RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: MBS-T10R

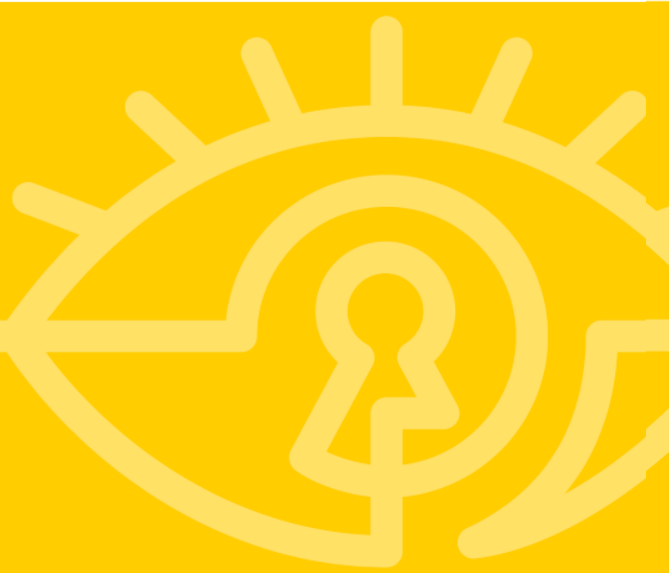
Ghosts in the Network: SS7 and RF Vulnerabilities in Cellular Networks

Les Goldsmith
Chief Executive Officer
ESD America Inc
@lesatesd

Trent Smith
Director of Project Overwatch
ESD America Inc
@trentatesd

Who are we

- ESD America is the North American & Asian Distributor of GSMK Cryptophone.
- 5 years ago we commenced a joint research project into ways that groups like the NSA hack cell phones.
- The research was conducted on behalf of a major European government customer.
- The research focused on two main areas of attack:
  - The SS7 Protocol on Cellular Networks
  - Over the air attacks using IMSI Catchers



SS7 Vulnerabilities

SS7 Vulnerabilities

- Our focus is on the results of testing cellular networks
- Not on theoretical attacks
- First to present these results publically
- To benefit providers, banking, government and others

SS7 Vulnerabilities

- In December 2014 Tobias Engel from GSMK Cryptophone demonstrated many of the attacks at the Chaos Communications Congress.

SS7 Vulnerabilities

- PT Security, Orange & Adaptive Mobile all released reports supporting the vulnerabilities.
- GSMA formally acknowledged the vulnerabilities to members

Network Reactions

- Many network operators responded immediately and began looking at ways to minimize the vulnerabilities discovered over SS7.
- Some operators assumed their networks were not vulnerable to these attacks.

Network Reactions

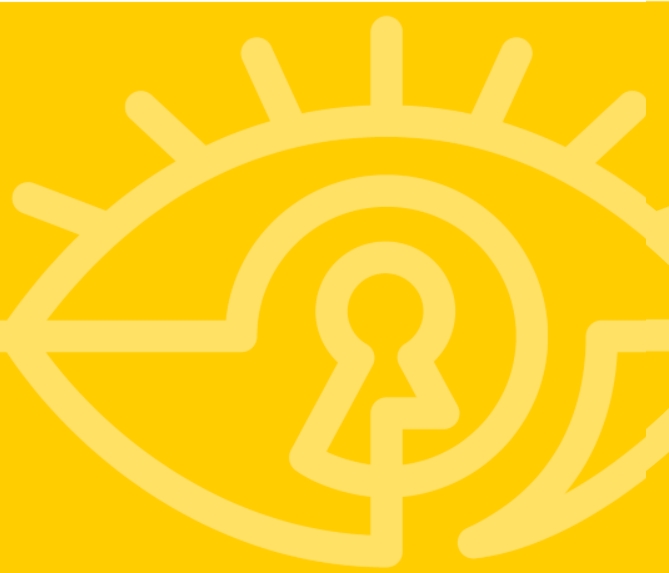
- Senior executives generally expressed concern regarding the possible vulnerabilities
- However many of the people responsible for SS7 at the providers considered the attacks fictional

Scale of SS7 Traffic

- Until you can visualize all the data, it's difficult to comprehend the sheer scale of SS7 traffic traversing the networks.

