**Have you been spoofed?**

Most people have been spoofed, but did not know it. Spoofing is the art of disguising communications by changing the identification of the real source to a third source. In recent years most people using email have received email purportedly from a known source, but in fact was a spoof to mislead. I, and most of my friends, have received requests for emergency money from a "friend", but it was actually from a scammer who was intended to be the real recipient, if I, or you, decided to send funds to help a friend who was in need.

In the world of foreign intrigue spoofing in communications is often used to misdirect security forces about the real location of a target. The target can be a person or persons of interest, or anything that needs to be eliminated by an armed drone.

The greatest spoofer in recent history is our old friend, **Vladimir Putin**. When he leaves home, his security team always travels in advance to protect him. When **Putin** travels to point A, anyone trying to track him electronically will be directed to point B (usually an airport). When he is at home, any electronic tracker will be spoofed to the wrong location. See Source:

Putin is under 24 hour electronic security, which always spoofs his location. The reason? National leaders, such as the popular Vladimir Putin, are always a target for drone assassination. So all VIPs need to be guarded 24/7/365 to stay alive.

We don't discuss this openly, but trust that our Secret Service is also electronically guarding whomever is our President, or Vice President, 24/7/365. We can assume that when our senior national leaders, civilian or military, are traveling, are also guarded 24/7 from a potential drone assassination attempt. Drones have put assassins with long rifles out of business. Tsk, tsk ...

**Source:**

**"Russia is Tricking GPS to Protect Putin," Elias Groll, *Foreign Policy*, April 3, 2019**

**Russia Is Tricking GPS to Protect Putin *The Kremlin’s manipulation of global navigation systems is more extensive than previously understood.***

**By** [**Elias Groll**](https://foreignpolicy.com/author/elias-groll/),  **April 3, 2019, *Foreign Policy***



***Russian President Vladimir Putin sunbathes during his vacation in the remote Tuva region in southern Siberia. The picture was taken between Aug. 1 and 3, 2017.***

Researchers at a Washington-based think tank have noticed that a funny thing happens whenever Russian President Vladimir Putin gets close to a harbor: The GPS of the ships moored there go haywire, placing them many miles away on the runways of nearby airports.

According to a new [report](https://foreignpolicymag.files.wordpress.com/2019/04/bcb4e-aboveusonlystars.pdf) by security experts with the group C4ADS, the phenomenon suggests that **Putin travels with a mobile GPS spoofing device** and, more broadly, that **Russia is manipulating global navigation systems on a scale far greater than previously understood**.

“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,” the report says.

As part of the Kremlin’s attempt to undermine the West’s military advantage in precision weaponry, the Russian military has made massive investments in electronic warfare, significantly increasing its ability to jam enemy communications that make possible U.S. ideas of networked warfare.

“Smart weapons need smart people to tell them smart things. They need positioning coordinates. They need navigation systems,” said Michael Kofman, a Russian military expert at CNA, a research organization. “The pace of operations requires constant access to data in real time,” and **the Russian military believes that electronic warfare “is part of the answer to U.S. dominance in precision weapons and airspace assault.”**

Russia has [pioneered](https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/) these technologies in Ukraine and Syria, jamming radio, GPS, and radar signals. In Syria, U.S. commanders have complained of an “aggressive electronic warfare environment,” and the U.S. military is now making moves to [upgrade](https://www.stripes.com/news/army-units-in-europe-first-to-get-electronic-warfare-upgrade-1.510688) its electronic warfare capabilities.

The Russian emphasis on electronic warfare extends to Putin’s personal security detail, which has embraced GPS spoofing as a way to protect the Russian leader against drone attacks. But the use of that spoofing technology can also be tracked and provides an unprecedented look at the effectiveness and scale of Russian electronic warfare capabilities.

Putin’s bodyguards are using what on its face is a counterintuitive approach to prevent assassination attempts by drone. The GPS spoofer that travels with Putin impersonates civilian GPS signals and provides the receiver with false coordinates for local airports. It chooses the coordinates of local airports because commercial drones typically come preprogrammed with safety mechanisms that make them automatically land or shut down when they enter the airspace of an airport.

In theory, drones operating near Putin will shut down or automatically land when they come within range of the spoofer. Fear of assassination by drone is a realistic one: Last year, Venezuelan President Nicolás Maduro [survived](https://www.bbc.com/news/world-latin-america-45073385) an attempt on his life that involved using drones to target him with explosives.

