Коммерсантъ, https://www.kommersant.ru/doc/3670677/w/kolpakov.

164 "Служба безопасности Президента (СБП)," Agentura.ru, Accessed March 21, 2019, http://www.agentura.ru/dossier/russia/fso/sbp/.

165 The cadastral number 23:40:0703000:19 listed on the alleged investment agreement corresponds to the Cape Idokopas Facility, Documents Held by Author.

166 Роман Анин, “Дворцовая площадь 740 тысяч квадратных метров перейти к обсуждению,” Новая газета, February 14, 2011, https://web.archive.org/web/20110218162606/https://www.novayagazeta.ru/data/2011/016/00.html.

167 Роман Анин, “Дворцовая площадь 740 тысяч квадратных метров,” Компромат, February 13, 2011, http://www.compromat.ru/page_30423.htm#ankor2.

168 Роман Анин, “Дворцовая площадь 740 тысяч квадратных метров,” Компромат, February 13, 2011, http://www.compromat.ru/page_30423.htm#ankor2.

169 “Treasury Sanctions Russian Officials, Members of the Russian Leaderships Inner Circle, And an Entity for Involvement in the Situation in Ukraine,” United States Department of the Treasury, Last modified March 20, 2014, https://www.treasury.gov/press-center/press-releases/pages/jl23331.aspx.

170 Олег Кашин, "Вот чего-чего, а контролеров у нас хватает," Коммерсант, Last modified April 20, 2011, https://www.kommersant.ru/doc/1625310.

171 Роман Анин, “«Тайны «Проекта Юг,»” Новая Газета, Last modified January 11, 2011, https://www.novayagazeta.ru/articles/2011/01/12/7376-tayny-171-proekta-yug-187.

172 “COUNCIL IMPLEMENTING REGULATION (EU) No 826/2014,” European Council, Last modified July 30, 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0826.

173 Kartoteka, Cyprus Commercial Registry, Documents Held by Author.

174 According to official records from the Russian company registry for Kompleks LLC and its shareholder JSC Binom, last consulted in February 2019, Ponomarenko appears to be the only natural person to own shares in Kompleks LLC through his shares in JSC Binom.

175 “UPDATE 1-Russian port Novorossiysk sets IPO range,” Reuters, Last updated October 22, 2007, https://uk.reuters.com/article/novorossiysk-ipo/update-1-russian-port-novorossiysk-sets-ipo-range-idUKL2238369200710 22.

176 “Бывшие владельцы НМТП заинтересовались покупкой госпакета порта,” Forbes, Last updated November 25, 2013, https://www.forbes.ru/news/247824-byvshie-vladeltsy-nmtp-zainteresovalis-pokupkoi-gospaketa-porta.

177 Roland Oliphant, “Friendly Oligarch Buys ‘Putin’ Palace,” The Moscow Times, Last updated March 3, 2011, https://www.themoscowtimes.com/2011/03/03/friendly-oligarch-buys-putin-palace-a5415.

178 In 2010, Sergey Kolesnikov accused Nikolai Shamalov of leading efforts to siphon off medical funds from the Russian Government for the construction of the Idokopas Palace.

179 “2018-014-Eastern Mediterranean Sea-GPS Interference,” United States Department of Transportation Maritime Administration, Last updated November 11, 2018, https://www.maritime.dot.gov/content/2018-014-eastern-mediterranean-sea-gps-interference.

180 David Duchet and Gerhard Berz, “GNSS RFI Mitigation: International Efforts to Protect Aviation,” The European Organization for the Safety of Air Navigation, Last updated September 24, 2018, https://www.gps.gov/cgsic/meetings/2018/duchet.pdf.

181 Joseph Trevithick, “The Russians Are Jamming US Drones in Syria Because They Have Every Reason to Be,” The Drive, Last modified April 10, 2018, http://www.thedrive.com/the-war-

zone/20034/the-russians-are-jamming-us-drones-in-syria-because-they-have-every-reason-to-be.

182 Elisabeth Braw, "The GPS Wars Are Here," Foreign Policy, Last Modified December 17, 2018, https://foreignpolicy.com/2018/12/17/the-gps-wars-are-here/.

