NYM ISSA MEETING

Cellular Eavesdropping: an Evidence-based Discussion

12 April 2011

Agenda

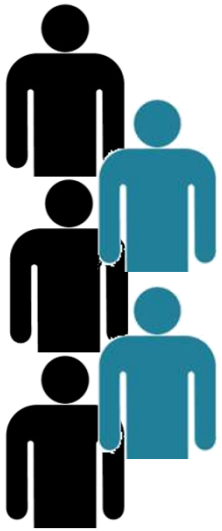
- Information Paths & The IA Security Gap
- Cellular & Security
- Eavesdropping Attack Vectors
- Protection Methods

Information Paths

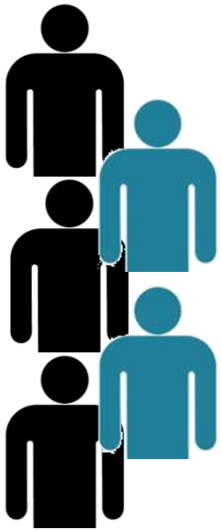
On a transaction,

from each party…

- Executives
- Boards
- Bankers
- Lawyers
- Consultants
- Auditors



3 Primary Information Paths

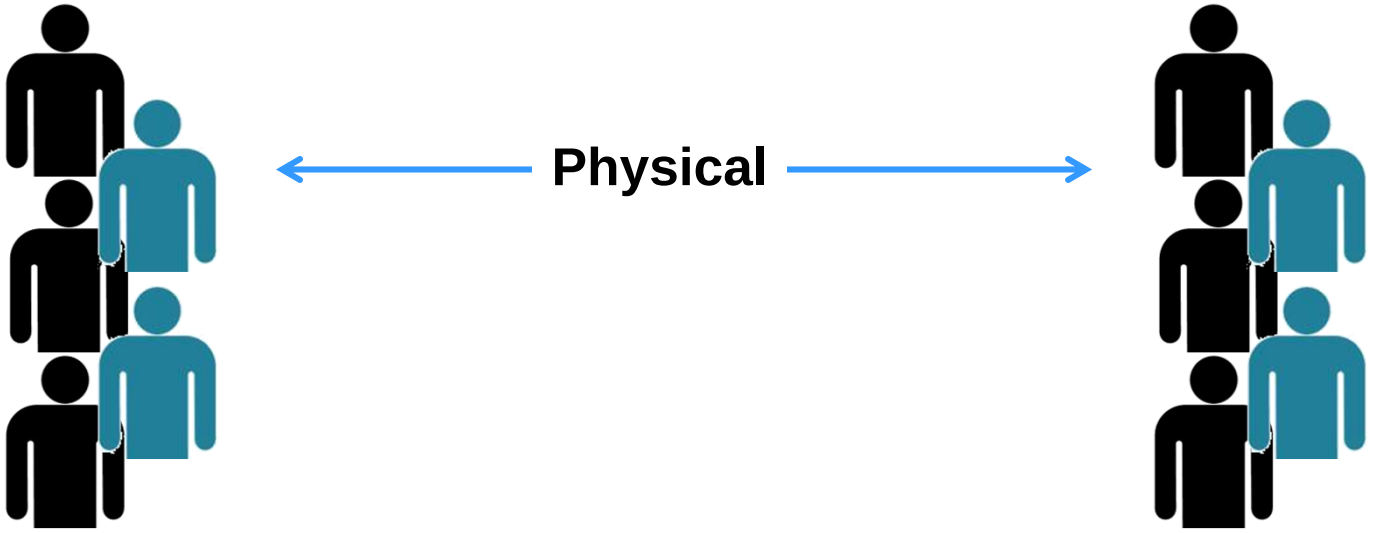


Information Paths

On a transaction,

from each party…

- Executives
- Boards
- Bankers
- Lawyers
- Consultants
- Auditors



- **Face-to-face meetings**
- **Overnight couriers**

