Cyber Threats Prompt Return of Radio for Ship Navigation

Posted by Eric Haun August 7, 2017

© donvictorio / Adobe Stock

The risk of cyber attacks targeting ships' satellite navigation is pushing nations to delve back through history and develop back-up systems with roots in World War Two radio technology.

Ships use GPS (Global Positioning System) and other similar devices that rely on sending and receiving satellite signals, which many experts say are vulnerable to jamming by hackers.

About 90 percent of world trade is transported by sea and the stakes are high in increasingly crowded shipping lanes. Unlike aircraft, ships lack a back-up navigation system and if their GPS ceases to function, they risk running aground or colliding with other vessels.

South Korea is developing an alternative system using an earth-based navigation technology known as eLoran, while the United States is

planning to follow suit. Britain and Russia have also explored adopting versions of the technology, which works on radio signals.

The drive follows a series of disruptions to shipping navigation systems in recent months and years. It was not clear if they involved deliberate attacks; navigation specialists say solar weather effects can also lead to satellite signal loss.

Last year, South Korea said hundreds of fishing vessels had returned early to port after their GPS signals were jammed by hackers from North Korea, which denied responsibility.

In June this year, a ship in the Black Sea reported to the U.S. Coast Guard Navigation Center that its GPS system had been disrupted and that over 20 ships in the same area had been similarly affected.

U.S. Coast Guard officials also said interference with ships' GPS disrupted operations at a port for several hours in 2014 and at another terminal in 2015. It did not name the ports.

A cyber attack that hit A.P. Moller-Maersk's IT systems in June 2017 and made global headlines did not involve navigation but underscored the threat hackers pose to the technology dependent and inter-connected shipping industry. It disrupted port operations across the world.

The eLoran push is being led by governments who see it as a means of protecting their national security. Significant investments would be needed to build a network of transmitter stations to give signal coverage, or to upgrade existing ones dating back decades when radio navigation was standard.

U.S. engineer Brad Parkinson, known as the "father of GPS" and its chief developer, is among those who have supported the deployment of eLoran as a back-up.

"ELoran is only two-dimensional, regional, and not as accurate, but it offers a powerful signal at an entirely different frequency," Parkinson told Reuters. "It is a deterrent to deliberate jamming or spoofing (giving wrong positions), since such hostile activities can be rendered

ineffective," said Parkinson, a retired U.S. airforce colonel.

Korean Stations

Cyber specialists say the problem with GPS and other Global Navigation Satellite Systems (GNSS) is their weak signals, which are transmitted from 12,500 miles above the Earth and can be disrupted with cheap jamming devices that are widely available.

Developers of eLoran - the descendant of the loran (long-range navigation) system created during World War II - say it is difficult to jam as the average signal is an estimated 1.3 million times stronger than a GPS signal.

To do so would require a powerful transmitter, large antenna and lots of power, which would be easy to detect, they add.

Shipping and security officials say the cyber threat has grown steadily over the past decade as vessels have switched increasingly to satellite systems and paper charts have largely disappeared due to a loss of traditional skills among seafarers.

"My own view, and it is only my view, is we are too dependent on GNSS/GPS position fixing systems," said Grant Laversuch, head of safety management at P&O Ferries. "Good navigation is about cross-checking navigation systems, and what better way than having two independent electronic systems."

Lee Byeong-gon, an official at South Korea's Ministry of Oceans and Fisheries, said the government was working on establishing three sites for eLoran test operations by 2019 with further ones to follow after that.

But he said South Korea was contending with concerns from local residents at Gangwha Island, off the west coast.

"The government needs to secure a 40,000 pyeong (132,200 square-metre) site for a transmitting station, but the residents on the island are strongly opposed to having the 122 to 137 meter-high antenna," Lee told Reuters.

In July, the United States House of Representatives passed a bill which included provisions for the U.S. Secretary of Transportation to establish an eLoran system.

"This bill will now go over to the Senate and we hope it will be written into law," said Dana Goward, president of the U.S. non-profit Resilient Navigation and Timing Foundation, which supports the deployment of eLoran.

"We don't see any problems with the President (Donald Trump) signing off on this provision."

The previous administrations of Presidents George W. Bush and Barack Obama both pledged to establish eLoran but never followed through. However, this time there is more momentum.

In May, U.S. Director of National Intelligence Daniel Coats told a Senate committee the global threat of electronic warfare attacks against space systems would rise in coming years.

"Development will very likely focus on jamming capabilities against ... Global Navigation Satellite Systems (GNSS), such as the U.S. Global Positioning System (GPS)," he said.

Spoofing Dangers

Russia has looked to establish a version of eLoran called eChayka, aimed at the Arctic region as sea lanes open up there, but the project has stalled for now.

"It is obvious that we need such a system," said Vasily Redkozubov, deputy director general of Russia's Internavigation Research and Technical Centre.

"But there are other challenges apart from eChayka, and (Russia has) not so many financial opportunities at the moment."

Cost is a big issue for many countries. Some European officials also say their own satellite system Galileo is more resistant to jamming than other receivers.

But many navigation technology experts say the system is hackable. "Galileo can help, particularly with spoofing, but it is also a very weak signal at similar frequencies," said Parkinson.

The reluctance of many countries to commit to a back-up means there is little chance of unified radio coverage globally for many years at least, and instead disparate areas of cover including across some national territories and shared waterways.

The General Lighthouse Authorities of the UK and Ireland had conducted trials of eLoran but the initiative was pulled after failing to garner interest from European countries whose transmitters were needed to create a signal network.

France, Denmark, Norway and Germany have all decided to turn off or dismantle their old radio transmitter stations.

Britain is maintaining a single eLoran transmitter in northern England.

Taviga, a British-U.S. company, is looking to commercially operate an eLoran network, which would provide positioning, navigation and timing (PNT).

"There would need to be at least one other transmitter probably on the UK mainland for a timing service," said co-founder Charles Curry, adding that the firm would need the British government to commit to using the technology.

Andy Proctor, innovation lead for satellite navigation and PNT with Innovate UK, the government's innovation agency, said: "We would consider supporting a commercially run and operated service, which we may or may not buy into as a customer."

Current government policy was "not to run large operational pieces of infrastructure like an eLoran system", he added.

(By Jonathan Saul; Additional reporting by Terje Solsvik, Jacob Gronholt-Pedersen, Yuna Park, Gleb Stolyarov, Sophie Louet,

Madeline Chambers and Mark Hosenball; Editing by Pravin Char)
• United States • Norway • West Coast