Corporate Risk Services

Intelligence Bulletin


# Supply Chain: Defeating the Security Watchdog

***The Threat of GPS Jamming Technology and Recommendations to Protect your Business***

## Executive Summary

Companies can achieve a state of heightened security awareness through compliance with both domestic and/or international regulations. Examples include Customs-Trade Partnership Against Terrorism (C-TPAT) and the completion of third-party reviews — facility risk assessments, employee background checks, and due diligence assessments of third-party vendors.

To truly safeguard cargo from production to distribution, however, the use of global positioning systems (GPS) has shown to be a deterrent to cargo theft and invaluable in recovering lost cargo. Many times, recovery takes place within minutes or a few hours of an occurrence if there is dedicated tracking and it is done in real-time.

Even with the adoption of enhanced security awareness and protection, cargo theft is constantly under reported, if reported at all.

This is based on the following factors:

- Loss of reputation
- Loss of business
- Financial loss
- Unexplainable circumstances
- Fear of termination
- Employee belief that GPS is invasion of privacy
- Avoidance of Quality Control Audits

As supply chains expand and technology advances, thieves will adapt and attempt to circumvent tracking. In many instances, thieves use electronic jamming to counter tracking devices or simply remove devices. Additionally, even with advancing technology, challenges in battery life, reliability, transmitting and area coverage all result in limitations.

## Background and Concern

In North America, cargo theft has developed into a big business that services several criminal sectors. Correspondingly, modern thieves are increasingly transnational, sophisticated, organized and generally not home grown. Cargo crime finances the activities of violent gangs, such as Mara Salvatrucha (MS-13).

In Canada, cargo crime is developing into a major activity for the Chinese Triad criminal organization. Additionally, cargo theft organizations may funnel money to terrorist organizations to finance attacks against North America, specifically the United States. These organized crime syndicates have proven to be adaptive, bold and violent.

Driven by insurance and regulatory requirements with the necessity of item identification, the pharmaceutical and electronics industries were early adopters of tracking technology in the private sector. The U.S. government routinely collaborates with private industry for new technologies to improve efficiency and productivity, increase global connectivity and enhance freight system performance and security.

New technologies currently enhance:

- Asset tracking
- On-board status monitoring
- Gateway facilitation
- Freight status information
- Network status information

With new technology comes new vulnerabilities. The advancing and increasingly available technology for commercial and private use is also enabling cargo thieves — using technology that once was only available to governments — to interdict cargo shipments and commercial carriers.

## Vulnerabilities

Commercial GPS has very low signal power. Since this signal is much weaker (equating to the same electrical power required to power a light bulb), it is more common to block the signal from the GPS satellite. GPS transmits on a civil frequency and has a well-known signal structure, making it an easy target for jamming and denying accuracy. The civilian signal (C/A-code) is short, well-known, and already widely available on several GPS signal generators.

As recent as 2015, major simplex data networks used for GPS tracking satellites do not encrypt data between tracking devices, satellites and ground stations. Additionally, the networks do not require the data be authenticated for legitimacy. Thus, the signal can be intercepted, jammed or spoofed.

For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310

# Supply Chain: Defeating the Security Watchdog

## Corporate Risk Services

Failure to report cargo theft is a vulnerability within the supply chain. Often considered an insurance problem, cargo theft may not be reported because of negative public perception of the cargo carrier's or contracting company's security standards, procedures and training.

Perceived supply chain weakness that could give competitors a strategic advantage may encourage wholesalers and retailers to not acknowledge that they were victims. Furthermore, cargo insurance may be insufficient and exclude coverage under certain conditions or in certain geographic areas.

Another vulnerability is the way GPS technology is used. Some are content, for insurance and compliance purposes, to simply "have" GPS. Oftentimes, however, vehicle GPS tracking systems are not monitored. A recent example involves a the ambush of a truck convoy. No one was monitoring the trucks to see that they were stopped in the middle of the highway. A third truck drove to the destination unaware of what had happened and no one communicated with the driver about the ambush.

The company responsible for monitoring the GPS system had a tracking computer in the corner of a room and was one of more than a dozen tasks for the operator. When the trucks and trailers were stripped of their GPS equipment, the monitoring center finally realized something was not right, but the cargo was gone.