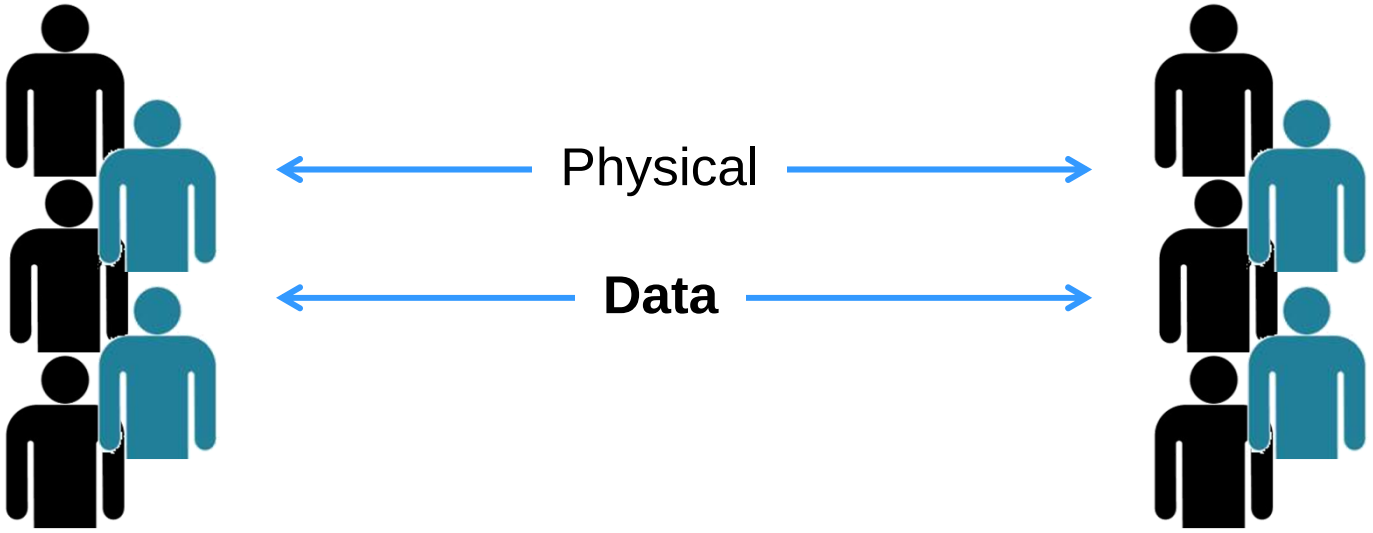
$

Information Paths

On a transaction,

from each party…

- Executives
- Boards
- Bankers
- Lawyers
- Consultants
- Auditors



- **Network protection**
- **Equipment protection**

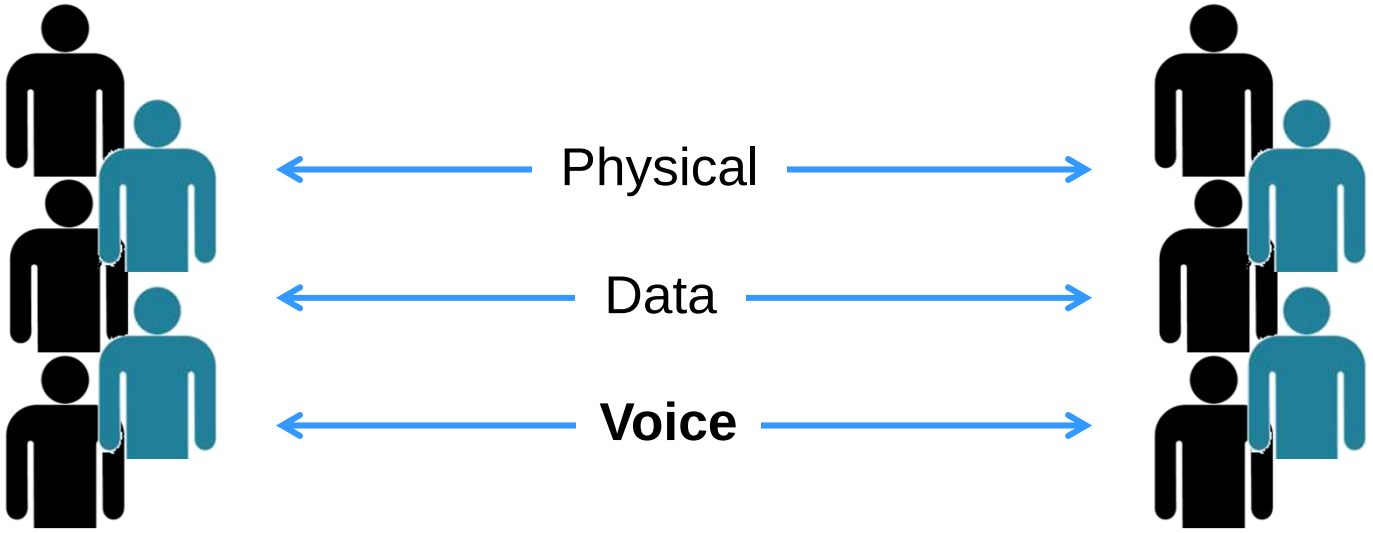
$$$

Information Paths

On a transaction,

from each party…

- Executives
- Boards
- Bankers
- Lawyers
- Consultants
- Auditors

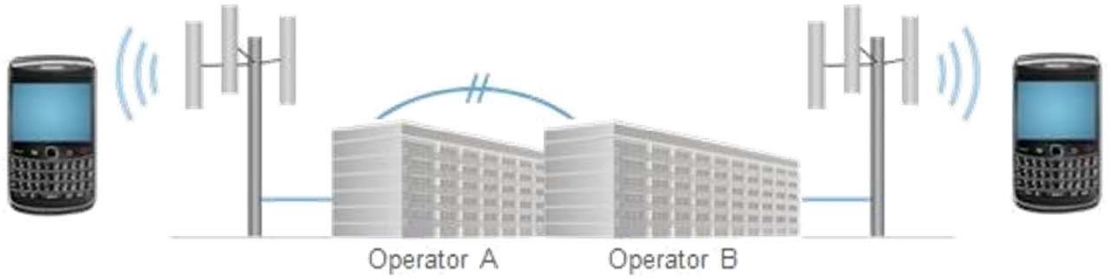


- **Mobile protection**
- **Landline protection**

???

Cellular & Security

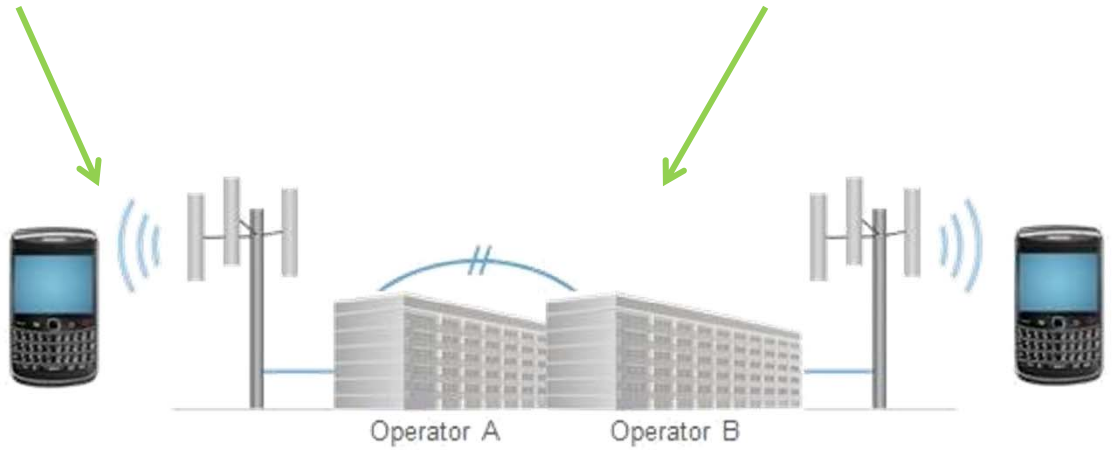
Typical Cell Call



Cellular Security

Air link authentication and encryption

“Gates, guards and guns”

