

# ISSWorld®

Intelligence Support Systems for Lawful  
Interception, Criminal Investigations and  
Intelligence Gathering

## ISS World Middle East 2014

Prague, CZ

3-5 June 2014

Washington, DC  
6-8 October 2014

## Welcome Remarks:

Presented By

Tatiana Lucas

ISS World Program Director, TeleStrategies

Brasilia, BR  
8-10 September 2015

Dubai, UAE

3-5 March 2014

Kuala Lumpur, MY  
2-4 December 2014

Johannesburg, ZA  
15-17 July 2014

# Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community and Other Challenges/Solutions

Presented By:

*Dr. Jerry Lucas  
President, TeleStrategies*

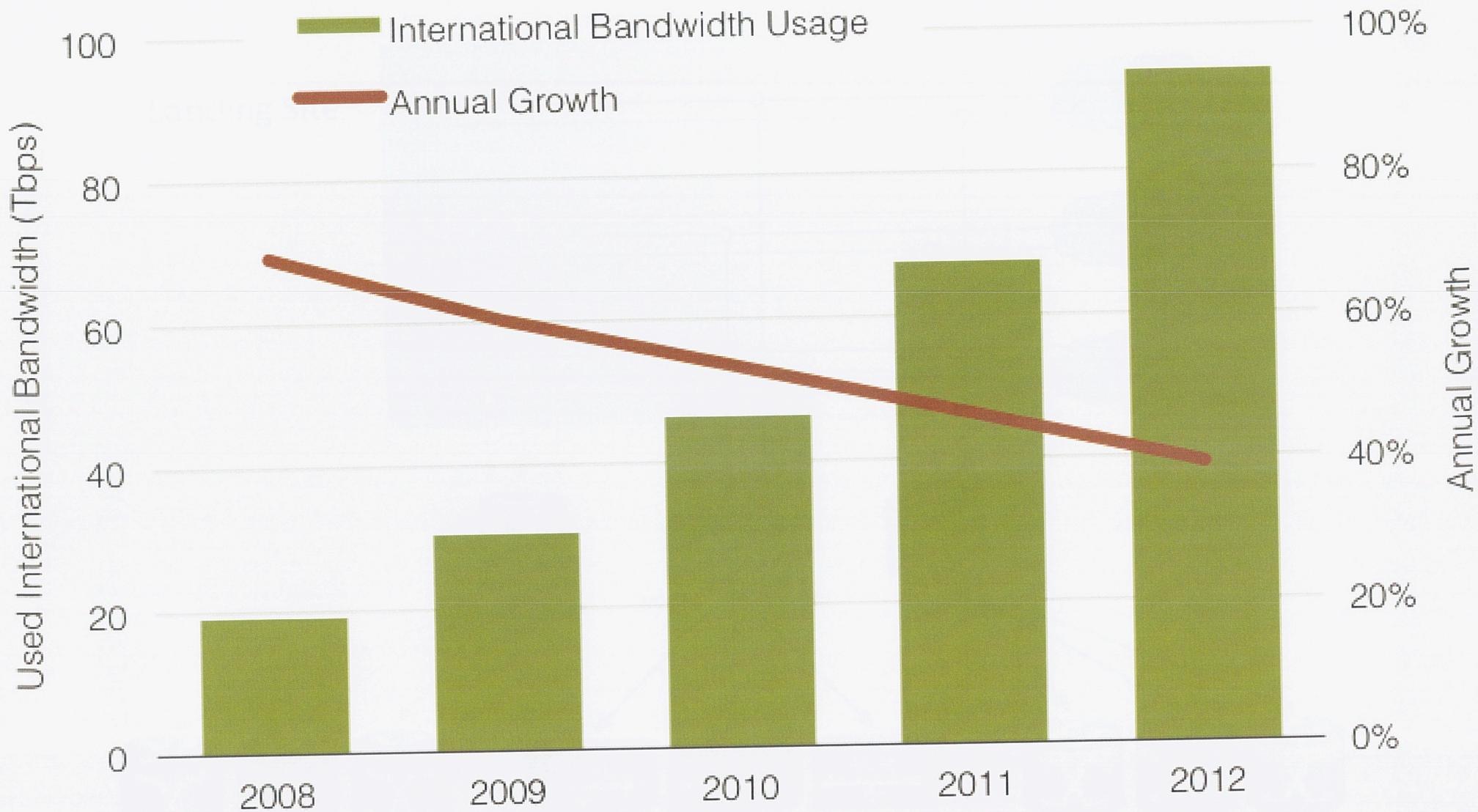
4 March 2014  
Dubai, UAE

# Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community

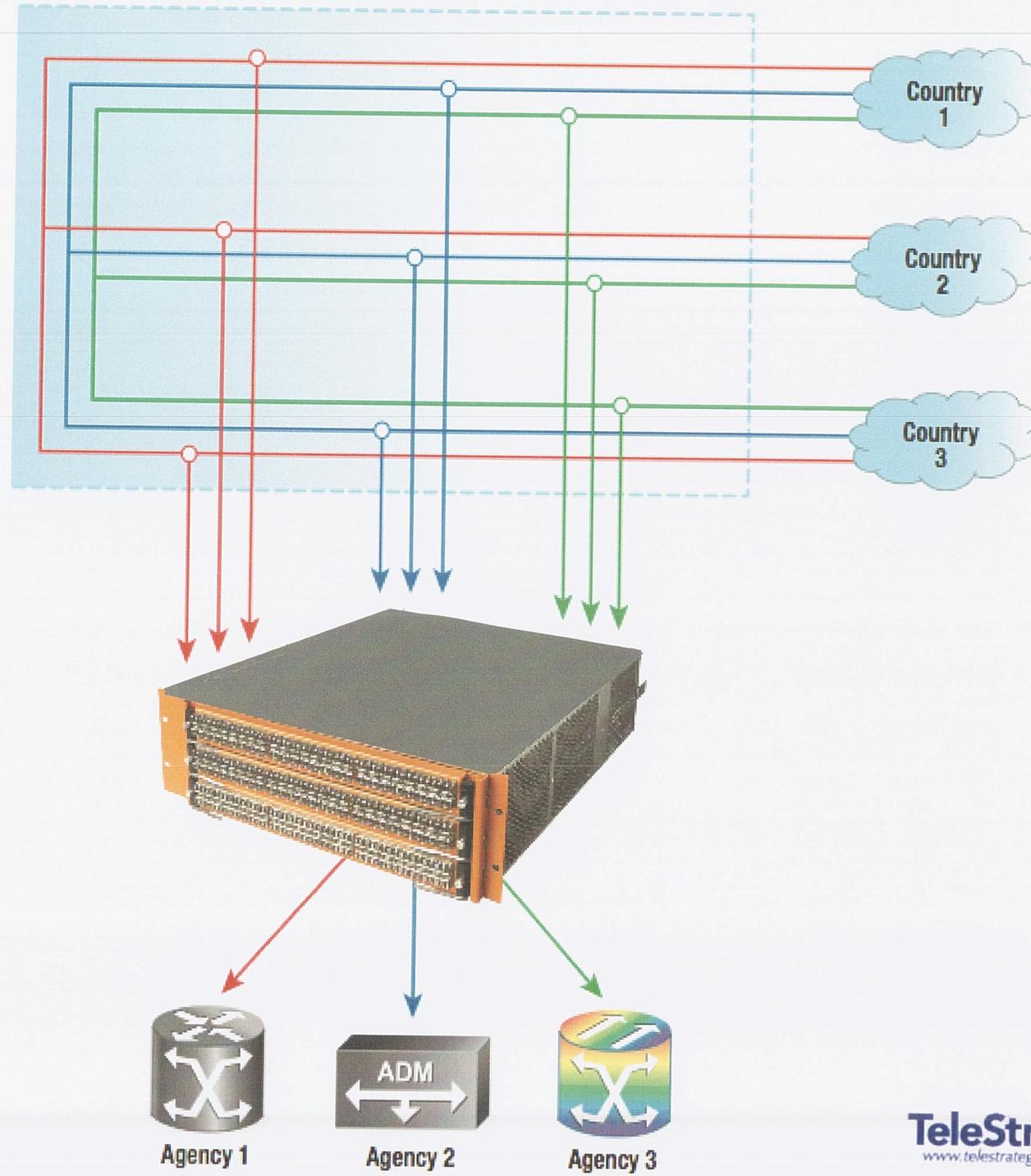
1. Fiber Bandwidth Growth
2. Smartphones
3. Encryption
4. Social Media Monitoring
5. Increasing Data Volume
6. Tactical Surveillance
7. All IP LTE Mobile
8. Dark Web
9. Dark Email
10. Regulatory Shortcomings