GPS monitoring centers must be tested and monitored to ensure they are not compromised. In places such as Brazil, Mexico and South Africa, monitoring centers are sometimes attacked simultaneously when monitoring personnel are threatened and coerced within the center.

Criminals demand that employees "look the other way" or threaten to target employee families. It is important for the monitoring centers to be able to perform their function effectively.

### GPS Monitoring Threats

There are three key threat vectors for GPS monitoring:

#### 1) Unintentional Interference

- Radio Frequency Interference (RFI)
- Ionospheric; Solar Max
- Spectrum Congestion

#### 2) Intentional Interference

- Jamming
- Spoofing – Counterfeit Signals

#### 3) Human Factors

- User Equipment & GPS Satellite Design Errors
- Lack of Knowledge/Training
- Over-Reliance

### ELECTROMAGNETIC INTERFERENCE (EMI) DEVICES

The greatest persistent and adapting threat is Intentional Interference. It remains easier and more efficient to mask tracking signals vice attempting to locate and remove or disable the tracking device.

Electromagnetic Interference (EMI) devices are used by thieves, unprincipled employees and privacy-conscious citizens to jam GPS signals within defined areas.

The "jamming" threat is the most prevalent form used in cargo thefts. Jamming devices come in various sizes and power, they require no technical expertise to operate, and are available on the internet for less than $50.

Some are small and mobile and can be plugged into a vehicle's auxiliary power adaptor outlet, such as the cigarette lighter. These have a range of approximately 30-65 feet. This makes it difficult for law enforcement to locate and identify the devices.

More robust jammers can disrupt GPS and other local frequencies over distances ranging from about 980 feet to more than five miles, depending on signal strength.

The Federal Bureau of Investigation (FBI) advises that mid-sized and larger jammers will mask the spectrum of GPS, cellphone, Wi-Fi, and other signals and thus also prevent the tracker from wirelessly reporting any location or status data.

For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310

## COMMON JAMMING DEVICES

### Multi Antenna Based Units

### Small Mobile Short Range Jammers

### Vehicle Mounted Short Range Jammers


For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310

# Supply Chain: Defeating the Security Watchdog

## Corporate Risk Services

### Eight Antenna (Multi Signal) Suitcase Jamming Device

A sophisticated eight antenna (multi signal) jamming device built into a suitcase. One such "serious kit" was recently used by a British drug courier in 2016.

### Russian GPS Jammer

This device is available on the open market.

Most freight carriers now use GPS tracking devices on their trucks and shipments. Criminals require the trackers to be disabled long enough to evade the crime scene or hide their contraband inside the cargo prior to returning the truck to the supply chain.

Many times, cargo thieves only need to disable the GPS tracker long enough to decouple and drop the trailer, then switch tractors before driving away.

Law enforcement continues to report that during cargo theft recoveries, jammers are found in the vehicle or nearby.

The timeline of recent incidents indicates a growing understanding of the viability and ease of jamming GPS tracking devices:

- As early as 2008, British police reported criminals possessing jamming equipment. It is believed that possession was a result of criminals adapting to previous use of vehicle-tracking evidence in successful prosecutions.
- In 2009, electronics engineers at Newark Liberty International Airport reported that satellite-positioning receivers for a new navigation aid would routinely lose signal at specific times. An Federal Aviation Administration (FAA) investigation discovered a local truck driver had installed a jammer in his vehicle. The driver used the jammer to hide his movements from his employer tracking. The airport's systems would temporarily fail when he routinely passed the airport.
- In July 2010, British police reported that two men were jailed for a total of 16 years after they admitted to being members of a gang that stole 40 trucks and their cargo with a total value of $9.6m. They used GPS jammers to prevent the vehicles from being tracked after the thefts. In Germany, some truck drivers have used jammers to evade the country's GPS-based road-tolling system.
- In September 2012, the Department of Homeland Security (DHS) reported that it took the FAA and Federal Communications Commission (FCC) two years (March 2009 - April 2011) to locate a GPS jammer operated by a trucker on the New Jersey Turnpike.
- In August 2013, the FCC reported that a New Jersey man, using a GPS jammer in his company pickup truck to hide from his employer, interfered with an air traffic control system tracking system at Newark Liberty International Airport. The jammer was available online for less than $100.
- On Oct. 2, 2014, the FBI reported cargo theft groups using jammers to mask GPS tracking devices.
  - In 46 reported incidents, the thieves placed one or more GPS jammers in cargo containers with stolen