Penetration Testing

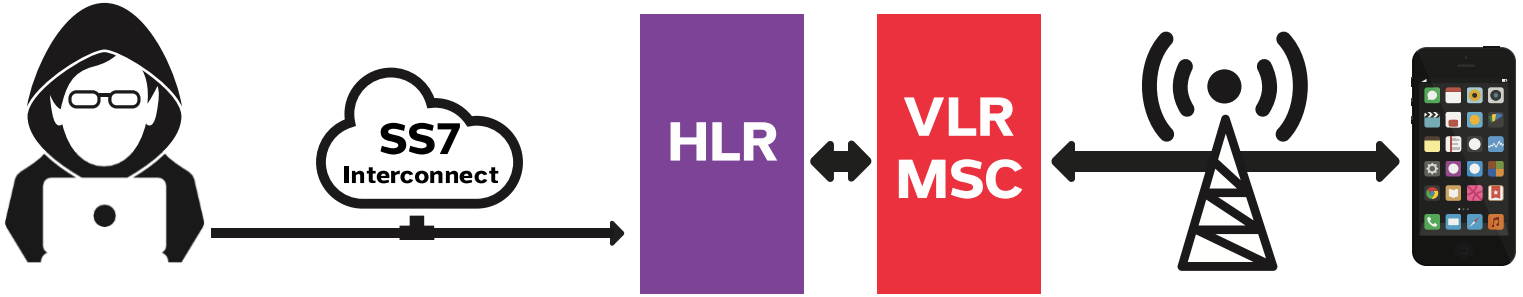
- In November 2014 we commenced penetration testing in Europe. Over the following 12 months we rolled out penetration testing worldwide.
- There are over 820 network operators using SS7.
- To this date less than 5% of network operators have been penetration tested.



Tracking & Interception Results

Tracking via SS7

1. Attacker asks HLR to provide current Cell ID for an MSISDN (`anyTimeInterrogation`)
2. HLR looks up IMSI and current VLR/MSC for subscriber and asks VLR to provide current Cell ID for that IMSI (`provideSubscriberInfo`)
3. VLR/MSC initiates paging of subscriber to retrieve current Cell ID
4. VLR returns Cell ID to HLR
5. HLR returns Cell ID to attacker