# Challenge 1: Fiber Bandwidth Growth

1. New Fiber System Deployments
2. Channel Speed: 100 GBPS and Growing
3. Multiple Layer 2 Protocols: WDM, ATM, Ethernet, MPLS and more
4. Multiple Intelligence Agency Access
5. Security Compartmentalization and more



Landing Site



# Optical Probes and DPI in 10 to 100 GBPS Networks

## TODAY'S SESSION ON THIS TOPIC

9:30-10:00

Track 1: True 100G Based – xRy Single Serve Capture, **FiberBlaze**

Track 5: Interception and Intelligence Gathering – Impact of Growing Bandwidth and New IP Applications, **SS8**

14:00-14:30

Track 1: Application Level Interception in 100G Networks, **Invea-Tech**

15:30-16:00

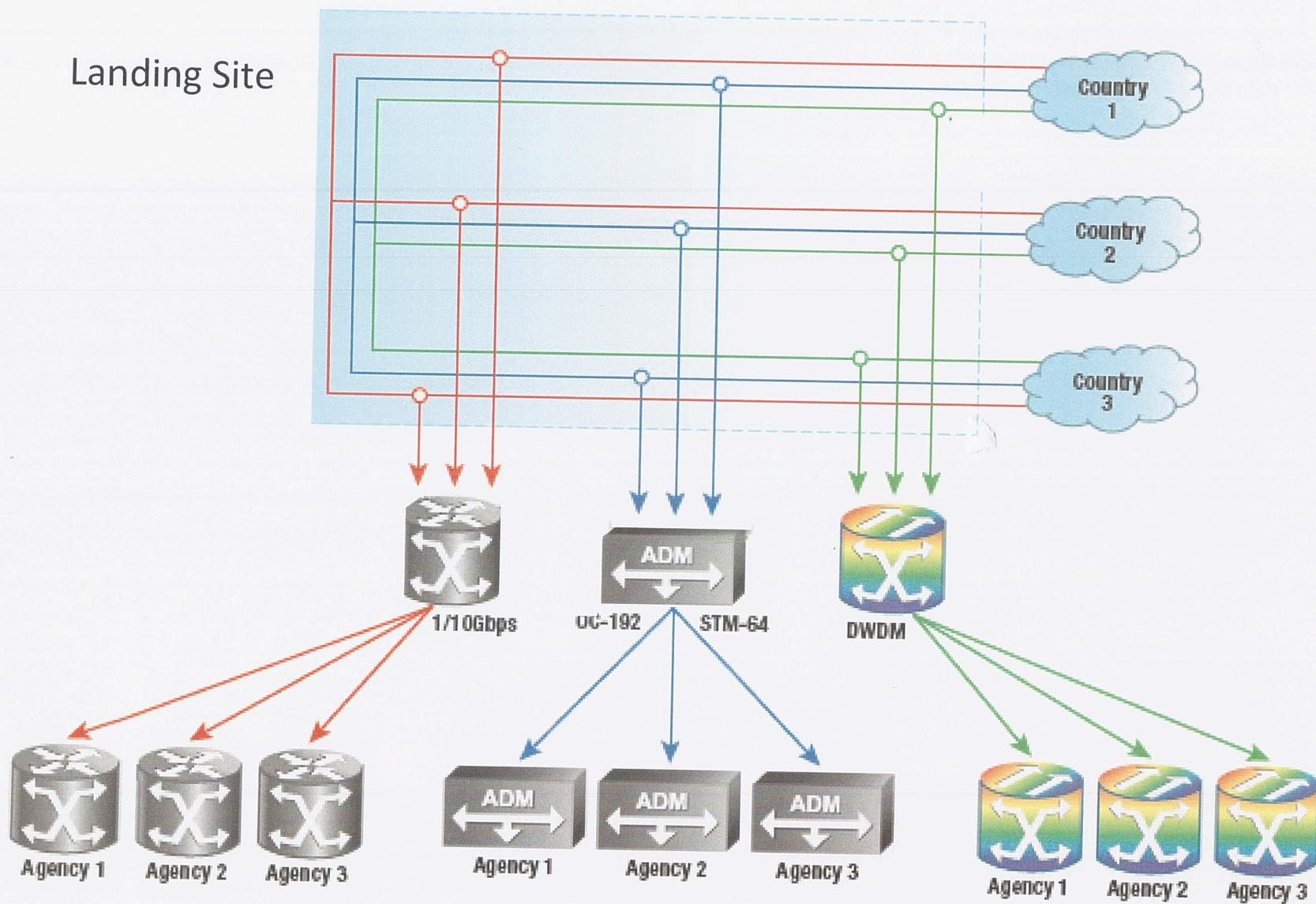
Track 1: Recall IP Intercept – The Next-Generation Interception at 10 Gigabites and Beyond, **iSolv Technologies**

## TOMORROW'S SESSION ON THIS TOPIC

10:30-11:30

Track 5: Sigint in High Bandwidth Networks, Deep Dive In Solutions Scenarios and Best Practices, **Network Performance Channel**

## TRADITIONAL



# #1 DPI and Optical Probe Vendors

Expert-Team  
Fiberblaze  
Glimmerglass  
Inveatech  
Narus  
NPC  
SS8

# Challenge #2: Smartphones

## What's Good

- Image capture with geolocation information
- High forensics value
- Useful law enforcement applications
- And more

But: SmartPhone create law enforcement and  
Intelligence Gathering Challenges

# Challenge #2: Smartphones

Why?

