Behind **Enemy** Lines

Practical & Triage Approaches to Mobile Security Abroad

Presentation **Objectives**

- Highlight the threats posed by traveling abroad with mobile devices
- Discuss lessons learned from real world experiences
- Provide practical recommendations for reducing these threats
- Do it all in 50 mins or less

About me

- Justin Morehouse (@mascasa)
  - Founder & Principal @ GuidePoint Security
  - Security Operations and Consulting
  - Co-author ‘Securing the Smart Grid’
  - OWASP Tampa Chapter Founder & Leader
  - Presented at DEF CON, ShmooCon, OWASP, and more...

My **addiction** to smartphones

- Since 2008 I've used and subsequently voided the warranties of the following:
  - BlackBerry Bold 9700 & 8820
  - HTC Nexus One (Android 2.3)
  - iPhone, 3G, 3GS, 4, 4s (All iOS versions)
  - Motorola Droid (Android 2.1, 2.2, 2.3)
  - Samsung Galaxy S (Android 2.1)
  - T-Mobile (HTC) Dash (Windows Mobile 6.5)

Why **mobile** security?

Everyone uses them...

Why **international** mobile security?

My **TripIt** profile page

Justin A Morehouse Pro

Email: justin.morehouse@gmail.com

Groups: GuidePoint Security

Basic Info | Upcoming Trips | Latest Activity

Home	Tampa, FL
Work	GuidePoint Security
More	Justin has traveled 154,528 mi to 46 locations including Washington, DC, Sydney, Australia, Denver, CO and Norfolk, VA

Connections (8)

Travel map Past Upcoming

Travel stats

	2012	Total
Trips	4	33
Days	35	181
Distance	36,077 mi	154,528 mi
Cities	12	46
Countries	5	9

Is **INTL** mobile security a **real** issue?

Domestic issues...

CARRIER iQ™

Home | Overview | Company | Support | Contact Us

Updated Dec 1, 2011 *Important clarification about the data received from mobile devices*

Carrier IQ is the leading provider of Mobile Service Intelligence Solutions to the Wireless Industry. As the only embedded analytics company to support millions of devices simultaneously, we give Wireless Carriers and Handset Manufacturers unprecedented insight into their customers' mobile experience.

"If I had this system in place when I planned our UMTS network, I could have saved 30% in costs, and made the network 50% more efficient"

Director of Network Planning, Tier 1 Carrier

Handsets currently deployed: 141,360,531

Raise Your IQ →

Domestic issues...

CARRIER iQ™

Home | Overview | Company | Support | Contact Us

Updated Dec 1, 2011 *Important clarification about the data received from mobile devices*

Carrier IQ is the leading provider of Mobile Service Intelligence Solutions to the Wireless Industry. As the only embedded analytics company to support millions of devices simultaneously, we give Wireless Carriers and Handset Manufacturers unprecedented insight into their customers' mobile experience.

"If I had this system in place when I planned our UMTS network, I could have saved 30% in costs, and made the network 50% more efficient"