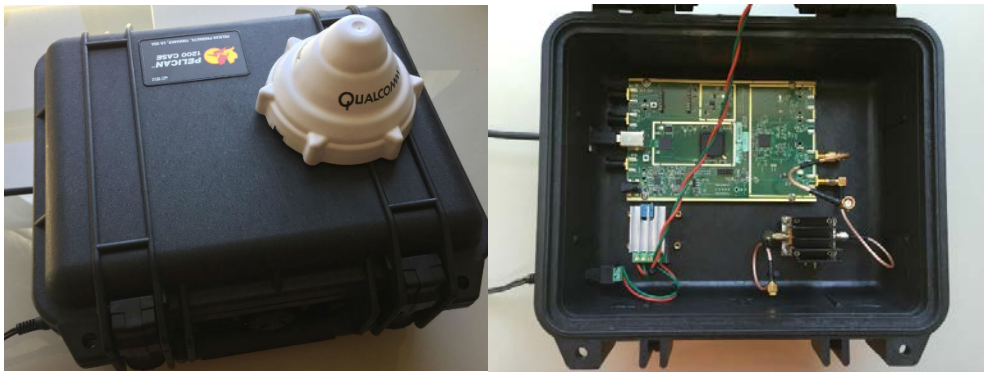
For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310

# Supply Chain: Defeating the Security Watchdog

## Corporate Risk Services

automobiles. The devices were made in China and could be bought for approximately $14 on the internet.

- In July 2014, criminals in Northern Florida used GPS jammers during a heist of a stolen refrigerated trailer. In this incident, the hauling tractor was swapped out by the cargo thieves. The Miami-based suspects were ultimately stopped and apprehended by the Florida Highway Patrol in mid-Florida during a routine vehicle stop; the shipment was recovered intact. Discovered hidden inside of the trailer's refrigerator unit were portable GPS jamming devices connected unobtrusively to a battery located inside the unit. The trailer was not equipped with a GPS tracking device; however, it is reasonable to believe that the thieves who planted the jammer thought there may have been one hidden somewhere inside the shipment and used the GPS jammer to counter tracking. This was one of the first confirmed uses of a GPS jamming device for cargo theft in the United States.




The device built by Synack to intercept data between GlobalStar tracking devices and its satellites (Colby Moore).

- In October 2014, U.S. Customs and Border Protection (CBP) further reported that several incidents were recorded in Italy, Mexico, and most countries of South America, in which thieves used GPS jamming devices to hijack cargo trucks.
- In September 2015, Fleet Owner Magazine and the Ontario Trucking Association reported that "Italian gangs began targeting shipments of scrap metal. They hijack a truck, force the driver to pull over, hold the driver captive and then use a GPS jammer so the cargo can't be tracked as they drive off with it."
- In early 2016, a drug courier meeting a flight of illicit drugs from Germany at a small airport in Britain used a suitcase-mounted "very serious kit" that jammed GPS, mobile phones, Bluetooth, Wi-Fi and the frequency used by stolen vehicle recovery systems. The device jammed signals for several hundred meters around the airport.

The "spoofing" threat (i.e. sending a fraudulent signal to the receiver) is escalating. As the two signals align, the fake signal replaces the real one, and the target receiver thus provides an inaccurate location.

In theory, criminals using a GPS receiver modified with inexpensive components and open source software would steal a vehicle and replicate its GPS tracker signal to continue reporting its location where it's scheduled to be. This would allow considerably more time to commit a crime and execute an undetected escape.

In June 2013, University of Texas researchers built a handheld spoofing device for $2,000. They were successful in replicating the GPS signal of a yacht sailing the Mediterranean Sea. The researchers moved the ship's position three degrees off course and convinced the yacht's GPS system that it was underwater. Other tests targeting unmanned aerial vehicles indicated this type of device could operate at a distance of 18.5 miles from a target.

In 2015, two researchers developed cost-effective spoofing devices. A team from Chinese firm Alibaba Group demonstrated that one could be built for less than $300. Another researcher at security firm Synack developed a device with commercial off-the-shelf components and software for $1,000.

There are no publicly disclosed incidents of spoofing used for cargo theft. However, the actual occurrence of spoofing is suspected due to the publicly known vulnerabilities of GPS, commercially available technology, adaptive aggressiveness of organized crime, and high probability of unreported events.