- 1) Call set-up not visible to telecoms.
- 2) Non-regulated third party based
- 3) Little if no call detail records kept
- 4) Most traffic peer-to-peer
- 5) Third party servers located out of country
- 6) Traffic likely to be encrypted
- 7) Emerging product market for criminals and terrorists

And timely smartphone vendor support!!!

# Smart Phone Sessions and Exhibitors at ISS World Middle East

## Track 3: Open to All Attendees (11 Sessions)

## Track 5: Product Demonstrations

- **NeoSoft** Product Demonstrations Today (11:30 AM) and Tomorrow (10:30 AM)
- **EXFO** Technologies Demonstration Today (15:30)

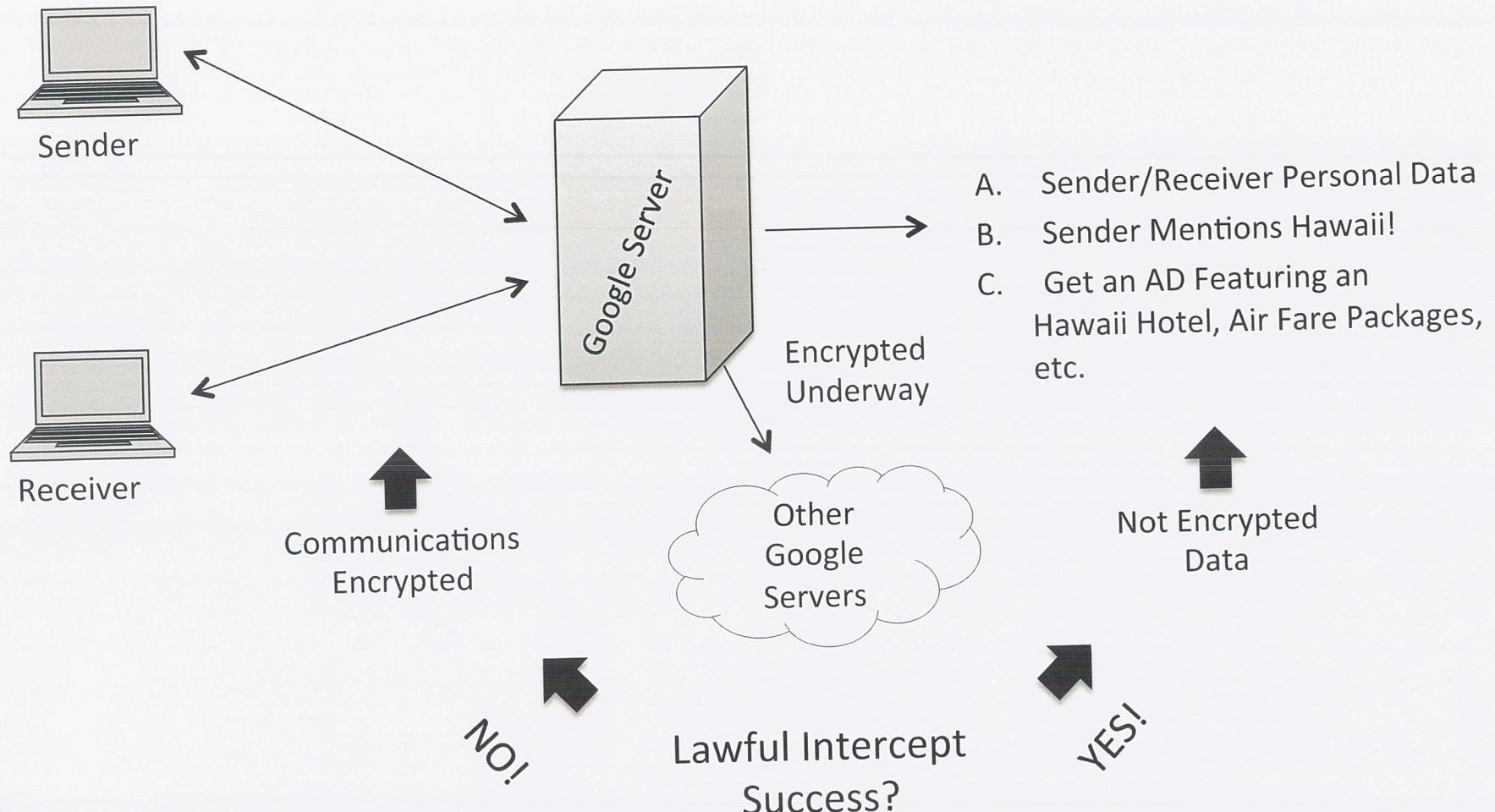
## #2 MOBILE LOCATION AND SURVEILLANCE EXHIBITORS AT ISS WORLD MIDDLE EAST

1stWAP	Esri	Ntrepid	SIM
Advanced Systems	EXFO	Octastic	Sinovatio
Aglaya	Gamma Group	Polaris Wireless	Sirius
Aqsacom	Group2000	Providence	UK Speedog
BTT	LEC	RCS	Utimaco
Covidence	Mobilaris	S3tel	VASTech
Creativity Software	NeoSoft	Semptian	

## Challenge #3: Encryption

- Encryption Products are Available at Low Cost ( $\approx \$50$ ) or Free with Easy Installation for Almost any IP Enabled Smart End-Device Yielding End-To-End Encryption
- Many P2P, Social Networks, Webmail and VoIP Services (Skype) are Encrypted
- Traditional Lawful Interception Solutions cannot Provide Content De-Encryption and Encrypted Content is Useless to LEA/IC
- Can't Block All Encrypted Traffic!

