GNSS Vulnerability Detection & Mitigation

Chronos Technology Ltd
sales@chronos.co.uk
+44 1594 862 200
Agenda

- Overview of Chronos Technology
- Overview of GPS
- Jammers
- Chronos’ Portfolio
How did we get here?

1986
Chronos begins supplying critical infrastructure with time & sync solutions.

2000's
We branched out to install GPS broadcasting inside premises such as airport hangers.

2008
We launched project SENTINEL.

2014
We released our range of GPS Interference detection devices.
What is GPS?

- 33 satellites
- 12,500 miles away
- L1 - Civilian = (1575.42MHz)
- L2 - Military (1227.60 MHz)
- L5 - Proposed safety-of-life signal (1176.45 MHz)

GPS is just one of many Global Navigation Satellite Systems (GNSS) available, including Galileo (Europe), GLONASS (Russia) and BeiDou (China)
Who is vulnerable to GPS Disruption?

- Navigation
- Telecommunications
- Bank trading
- Power grids
- Emergency services & Armed forces

GPS is especially vulnerable to interference
Common Jamming devices

Small
Easy to plug into a vehicle, cheap and common

Handheld
Covers multiple frequencies, can often jam mobile signal and trackers

High Power
Jams GPS, trackers, WiFi, Bluetooth, car keys, Police comms, phone signal, etc.
Who uses Jammers?

**Vehicle Theft**
Criminals knock out vehicle and asset tracking

**International warfare tactics**
Russia are suspected of using GPS Jamming and spoofing to interfere with navigation

**Hiding from a tag**
GPS Leg tag offenders can block the signal

**Plant Theft**
Machines worth upwards of £100,000 are stolen frequently

**Organised crime gangs**
To hide their movements, gangs will jam their surroundings

**Skipping off for lunch**
Hiding from fleet telematics, while causing issues to infrastructure
New 12V 2W Vehicle Car GPS Signal Interference Shield Tracking Interceptor

Condition: New

Quantity: 1

0 available
32 sold

£4.99

Collect 5 Nectar points
Redeem your points | Conditions

Postage: Free Economy Delivery | See details
Item location: HAYES, United Kingdom
Posts to: Worldwide See exclusions

Have one to sell? Sell it yourself
A12 30W Super High Power GPS WiFi Lojack 3G 4G 5.8G Jammer

This is a super high power 12 band multifunction jammer. 30W high power, interference distance up to 75 meters. The interference distance can be adjusted as needed. The jamming performance is very stable.

$658.58 $1176.03 44% OFF
CTL3510 GPS Jamming Detector

Chronos’ handheld detection device

POCKET SIZE
Small enough to be equipped on your person or mounted in a vehicle.

VIBRATION ALERT & LOGGING
Internal vibration and covert mode, with a logging feature.

VISUAL INDICATION
Colour-based LEDs show the growing severity of interference.

EXTENDED BATTERY LIFE
8 hour standby battery life, or keep on while charging.
CTL3520 GPS Jamming Detector and Locator

Chronos’ handheld detection and location device

ERGONOMIC HANDLES

Easy to hold for directional finding abilities.

DIRECTION INDICATION

Direction bar displays the direction of the source of interference.

ADJUSTABLE ATTENUATION

Change the sensitivity of the device to locate the source in close proximity.

LCD DISPLAY SCREEN

Visual display of data including battery life and attenuation.
Detection of 3W GPS Jamming

Detected at approximately 6Km in a direct line of sight
Who uses Jamming Detectors

- Military
- Law Enforcement
  - Highway departments / patrols
  - Car Theft Units
  - Organised Crime departments
- Central Government Agencies
  - Border agencies
- Homeland Security
- Infrastructure
  - Power
  - Telecommunications
  - Survey
Mitigation Infrastructure
Microchip BlueSky Firewall
GNSS is a single point of failure for Critical Infrastructure
Signal-in-Space Vulnerabilities

- Signal in space vulnerabilities are generally categorized based on the failure mode they induce in a GNSS receiver
  - **Jamming**: Partial or complete loss of ability to receive GNSS signals
  - **Spoofing**: Tricking a GNSS receiver into receiving illegitimate signals

---

### Signal-in-Space Systems

<table>
<thead>
<tr>
<th>System</th>
<th>GPS</th>
<th>GLONASS</th>
<th>BeiDou</th>
<th>Galileo</th>
<th>IRNSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner</td>
<td>United States</td>
<td>Russian Federation</td>
<td>China</td>
<td>European Union</td>
<td>India</td>
</tr>
<tr>
<td>Coding</td>
<td>CDMA</td>
<td>FDMA</td>
<td>CDMA</td>
<td>CDMA</td>
<td>CDMA</td>
</tr>
<tr>
<td>Frequency</td>
<td>1.57542 GHz (L1 signal) 1.2276 GHz (L2 signal)</td>
<td>Around 1.602 GHz (SP) Around 1.246 GHz (SP)</td>
<td>1.561098 GHz (B1) 1.589742 GHz (B1-2) 1.20714 GHz (B2) 1.26852 GHz (B3)</td>
<td>1.164–1.215 GHz (E5a and E5b) 1.260–1.300 GHz (E6) 1.559–1.592 GHz (E2-L1-E11)</td>
<td>1.17645 GHz (L5) 2.492028 GHz (S1)</td>
</tr>
</tbody>
</table>

---

We cannot solve our problems with the same thinking that we used when we created them.

- Albert Einstein
Firewall Concept

Physical Firewall at Electrical Substation

Unprotected PNT from the Sky

Secure PNT for Critical Infrastructure
Secure Firewall Overlay

- Protects GPS systems from spoofing and jamming
- Simple connection between GNSS antenna and GPS system
- Optional internal MAC for holdover
- 1PPS and 10 MHz timing reference inputs for extended holdover (connection to external cesium reference)
- Redundant AC or DC power options
- Command Line Interface (CLI) in addition to secure and easy-to-use web interface
- “BlueSky Performance Monitoring” integrated within TimePictra (included as part of BlueSky Subscription)
- New steel chassis with CE compliance
Thank You

Chronos Technology Ltd
sales@chronos.co.uk
+44 1594 862 200

©2020 Chronos Technology: COMPANY PROPRIETARY