U.S. Customs and Border Protection

Customs-Trade Partnership Against Terrorism

Alert

Conveyance Security Exposure
GPS Jamming Devices and Unmanifested Cargo Introduction

The Customs-Trade Partnership Against Terrorism (C-TPAT) program is one layer in U.S. Customs and Border Protection's (CBP) multi-layered cargo enforcement strategy. Through this program, CBP works with the trade community to strengthen international supply chains and improve United States border security.

To enhance communication with its members, C-TPAT routinely highlights security matters for the purpose of raising awareness, renewing Partners' vigilance, and recognizing best practices implemented to address supply chain security concerns.

Example of a GPS Jamming Device

The purpose of this C-TPAT Alert, generated in cooperation with BSI Supply Chain Solutions, is to highlight the increased use of Global Positioning System (GPS) jamming devices to disrupt supply chains in many countries around the world. GPS jamming devices pose a serious risk to conveyance security, as the integrity of a shipment may be compromised without the knowledge of the importer or the transportation company. GPS jamming devices are used to disable tracking devices installed on cargo trucks and temporarily remove vehicles from monitoring systems. When a tracking device "goes dark," it could be an indication of theft, contraband introduction, or other illicit activity affecting the goods carried inside a container or trailer.

BSI has recorded the use of GPS jammers in every region of the world. GPS jamming devices are inexpensive and easy to acquire, increasing their appeal to criminals. While these devices have been most commonly used for cargo theft purposes, the ability of a jammer to conceal the location of a shipment demonstrates that these items may be used to carry out any number of illicit activities including the smuggling of illegal drugs, weapons, stowaways, or other contraband.

Furthermore, the increased use of GPS jamming devices highlights the constantly evolving tactics of cargo criminals. Thieves and smugglers are constantly developing new modus operandi in order to carry out their criminal schemes. As the use of GPS tracking systems becomes more prevalent worldwide, the use of jamming devices for cargo disruption purposes will very likely increase as well, underscoring the need to implement robust supply chain security protocols to protect the integrity of in-transit consignments.

Background

GPS jammers work by emitting a strong electromagnetic signal that interferes with the connection between GPS satellites and a tracking device placed inside a cargo shipment or attached to a vehicle. Jamming devices (or "jammers") typically have multiple antennas that emit signals at different frequencies, increasing the chance the jammer will successfully interfere with a tracker placed in a shipment or vehicle.

Most commercially available GPS jammers have an effective range of only a few feet, meaning they must be placed within a consignment in order to disrupt the tracking signal. However, thieves have used more powerful, long-range jammers that enable them to trail in-transit goods using a car or other mobile platform and block the shipment's GPS signal for miles.

Consumer GPS jammers can be easily purchased online for as little as $60 - $100 depending on the sophistication of the model. Some models of GPS jamming devices have a multi-frequency system capable of blocking cellular and radio frequencies and jam (prevent) communication between the driver and his superiors and law enforcement authorities.

The legality of GPS jamming devices varies depending on the country, although the items are illegal to use in most developed nations. **GPS jammers are illegal to market, sell, or operate in the United States**. However, the U.S. government has not prosecuted any individuals for signal jamming, and it remains to be seen if criminals who use jammers to conduct cargo theft will be charged under anti-jamming laws. Canada and Australia have laws similar to the United States, banning the sale or use of GPS jammers. In the United Kingdom, the purchase of jammers is legal, although the devices' use is prohibited. Laws in Brazil also restrict the use of GPS jammers, but reports also cite the ease of acquiring the device.

Several incidents have been recorded in multiple countries, including Mexico, the United States, Italy, and most countries of South America, in which thieves have used GPS jamming devices to hijack cargo trucks.

GPS Jammers and Un-manifested Cargo Introduction

The use of GPS jamming devices poses a serious threat to international supply chains. From a cargo theft perspective, the nature of GPS jammer usage increases the risk that large-quantity, high-value shipments will be stolen in a single theft attempt. Cargo thieves primarily use jammers to steal entire truckloads of goods and delay law enforcement's response efforts to recover the stolen items and apprehend the suspects. The use of GPS jammers for high-value thefts is exacerbated by the relative ease with which the jammers can be acquired and the lack of clear legal consequences for using the devices for theft in many countries.

In addition to their use in cargo theft schemes, GPS jammers pose other risks that could threaten the integrity of a company's supply chains and make it more vulnerable to the introduction of contraband. Most notably, any time that a jamming device is used and a shipment is "off the grid", the company is no longer able to track the security of the goods contained in the consignment. While the most notable example of a breach in cargo integrity is a theft, the possibility exists that criminal organizations may use GPS jammers to introduce contraband goods, including illegal drugs or small arms, into a diverted consignment for smuggling abroad. Countries with the highest rate of GPS jamming device usage generally suffer from elevated, high, or severe threats of un-manifested cargo introduction, or the risk posed to supply chains by the introduction of illegal drugs, arms and weapons, and stowaways.

Conveyance Tracking and Monitoring Procedures

Conveyance security is a major component of the C-TPAT program. C-TPAT carriers are required to practice and implement security procedures to prevent the un-manifested introduction of contraband into legitimate shipments of goods. Conveyance tracking and monitoring procedures fall under the overall conveyance security umbrella and require carriers to use a driver log or a GPS tracking device to maintain the integrity of the shipment. Carriers must also establish predetermined routes and have drivers notify the dispatcher of any deviations in the route due to weather or traffic. Under conveyance tracking and monitoring procedures, random route checks should be conducted and documented to verify the time between points including the loading or pickup site and delivery destinations. The management of the carrier should conduct random, but documented audits to ensure that logs are properly maintained and conveyance monitoring and tracking procedures are being followed. Drivers must also report any suspicious conveyance security activity.

C-TPAT Partners are encouraged to implement the following recommendations to protect shipments from GPS jamming devices and mitigate the threat of un-manifested cargo introduction:

- Audit transportation suppliers to ensure compliance of conveyance security requirements.
- Ensure conveyance tracking and monitoring protocol has been established and followed.
- Investigate loss of GPS signal from cargo shipments that disappear from monitoring system.
- Report suspicious conveyance security activity to your Supply Chain Security Specialist

CBP.GOV/CTPAT
1300 Pennsylvania Avenue, NW
Washington, DC 20229

(202) 344-1180
Industry.partnership@dhs.gov