# Google Gmail Intercept: An Example



# LEA/IC Methods to Defeat Encryption

1. Crack the Encryption Code (256 and 1024 Bit Keys)???
2. Coerce the Private Key Holder (Certificate Authority) to Turn the key over
3. Man-in the middle attack:
4. Introduce weakness in encryption standards (NIST issue)
5. Install Spyware
6. Snare the messages before they are encrypted!!!
7. Or just collect the Metadata

# ISS World Program Addressing Encryption

Track 4: Encrypted Traffic Monitoring and IT Intrusion  
Product Training and Demonstrations  
(11 Scheduled 1 Hour Sessions)

# ISS World Middle East 2014 – IT Intrusion Exhibitors and Presenters

AGT

ClearTrail

FinFisher

GR Sistemi

Hacking Team

iPS

iSolv

VuPEN

# Internet Challenge #4: Social Media Monitoring

## Exponential User Growth (Facebook Example)

- 1.1 Billion Subscribers (July 2013)
- 900 Million Subscribers (June 2011)
- 400 Million Subscribers (January 2010)
- 600 Million Subscribers (November 2010)
- 750 Million Subscribers (October 2011)
- 300 Million Subscribers use Facebook for messaging (November 2010)

## Why Monitor Social Networks?

### A. Criminals and Terrorists Use Them To:

- Communicate
- Plan Illegal Activities
- Fundraise
- Training and More

### B. Population Shift From Traditional Telecom Services to Social Network Based Services

### C. No Intercept Infrastructure (in general) to Support Lawful Interception and Intelligence Gathering

And More !!!

# Specific Social Network Monitoring Sessions Today

9:00-10:00 Track 6

Deep Intelligence From Twitter & Facebook – A Live Demo of KIS, **Knowlesys**

11:30-12:00 Track 2

POMS: An Intelligent Tool to Drill Down on Facebook and Twitter, **Semptian**  
Social Media Intelligence, **ISmSC**

11:30-12:30 Track 6

War on Social Media and Stealing Intelligence, **AGT**

14:00-15:00

Safe use of Social Media, **Raytheon**

# Specific Social Network Monitoring Sessions Tomorrow

8:30-9:30 Track 6

“IO Network Monitoring” – Social Media Monitoring Solutions, **GsmSoft**

10:30-11:30 Track 2

Social Media and LI Technology Perspective, **C2Tech**  
Integrated Intelligent Profiling with OSINT, **Tasheel**

12:00-13:00 Track 6

Social Network Monitoring Session, **ClearTrail Technologies**

# ISS World Middle East 2014– Intelligence Center Analytics Vendors

Advanced ME Systems  
AGT  
ATIS  
BAE Systems  
C2TECH  
ClearTrail  
Cyberpoint  
GR Sistemi  
Group2000  
GsmSoft  
ISnSC  
Knowlesys  
Narus  
Nuance  
PGI  
Phonexia  
Raytheon  
Semptian  
Tasheel  
Trovicor  
Xalted

# Challenge #5: Increasing Data Volume

Each Minute\*:

- 47,000 People Download an Apple App.
- 100,000 Tweets hit Twitter
- 300,000 People Log on to Facebook

Plus New, Volumeous Data Sources

- License Plate Readers
- Surveillance Cameras
- Biometric Data
- And More

\*Source: Investment Business Daily (April 4, 2012)

# Solution: Big Data Analytics

What is it?

- About the process of examining a large amount of data
- Data of different types
- Used to uncover different patterns, unknown correlations and other useful information

Key Advantages: Can use web analytics to manage and monitor large amounts of data

# Big Data Analytics Sessions

## Today, Track 6:

9:00-10:00 An Overview of Data Clarity: Using Visual Analytics to Investigate Desparate Content,  
**Raytheon**

11:30-12:30 Klarios Analytics: Finding the Truth, **ATIS Systems**

## Today, Track 2:

12:00-12:30 SIGINT, OSINT, Humins: Massive Data Fusion, Search and Analytics in 3 clicks,  
**Advanced Systems**

12:00-12:30 IP Deep Investigation Analytics, **trovicor**

14:30-15:00 Engineering a Safer World – Oceans of Data, **Xalted**

15:30-16:00 Gain Situational Awareness with Big Data Analytics, **NARUS**

16:00-16:30 Speech Intelligence Platform – How to Mine Data from Speech Records, **Phonexia**

16:30-17:30 IntelliCenter – Real Time Insight to make informed decisions, **Xalted**

# ISS World Middle East 2014 – Social Network Monitoring and Big Data Analytics Exhibitors

Advanced ME Systems

AGT

ATIS

BAE Systems

C2TECH

ClearTrail

Cyberpoint

GR Sistemi

Group2000

GsmSoft

ISnSC

Knowlesys

Narus

Nuance

PGI

Phonexia

Raytheon

Semptian

Tasheel

Trovicor

Xalted

# Challenge #6: Tactical Surveillance

1. Processing and Analyzing “Geofensed” Call Detail Records
2. Inbuilding Locations
3. 3G and 4G Antenna Coverage
  - First Omni Directional (360°) and Large Cell Site Coverage Area
  - Second Development: Sectorized Antenna (120°) and Microcell Coverage
  - Today 3G & 4G: MIMO Antenna and In Building Coverage

MIMO = Multiple-Input and Multiple Output

# Challenge #6 : Tactical Surveillance

Tracks 3 and 7 Sessions Today and Tomorrow

Track 3: 11 Sessions

Track 7: 11 Sessions

## Location Exhibitors

1stWAP	Gamma Group
Advanced Systems	Group2000
Aglaya	LEC
Aqsacom	Mobilaris
BTT	NeoSoft
Covidence	Ntrepid
Creativity Software	Octastic
Esri	Polaris Wireless
EXFO	Providence

## Surveillance Exhibitors

Covidence	Semptian
Gamma Group	Sinovatio
Providence	UK Speedog

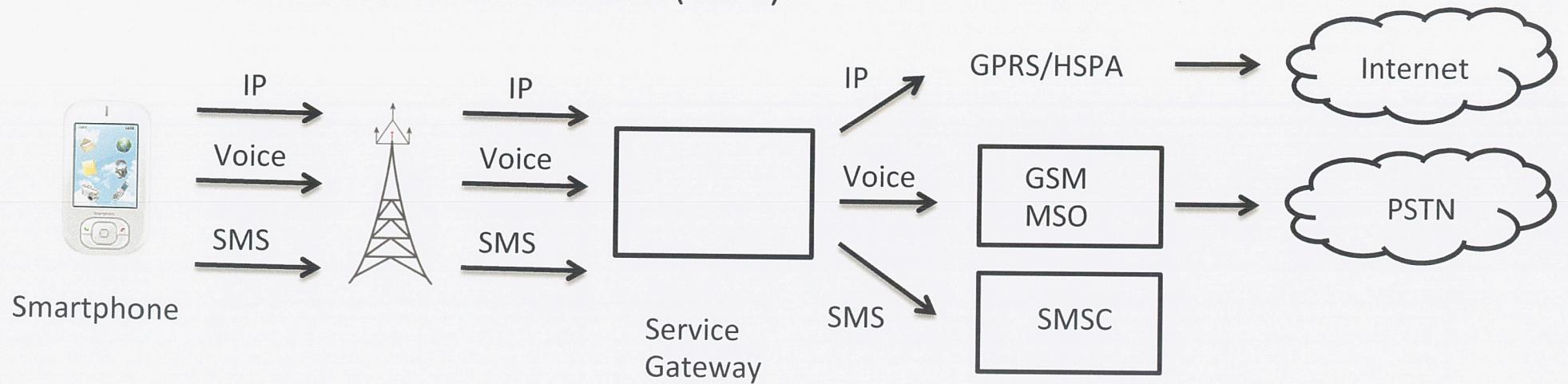
# Challenge #7: An All IP LTE Infrastructure