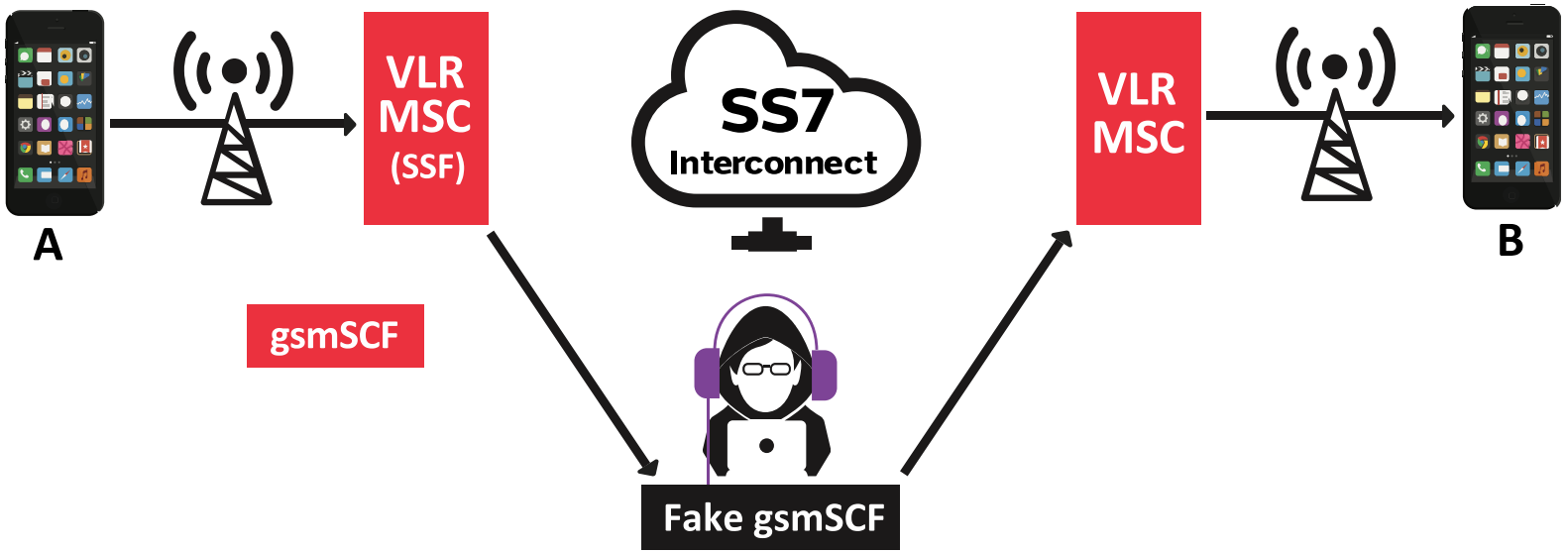


- The *anyTimeInterrogation* request enables asking for the Global Cell-ID, a privacy violation by any attacker with SS7/MAP access

Tracking via SS7

- How many networks were vulnerable to tracking by third parties?