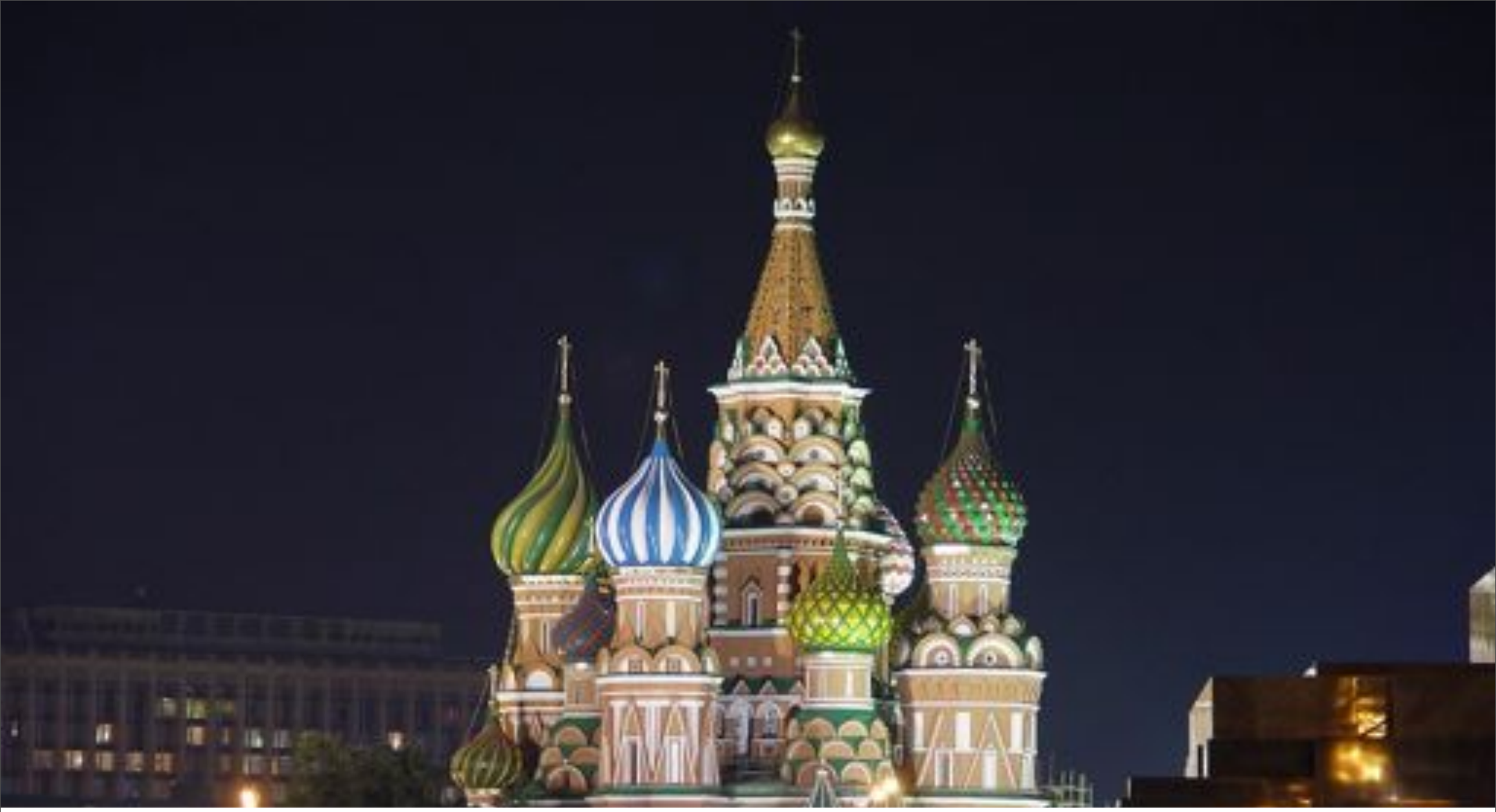
Director of Network Planning, Tier 1 Carrier

Handsets currently deployed: 141,360,531

Raise Your IQ →

“Unique” **international** issues...

Example #1



Example #2

personal **skepticism**

Wikileaks Spy Files

Wikileaks Spy Files

Wikileaks Spy Files

ability

Advance GSM Active Solution

Ability Computers & Software Industries (Israel)