## Long Term Evolution (LTE) and Voice Service Options

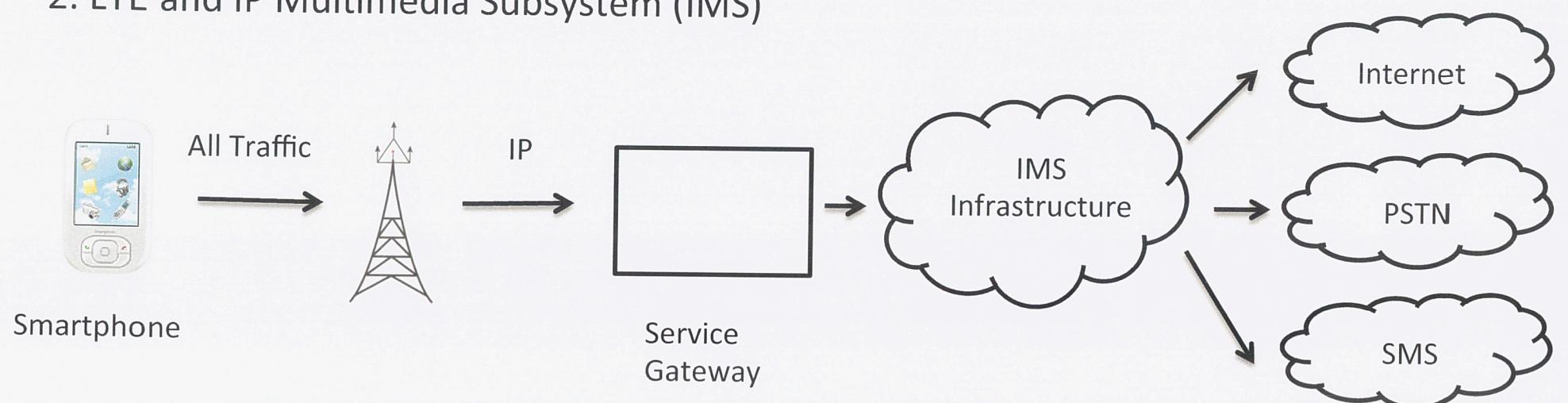
1. Use 2G/3G Circuit Switching for Voice  
(So Called LTE-CSFB)
2. Send Voice as VoIP over Data Broadband Service  
(So Called Over The Top)
3. Replace Circuit Switching and Move to an All IP Infrastructure  
(So Called LTE – With IP Multimedia System (IMS))

# LTE and Voice Network Options

## 1. LTE and Circuit Switched Fall Back (CSFB)



## 2. LTE and IP Multimedia Subsystem (IMS)



# LTE Evolution and Lawful Interception Session

Track 1 Today: 15:30-16:00

Lawful Interception of LTE, VoLTE and RCS, **Utimaco Software AG**

Track 7 Today: 11:30-12:30

CDMA Catcher and GSM/3G/LTE Catcher with Public Number  
Detection, **NeoSoft AG**

# Mediation, Data Retention and Monitoring Center Vendors at ISS World Middle East 2014

Advanced Systems  
AGT  
Aqsacom  
AREA  
ATIS  
BTT  
ClearTrail  
COM-SUR  
Global Security Network  
GR Sistemi  
Group2000  
INNOVA  
iPS  
iSolv  
RCS  
Sinovatio  
SS8  
Trovicor  
Utimaco