Regardless of what device is used, criminals monitor security improvements and attend trade shows to constantly adapt to new security measures. Well-financed criminals will adapt faster than many commercial cargo carriers.

### Security Solutions

The general observations from industry are conservative:

- The clear majority of successful jamming events in a cargo theft incident have taken place after the thieves have taken control of the truck
- A multi-layered security program, utilizing multiple tracking devices (to include covertly placed units within a shipment) provides the best mitigation against jamming
- Jammers have limited range and successful jamming, particularly if a covert device is placed inside the load, and has proven difficult to maintain for extended periods of time. Active monitoring of GPS tracking in areas of high risk for jamming activity can be the best and earliest detection of illegal activity – which can ultimately lead to successful law enforcement intervention

However, as the threat of GPS tracker jamming has developed, so has the technology to counter jamming and other signals interference for supply chain logistics. GPS tracking device manufacturers are engineering anti-jamming

For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310

and anti-spoofing signal monitoring into modern devices. These include inertial sensors, antennas that draw from multiple Global Navigational Satellite Systems (GNSS) or can determine the direction from which signals are arriving to at least improve the chances that they can withstand a malicious attack or GPS outage.

The devices use signal filtering techniques to identify interference signatures. When jamming is detected, the device enters an enhanced transmit mode override jamming and ensure message delivery.

The multi-layer security solution integrates new countermeasure technology:

- **Detection:** Trackers are configured to monitor the signal for interference on GPS and other frequencies
- **Alert:** The tracking device attempts to send coded alerts when interference is detected
- **Response:** Monitoring operators investigate and act on alerts
  - Responses vary based on customer requirements and procedures
  - Specific assessed jamming risks for the route or region are considered and applied to a specific response (sensor readings, location of the tracking device, and whether it's moving or reporting location information. Response may include direct communication with the driver, dispatcher or law enforcement

The DHS guidance for conveyance tracking and monitoring includes the Customs-Trade Partnership Against Terrorism (C-TPAT) program. C-TPAT is one layer in CBPs multi-layered cargo enforcement strategy. This program helps strengthen international cooperation and enhance security measures of cargo prior to entry into a country's borders.

C-TPAT carriers are required to practice and implement security procedures to prevent the un-manifested introduction of contraband into legitimate cargo shipments. The use of driver logs and/or GPS tracking are two of the ways to maintain cargo logistics integrity.

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.

Carrier management 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.

Lastly, the carrier must report all significant security incidents to the contracting party, law enforcement where applicable, and to C-TPAT (U.S. Customs and Border Protection).

A device used by authorities to detect truckers using jammers (Chronos Technology Ltd.)

It is important to note that C-TPAT also has standards for carriers in high-threat areas where the use of GPS is mandatory (e.g., long haul highway carriers in Mexico). Such carriers must utilize GPS to track the movement and location of the tractor and the trailer carrying U.S. bound cargo. The GPS system should be permanently installed in the tractor, and preferably hidden to prevent tampering or removal.

There must be a sensor coupling or connector from the tractor to the trailer to ensure monitoring and tracking of the trailer as well. C-TPAT also requires that the monitoring and tracking data for all transits carrying U.S. bound cargo must be maintained and stored for six months in the event CBP and long haul highway carrier management must conduct a review resulting from a security incident. Also, an employee of the long-haul highway carrier, held accountable to senior management, should be responsible for know where the loaded Long Haul Highway Carrier conveyance is at all times during transits northbound carrying U.S. bound cargo.

C-TPAT Partners are encouraged to implement the following recommendations for all conveyances to protect cargo 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

Jamming detection devices are becoming standard for use by law enforcement. Intended primarily for monitoring trucking and interstate highway traffic, they can be used in any surveillance scenario where a signals jammer may be suspected.

Finally, the U.S. government is starting to address broader GPS vulnerabilities. A multiagency committee is investigating a GPS backup solution that would make jamming and spoofing of GPS much harder. It is developing requirements for backup timing system, navigation and positioning. The committee is expected to issue recommendations in the fall of 2017.