But Russia’s use of spoofing technology is having some surprising side effects. In September 2016, Putin [traveled](http://en.kremlin.ru/events/president/news/52900) to the Kerch Strait along with Prime Minister Dmitry Medvedev to inspect progress on a $4 billion bridge to the Russian mainland and meet with workers. While the two Russian leaders were there, the automatic identification systems of nearby ships—systems that rely in part on GPS—started reporting their locations as the Simferopol Airport about 125 miles away.

Two years later, Putin [returned](https://www.apnews.com/e507a38f44cf4cdc89ca9b14cd3dafef) to Kerch to lead a convoy of construction vehicles across the newly constructed bridge. Again, ships in the area reported strange location information, showing up at the Anapa Airport in mainland Russia.

By examining maritime location data, which is publicly available, researchers at C4ADS were able to provide the first estimate of the widespread impact of Russian spoofing activities. Between February 2016 and November 2018, C4ADS recorded 9,883 spoofing instances affecting 1,311 vessels, indicating that Russian spoofing is both more widespread and more indiscriminate than was previously understood.

“It’s really interesting because it helps us to understand the impact and look at who it impacts geographically,” Kofman said. “The challenge with electronic warfare is you can’t measure it.”

That number represents a minimum figure for the number of incidents of GPS spoofing, as it documents just one type of affected systems. The C4ADS report focuses on maritime GPS signals because of their easy availability, and other civilian systems that don’t broadcast their location publicly would likely be impacted as well.

The locations affected by GPS spoofing and documented by C4ADS include areas around Crimea, St. Petersburg, Moscow, in the far east of Vladivostok, and around Russian military bases in Syria.

C4ADS documented the deployment of anti-drone GPS spoofers in official Russian residences and unofficial government buildings, including an [Italianate palace on the Black Sea](https://www.bbc.com/news/magazine-17730959). The Kremlin has always denied that the palace is Putin’s, but the presence of the system suggests otherwise. C4ADS was able to determine that a GPS spoofer is in near-constant operation on or near the grounds of the palace.

The researchers also found the technology deployed at Russia’s military base in Syria, which militant groups have attacked with drones.

There is no indication that Russian GPS spoofing has caused direct civilian harm—yet. This year, GPS jamming [kept](https://www.tv2.no/nyheter/10397144/) an ambulance plane out of operation in northern Norway, and Russia’s neighbors have recently complained bitterly about the interference.

During last year’s NATO exercises in Scandinavia, pilots reported experiencing problems with their GPS systems. “This is not a joke. It threatened the air security of ordinary people,” [said](https://www.bbc.com/news/world-europe-46178940) Finnish Prime Minister Juha Sipila, an [experienced pilot](https://www.thejournal.ie/finland-prime-minister-flies-own-plane-3329158-Apr2017/) who sometimes flies his own plane on government business.

Norwegian intelligence later [traced](https://thebarentsobserver.com/en/security/2019/02/stoltenberg-condemns-gps-jamming-border-region-he-was-first-get-visa-freedom) the jamming to the Russian military.

The Russian military isn’t alone in practicing to jam GPS signals. This year, the U.S. military [warned](https://theaviationist.com/2019/02/08/basically-carrier-strike-group-4-is-jamming-gps-across-u-s-southeast-coast/) that GPS interference exercises would likely affect systems across a huge swath of the southeastern United States. It’s unclear exactly what technical systems the U.S. Secret Service uses to protect American leaders from drone threats.

Such activity illustrates just how vulnerable GPS systems are to manipulation. Security researchers have [pointed out](https://www.spirent.com/blogs/positioning/2017/september/defcon-25) for years that such systems can be [easily spoofed](https://arstechnica.com/information-technology/2018/07/a-225-gps-spoofer-can-send-autonomous-vehicles-into-oncoming-traffic/), and it isn’t clear that the manufacturers of such systems are taking countermeasures to protect them.

GPS systems have become nearly ubiquitous in the modern economy, deployed in smartphones, cars, and industrial control systems. The U.S. electric grid, for example, uses GPS for a [variety of purposes](https://www.gps.gov/cgsic/meetings/2016/silverstein.pdf).

With the advent of software-defined radios, spoofing GPS signals has become both easy and cheap. According to C4ADS, the cost of the equipment used to spoof a GPS signal is about $350, down from about $10,000 a few years ago.

“The proliferation potential and the technology used to conduct this activity presents a unique threat. You could hypothetically outfit illicit actors to deploy elsewhere,” the author of the C4ADS report told FP, who spoke on condition of anonymity, fearing possible Russian retaliation.

There is evidence such activity is already taking place. In 2015, U.S. government officials [cautioned](https://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/) that drones deployed along the U.S.-Mexico border were seeing their GPS systems spoofed, probably by drug cartels.

**Elias Groll** is a staff writer at Foreign Policy.