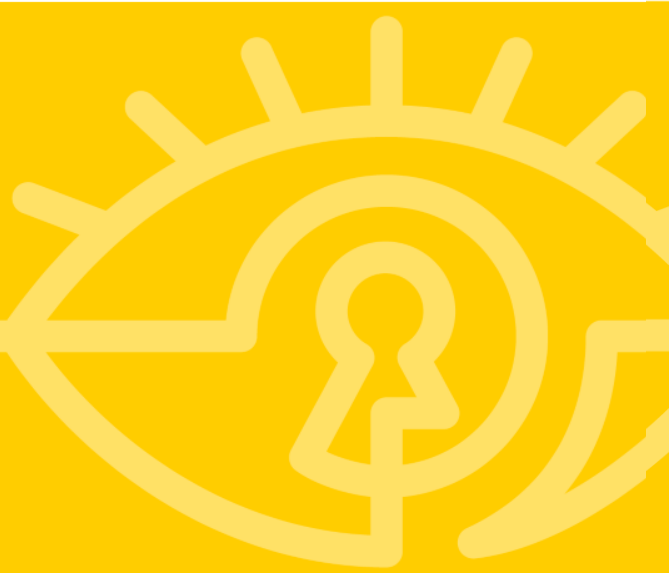
Listening via SS7



- The same approach can be used for SMS data

Listening via SS7

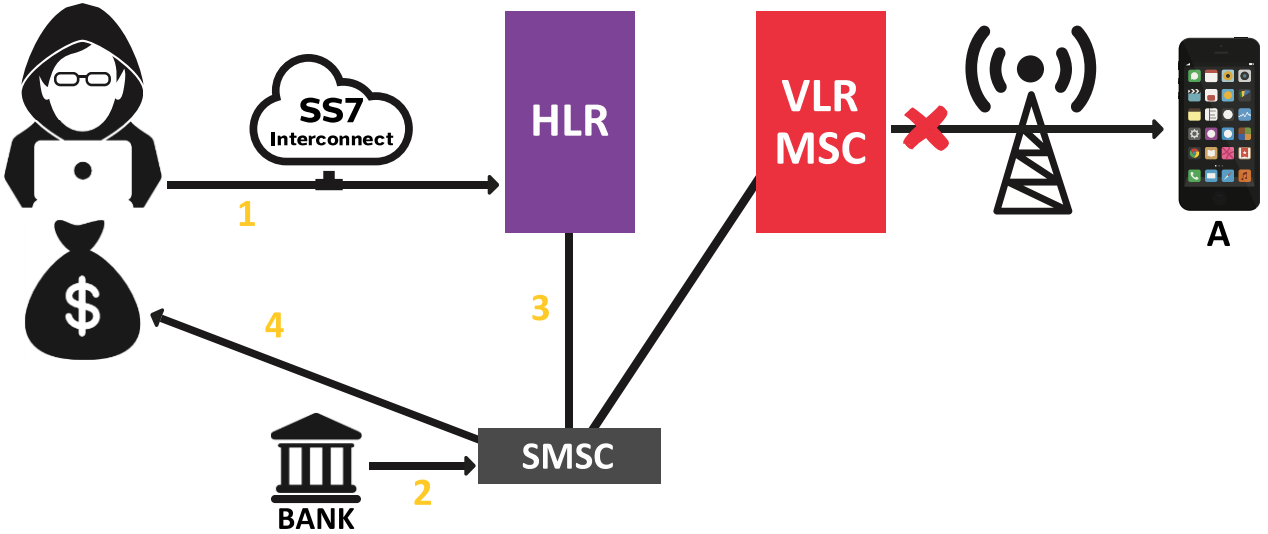
- How many networks were vulnerable?



Billing, Banking & Fraud

SMS Banking Authentication

1. Attacker tells HLR that subscriber A is now logged onto his network (`updateLocation`)
2. Bank sends text message with mTAN to subscriber **A**
3. SMSC gets referred to attacker's "VLR" as destination by HLR (`sendRoutingInfoForSM`)
4. SMS is delivered to attacker (`mtForwardSM`)



SMS Banking Authentication

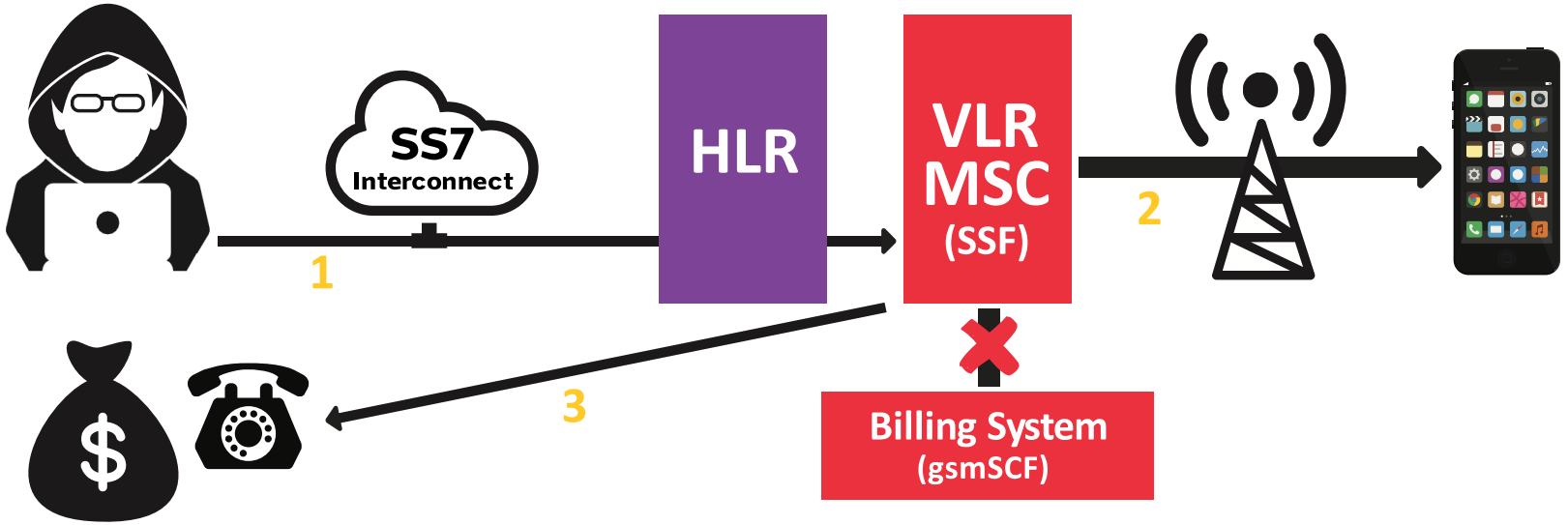
- Could this happen to you?

