GPS Spoofing Patterns Discovered

BY MARK B. GOWARD TO THE SOUTH

Examination of global ship tracking data for the last two years has shown several instances of multiple vessels reporting their locations as being on land or at airports for times when the ships were operating at sea.

"We first became interested in this problem in June when a vessel reported in the Black Sea (see image 1) GPS signals showing its location at the Gelendzhik airport, about 25 miles from its real location," said Dana A. Goward, President of the non-profit Resilient Navigation and Timing Foundation. "We provided photographs of equipment and other information that convinced experts his GPS receiver was being deliberately spoofed."

About 20 other vessels in the area were reported to be similarly affected.

"Sporadic" GPS receivers are a technology of luster GPS signals to cause it to provide incorrect time or location information. "Jamming" is blocking reception of GPS with strong signals and is easier and more common than spoofing.

"In July, we followed up on the June report and found evidence that, for some in the Black Sea, GPS signals were still being deliberately disrupted. We then contacted Windward Ltd., a leader in maritime data and analysis to investigate further," said Goward.

By running the data algorithms an data from vessels "Automatic Identification System (AIS), Windward experts identified two additional instances of mass GPS interference in 2017, looking for several weeks.

"Because we see the same distortion patterns in multiple vessels and in specific areas, it appears that the issue is GPS rather than AIS disruption and is therefore likely to affect everything in the area, not just ships," said Mark Peled, Go-Reader of Windward.

"Most interestingly, all three locations involve airports: Gelendzhik airport and Bill and International Airport near the Sochi, and an International airport near the Gelendzhik. We looked and found that some of the ships that initially reported in Sochi airport were really located near Gelendzhik, about 250 kilometers (125 miles) away. By October we were even more sure and located several vessels at Sochi airport and 20 kilometers (12 miles) from their actual positions near the Sochi airport," said Peled.

"These incidents dovetail with reports people in lullaway through the weather other that GPS receivers receiving their position from a vessel's 'Dynamics of vessels' airport, about 25 miles away," said Goward. "We don't know where all these false signals are coming from, or the motivation behind them. From a safety perspective, it is far better for them to cease being so as to provide erroneous information. Most people probably realize right away, for them encountering or not working properly or not at all. When subtle errors caused by spoofing visual results than for GPS who are involved in marine navigation and safety.

While spoofing GPS takes more sophisticated equipment than jamming, the equipment is readily available. In 2015 a Chinese researcher at a University in China provided instructions to build a spoofing device and sold kits for 300. "Reports made "GPS signal generation" are now available on the Internet and are very popular with Pakistan-GPS enthusiasts. They are used to trick cell phones into collecting geolocation from network towers without having to physically be there."

"The real lesson from all of this," according to Goward, "is that GPS signals can be easily spoofed. Users should beware and take precautions."

One precaution users might take while in Russia and some other parts of the world is using GPS signals in combination with terrestrial Loran-C or Chayka. The land-based electronic navigation system operates at very high power and is nearly impossible to disrupt. Russia, China, South Korea, Saudi Arabia and India operate such systems. The United States has said it will build an eLoran system, and eLoran is reportedly very high power and is nearly impossible to disrupt. Russia, China, South Korea, Saudi Arabia and India operate such systems. The United States has said it will build an eLoran system, and eLoran is reportedly very high power and is nearly impossible to disrupt. Russia, China, South Korea, Saudi Arabia and India operate such systems. The United States has said it will build an eLoran system, and eLoran is reportedly very high power and is nearly impossible to disrupt. Russia, China, South Korea, Saudi Arabia and India operate such systems. The United States has said it will build an eLoran system, and eLoran is reportedly very high power and is nearly impossible to disrupt. Russia, China, South Korea, Saudi Arabia and India operate such systems. The United States has said it will build an eLoran system, and eLoran is reportedly very high power and is nearly impossible to disrupt. Russia, China, South Korea, Saudi Arabia and India operate such systems. The United States has said it will build an eLoran system, and eLoran is reportedly very high power and is nearly impossible to disrupt. Russia, China, South Korea, Saudi Arabia and India operate such systems. The United States has said it will build an eLoran system, and eLoran is reportedly very high power and is nearly impossible to disrupt.