IBIS - II

In Between Interception System

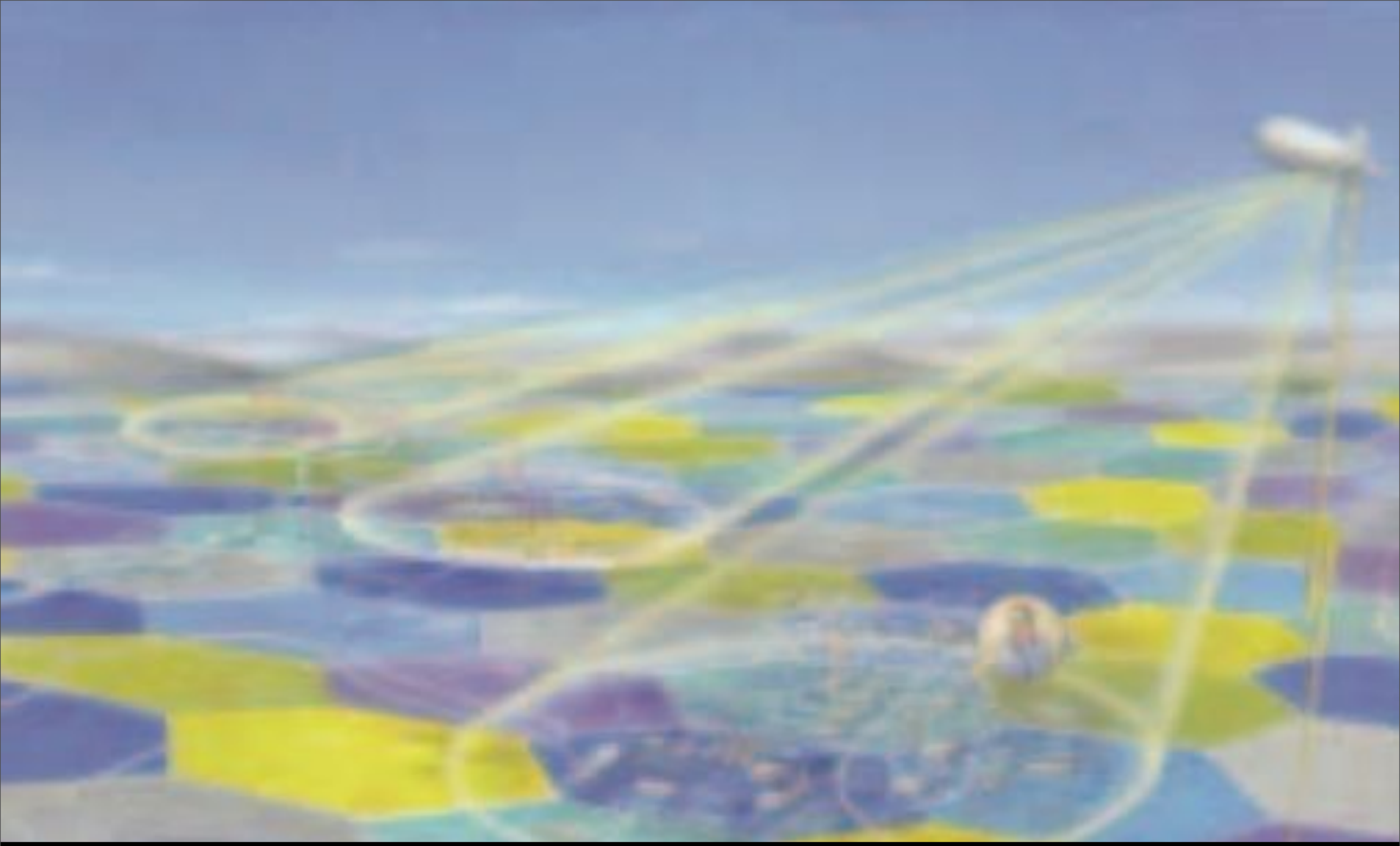
2nd Generation

VASTech (South Africa)

Elaman (Germany)

elaman

GSM-Monitoring System Semi Active – Falcon E+



ELTA (Israel Aerospace Industries)

