



# Pen Testing a City

Greg Conti, Tom Cross and Dave Raymond

# Disclaimer

The views expressed in this talk are those of the authors and do not reflect the official policy or position of Drawbridge Networks, West Point, the Department of the Army, the Department of Defense, or the United States Government.

We are not lawyers, please consult your legal advisor before considering pen testing anything.



# Our Background



Tom Cross

Drawbridge Networks

@\_decius\_



David Raymond

Virginia Tech

@dnomyard



Greg Conti

West Point

@cyberbgone

# Why, So What, Who Cares



- Importance of Scaling Up
- Cities are critical to national security
- Hard to pen test a nation without an Army
- Cities are microcosms to explore best practices
- Generalized results can be applied across many cities

# Even without an Adversary...



**Two Inches of Snow in Atlanta (2014)**



**East Coast Power Outage (2003)**



**New York Blackout (1977)**



**San Francisco Earthquake (1906)**

<http://abcnews.go.com/us/wrong-atlanta-storm-chaos/story?id=22294035>  
<https://www.baruch.cuny.edu/nycdata/disasters/images/blackout-1977.jpg>

[http://en.wikipedia.org/wiki/Looking\\_Down\\_Sacramento\\_Street,\\_San\\_Francisco,\\_April\\_18,\\_1906#/media/File:San\\_Francisco\\_Fire\\_Sacramento\\_Street\\_1906-04-18.jpg](http://en.wikipedia.org/wiki/Looking_Down_Sacramento_Street,_San_Francisco,_April_18,_1906#/media/File:San_Francisco_Fire_Sacramento_Street_1906-04-18.jpg)



- **Introduction**
  - **Why, So What?**
  - **What is a City?**
  - **Smart Cities & Dumb Cities**
- Pen Testing
- Dissecting a City
- Cross Sectioning
- Pressure Points
- Risk Analysis
- Solutions

# What is a *city*?

cit·y

/'sɪdē/

*noun*

1. a large town.

“one of Italy’s most beautiful cities”

2. informal

a place or situation characterized by a specific attribute.

“panic city”

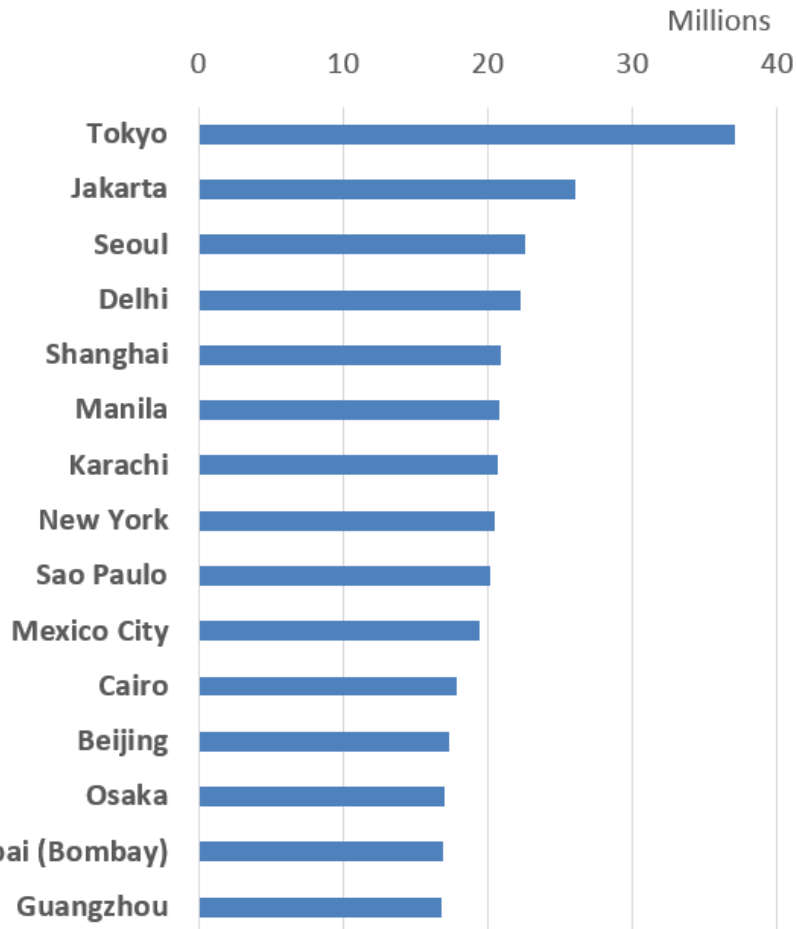
Google:

## **Attributes:**

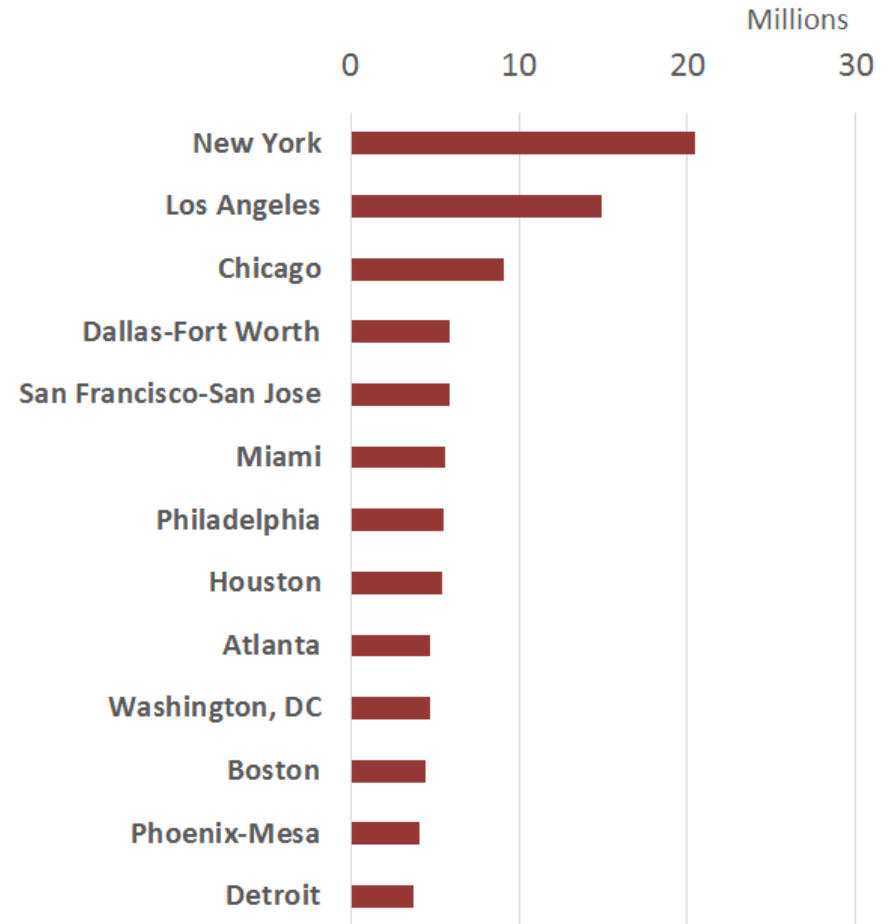
- A center of population, commerce, and culture (*thefreedictionary.com*)
- Incorporated municipality, usually governed by mayor and council (*Dictionary.com*)
- Has complex systems for sanitation, utilities, land usage, housing, and transportation (*Wikipedia*)

# Largest Cities

## Global



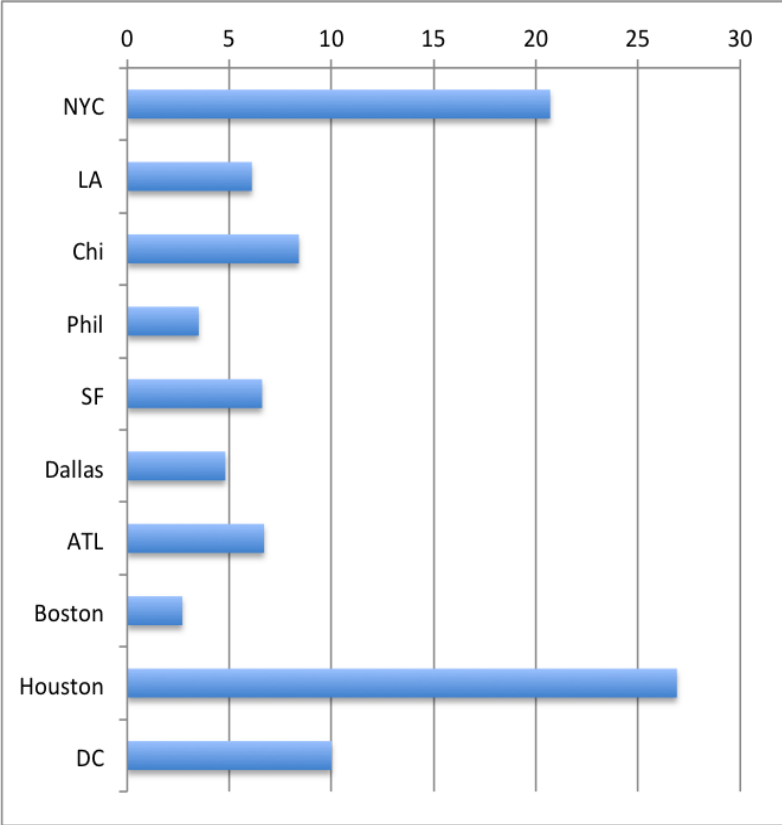
## US





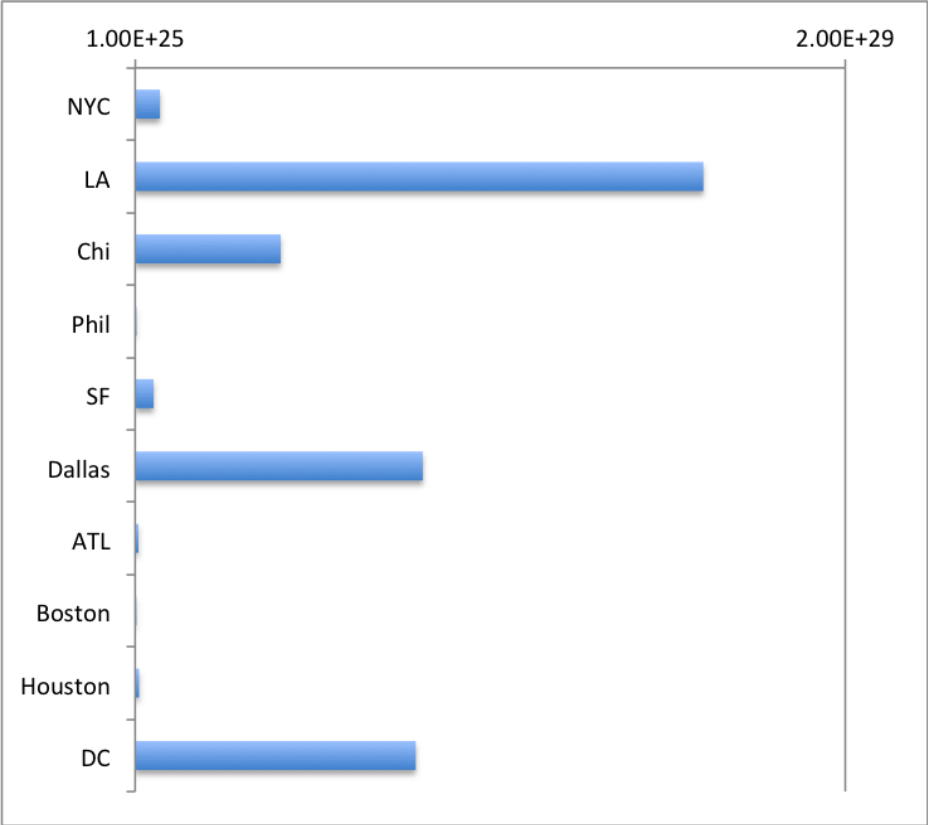
# IP Addresses per Metro Area DMA Code

IPv4 (millions)

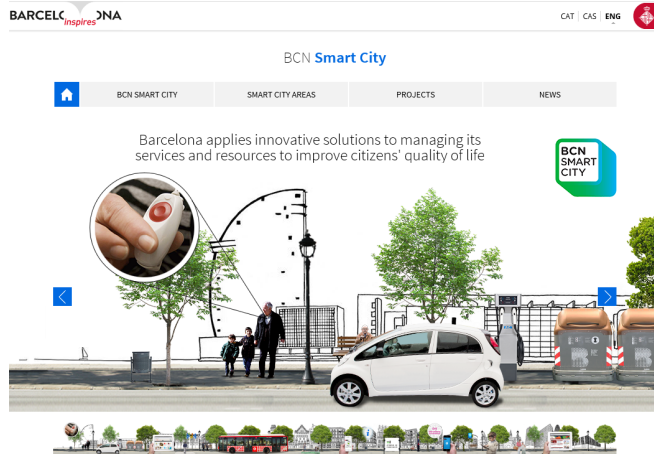


IPv6

(Illustrates relative adoption, but baseline is e^25.)