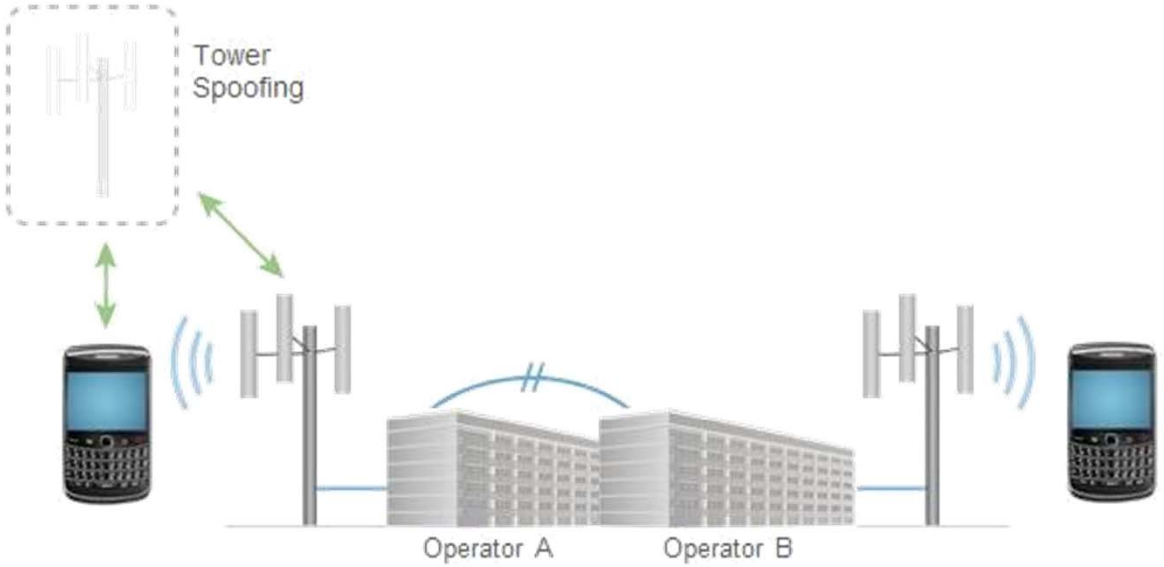


Do You Need Additional Security?

- *How sensitive is your information shared on mobile calls?*
- As with any communications system, information value/confidentiality dictates the level of security solution required
- AT&T Mobility and leading carriers around globe can support any level of mobile security – from normal use to the most sensitive information anywhere