183 Knut-Sverre Horn, "Støy fra Russland slo ut GPS-signaler for norske fly," NRK, Last modified October 5, 2017, https://www.nrk.no/finnmark/stoy-fra-russland-slo-ut-gps-signaler-for-norske-fly-1.13720305.

184 Mark Pomerleau, "Why Syria may be the most aggressive electronic warfare environment on Earth," C4ISRNet, Last modified April 24, 2018, https://www.c4isrnet.com/electronic-warfare/2018/04/24/socom-chief-syria-most-aggressive-ew-environment-on-earth/.

185 Courtney Kube, "Russia has figured out how to jam U.S. drones in Syria, officials say,“ NBC News, Last modified April 10, 2018, https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931.

186 Courtney Kube, "Russia has figured out how to jam U.S. drones in Syria, officials say,“ NBC News, Last modified April 10, 2018, https://www.nbcnews.com/news/military/russia-has-figured-out-how-jam-u-s-drones-syria-n863931.

187 David Duchet and Gerhard Berz, "GNSS RFI Mitigation: International Efforts to Protect Aviation," The European Organization for the Safety of Air Navigation, Last updated September 24, 2018, https://www.gps.gov/cgsic/meetings/2018/duchet.pdf.

188 "Moscow cements deal with Damascus to keep 49-year presence at Syrian naval and air bases," TASS, Last modified January 20, 2017, http://tass.com/defense/926348.

189 "On Syria, Russia digs in for the long haul with 'indefinite' deployment," Deutsche Welle, Last modified October 14, 2016, https://www.dw.com/en/on-syria-russia-digs-in-for-the-long-haul-with-indefinite-deployment/a-36038662.

190 Joseph Trevithick, "Russia Releases First Official Video of Its Su-57s on Their Absurdly Short Trip to Syria," The Drive, Last modified November 19, 2018, http://www.thedrive.com/the-war-zone/24997/russia-releases-first-official-video-of-its-su-57s-on-their-absurdly-short-trip-to-syria.

191 A documentary by Telekanal Zvezda on Khmeimim focuses solely on kinetic systems deployed at the Airfield. Footage of EW systems deployed at the airfield appears to be incidental. See Телеканал Звезда, "Военная приемка в Сирии. База Хмеймим. Часть 2,“ Youtube, Video File, June 11, 2017, https://www.youtube.com/watch?v=JDM2VI0Qp8o.

192 One potential example where videos of EW systems deployed at Khmeimim are no longer available: "Jamming the Jihad: Russian Electronic Warfare Systems Spotted in Syria," Sputnik News, Last modified October 5, 2015, https://sputniknews.com/world/201510051028033057-syria-russia-electronic-warfare-systems/.

193 David Axe, "How Russia Says it Swatted Down a Drone Swarm in Syria," Motherboard Vice, Last modified January 12, 2018, https://motherboard.vice.com/en_us/article/43qbbw/russia-says-it-swatted-down-drone-swarm-syria-isis.

194 "Head of the Russian General Staff's Office for UAV Development Major General Alexander Novikov holds briefing for domestic and foreign reporters," Ministry of Defence of the Russian Federation, Last modified January 11, 2018, http://eng.mil.ru/en/news_page/country/more.htm?id=12157872@egNews.

195 "Head of the Russian General Staff's Office for UAV Development Major General

Alexander Novikov holds briefing for domestic and foreign reporters,” Ministry of Defence of the Russian Federation, Last modified January 11, 2018, http://eng.mil.ru/en/news_page/country/more.htm?id=12157872@egNews.

196 Catherine Shu, “DJI adds much of Iraq and Syria to its list of no-fly zones for its drones,” Tech Crunch, Last modified April 26, 2017, https://techcrunch.com/2017/04/26/dji-adds-much-of-iraq-and-syria-to-its-list-of-no-fly-zones-for-its-drones/.

197 “Drone Drops Grenade on Munitions Dump in Stadium,” Drone Shield, https://www.droneshield.com/isis-use-drone-to-drop-grenade-on-tank-1/#.

198 “Krasukha-4 1RL257 broadband multifunctional jamming station electronic warfare system technical data sheet pictures video 10610156,” Army Recognition, Last modified October 6, 2015, https://www.armyrecognition.com/russia_russian_military_field_equipment/krasukha-4_1rl257_broadband_multifunctional_jamming_station_electronic_warfare_system_technical_data_sheet_pictures_video_10610156.html.