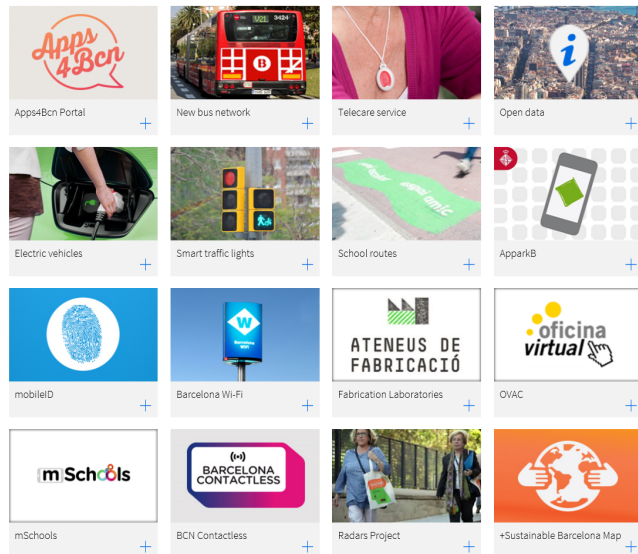
# Smart Cities = Larger Attack Surface



Barcelona, Spain

“cities and regions that use technology not just to save money or make things work better, but also to create high quality employment, increase citizen participation and become great places to live and work.”

- Intelligent Community Forum



Representative Projects

# Major Industry Initiatives

**Smart+Connected Communities**

**Transforming the Urban Experience**

Smart cities demonstrate the power of the Internet of Everything. (3:51 min)

**Addressing the Challenges of a Changing World**

As world populations migrate to urban areas, cities are faced with new challenges. These may include traffic jams, overcrowding, pollution, resource constraints, inadequate infrastructure, and the need for continuing economic growth. Cisco Smart+Connected Communities solutions can help city leaders address these problems using intelligent networking capabilities. The solutions can provide the information and services needed to create more livable cities, and help them thrive.

**Smart+Connected City**

The Smart+Connected City solution portfolio includes remote access to government services as well as City Infrastructure Management solutions for connected parking, traffic, and safety and security. Smart+Connected City solutions include:

- Smart+Connected City Wi-Fi
- Smart+Connected City Safety and Security
- Remote Expert Smart Solution for Government Services

Cisco's Smart Connected Communities

**IBM Intelligent Operations Center**

Operational insight helps city leaders manage a safer, smarter city.

**Intelligent Operations Center for Smarter Cities**

IBM® Intelligent Operations Center helps government leaders manage complex city environments, incidents and emergencies with a city solution that delivers operational insights. It offers integrated data visualization, near real-time collaboration and deep analytics to help city agencies enhance the ongoing efficiency of city operations, plan for growth and coordinate and manage response efforts. IBM Intelligent Operations Center provides integrated maps, online dashboards, customizable reports, multiple analytic algorithms, interactive standard operating procedures and other tools for improved city operations and incident or emergency response.

IBM Intelligent Operations Center enables you to:

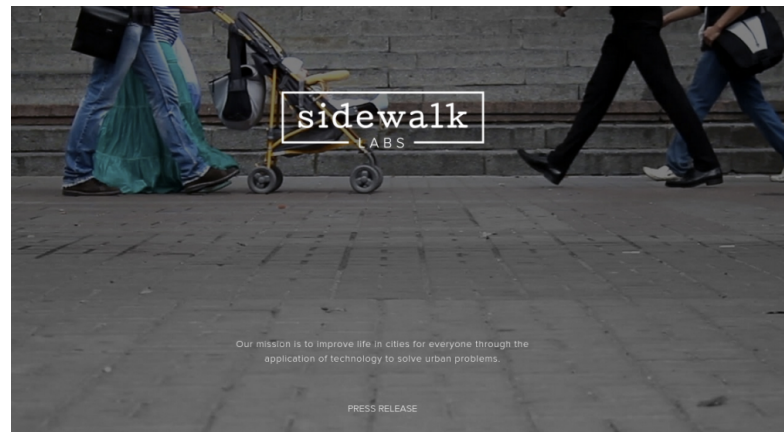
- Monitor and manage resources, events and incidents through situational awareness.
- Optimize city growth and operations through deep analysis of the city environment and resources.
- Stay connected with citizens and address their concerns through citizen collaboration tools and services.
- Keep citizens safer with crime risk hot-spot analytics.
- Integrate data from various departments and agencies through a common platform.

**Product support**

**Video: An Intelligent Operations Center for emergency management in the Philippines**

The Philippines Department of Science & Technology and IBM collaborate to build an Intelligent Operations Center for emergency management as a centralized source of data and analytics to help mitigate risk and improve

IBM's Intelligent Operations Center



Google's Sidewalk Labs

# But Don't Forget Dumb Cities





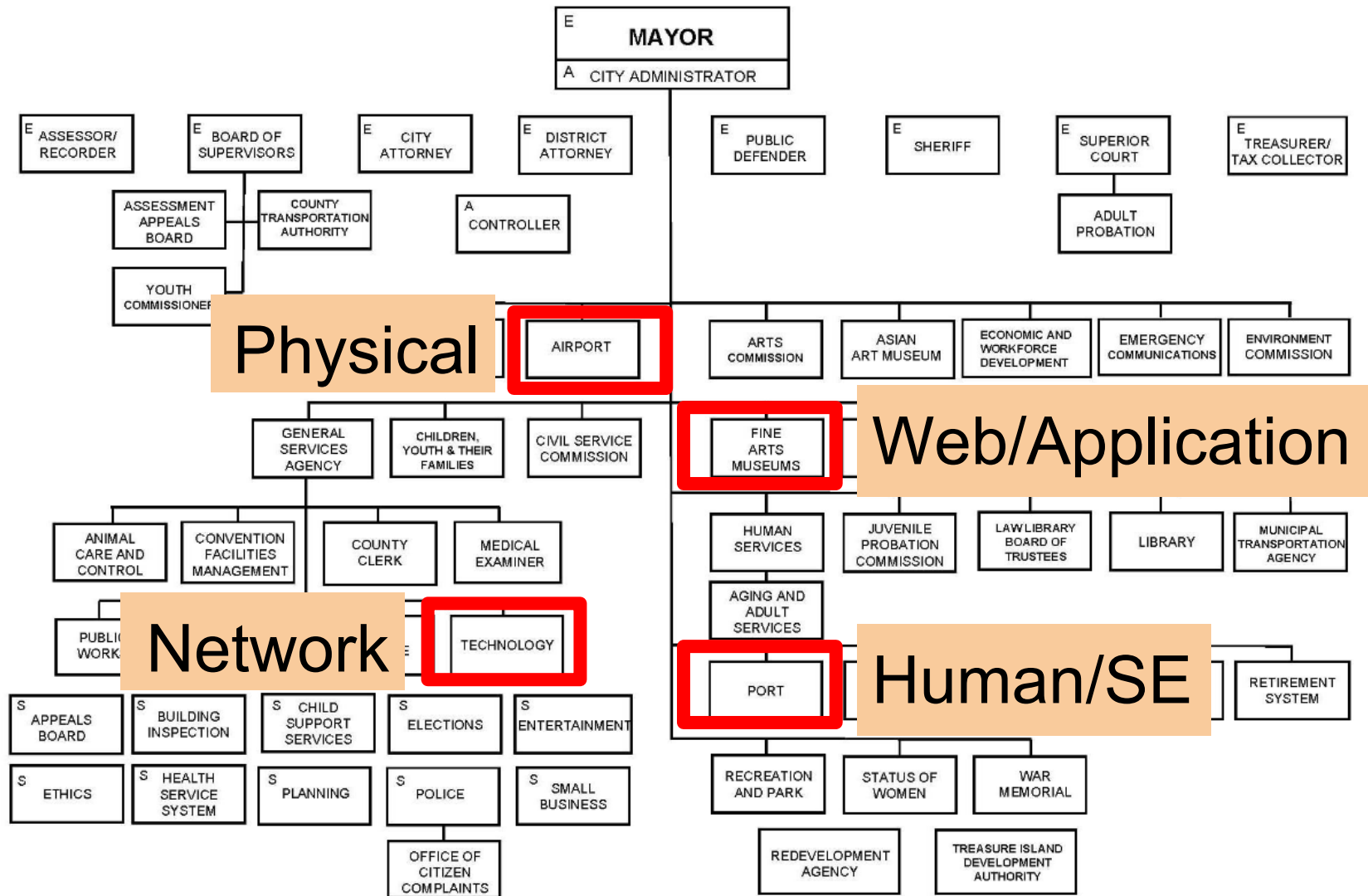
- Introduction
- **Pen Testing**
- Dissecting a City
- Cross Sectioning
- Pressure Points
- Risk Analysis
- Solutions

# SANS Network Pen Testing Process\*

1. Preparation
  - a. NDA/permission memo
  - b. Scoping and ROE
2. Testing
  - a. Reconnaissance
  - b. Scanning
  - c. Exploitation
  - d. Password attacks
  - e. Wireless attacks
  - f. Web app attacks
3. Conclusion
  - a. Analysis and retest
  - b. Pen test report

But how does this fit when thinking at City scale?

# Traditional Pen Testing



A = Appointed by Mayor and confirmed by Board of Supervisors / E = Elected / S = Shared – appointed by various elected officials.

# Traditional vs. City-Level Process

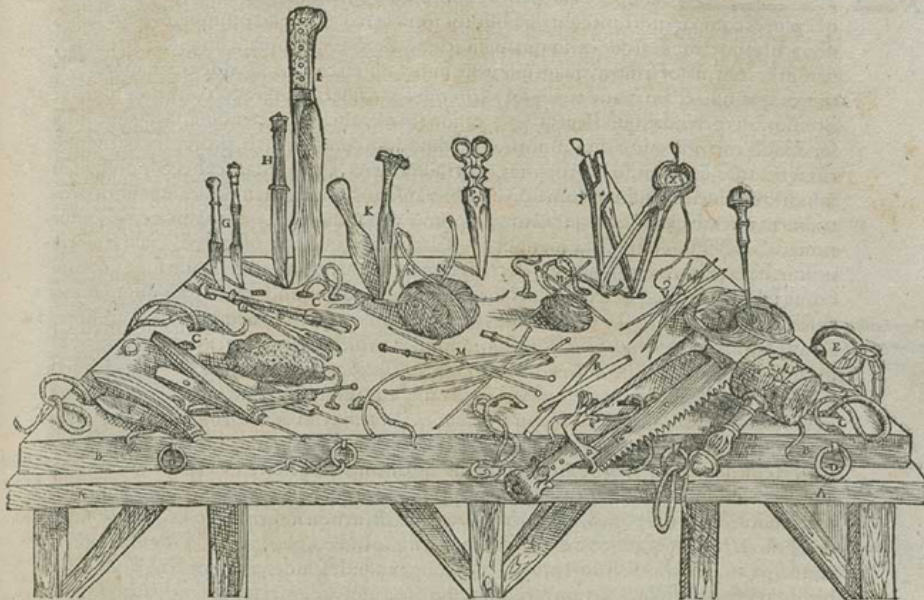
1. Preparation
  - a. NDA/permission memo
  - b. Scoping and ROE
2. Testing
  - a. Reconnaissance
  - b. Scanning
  - c. Exploitation
  - d. Password attacks
  - e. Wireless attacks
  - f. Web app attacks
3. Conclusion
  - a. Analysis and retest
  - b. Pen test report

VS.