Unbilled Calls

1 Attacker deletes gsmSCF address from VLR/MSC (`deleteSubscriberData`)

2 Attacker starts a call to a premium rate number he controls

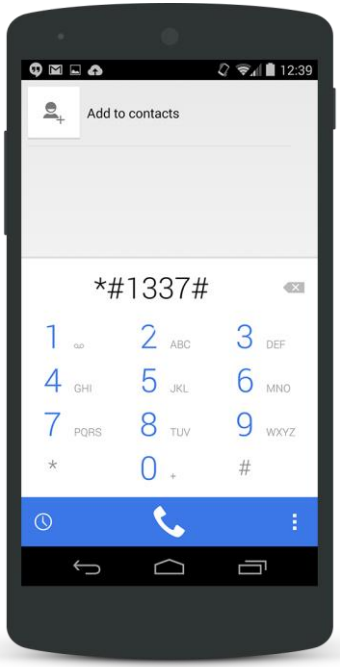
3 MSC recognizes subscriber as post-paid and permits call to continue at network operator's expense



Unbilled Calls

- How much money can be lost through this attack?
  - With one SIM card an operator lost $250k in 10 minutes
  - The amount of SIM cards used is limitless

USSD Codes



- USSD codes can be executed for other subscribers
- Some carriers offer transfer of prepaid credits via USSD
- Call forwarding can be set/deleted
- Switch active SIM in case of Multi-SIM

USSD Codes

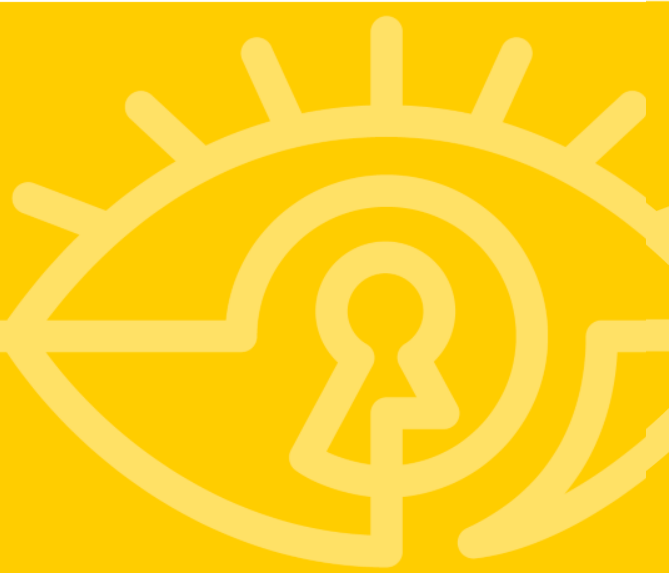
- How many networks did this effect?

Vulnerabilities Recap

Vulnerabilies
Track Subscribers
Call Forward
Man in the Middle Intercept
Access Voicemail
Identify Phone Model
Steal Credits
Change Subscriber State
Denial of Service

More Testing

- More penetration testing is needed
- Within the next 12 months we expect to test another 40 to 60 providers
- In some cases government may be needed to address national security concerns



IMSI Catchers & Cell Manipulation

What's a IMSI Catcher

- IMSI - Individual Mobile Subscriber Identity
- A IMSI Catcher is a device that pretends to be a cell tower in order to trick your phone into connecting to it.
- In truth, your phone has no idea the IMSI Catcher is not part of the real network.