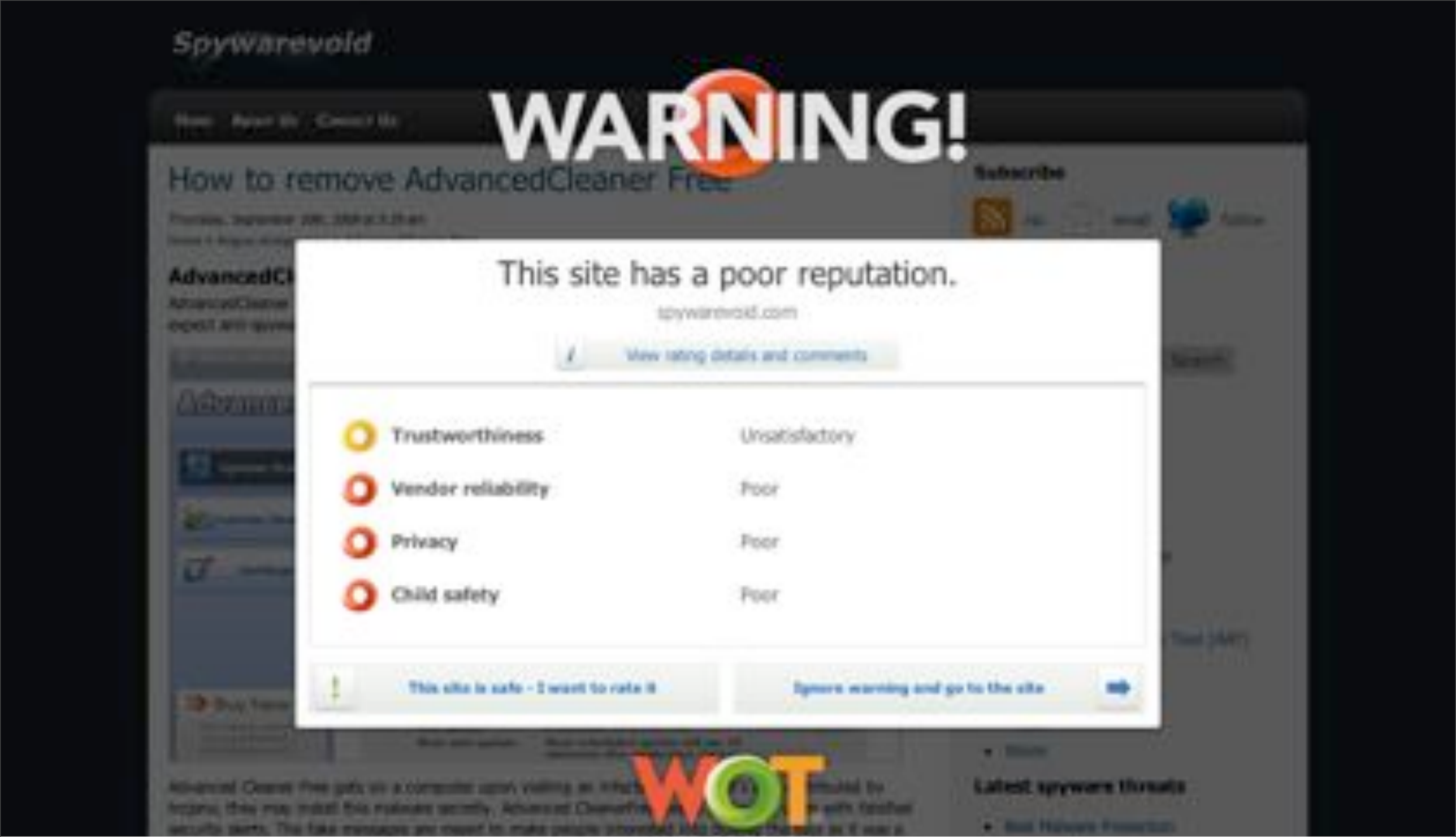
Spy Files **Continued...**

How you are **targeted** by threat agents


AT&T 3G
11:26 AM
Messages
51684
Edit
Thanks for your interest in our mobile donation program. Help us save lives today. Click the link below to make a donation: http://www.tmx.com
Jan 14, 2010 11:15 AM
Send

...phishing

evil maid attack



...and **drive-by** downloads

Not all **threats** are created equal...

Advanced Threats

Minimal Threats

Moderate Threats

Practical mitigation steps

Have a **plan**...