1. Define “City” (Scope)
2. Determine audit surface area @ each level of abstraction
  - a. Determine how to collect information @ each level
3. Cross sectional analysis
4. Pressure point analysis
5. Risk analysis of threat actors
  - a. Most likely courses of action
  - b. Most dangerous courses of action

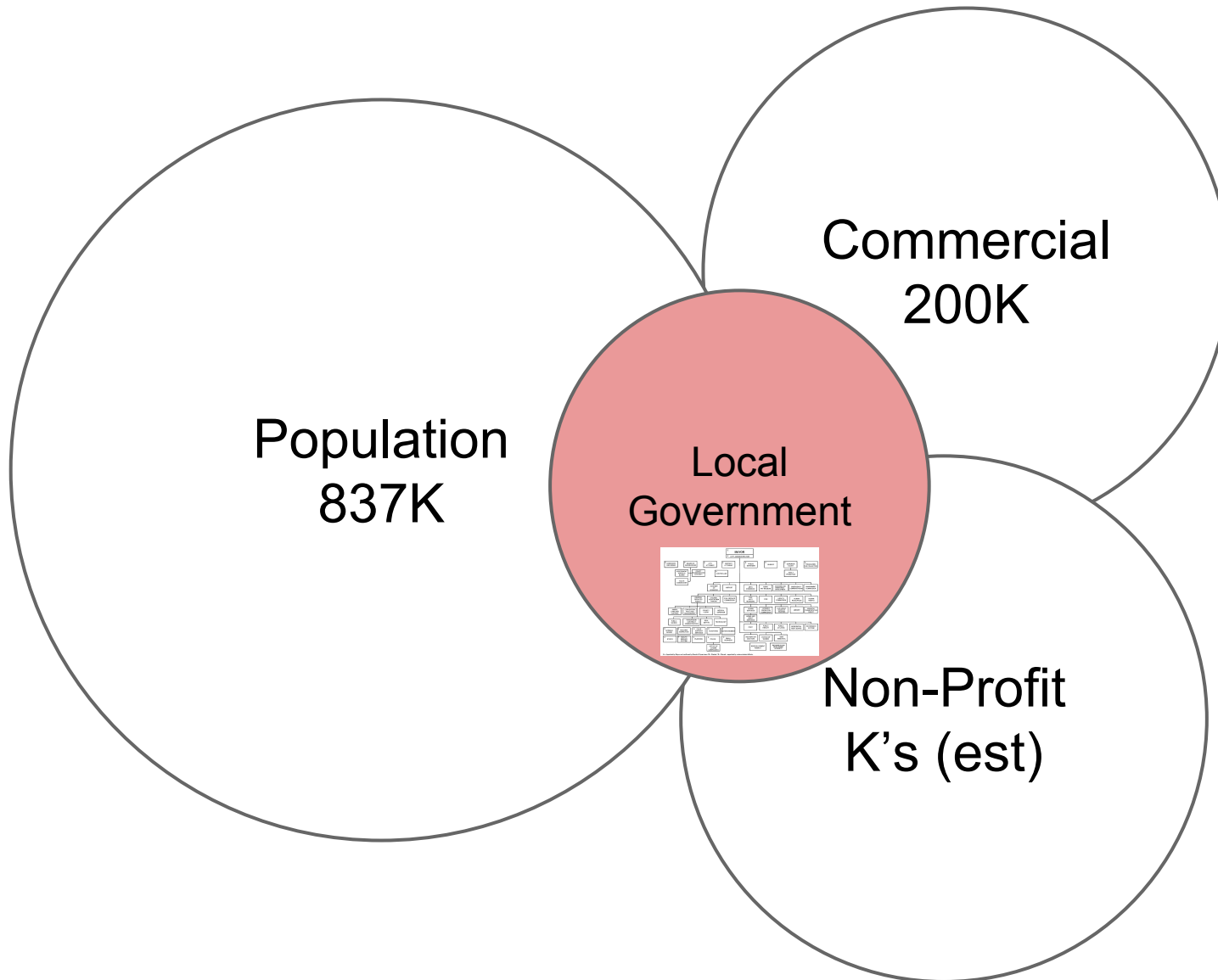


ANATOMICORVM INSTRVMENTORVM DELINEATIO.

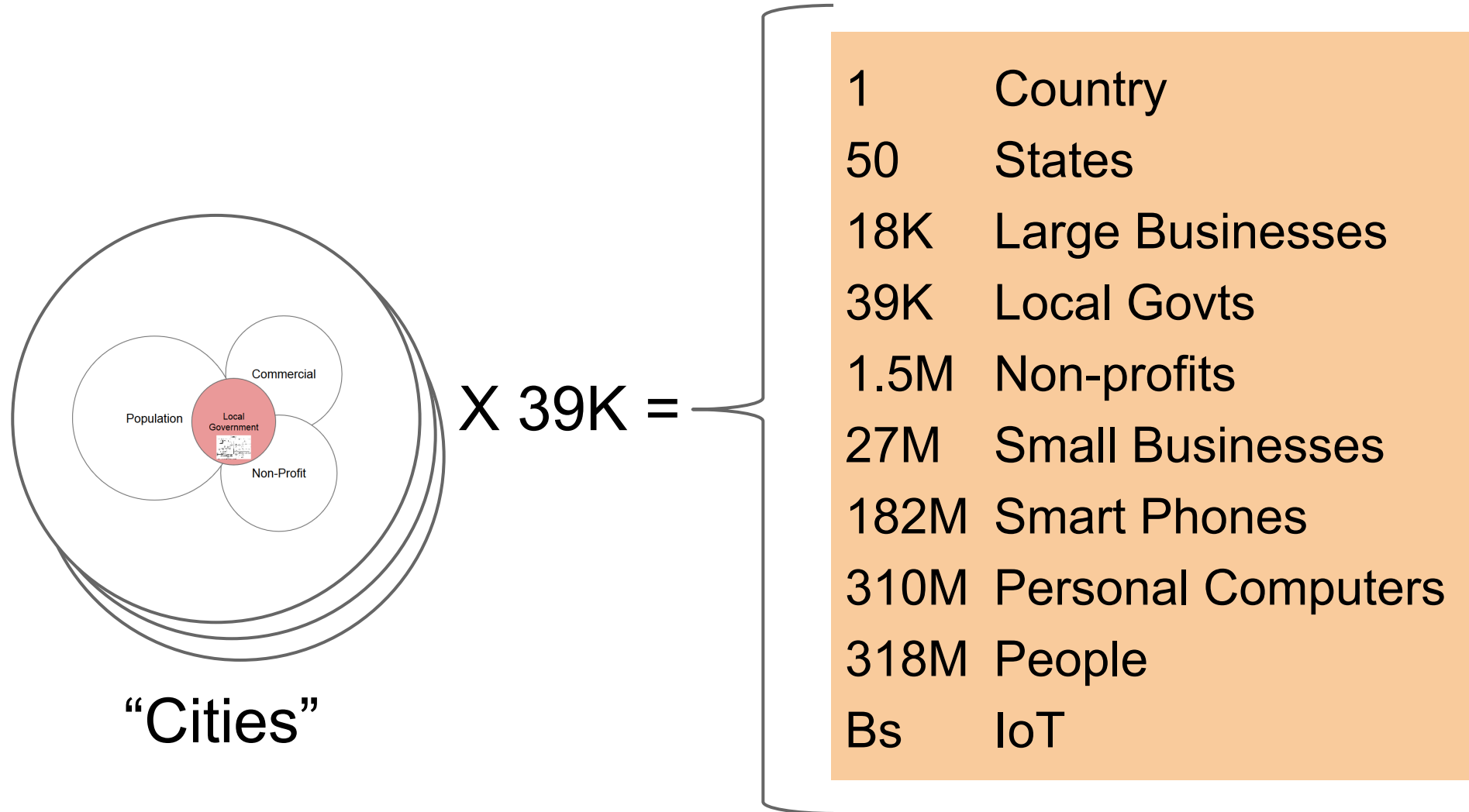


- Introduction
- Pen Testing
- **Dissecting a City**
- Cross Sectioning
- Pressure Points
- Risk Analysis
- Solutions