Why do phones trust them

- Cell phones are designed to look for other towers with better reception.
- The IMSI Catcher operator must adjust settings to replicate a cell tower in your area.
- The phone will connect to the IMSI catcher if it's made to look more 'attractive' than the real network.
- By not configuring the IMSI Catcher to pass calls to the networks the users phone can't call out.

How do they work

- A catch-all IMSI Catcher is configured to tell all cell phones within range that it is the only available cell tower.
- Tricking your phone into thinking its the only available connection.
- A catch-all IMSI Catcher can be used for collecting IMSI's from a particular area or to deny service to cell phone users.
- By not configuring the IMSI Catcher to pass calls to the networks the users phone can't call out.

Tracking with IMSI Catchers

- They can be used for collecting IMSI's from a particular area or to deny service to cell phones that connect to it.
- Most IMSI Catchers used by local law enforcement are used for tracking.
- By knowing a targets IMSI, the operator can program the IMSI Catcher to only connect with that target's phone when in range.
- Once connected the operator use a process of RF Mapping to direction find the target.

Can a IMSI Catcher listen to calls

- A basic IMSI catcher just captures the cell phone's IMSI number.
- To intercept calls a it would require a number of additional features charged for separately by manufacturers
- 2G calls are easy to listen to. Systems for this have been available for over a decade and can be built for less than $1500.
- The price of these call intercept systems are base on the number of cellular bands (2G/3G/4G), effective range, decryption speed.

Are 3G & 4G calls safe

- Yes, kind of. 3G and 4G use better encryption for calls than 2G. But..
- IMSI Catchers can feature add-ons that trick a 3G or 4G phone into thinking those connections are unavailable.
- Your 3G or 4G phone is then forced to drop down to the weaker 2G encryption. Ripe and ready for monitoring.
- ‘Forced’ by either telling phone to switch, or jamming 3/4G networks so only the 2G signal from the IMSI catcher is available.

Detecting IMSI Catchers

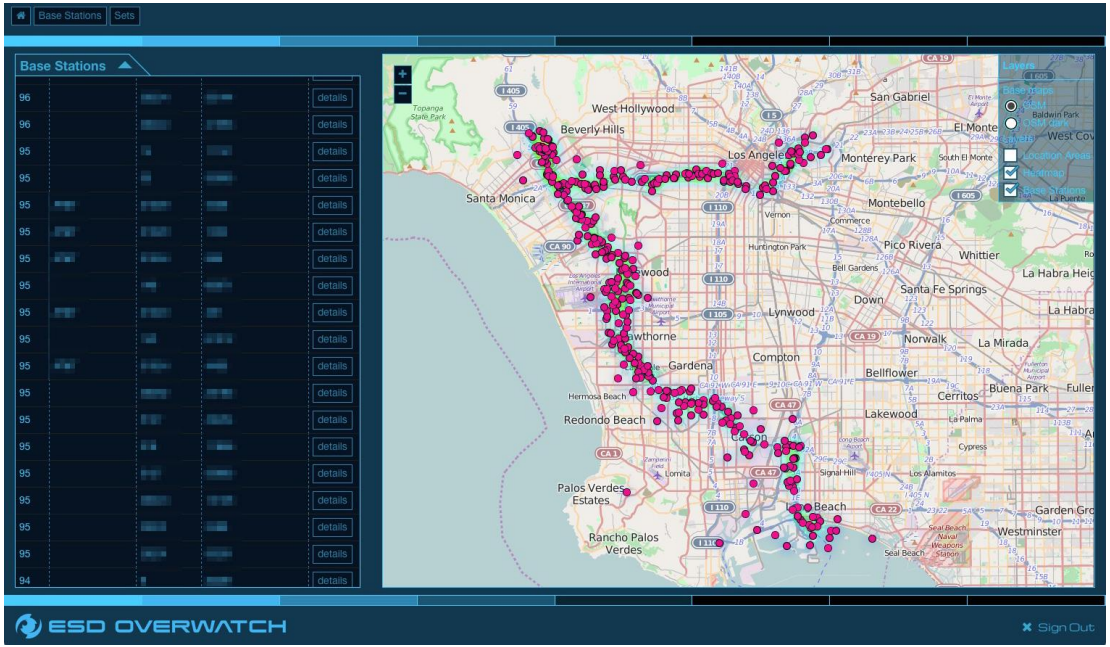
- Network Operators sometimes see the anomalies but cannot locate them or verify what they are.
- The FCC has teams of people to deal with network anomalies. However knowledge of IMSI Catcher operation and response times are an issue.
- Cellphone users often download apps to detect IMSI catchers. But most of these cannot verify what signal is received over the radio stack.