Eavesdropping Attack Vectors

Eavesdropping Attack Vectors

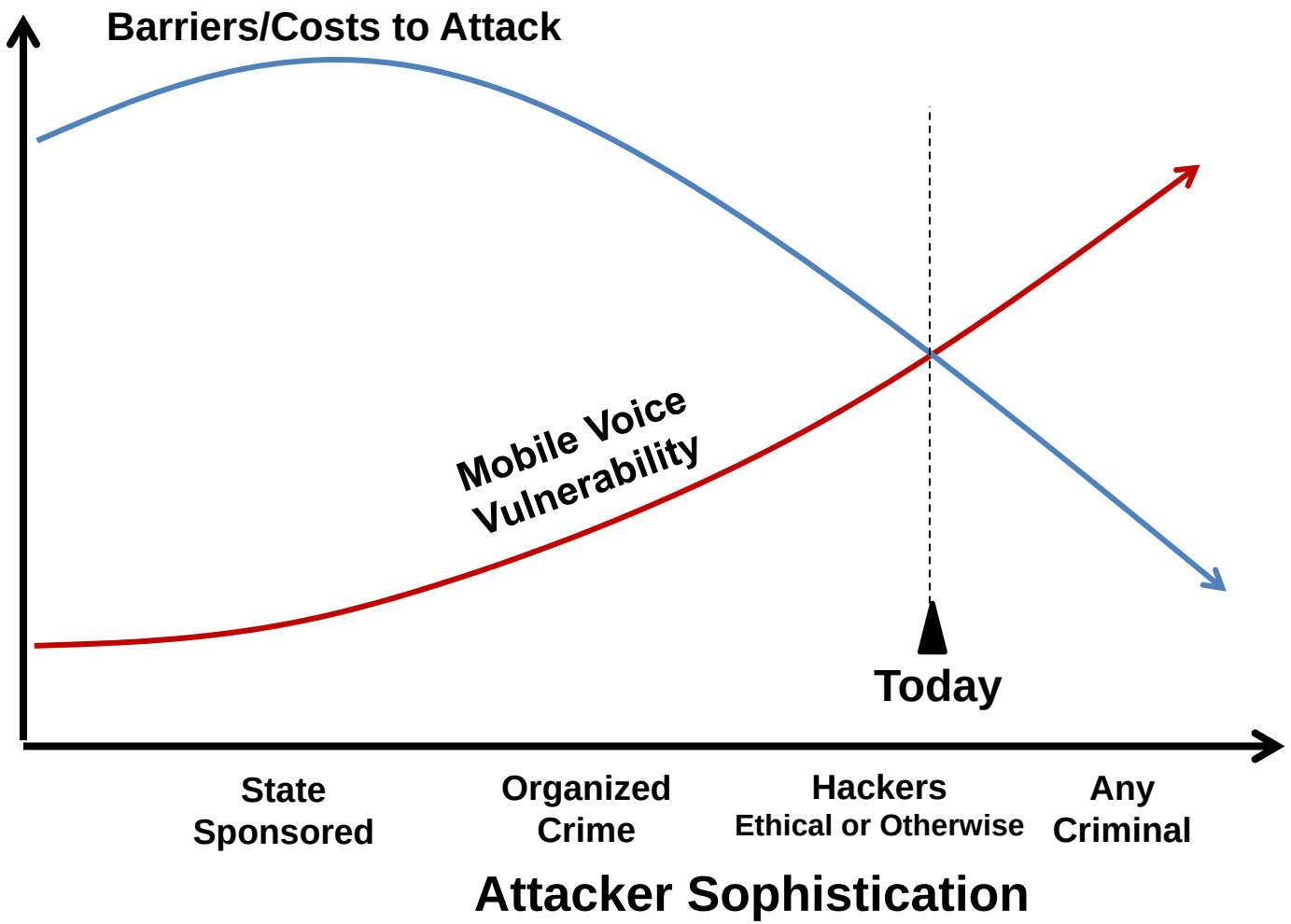


Tower Spoofing

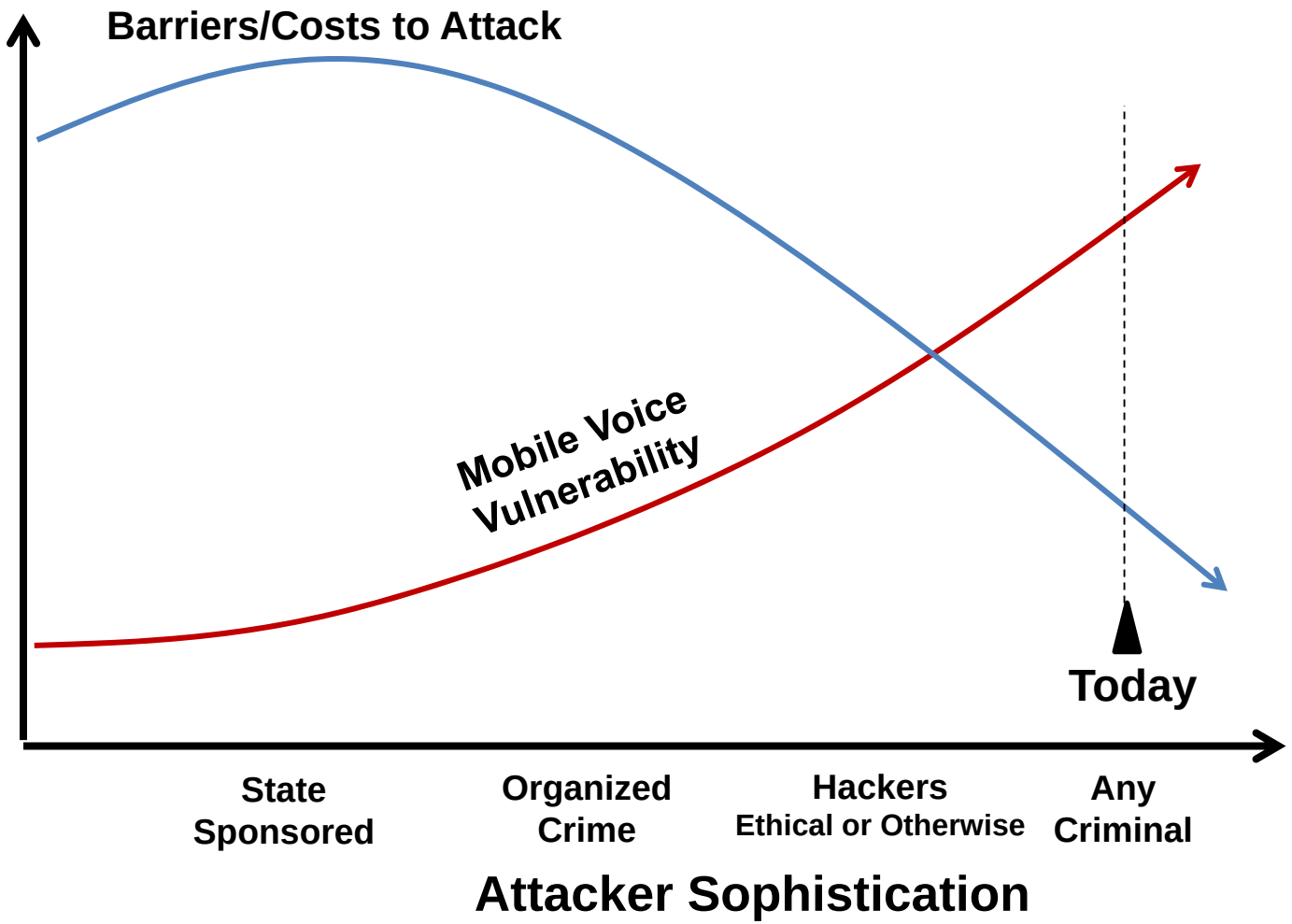
DefCon August 2010 – Las Vegas

- Phone automatically connects to strongest signal rogue tower
- “IMSI catcher” exploits authentication framework
- Cost of attack reportedly $1,500, primarily RF equipment
- “Bases station” code downloadable open source