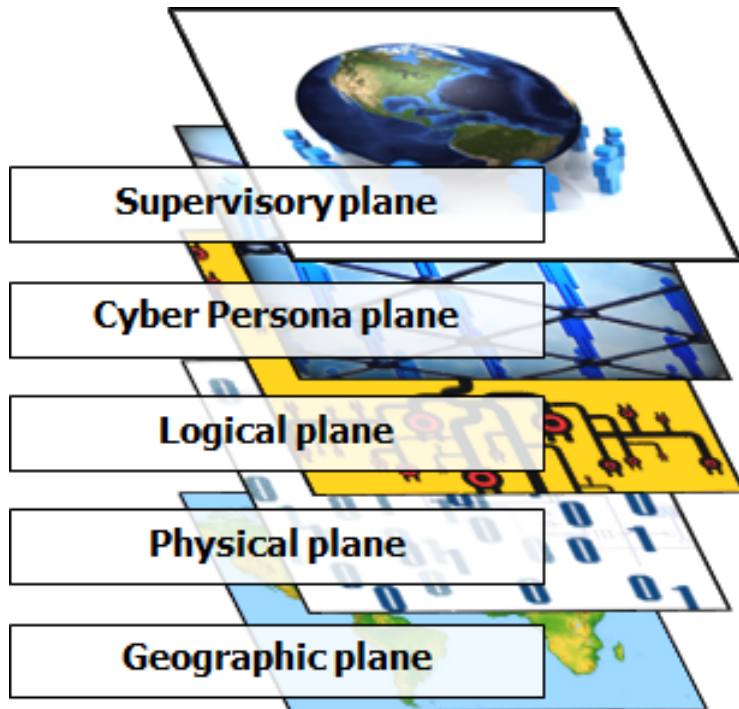
# A Quick Look at San Francisco



# A Quick Look at the United States

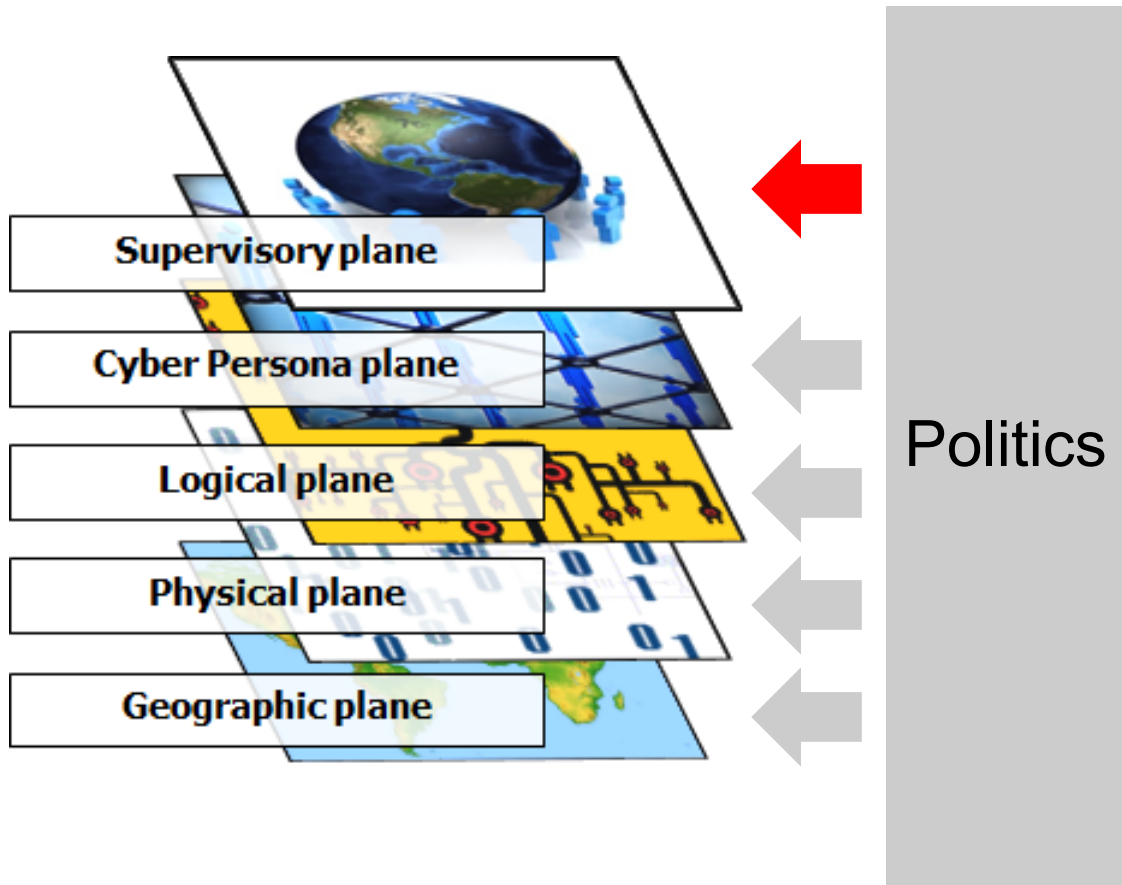


# Cyberspace Planes



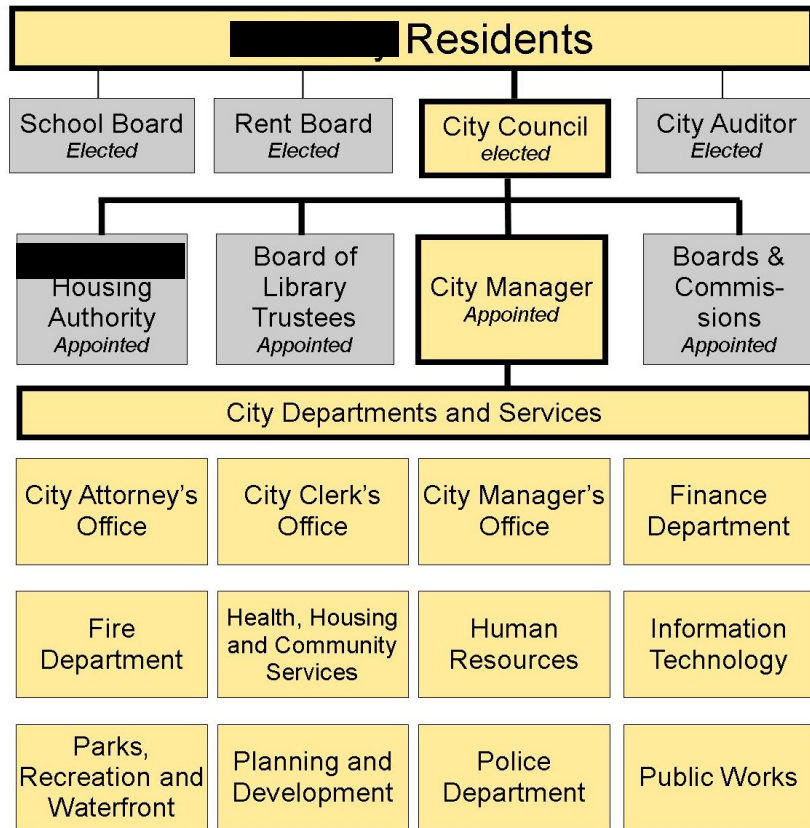
- **Supervisory** - Often siloed/compartmentalized between sectors
- **Persona** - Relevant identities or accounts; do you know who to contact in other sectors?
- **Logical** - System compatibility; how do various networks and systems communicate?
- **Physical** - Redundancy; can connectivity be compromised?
- **Geographic** - Physical location can be important!

# Cyberspace Planes





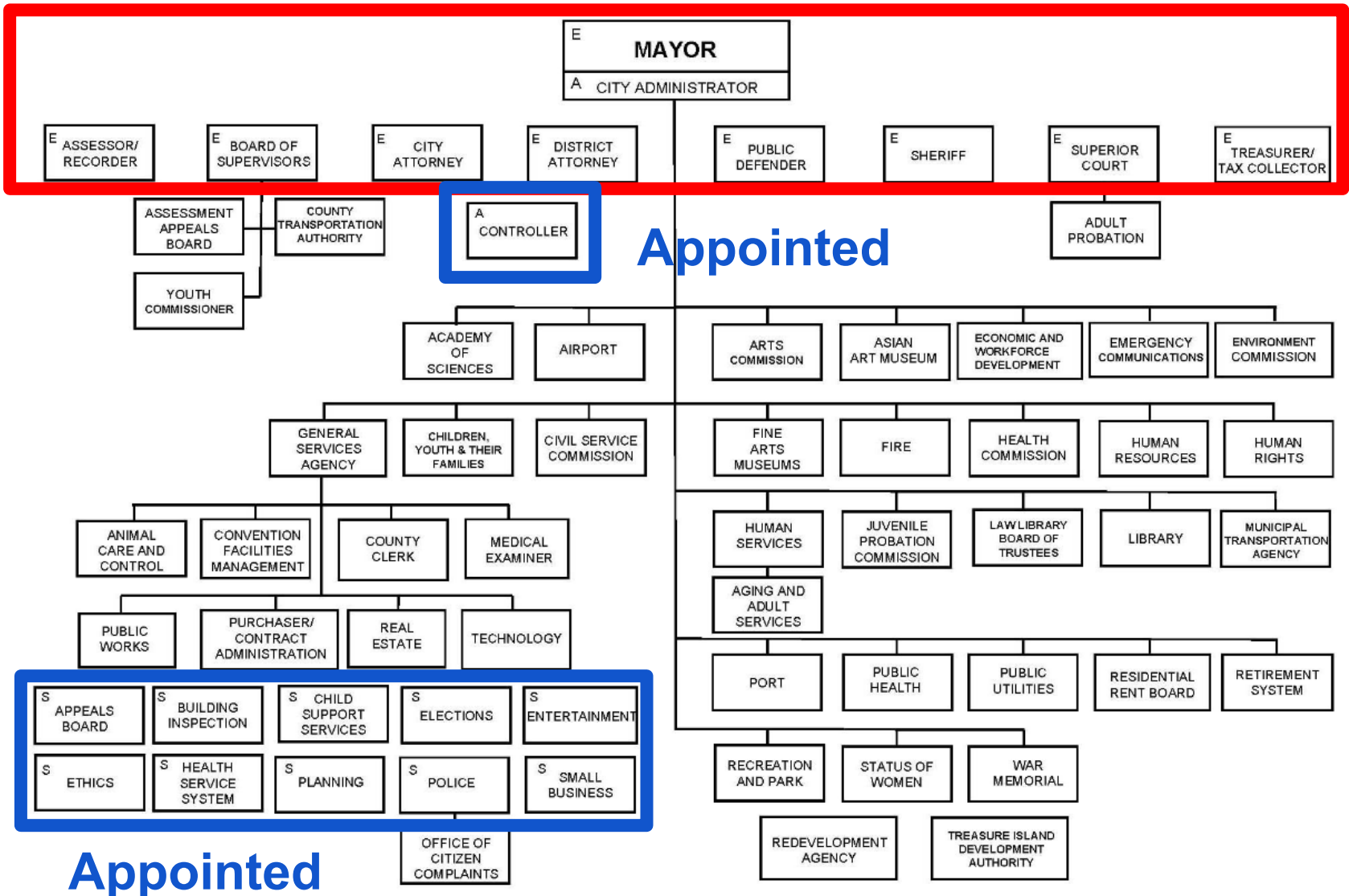
# Supervisory Plane



- Forms of Municipal Government
  - Council-Manager (*Las Vegas*)
  - Mayor-Council
  - Commission
  - Town Meeting
  - Representative Town Meeting
- Umbrella organizations
  - National League of Cities (NLC) - Organized into 49 State Leagues (not Hawaii)
  - International City/County Management Association (ICMA)
  - *Las Vegas active in both*

# Political Pressures are Baked In

Elected



Appointed

Appointed

A = Appointed by Mayor and confirmed by Board of Supervisors / E = Elected / S = Shared – appointed by various elected officials.



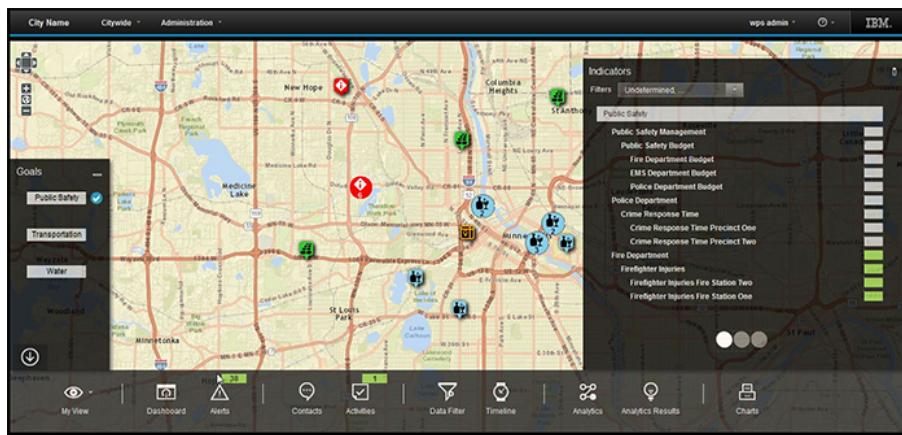
# Persona Plane



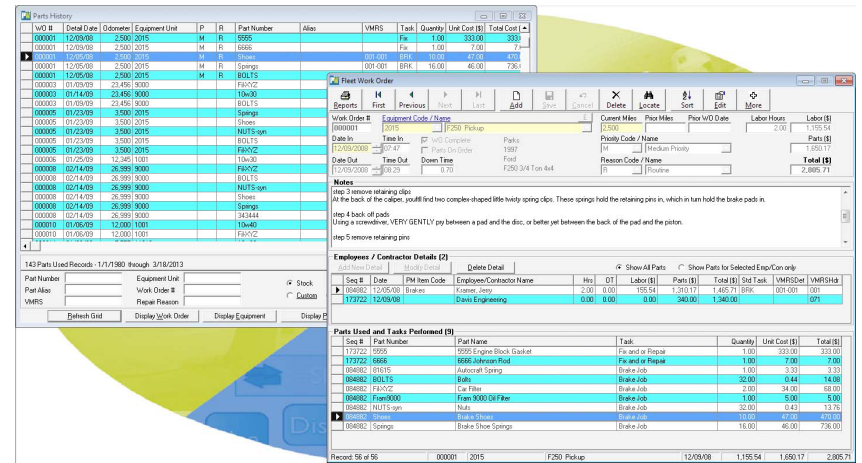
## Cities tend toward openness

- Most feel obligated to publish data on local officials
- Email addresses often easy to get using open-source recon
- Very active social media presence and all that affords