199 Roger N. McDermott, “Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum,” International Centre for Defence and Security, Last modified September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

200 Roger N. McDermott, “Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum,” International Centre for Defence and Security, Last modified September 2017, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

201 See 01:02, News-Front International, “Сирия: аэропорт Алеппо готов принимать и отправлять самолеты,“ YouTube, Video File, December 23, 2016, https://www.youtube.com/watch?v=CD1CF1OH70c.

202 Roger McDermott, “Moscow Deploys Latest Electronic Warfare Systems in Kaliningrad,” Jamestown Foundation, December 11, 2018, https://jamestown.org/program/moscow-deploys-latest-electronic-warfare-systems-in-kaliningrad/.

203 “Эксперты рассказали о принципах работы комплексов РЭБ «Самарканд,»” Izvestiya, October 28, 2018, https://iz.ru/805723/2018-10-28/eksperty-rasskazali-o-printcipakh-raboty-kompleksov-reb-samarkand.

204 Jonas Kjellèn, “Russian Electronic Warfare. The role of Electronic Warfare in the Russian Armed Forces,” Swedish Defense Research Agency, October 3, 2018, https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4625--SE.

205 Arthur Holland Michel, “Counter-Drone Systems,” The Center for the Study of the Drone, February 2018, https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf.

206 “UAV Interception System Was Shown at Army-2016 Forum,” Ruaviation.com. September 13, 2016, https://www.ruaviation.com/news/2016/9/13/6857/?h.

207 Yury Barmin, “Russia deployed state-of-the-art Krasukha-4 electronic warfare system to Syria. Krasukha is a jamming station,” October 5, 2015, https://twitter.com/russia_mideast/status/651066868522983425.

208 See 6:25, Телеканал Звезда, “Военная приемка в Сирии. База Хмеймим. Часть 2,“ Youtube, Video File, Posted June 11, 2017, https://www.youtube.com/watch?v=JDM2Vl0Qp8o.

209 Ult, “Russian Military Intervention and Aid to Syria #3 – Page 33,” Russiadefense.

net [Forum], October 24, 2015, http://www.russiadefence.net/t7301p800-russian-military-intervention-and-aid-to-syria-3.

210 David Hambling, “Frontline Tech: Satellite Navigation—Lost In Space?” Forces.net, August 27, 2018, https://www.forces.net/technology/frontline-tech-satellite-navigation-lost-space.

211 Paul McLeary, “Russia’s Winning the Electronic War,” Foreign Policy, October 21, 2015, https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/.

212 350 meters from Krasukha-4 location identified in this photo: https://i.imgur.com/1FzGWaA.jpg.

213 See 01:02, News Front International, “Сирия: аэропорт Алеппо готов принимать и отправлять самолеты,” YouTube, Video File, December 23, 2016, https://www.youtube.com/watch?v=CD1CF1OH70c.

214 “R-330Zh,” Rosoboronexport, Accessed March 20, 2019, http://roe.ru/eng/catalog/air-defence-systems/elint-and-ew-equipment/r-33ozh/.

215 Imagery of hangar constructed in February 2018 is not included in image below. For more information on the February 2018 hangar, see ImageSat International’s analysis published at: Ami Dombe, “Russia Expanding UAV Activity in Syrian Khmeimim Airbase,” Israeldefense.co.il, Last modified February 19, 2018, https://www.israeldefense.co.il/en/node/33123.

216 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/.

43.41420° N, 34.2846° E
34.1132° N, 32.7881° E
43.3040° N, 34.2288° E
33.1010° N, 44.2200° E
43.1220° N, 34.2865° E
34.2230° N, 33.9986° E
43.0943° N, 34.2939° E
34.2110° N, 33.9431° E
43.4444° N, 34.0313° E
36.3333° N, 44.4400° E
43.41
35.0130
43.4130° N, 34.2993° E
34.3000° N, 43.3239° E
43.4150° N, 34.4432° E
36.0143° N, 33.3300° E
35.0130° N, 34.3335° E
42.2341° N, 34.2993° E
41.5320° N, 32.2003° E
43.4130° N, 34.6871° E
35.1132° N, 34.3869° E
35.1232° N, 43.1234° E