## Recommendations

The best offense against jamming technology is a well-planned multi-layered security program. The program normally would include:

For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310

# Supply Chain: Defeating the Security Watchdog

## Corporate Risk Services

- Strong Intelligence to fully understand the threat
- Technology to properly leverage tracking device placement, configuration, and utilization of technical jamming countermeasures in regions where the threat is significant
- Operational policies and procedures to recognize jamming threats and to encourage rapid, well-constructed and targeted responses

Although cargo theft cannot be eliminated, carriers can be more resilient and less vulnerable with multi-layered technology, to include incorporation of intelligence driven situational awareness monitoring to ensure sufficient monitoring, tracking, and recovery capabilities are not overlooked or missed. Some of the areas that can assist are:

- **Education/Awareness:** Instructing employees about why their cargo is of high risk and what to look for when conducting inspections, audits, etc.
- **Training:** Conduct periodic training to inform all employees, especially drivers, why they (or the vehicle) are being tracked. This is an opportunity to be specific regarding the criminal threat, dangers, expectations, and that GPS tracking is used to ensure compliance with government requirements, company policy and contract/insurance specifications. Also, it should be explained that tampering or interfering with the device is illegal and punishable under law.
- **Device location:** To reduce the chance of discovery and the temptation for tampering, the device location should be as inaccessible and inconvenient as possible to be reached or unknown to anyone that is loading or transporting the cargo.
- **Monitoring:** Ensure the devices are actively tracked and the staff responsible for monitoring tracked assets are adequately trained to identify routes of cargo (difference between expectant stops and unexpected), times and distance of transportation, tampering of locks and devices and how spoofing works.
- **Ensure monitoring centers are not compromised:** Use layers of redundant monitoring so the compromise of a single employee cannot negate the entire monitoring process
- **Software Upgrades:** Ensure all software and hardware are up-to-date with software upgrades and routinely checked by a third party for cyber-attacks or penetrations
- **Policy and Procedures:** Develop a multi-layered approach to a secure, end-to-end chain of custody that includes well-defined and enforced protocols regarding:
  - Employee Training
  - Reporting processes
  - Importance of Information and Operations Security
  - Physical security measures such as the use of tamper-evident packaging, air brake locks on trucks and locking bars on trailers
  - Thorough carrier vetting and driver identification
  - Video surveillance (24x7) of warehouses, loading docks and gate areas, and even on vehicles so someone, for example, cannot climb aboard the truck/trailer undetected while the vehicle is moving
  - Use of secure facilities, lots and drop yards
  - Law Enforcement Liaison

## Additional Security Measures

- Businesses should coordinate information sharing and local safety/security measures with public safety/law enforcement agencies to prepare for events and guard against criminal and suspicious activity
- Businesses should verify the identity of persons driving company vehicles and their documents and use E-verify where appropriate. Additionally, businesses should include situational awareness as a component of company safety orientation with periodic updates to all drivers
- Drivers should not park vehicles without approval. Parking should only be authorized in secure, well-lighted areas; off the street where possible, in a pre-approved truck parks. Vehicles and their loads should be secured when left unattended. The cab should always be secured with valuables and documents kept out of sight
- Conduct risk assessments and select pre-determined lowest threat routes
- Geo-fence all pre-planned routes to provide alerts at the monitoring center whenever a vehicle varies from its designated route
- Vehicles should be equipped with a duress signaling device
- There should be a redundant policy and plan for GPS, communications, and capability for the monitoring center to communicate with a driver
- The GPS/Security monitoring center should have the capability to remotely activate disabling equipment
- An appropriate response should be determined for various incident scenarios
- There should be more than one GPS antenna on a truck tractor and trailer if they are separate entities, or on the combined truck/trailer. GPS antennas should be hidden and one dummy antenna should be used as a decoy
- Monitor truck parking areas, empty trucks/trailers to ensure that the vehicles cannot be misappropriated
- Companies using heavy-duty vehicles and/or trucks, including rental companies, should consider applying the following security standards for transportation conveyances to their fleets, with this threat in mind: Transported Asset Protection Association (TAPA), Authorized Economic Operator (AEO) programs such as the Customers Trade-Partnership Against Terrorism (C-TPAT), Canada's Partners in Protection (PIP), and Mexico's Nuevo Esquema de Empresas Certificadas (NEEC), along with ISO 28000 supply chain security standards

Remember that GPS is a security tool but is not, in and of itself, a total supply chain security solution!

For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310