# Logical Plane



IBM Intelligent Operations Center

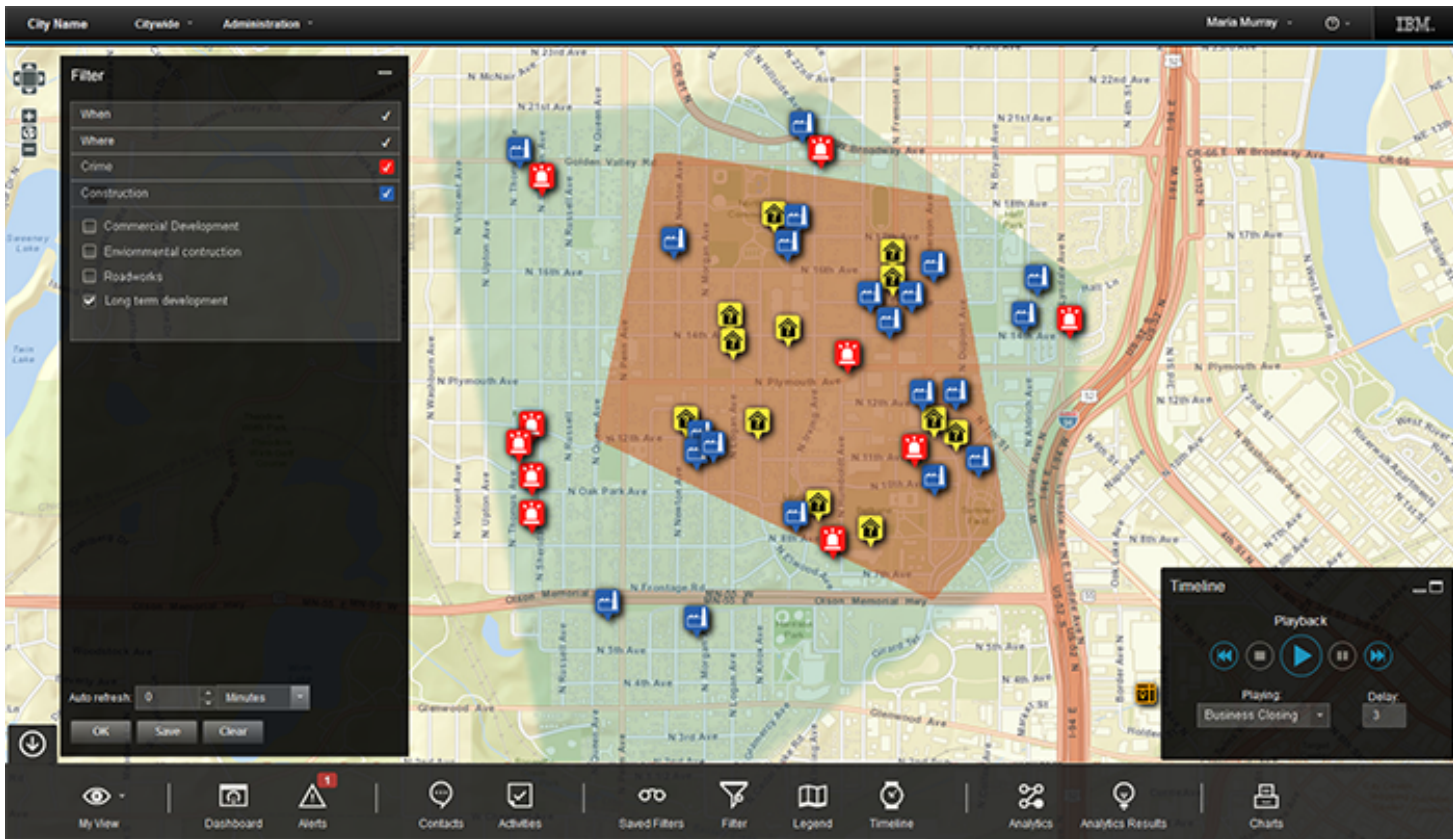


PubWorks

## City Management Software

- IBM Intelligent Operations Center - helps manage all aspects of city operations
- PubWorks - manages work orders, service requests, fleet maintenance, etc.

# IBM Intelligent Operations Center



- View city conditions and assess critical issues
- View and analyze citizens' social media sentiments
- View problems reported by citizens and see locations on a map
- Monitor trends

# Nevada Freeway and Arterial System of Transportation (FAST) Dashboard

Home About Incident Freeway Ramp ITS Device Other Areas Report Contact Us Test [Log In] [Register]

ID	Location
100	I-15 SB at I-515/US-95 interchange
101	I-15 SB at I-515/US-95 interchange
102	I-15 SB at Bonneville
103	I-15 NB at Charleston
104	I-15 NB at Sahara North
105	I-15 SB at Sahara South
106	I-15 SB at Desert Inn
107	I-15 SB at Spring Mtn
108	I-15 SB at Flamingo
109	I-15 NB at Tropicana
110	I-15 SB at Hacienda
111	I-15 SB S of Russell
112	I-15NB at Sunset
113	I-215 at I-15
114	I-15 NB at I-215
115	Blue Diamond North
116	I-15 NB Blue Diamond South
117	I-15 SB DMS 42
118	I-15 NB DMS 1
119	I-15NB at Silverado Ranch North
120	I-15NB at Silverado Ranch South
121	I-15NB Starr Ave
122	I-15NB 1 mile N of St Rose
123	I-15NB St. Rose
124	St Rose WB DMS 43
125	I-15NB 1 mile S of St Rose
126	I-15NB Sloan

Map: Road Aerial | Toggle Full Screen | Zoom Back | Corridor View

CCTV #5004  
5004 BLDR HW/HORIZON SOUTH  
6/10/2015 7:40:43 AM

© 2010 NAVTEQ © AND © 2015 Microsoft Corporation

Home About Incident Freeway Ramp ITS Device Other Areas Report Contact Us Test [Log In] [Register]

View Traffic Heat | Technology | User Defined | (Choose Users Check This)

Toggle Full Screen | Zoom Back

Daily Peak Speeds  
Line Graph showing speed (MPH) vs Time (AM/PM)

Freeway Performance Report  
Freeway Performance Report 2015, 1<sup>st</sup> Quarter (US In)

Freeway Average Speed  
Gauge showing Average Speed (MPH)

Congestion  
Pie chart showing Congestion levels: Light Congestion (47%), Heavy Congestion (11%), No Congestion (42%)

Home About Incident Freeway Ramp ITS Device Other Areas Report Contact Us Test [Log In] [Register]

CCTV Snapshot Wall

Map View

Click to refresh; click on the image to popup its animation window.

Grid of camera feeds:

- 101 I-15 NB AT CHARLESTON SOUTH
- 102 I-15 NB BONNEVILLE SOUTH
- 103 I-15 NB AT CHARLESTON SOUTH
- 104 I-15 NB SAHARA NORTH
- 105 I-15 NB SAHARA SOUTH
- 106 I-15 NB AT FLAMINGO NORTH
- 107 I-15 NB AT SPRING MOUNTAIN NORTH
- 108 I-15 NB AT FLAMINGO SOUTH

Home About Incident Freeway Ramp ITS Device Other Areas Report Contact Us Test [Log In] [Register]

Intelligent Transportation System (ITS) Coverage  
Hover the mouse over the coverage to see the description.

Toggle Full Screen | Zoom Back

Legend: Existing, Construction, Planning

© 2010 NAVTEQ © AND © 2015 Microsoft Corporation

# Many City governments have provider independent IP addresses

The screenshot shows the ARIN website interface. At the top left is the ARIN logo (American Registry for Internet Numbers). To the right is a search bar labeled "SEARCH WhoisRWS" with a search button and a link to "advanced search". Below the search bar is a navigation menu with links: NUMBER RESOURCES, PARTICIPATE, POLICIES, FEES & INVOICES, KNOWLEDGE, and ABOUT US. On the left side, there is a vertical red bar with a blue button labeled "ARIN Online enter". The main content area is titled "WHOIS-RWS" and contains a table of network details. To the right of the table is a "RELEVANT LINKS" section with several links.

**ARIN Online**  
enter

**SEARCH WhoisRWS**  
all requests subject to [terms of use](#) [advanced search](#)

[NUMBER RESOURCES](#) | [PARTICIPATE](#) | [POLICIES](#) | [FEES & INVOICES](#) | [KNOWLEDGE](#) | [ABOUT US](#)

## WHOIS-RWS

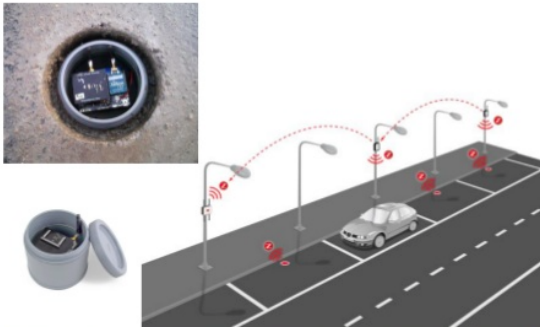
Network	
Net Range	205.153.112.0 - 205.153.115.255
CIDR	205.153.112.0/22
Name	CLVNV-2
Handle	NET-205-153-112-0-1
Parent	NET205 (NET-205-0-0-0-0)
Net Type	Direct Assignment
Origin AS	
Organization	City of Las Vegas (CLV)
Registration Date	1995-05-24
Last Updated	2005-03-01
Comments	
RESTful Link	<a href="http://whois.arin.net/rest/net/NET-205-153-112-0-1">http://whois.arin.net/rest/net/NET-205-153-112-0-1</a>
See Also	<a href="#">Related POC records.</a>
See Also	<a href="#">Related organization's POC records.</a>
See Also	<a href="#">Related delegations.</a>

**RELEVANT LINKS**

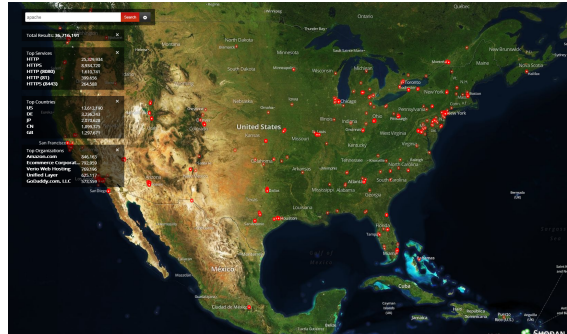
- > [ARIN Whois/Whois-RWS Terms of Service](#)
- > [Report Whois Inaccuracy](#)
- > [Whois-RWS API documentation](#)
- > [ARIN Technical Discussion Mailing List](#)
- > [Sample stylesheet \(xsl\)](#)