Voice Intercept Becoming Cheap and Easy



Phishing, Bots, Etc… Already Cheap and Easy



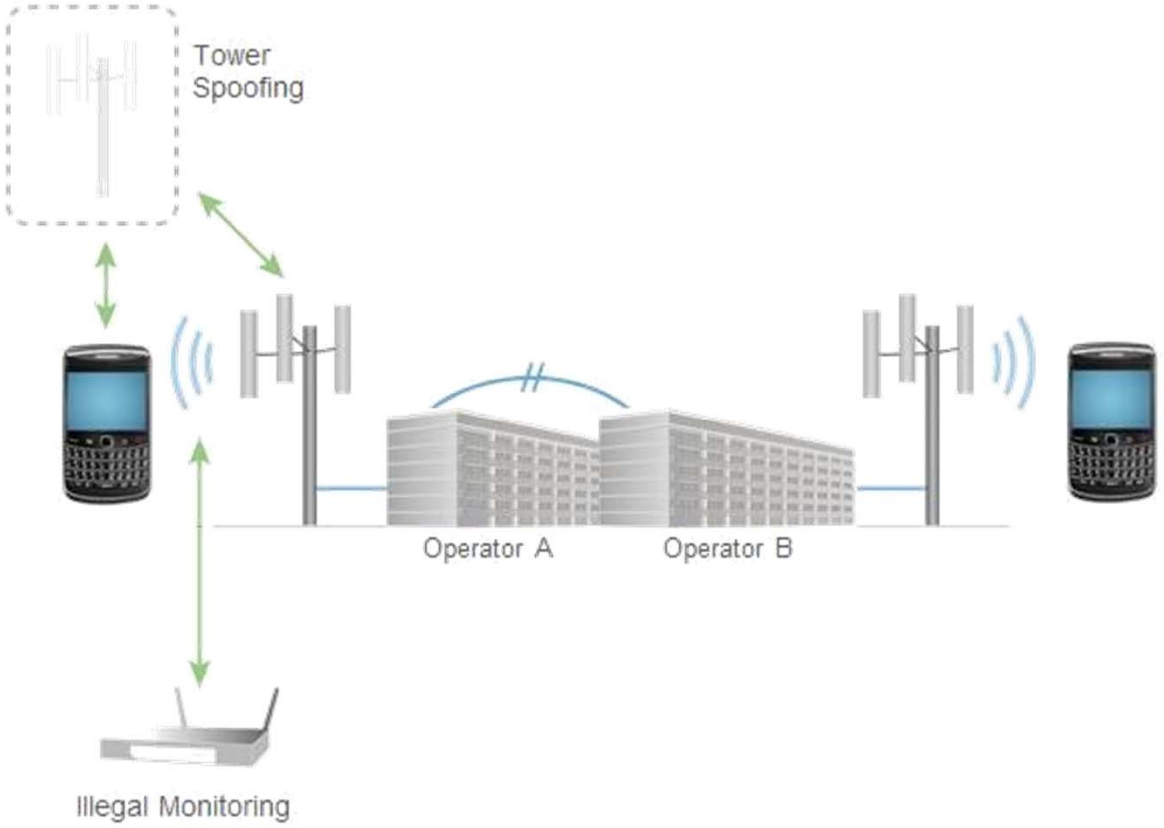
Tower Spoofing

http://www.youtube.com/meganetcorp#p/u/1/1eJ-WGpNQko

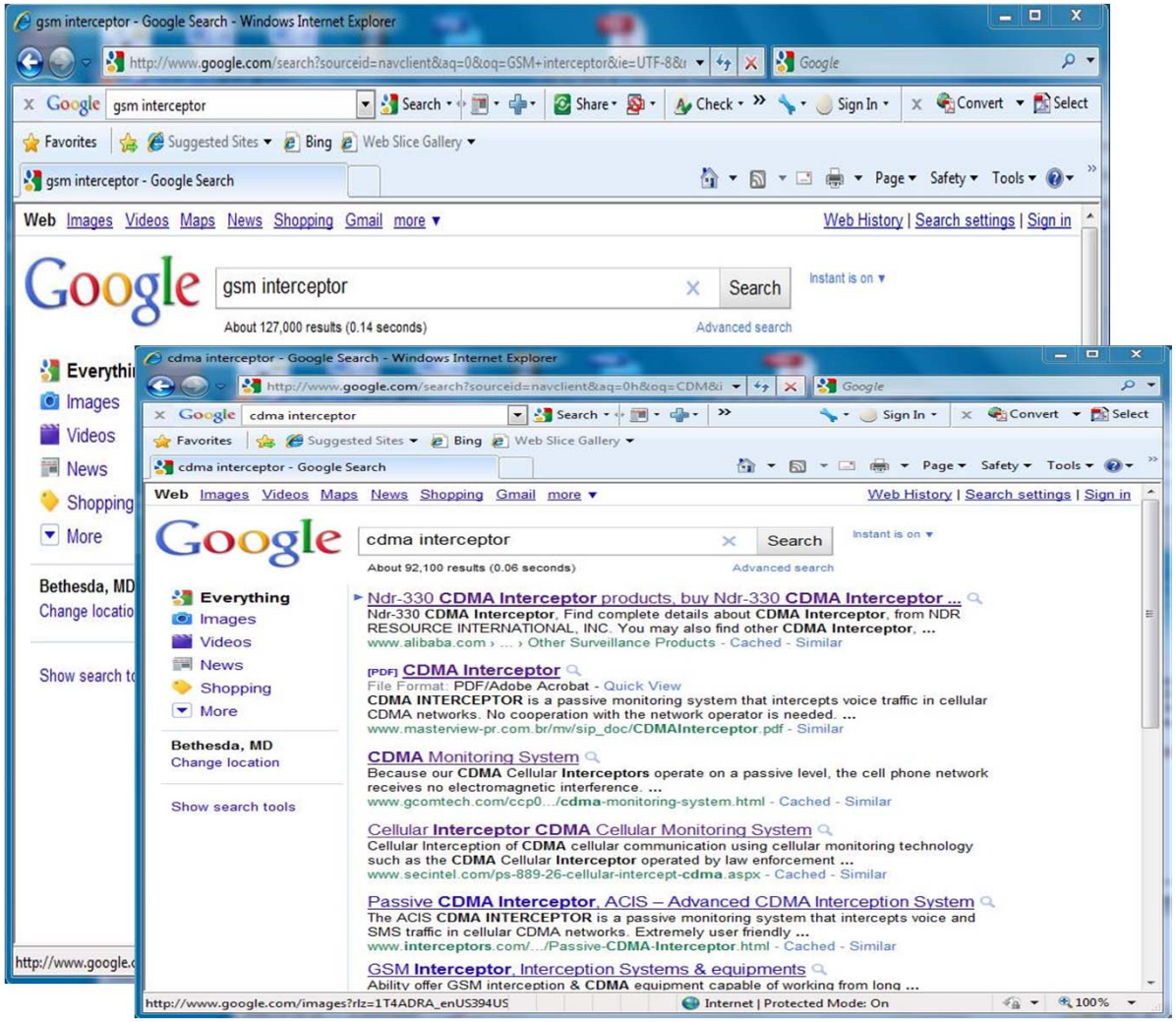
"Meganet's Dominator I snoops on four GSM convos at once, fits in your overnight bag"