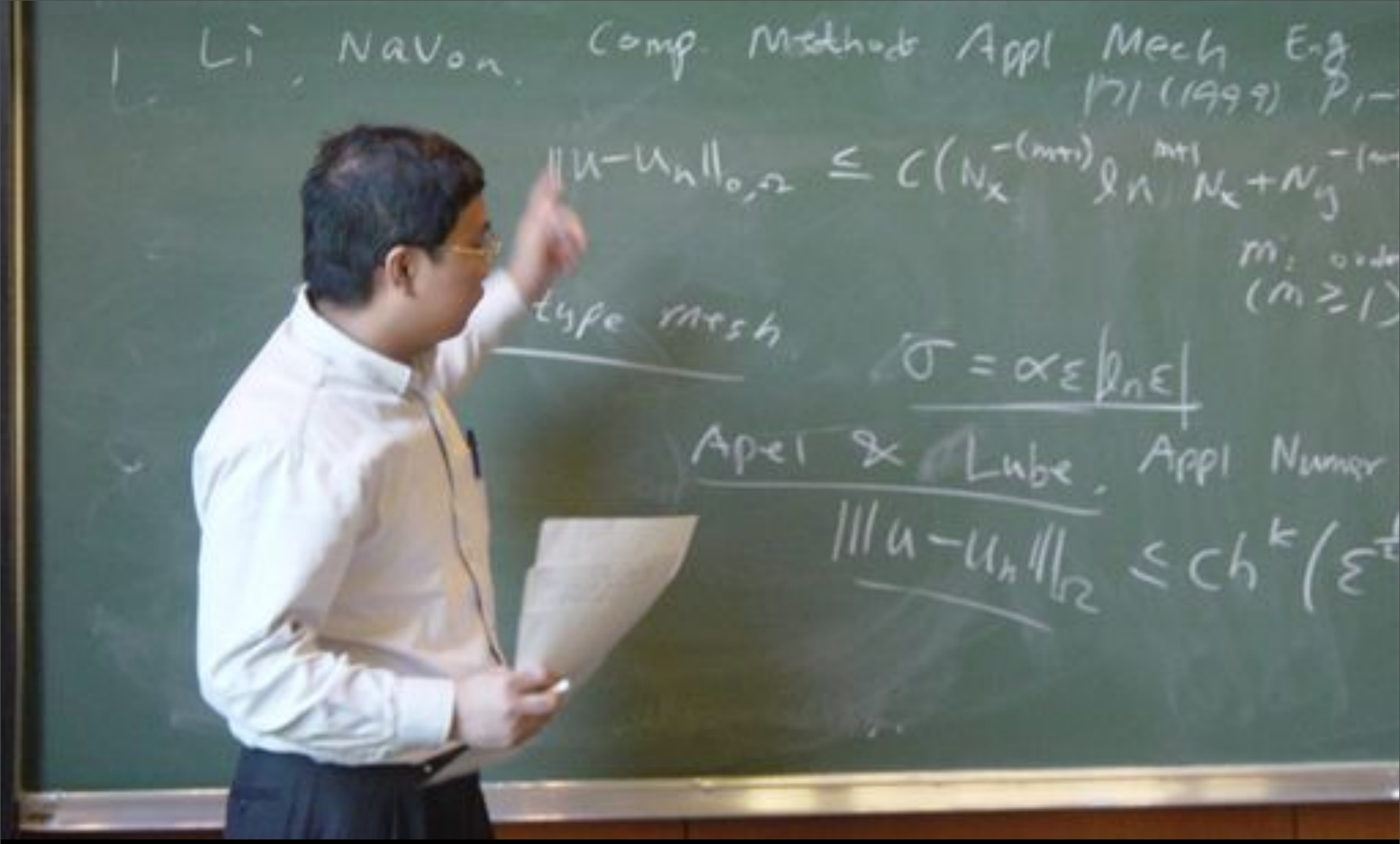
Make yourself
anonymous

(as possible)

the beauty of **prepaid**...

old school & **low** tech...

what about **data**?


Li, Navon Comp Methods Appl Mech Eng
171 (1999)
$\|u-u_h\|_{0,\Omega} \le C(N_x^{-(m+1)} \ln^{m+1} N_x + N_y^{-(m+1)}$
m: order
$(m \ge 1)$
type mesh
$\sigma = \alpha \varepsilon |\ln \varepsilon|$
Apel & Lube, Appl Numer
$|||u-u_h|||_\Omega \le Ch^k(\varepsilon^{\frac{1}{2}}$

Case Study

Client Overview

- Well-known multi-national organization w/ US HQ
- Executives traveling to hostile countries with moderate threats
- Loss of IP would be harmful to organization if obtained by competition

Proposed Solution

- Utilize factory unlocked iPhone 4s ‘burner’ phones
- Preconfigure with VPN, encryption, PIN, remote wipe
- Purchase local SIM (with cash) upon arrival
- Perform forensics on phone upon return

Solution **Issues**

- Executives often forgot to enable VPN before using data services
- Local SIM purchase required detailed information (passport)
- Executives used public wireless networks on several occasions

Lessons **Learned**

- Utilize configuration utilities to enforce policies on devices (No WiFi, VPN, etc.)
- Purchase local SIM cards in advance using anonymous(ish) means (BitCoin)
- Disable local syncing in favor of web-based solutions
- Require two-factor authentication for all web-based solutions
- Setup local # that forwards to US
- Tunnel your tunnels (VPN & SSL)

Effective mobile security triage

Plan for the **Worst**

- Knowledge is key (DO's and DON'Ts cheat-sheet)
- Rule of ~~3~~2 (w/ prepaid [anon] SIM)
- Remote deployment solutions (Wipe & rebuild required)
- Overnight INTL shipping

Questions?

Justin Morehouse
justin.morehouse@guidepointsecurity.com
www.guidepointsecurity.com
@mascasa