# Physical Plane



Wireless Sensors



Shodan Maps



Buried Fiber

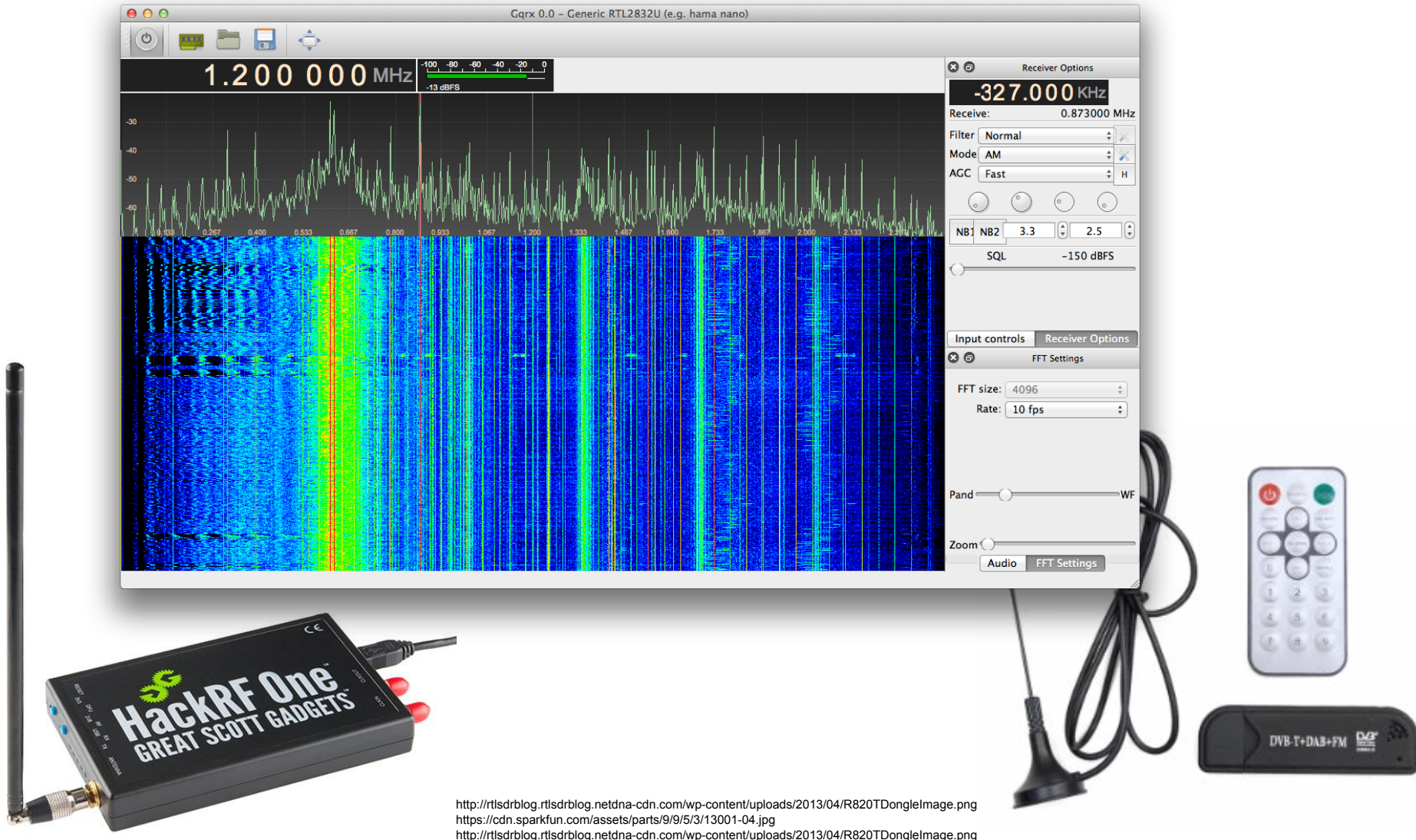


Emergency Broadcast System



Municipal Wifi

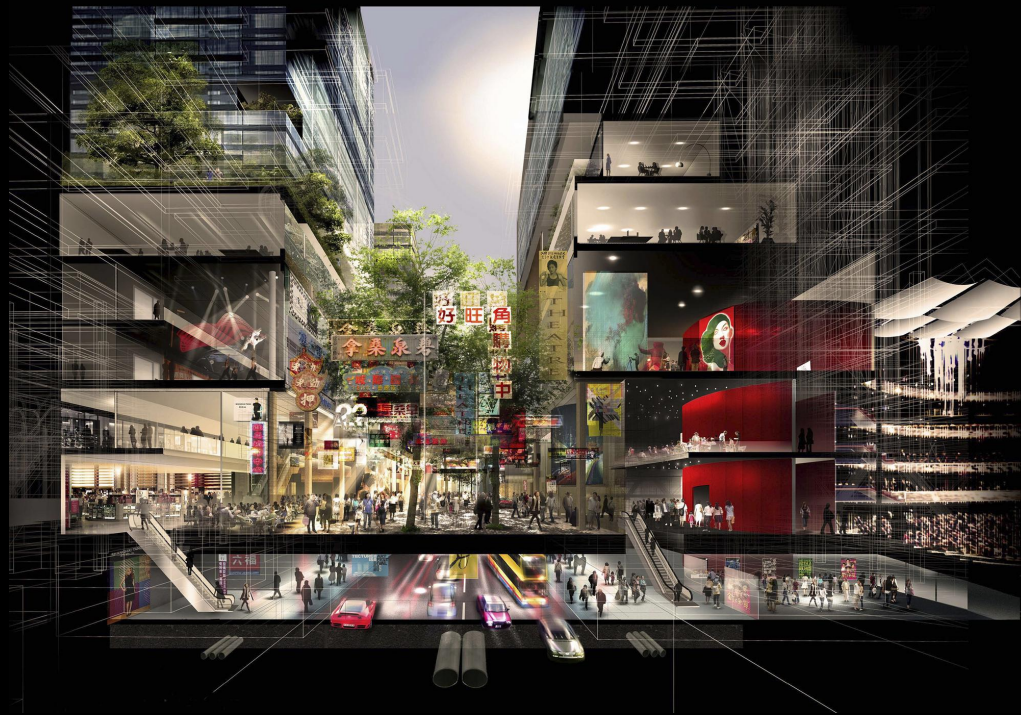
# Auditing the Wireless Spectrum





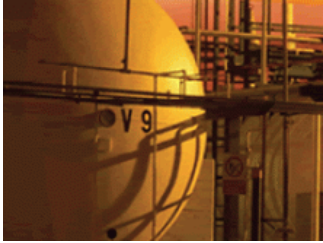
# Geographic Plane





- Introduction
- Pen Testing
- Dissecting a City
- **Cross Sectioning**
- Pressure Points
- Risk Analysis
- Solutions

# Critical Infrastructure Sectors (DHS)



Chemical



Financial Services



Commercial Facilities



Food and Agriculture



Communications



Government Facilities



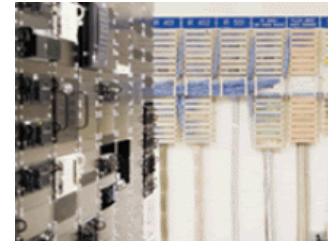
Critical Manufacturing



Healthcare and Public Health



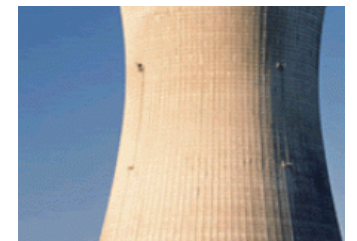
Dams



Information Technology



Defense Industrial Base



Nuclear



Emergency Services



Transportation Systems



Energy

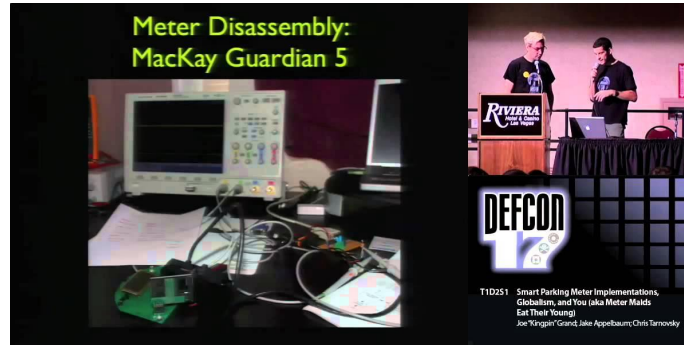


Water and Wastewater

# InfoSec Community Research



Hacking Traffic Control Systems DEFCON 22



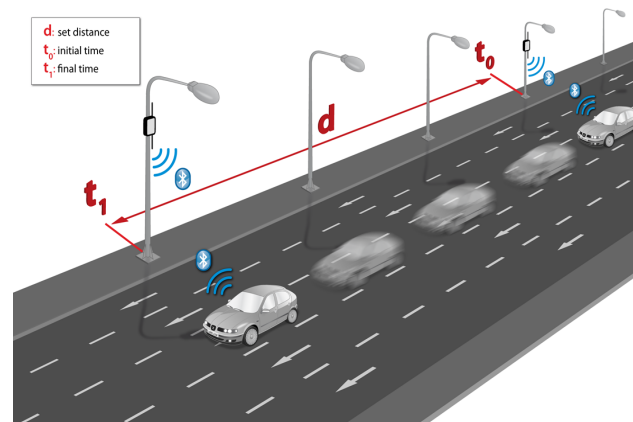
Smart Parking Meters DEFCON 17



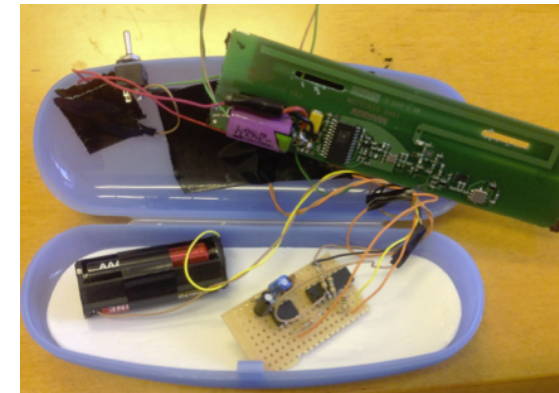
Electronic Road Signs



Gas Stations



Bluetooth Traffic Monitoring DEFCON 22

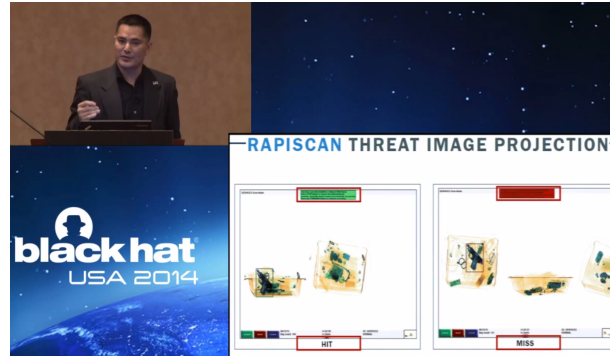


Toll Collection Systems DEFCON 21

# InfoSec Community Research



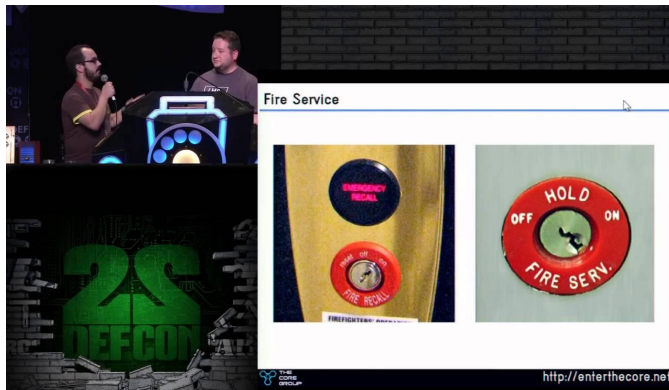
Power Meters  
DEFCON 20



Airport Security & Air Traffic Control  
BH 2014 / DEFCON 18



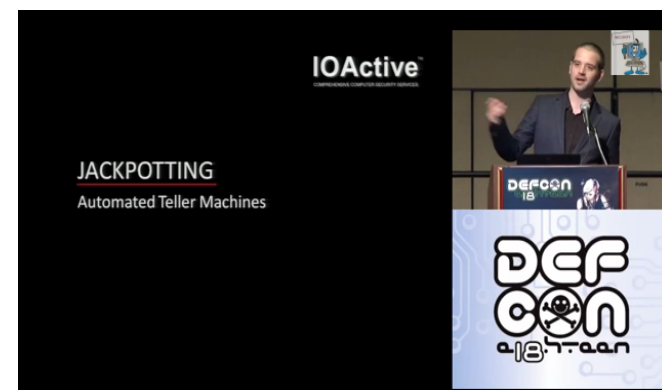
Water Plants  
DEFCON 18



Elevators  
DEFCON 22

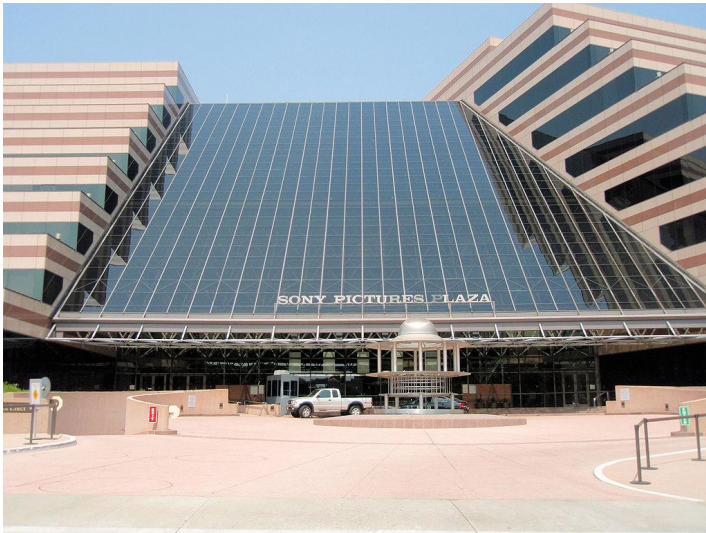


Municipal Surveillance  
DEFCON 22



ATMs  
DEFCON 18

# and It Isn't All Just Researchers...



Sony Hack (2014)

