Russia Accused of Jamming GPS Signals During Major NATO Wargames

13 Nov 2018

Russia has been accused of disrupting the satellite signals vital to the operation of the Global Positioning System (GPS) during a major NATO military exercise last week, moving the Russian government to deny involvement.

The ability to receive GPS signals — the near ubiquitous U.S. satellite system widely used in both military and civilian applications for navigation — was impaired by a significant jamming effort across northern Finland last week, as the largest NATO wargames since the end of the Cold War took place in the area.

According to NATO figures, 50,000 people took place in exercise Trident Juncture, which saw 250 aircraft, 65 ships and boats, and 10,000 vehicles deployed for training.

Russia has been blamed for the attempt to disrupt the exercise by knocking out navigation systems, which Britain’s Times newspaper reported was a “massive” interference.

The disruption of GPS signals did not only impact the military exercise, with airline pilots in the area resorting to back-up navigation systems, and personal GPS systems in smartphones and cars also being affected.

Finnish prime minister Juha Sipilä was one who pointed the finger of blame at Russia, remarking Sunday: “Disrupting radio signals in open space is technically relatively easy and yes, it is possible that Russia is involved in the disruption in this case… Russia is known to possess such capabilities. This is not a joke, it threatened the air security of ordinary people.”

A Kremlin spokesman denied knowledge of the interference and claimed: “There is a tendency nowadays to accuse Russia of all sins, mortal or otherwise.”

AFP reported Norwegian authorities have experienced GPS outages during military exercises before, such as during Russia’s Zapad exercise in 2017. Industry magazine GPS World has also written of widescale so-called GPS spoofing in the Black Sea in 2017 near to Russian territory, causing ships’ computers in the area to believe they were miles away from their actual location.

In October 2017, NATO troops stationed Poland and the Baltic claimed their smartphones were being targeted by hackers, with attacks traced back to Russian Internet Protocol addresses.
The military utility of GPS spoofing and disruption has long been discussed and follows a long tradition of electromagnetic warfare including Radar countermeasures that stretch back to the Cold War.

The potential consequences of such an attack were dramatically underlined last week when a modern Spanish-built frigate of the Norwegian navy was rammed by a Maltese-flagged tanker. While the commercial ship suffered only light damage, the frigate started taking water and was grounded to permit the evacuation of its crew, finally sinking five days later.

GPS is increasingly relied upon by merchant vessels for navigation which now typically go to sea with historically low crewing levels to save money, reducing the number of sailors available to keep watch for danger. In the crowded waterways of Northern Europe shared between civilian and military traffic, GPS disruption and spoofing could be a potent weapon in the future.

A full investigation has not yet been conducted into the situation leading up to the collision and it is not known whether GPS was involved in the incident.

*Oliver JJ Lane is the editor of Breitbart London — Follow him on Twitter and Facebook*