~ Engaget

Eavesdropping Attack Vectors

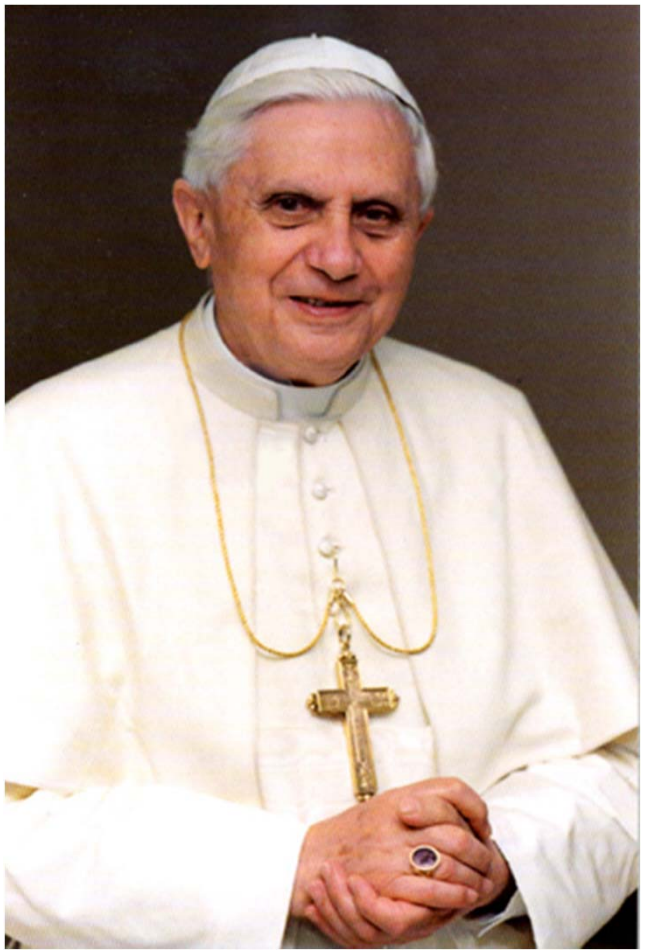


Illegal Monitoring

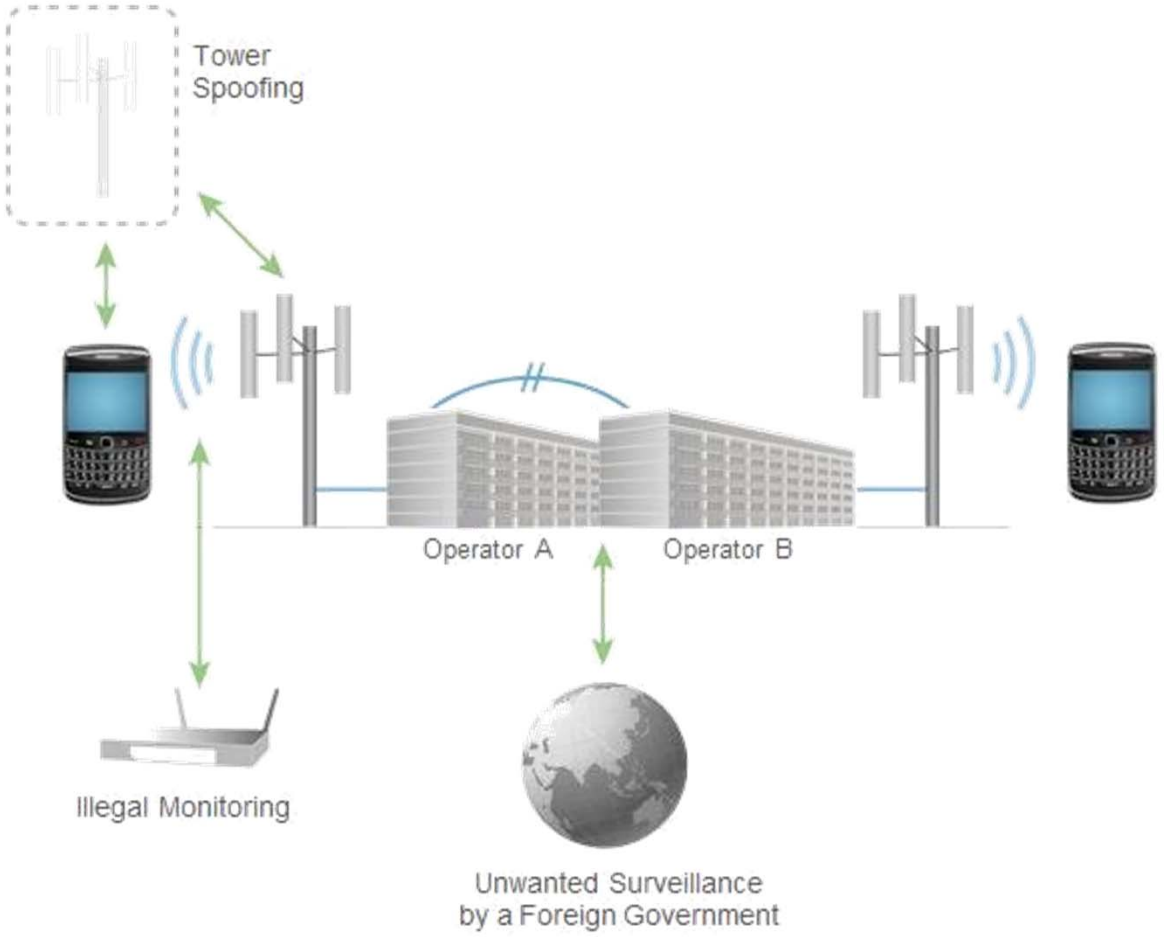


- Passive systems
- Similar to analogue scanners

What do they have in common?



Eavesdropping Attack Vectors



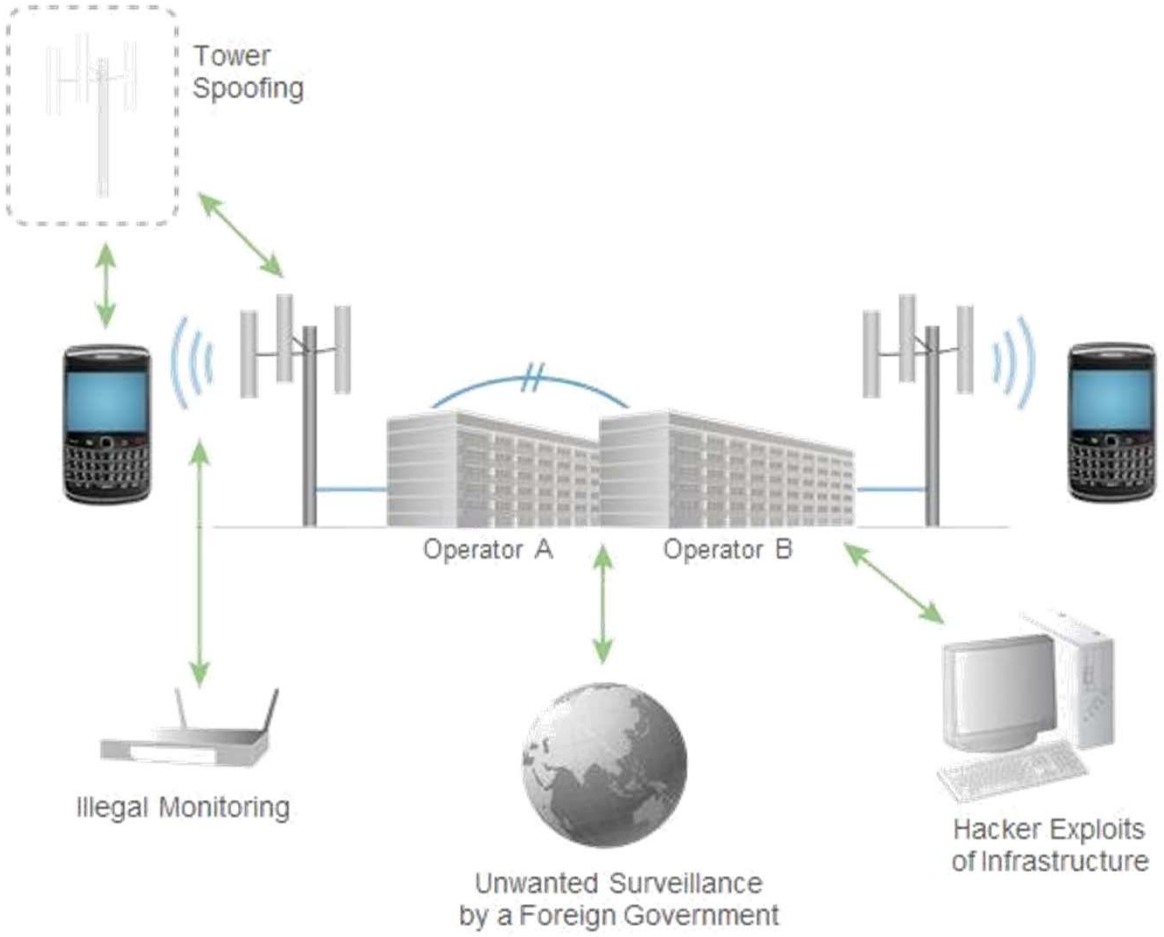
Unwanted Foreign Government Surveillance

The Telegraph

"Wiretapping is a widespread practice in Italy. Just this week it emerged that both Pope Benedict XVI and Hillary Clinton, the US secretary of state, had been inadvertently taped by Italian investigators."