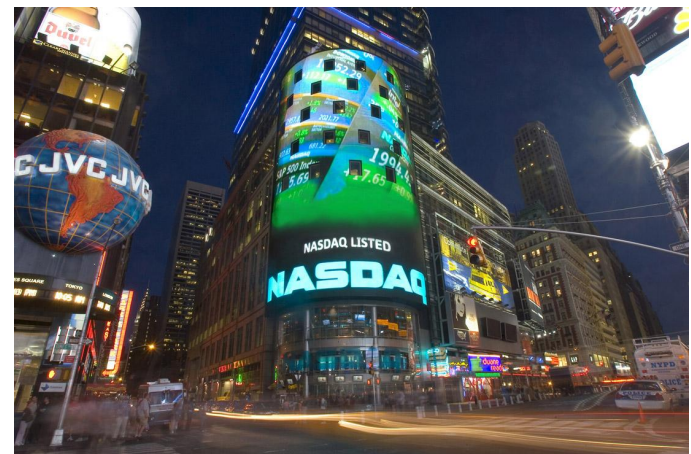


أرامكو السعودية  
Saudi Aramco

Saudi Aramco Hack (2012)



Sands Casino (2014)



Sands Casino (2010)

# At Next Year's Black Hat



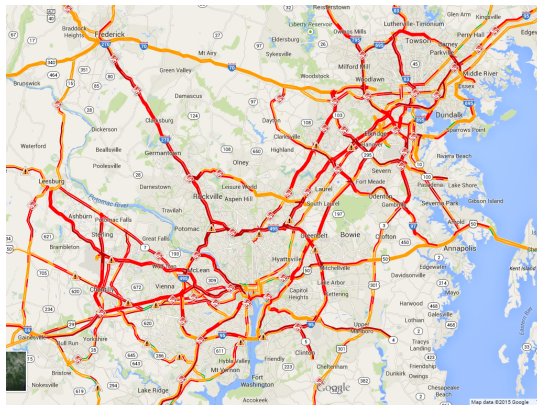
Roadway Sign Networks



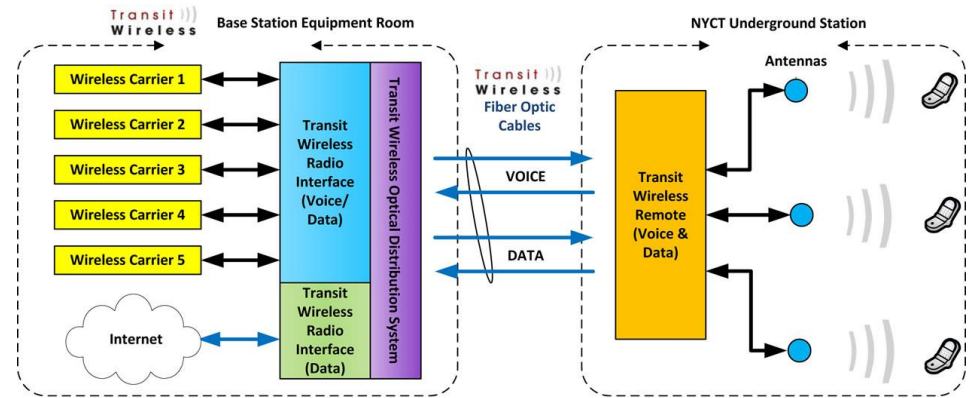
Electronic Billboards



Smart Highways



Traffic Reporting Systems



Mass Transit Wireless Networks

# Effects

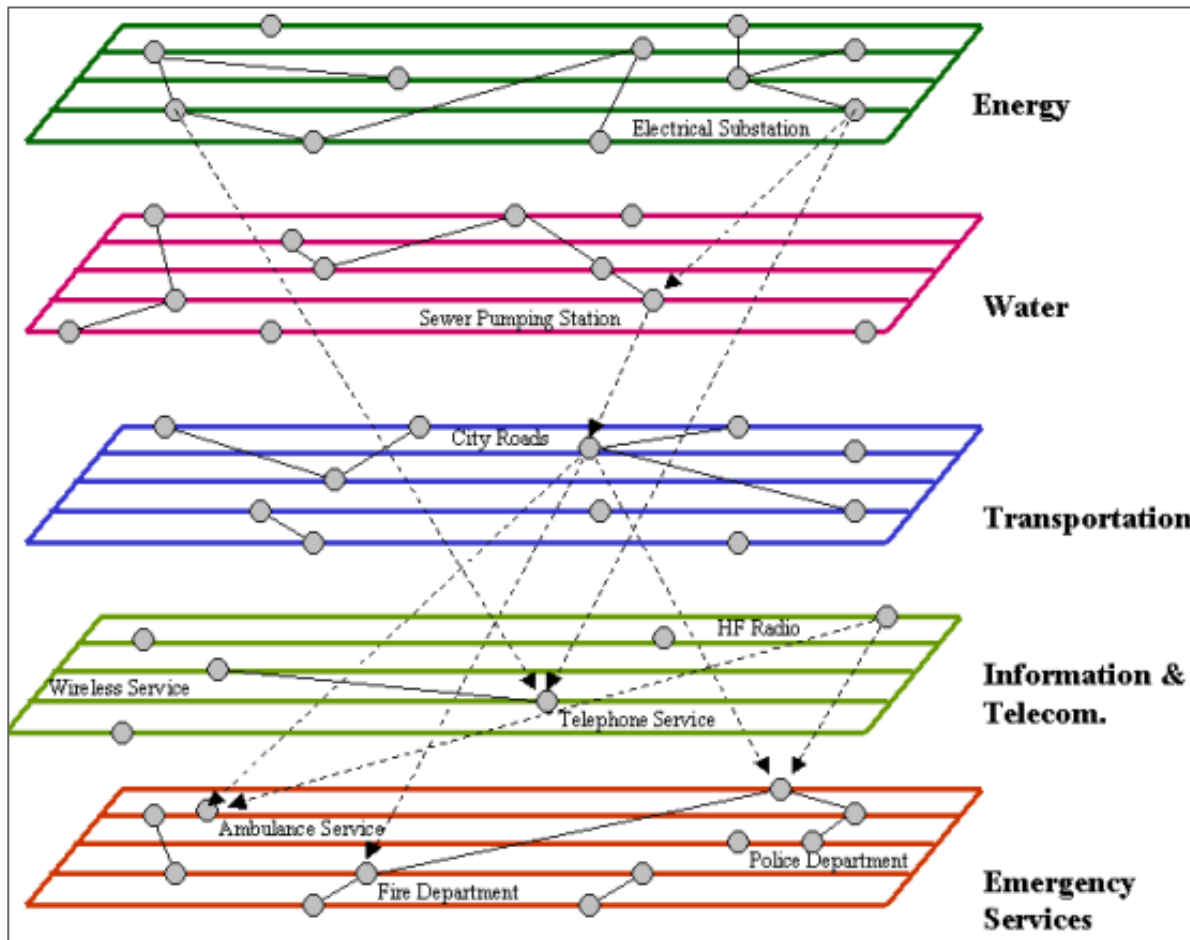


- **Deceive** - Cause a person to believe what is not true
- **Degrade** - Temporary reduction in effectiveness
- **Delay** - Slow the time of arrival of forces or capabilities
- **Deny** - Withhold information about capabilities
- **Destroy** - Enemy capability cannot be restored
- **Disrupt** - Interrupt or impede capabilities or systems
- **Divert** - Force adversary to change course or direction
- **Exploit** - Gain access to systems to collect or plant information
- **Neutralize** - Render adversary incapable of interfering with activity
- **Suppress** - Temporarily degrade adversary/tool below level to accomplish mission

Don't forget "Non-effects" - Silent information gathering and pre-positioning



# Interdependency Modeling (Flooding Event)

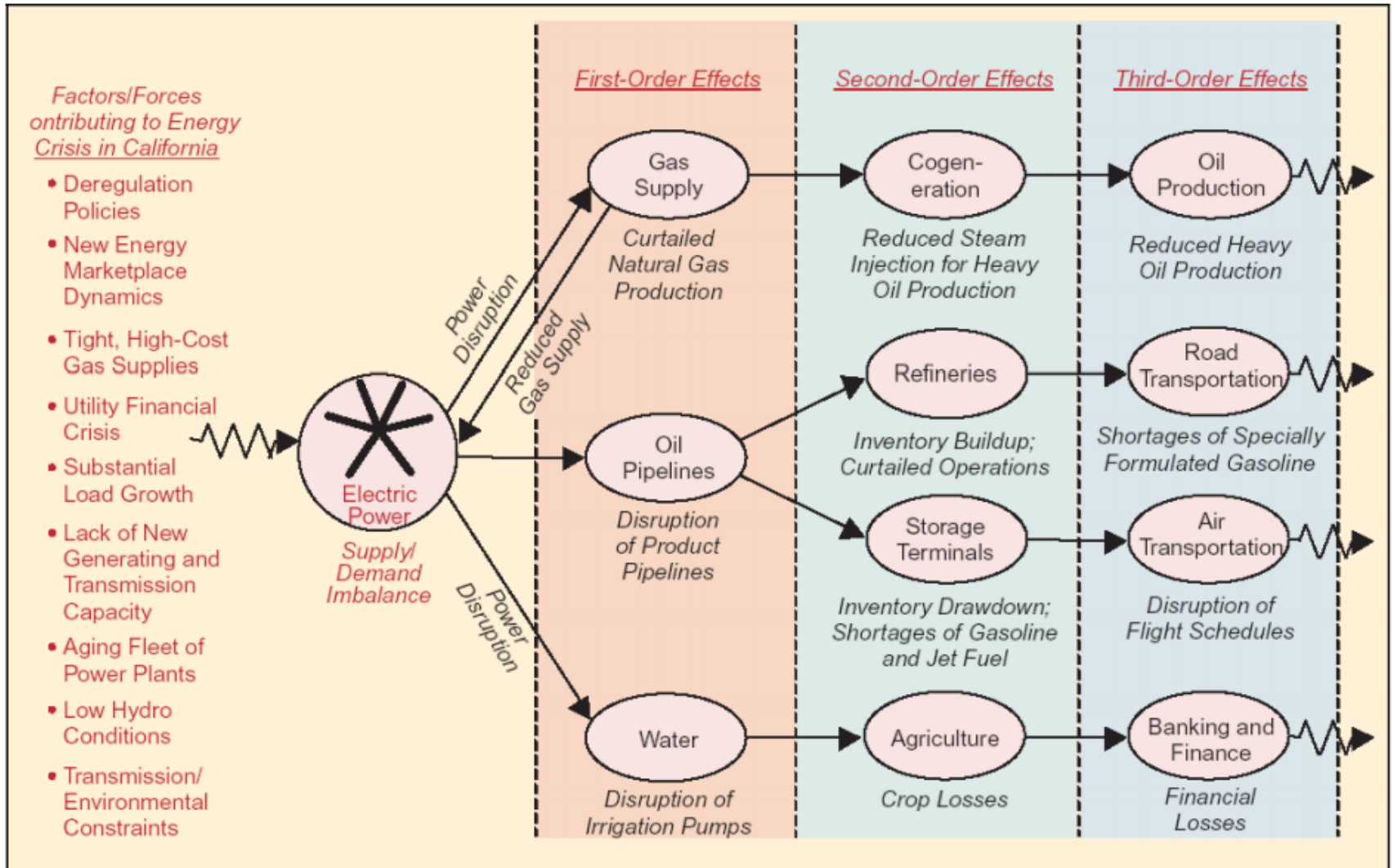


- Individual infrastructures are represented on a single plane
- Parallel lines represent subsets of infrastructure
- Nodes represent key infrastructure components
- Dotted lines indicate interdependencies