# Challenge #8: Dark Web

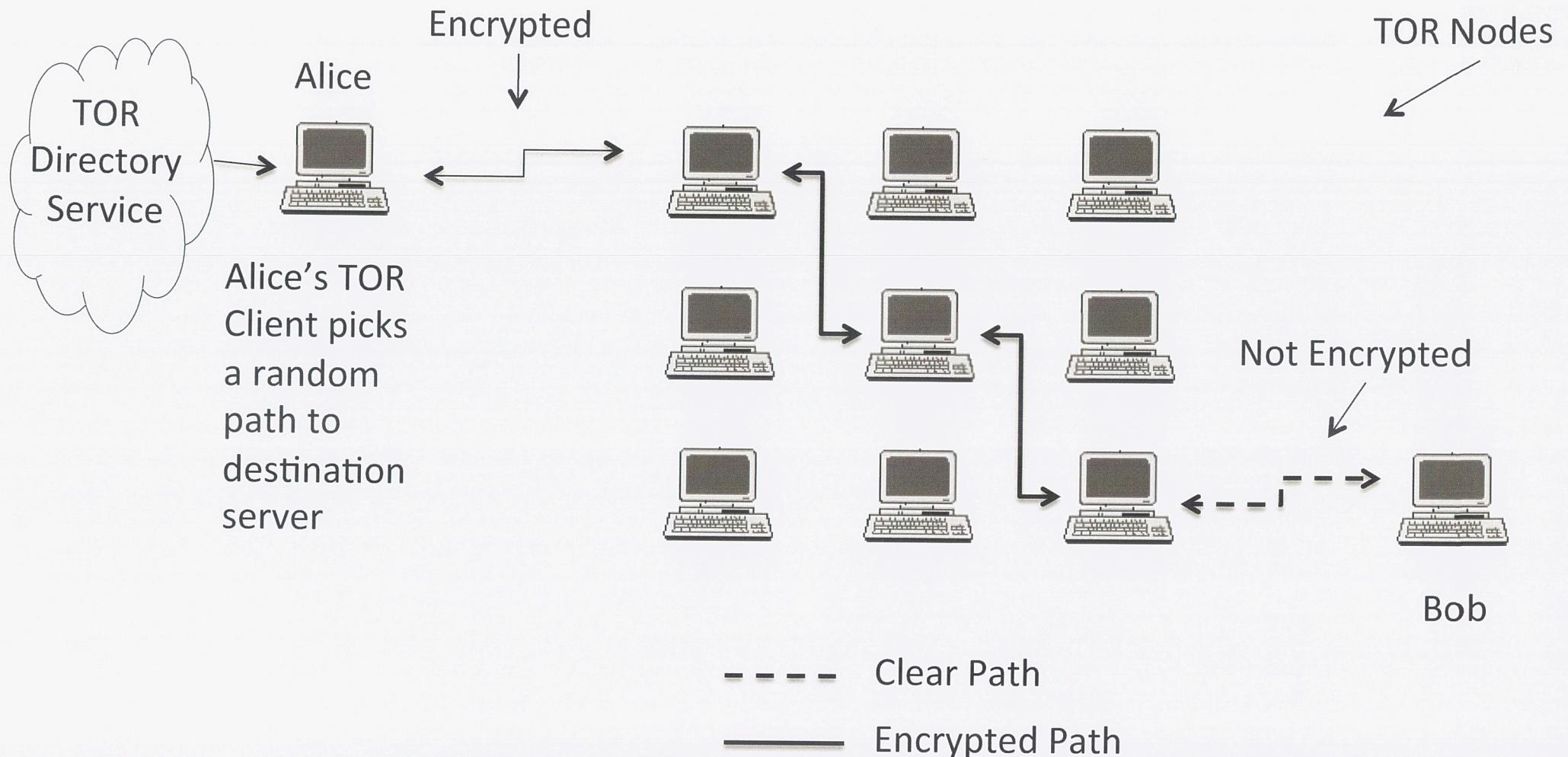
## Dark Web Example: Silk Road

- The eBay of Illegal Drugs
- US FBI Says \$1.2 Billion Transactions Until Shut Down
- Took The FBI Two And A Half Years to Shut It Down and Just Four Weeks for Another to Pop Up As #1

## What Enables Dark Web?

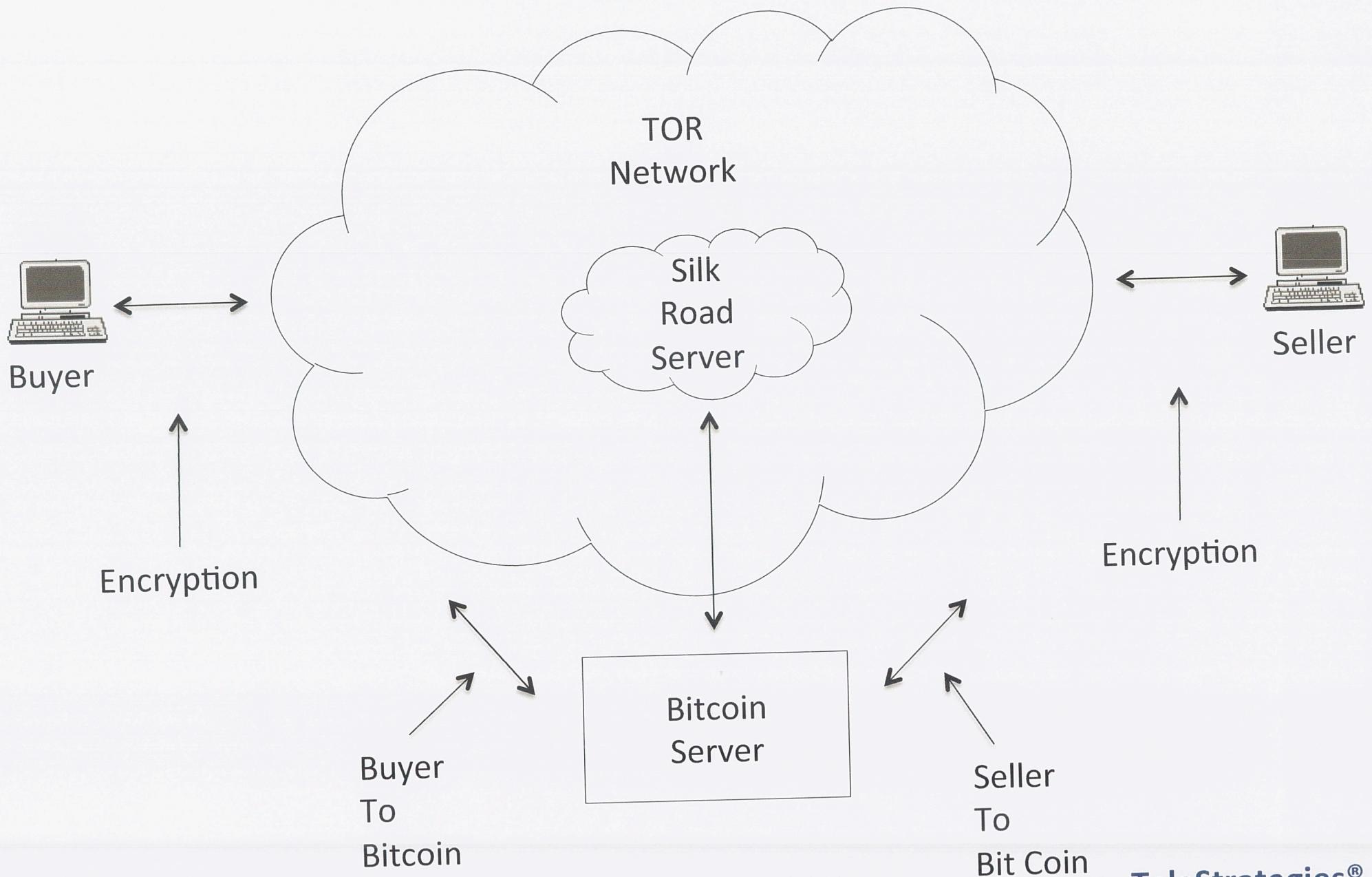
- 1) TOR (Suite of Software and Routers Enabling Anonymity)
- 2) Bitcoin (Crypto Currency That Is Virtual, Anonymous and Virtually Untraceable Currency)

# How TOR Works



\* Destination Identifies Message Sender as Last TOR

# Today's Dark Web



# Defeating Dark Web Operations

(Source: Bloggers and the Press)

1. Identify TOR Users
  2. Shift Traffic to “Government Man-in-the-Middle” Router
  3. Attack the Targets Installed TOR Web Browser
  4. Create a TOR Users Database
  5. Infect The Targets with Intrusion Software
- 

But, you need the assistance of Telecom Operators to identify  
TOR users and routing traffic to MITM infrastructure

Who has solutions at ISS World Middle East 2014?

Ask the IT Intrusion Vendors!