10 June 2010

Eavesdropping Attack Vectors



Hacker Exploits

THE WALL STREET JOURNAL

Vodafone, Ericsson Get Hung Up In Greece's Phone-Tap Scandal

June 2006

ieee spectrum INSIDE TECHNOLOGY

The Athens Affair

How some extremely smart hackers pulled off the most audacious cell-network break-in ever

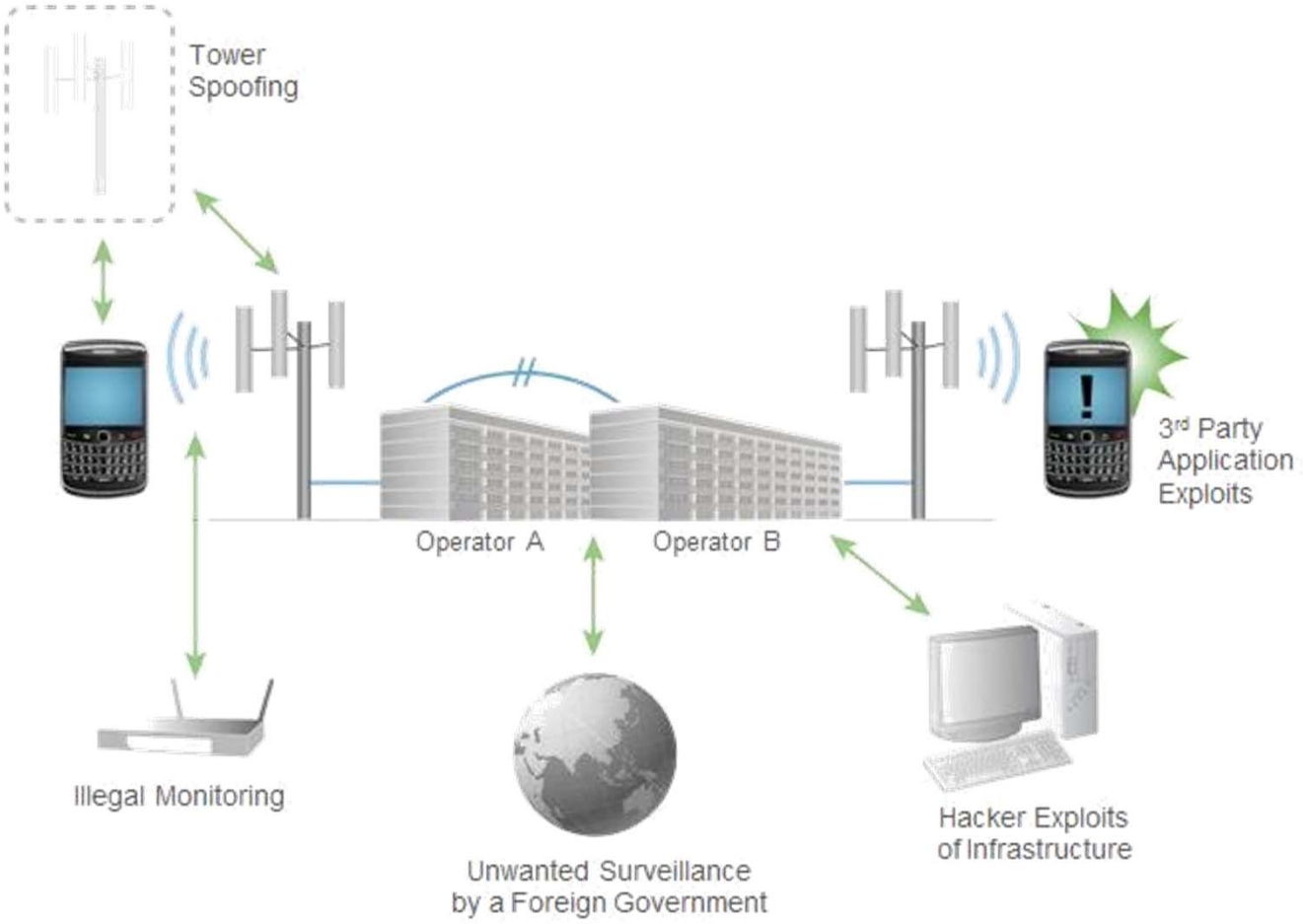
July 2007

Hacker Exploits

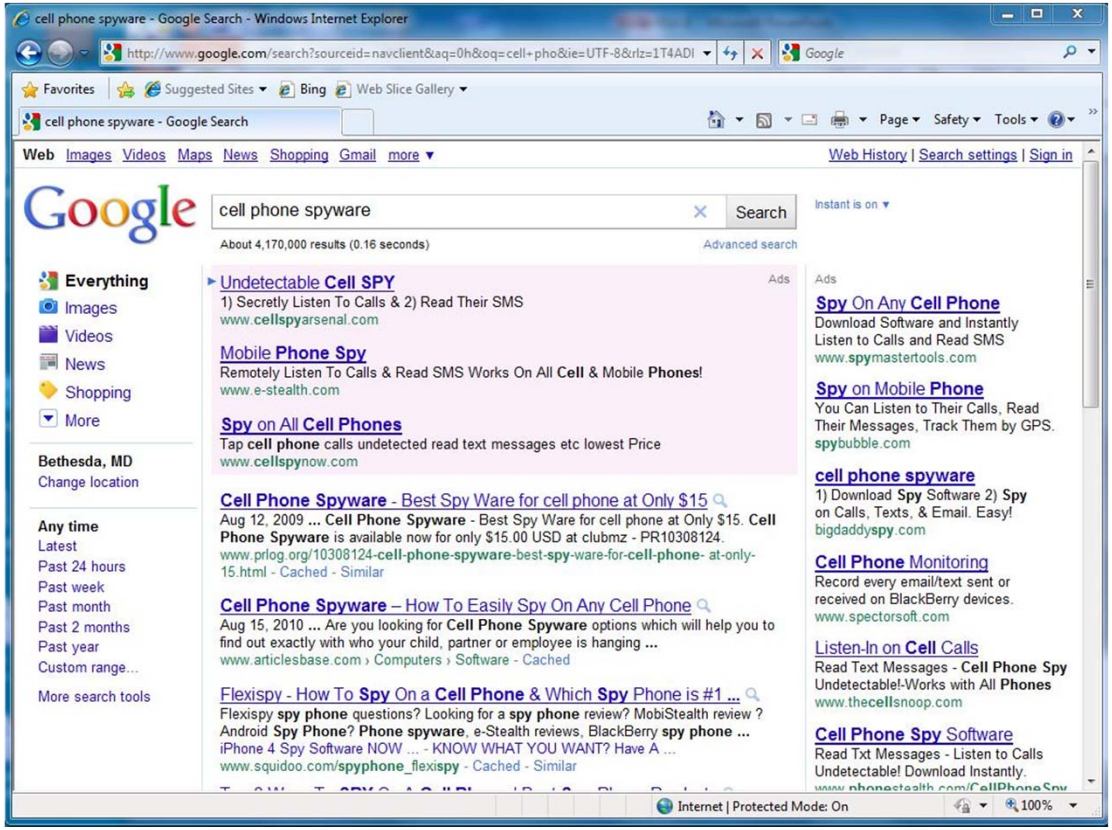
Chaos Computer Club December 2010 - Berlin