IMSI Catchers across the USA

- 78 IMSI Catchers detected in 2015
- 8 of those were mobile at the time of detection
- 80 Cell towers with encryption disabled
- 7 cases of operators using the same channel in a coverage area

Los Angeles

- Detected 20 different cases of cellular jamming
- 7 IMSI Catchers

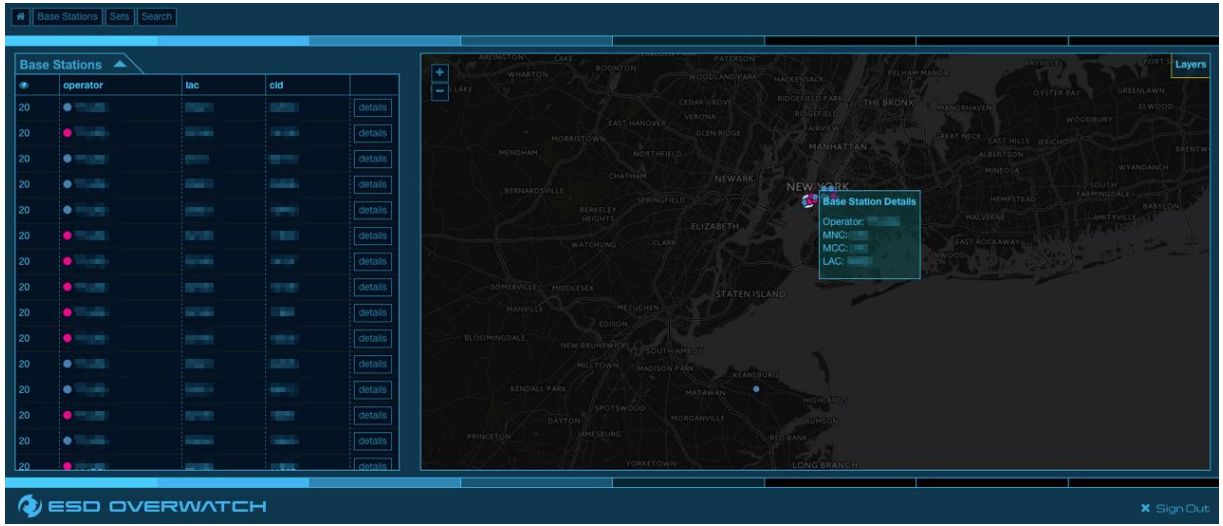


Washington DC

- 9 IMSI Catchers in just 3 days of surveys
- 3 of those focused on the same target area

New York

- 11 Cases of Cell Jamming over 3 days
- 7 IMSI Catchers deployed across Brooklyn, Manhattan & Financial District



Around the World

- More than 140 IMSI Catchers detected
- Hundreds of cell towers with encryption disabled
- Detected 7 IMSI Catchers operating in one Middle Eastern city in 45 minutes

What can be done

- In reality network operators need to consider the effect on IMSI Catchers on customer services
- Government needs to take a proactive role in detecting and prosecuting users of IMSI Catchers
- Prompt investigation of potential threats is required
- To defend against IMSI Catchers, you need to be able to find them first.

Questions