# Challenge #9: Dark Email

## Today's Email

- 95% Non-Encrypted
- But, You Have Free Encryption Called Pretty Good Privacy and Public-Key Cryptography
- Privacy Advocates Problem with P.G.P. – Metadata Sent in the Clear

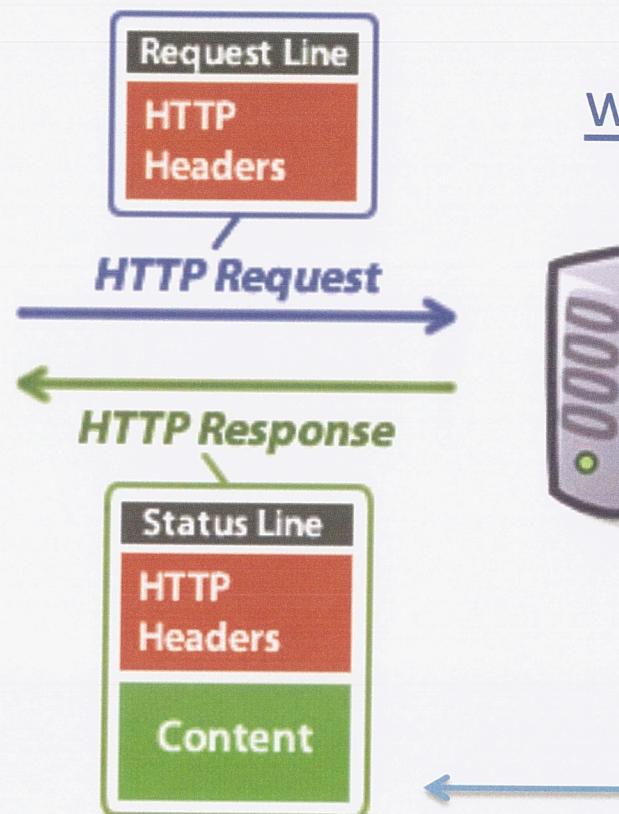
## Two Initiatives to An All Encrypted Email World

1. IETF's Prism-Proof Email Protocols or HTTP 2.0
2. Dark Mail Alliance

# How does HTTP work?

Request/response protocol

Phone, laptop,  
tablet, ...



[www.telestrategies.com](http://www.telestrategies.com)

Web Content ...  
Displayed in  
Browser

# HTTP 1.1 vs. HTTP 2.0

## HTTP 1.1 is slow

- Request one at a time, text then image & next image
- Each request is acknowledged and processing goes on

## HTTP 2.0: Fast, complex and will be an LEA/IC challenge

- Multiple requests, multiple HTML elements per connection
- HTTP headers are compressed
- Encryption mandatory
- IETF determined to Prism-Proof the Internet with HTTP 2.0
- And more

# Dark Mail Alliance

1. Privacy advocate short comings of third party encryption services like Lava Bit and Silent Circle:

They store your encryption key and are subject to court orders to release the crypto keys.

2. Dark mail alliance started up by Lava Bit, Silent Circle and outside investors

3. What is the Goal:

- All content, subject line and metadata sent encrypted
- Generated keys are only held shortly and never on a server
- Device generated keys and a new one for each email

# Solutions to Dark Mail?

Ask The IT Intrusion Vendors at ISS World Middle East

But Both HTTP 2.0 and Dark Mail Alliance Are Works in Progress

# Challenge #10: Regulation Shortcomings

1. Most Lawful Intercept Laws are Outdated and It's Voice Circuit Switched Based
2. GPS Tracking and Conflicting Court Decisions
3. No "Lawful Intercept Type" Mandates for Portals and Social media
4. No Inter-Service Provider User Authentication
5. IETF and Its "Prism-Proof" Internet Goal

And more!

Recommended Session Tomorrow:

8:30-9:00

New LI/RD Standards Initiatives

*Tony Rutkowski, VP, Yaana Technologies*

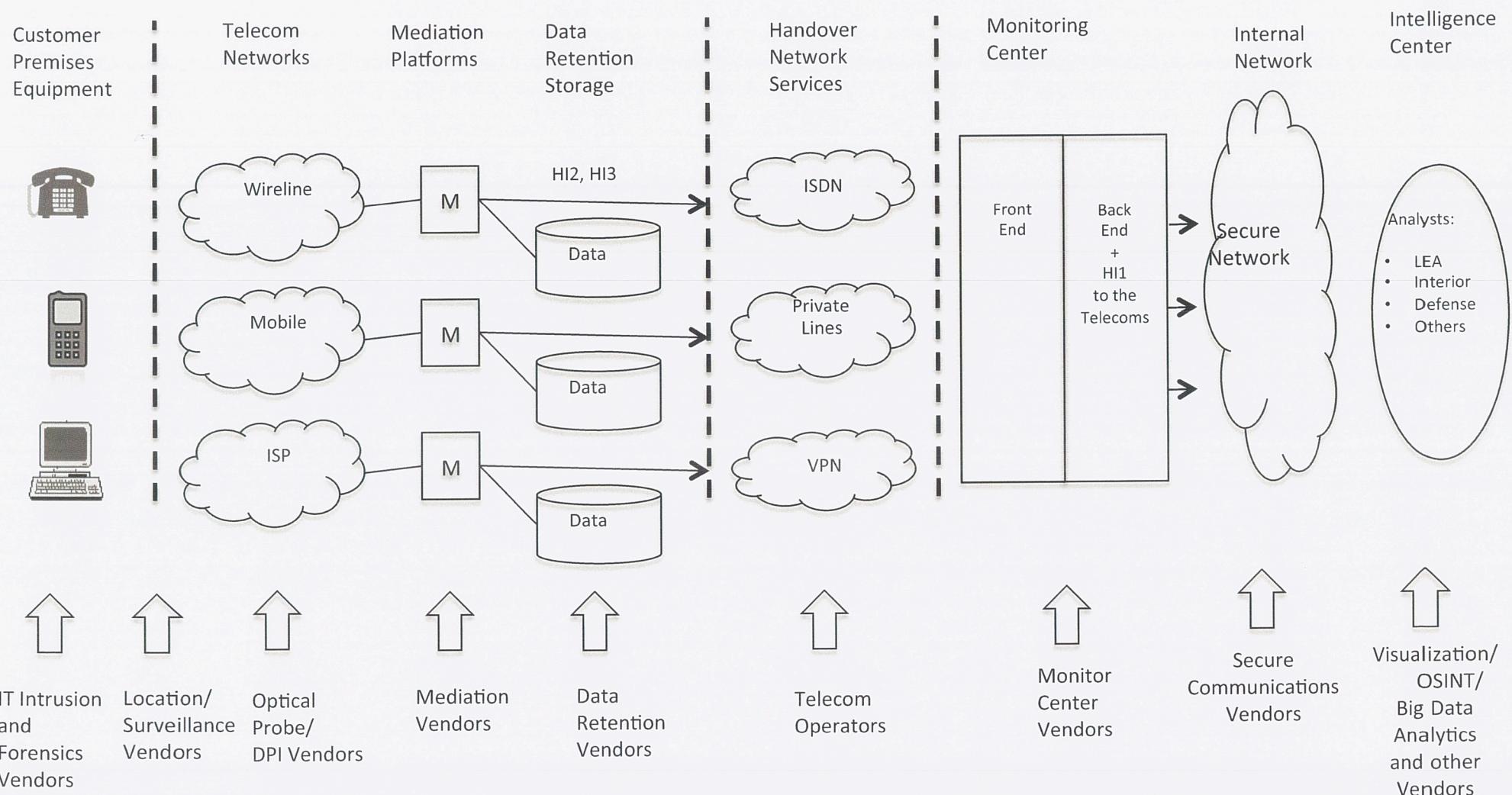
# Top Ten Internet Challenges Facing Law Enforcement and the Intelligence Community