- Exploit involves device targeting via Internet service and ‘broken’ SMS messaging technique
- Cost of attack reportedly 10 Euros for each of 4 phones
- Firmware downloadable open source

Eavesdropping Attack Vectors

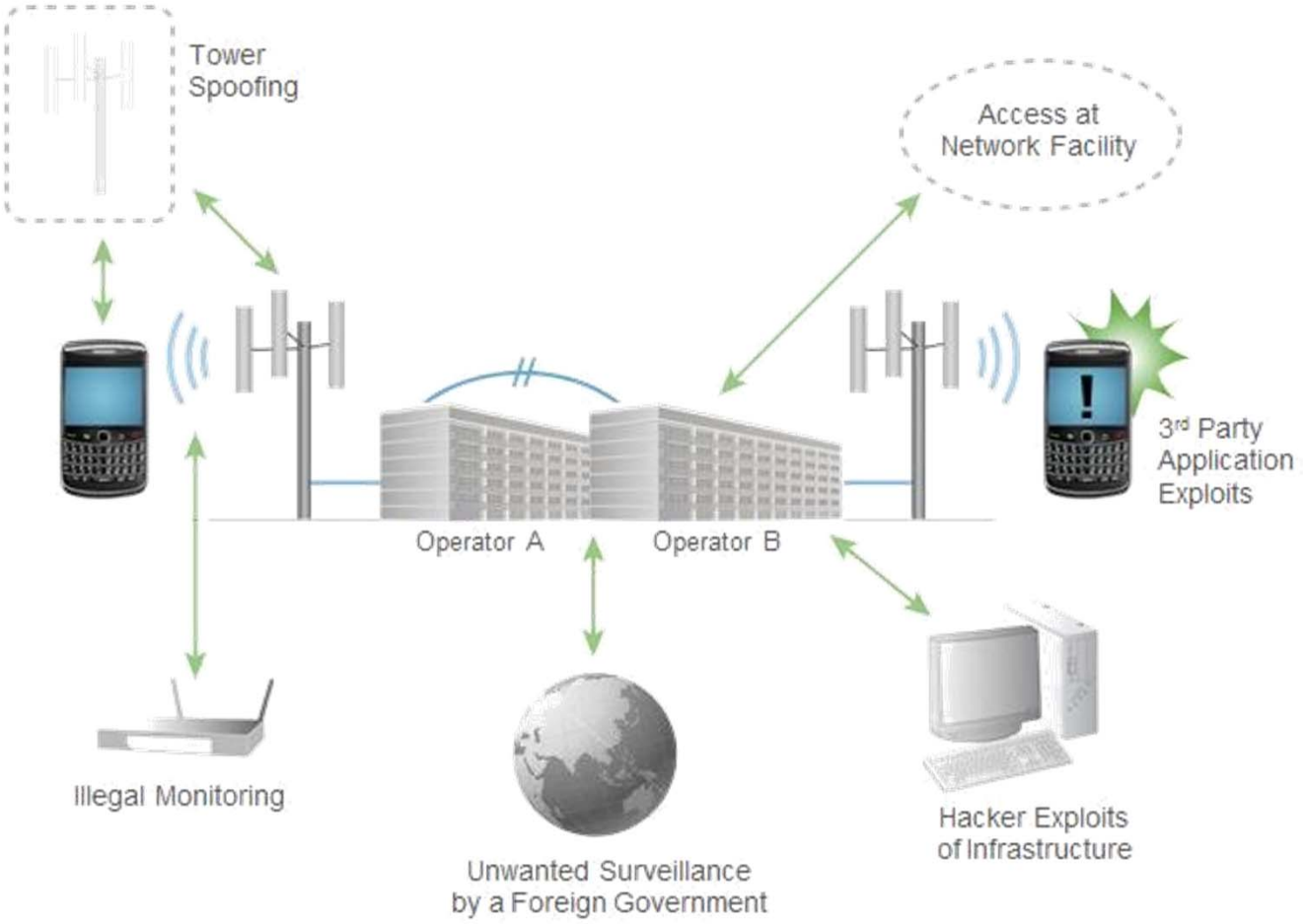


3rd-Party App Exploits



"KSL 5 Investigation: How your cell phone can be used against you"

Eavesdropping Attack Vectors



Access at Network Facility

"The *2009 CSI Computer Crime Survey*, probably one of the most respected reports covering insider threats, says insiders are responsible for 43 percent of malicious attacks. Twenty-five percent of respondents said that over 60 percent of their losses were due to nonmalicious actions by insiders. I've read many damage assessment reports stating that although insiders are responsible for fewer incidents than are outsiders, insider incidents usually result in more damage. Thus, the CSI data seems credible."

~ InfoWorld

Protection

Encrypted Mobile Voice

Fully integrated hardware, software and service solution from AT&T, SRA and KoolSpan

MERK

MOBILE ENCRYPTION RESPONSE KIT

Ideal For

- Incident response
- Investigations
- Sensitive transactions
- Physical safety
- International travel
- Untraceable information leaks

MERK Includes

- 10, 20 and 50 units kits
- Fully configured
- Security chip and app
- Hosted infrastructure

THANK YOU