1. Fiber Bandwidth Growth
2. Smartphones
3. Encryption
4. Social Media Monitoring
5. Increasing Data Volume
6. Tactical Surveillance
7. All IP LTE Mobile
8. Dark Web
9. Dark Email
10. Regulatory Shortcomings

# ISS Product Segmentation

1. Target Terminals (Spyware & Forensic Vendors)
2. Location & Surveillance Vendors
3. Optical Probe/DPI Vendors
4. Mediation and Mediation/DPI Vendors
5. Data Retention and Mediation/Data Retention Vendors
6. Monitoring Center: Front End
7. Monitoring Center: Back End (or Office)
8. Secure Networks
9. Intelligence Center Analytics

# Lawful Interception, Intelligence Gathering, Telecom Networks and ISS Vendors



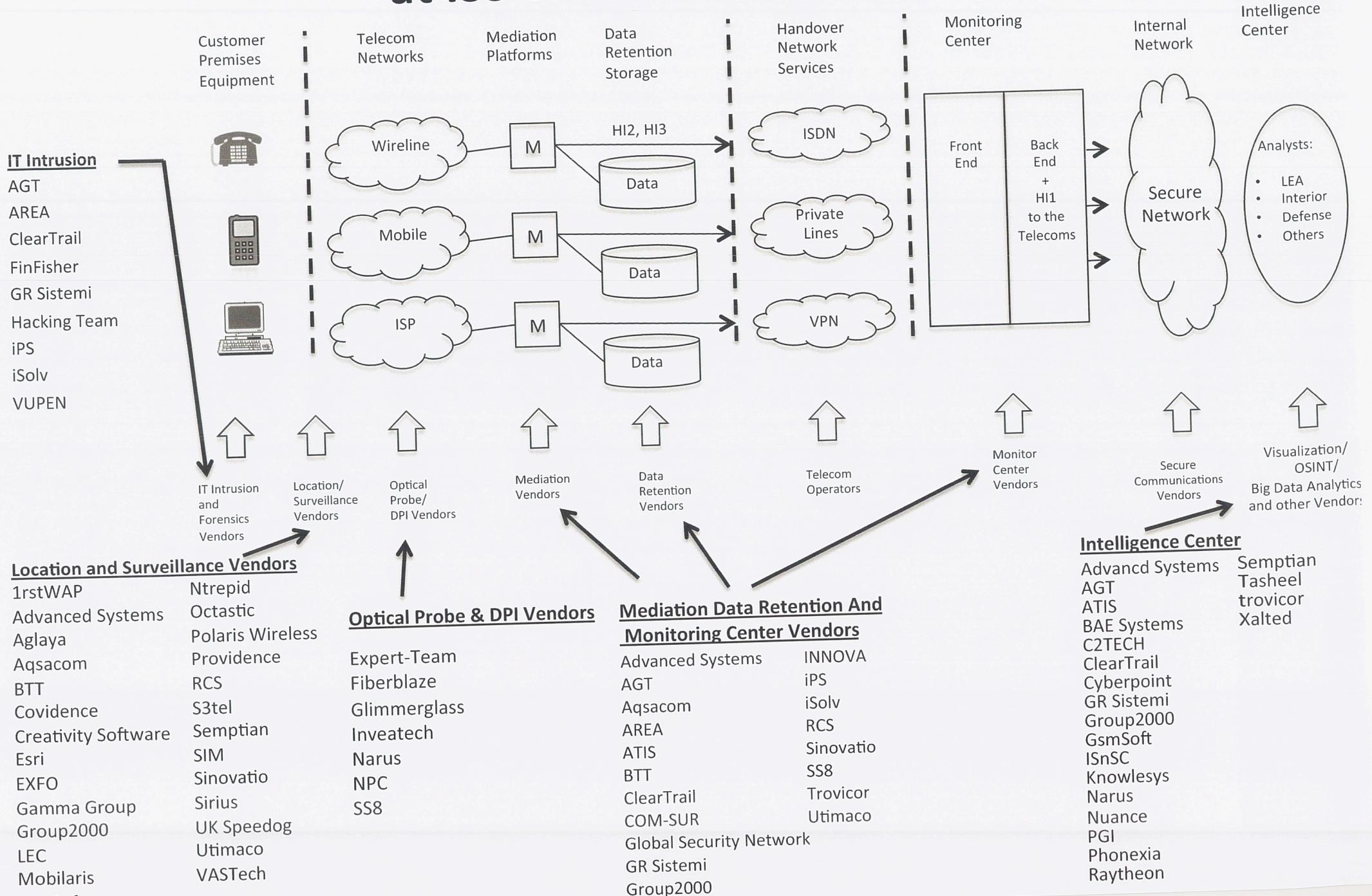
# ISS World® Middle East

**Intelligence Support Systems for Lawful Interception,  
Criminal Investigations and Intelligence Gathering**

## Exhibitors and Sponsors

1stWAP	FinFisher	Octastic
Advanced Systems	Gamma Group	PGI
Aglaya	Glimmerglass	Phonexia
AGT	Global Security Network	Polaris Wireless
Aqsacom	GR Sistemi	Providence
AREA	Group2000	Raytheon
ATIS	GsmSoft	RCS
BAE Systems	Hacking Team	S3tel
BTT	INNOVA	Semptian
C2TECH	Inveatech	SIM
ClearTrail	iPS	Sinovatio
Cobham	ISnSC	Sirius
COM-SUR	iSolv	SS8
Covidence	Knowlesys	Tasheel
Creativity Software	LEC	trovicor
cyberpoint	Mobilaris	UK Speedog
DataDirect	Narus	Utimaco
Esri	NeoSoft	VASTech
EXFO	NPC	VUPEN
Expert-Team	Ntrepid	Xalted
Fiberblaze	Nuance	

# Lawful Interception and Intelligence Gathering Exhibitors at ISS World Middle East



# Thank You for Joining us at ISS World Middle East 2014

Sessions Now Beginning at 9:00 AM

Exhibits Open at 10:00 AM with Refreshments

Lunch Served in the Exhibit Hall at 12:30 PM

NOTE: Drop Off Your Business Card or Fill Out Presentation  
and/or Training Certificate Request Form at the Registration Desk