# Critical Infrastructure Dependency Matrix (Example)

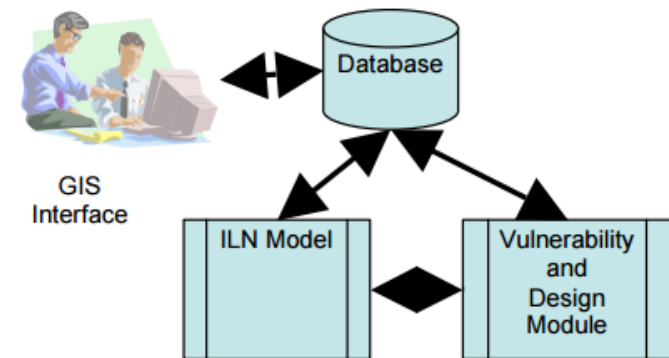
Sector	Element	Energy & Utilities					Services		
		Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	
		Key: <b>H</b> High <b>M</b> Medium <b>L</b> Low							

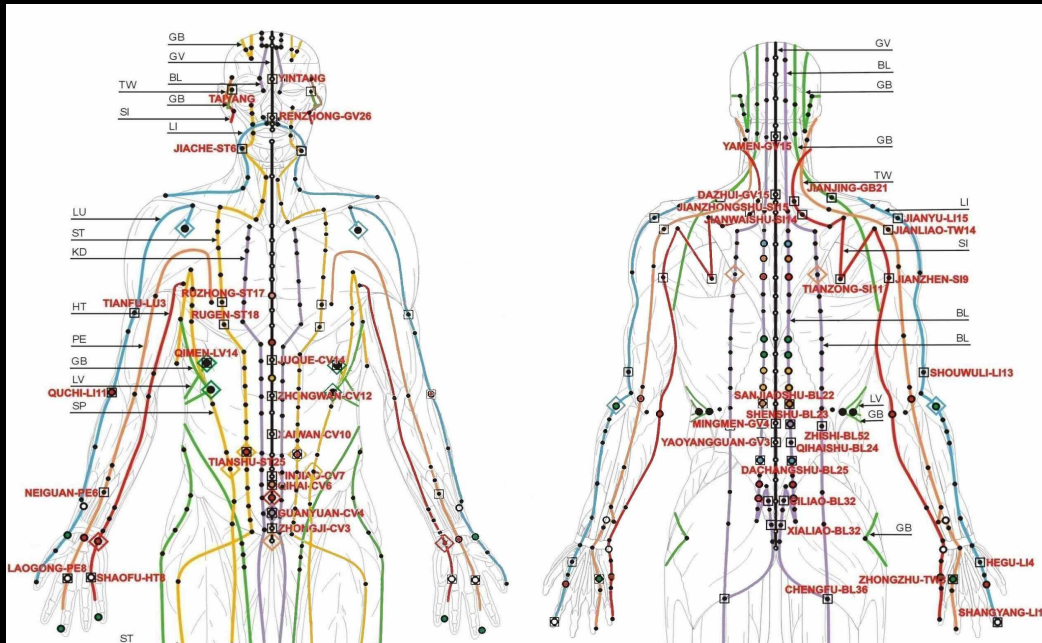
# Cascading Consequences



# Modeling Interdependencies

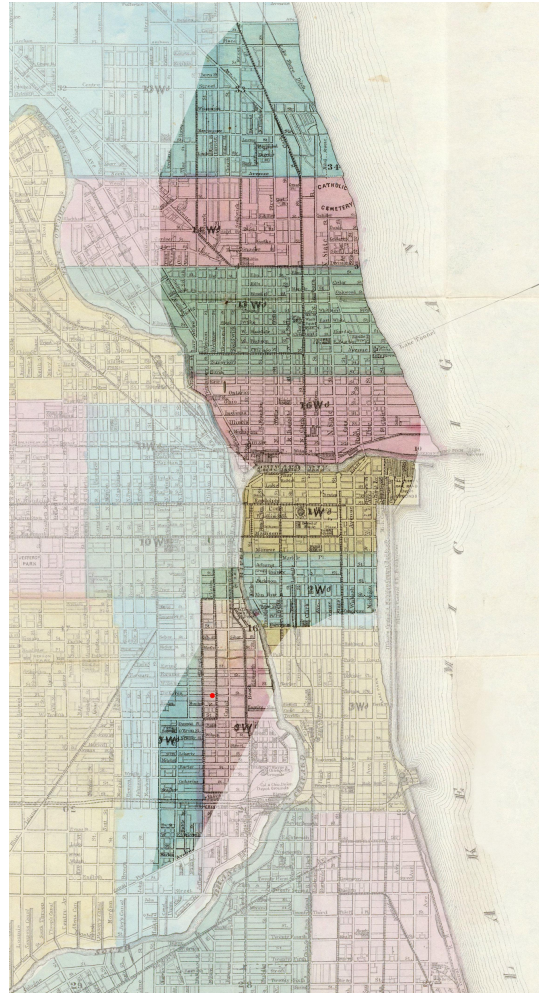
- National Infrastructure Simulation and Analysis Center (NISAC)
  - <http://www.sandia.gov/nisac/>
  - Suite of tools for analyzing interdependencies between sectors
- Multi-network Interdependent Critical Infrastructure Program for Analysis of Lifelines (MUNICIPAL)
  - RPI/NSF
  - Uses Interdependent Layered Network (ILN) mathematical model





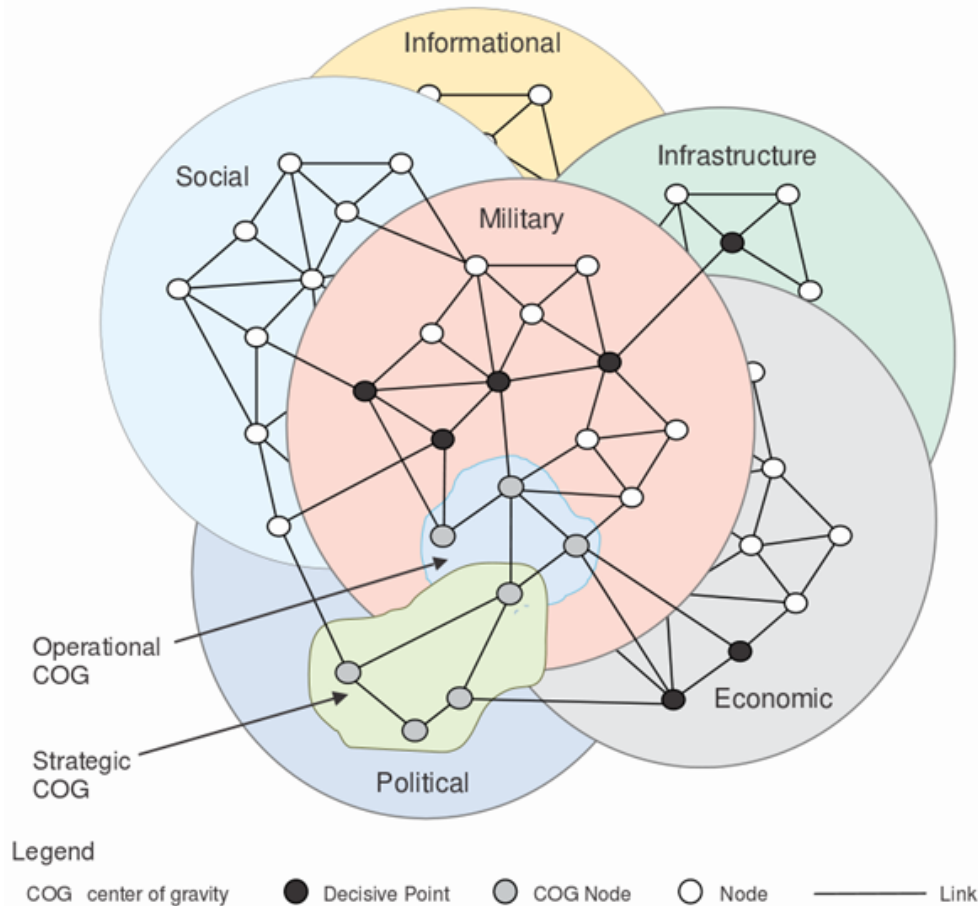
- Introduction
- Pen Testing
- Dissecting a City
- Cross Sectioning
- **Pressure Points**
- Risk Analysis
- Solutions

# A Small Barn Fire...



Region of Chicago destroyed in 1871  
by fire starting in a small barn

# Center of Gravity Analysis



“The source of power that provides moral or physical strength, freedom of action, or will to act.”

Thus, the center of gravity is usually seen as the "source of strength".

- DoD JP 1-02,  
2008

# Centers of Gravity

- Government
- Financial sector
- Retired people
- Gaming
- Energy/oil
- Food
- Entertainment
- Military
- Religion
- Others?

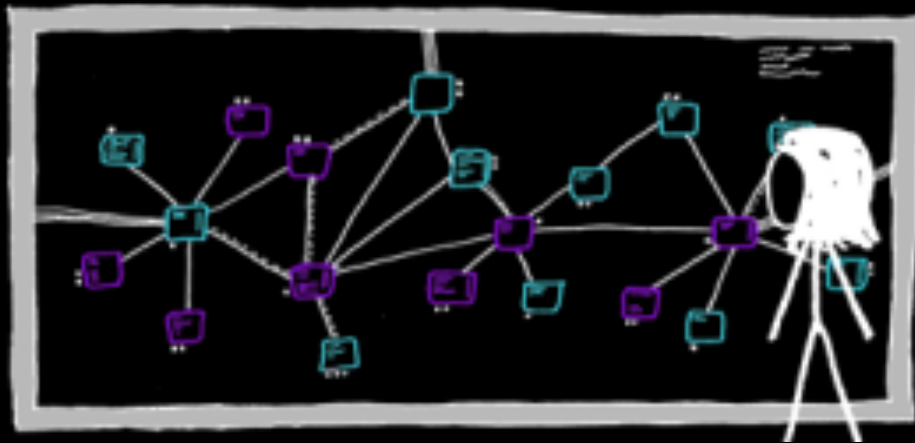




# “Non-Critical” Sectors

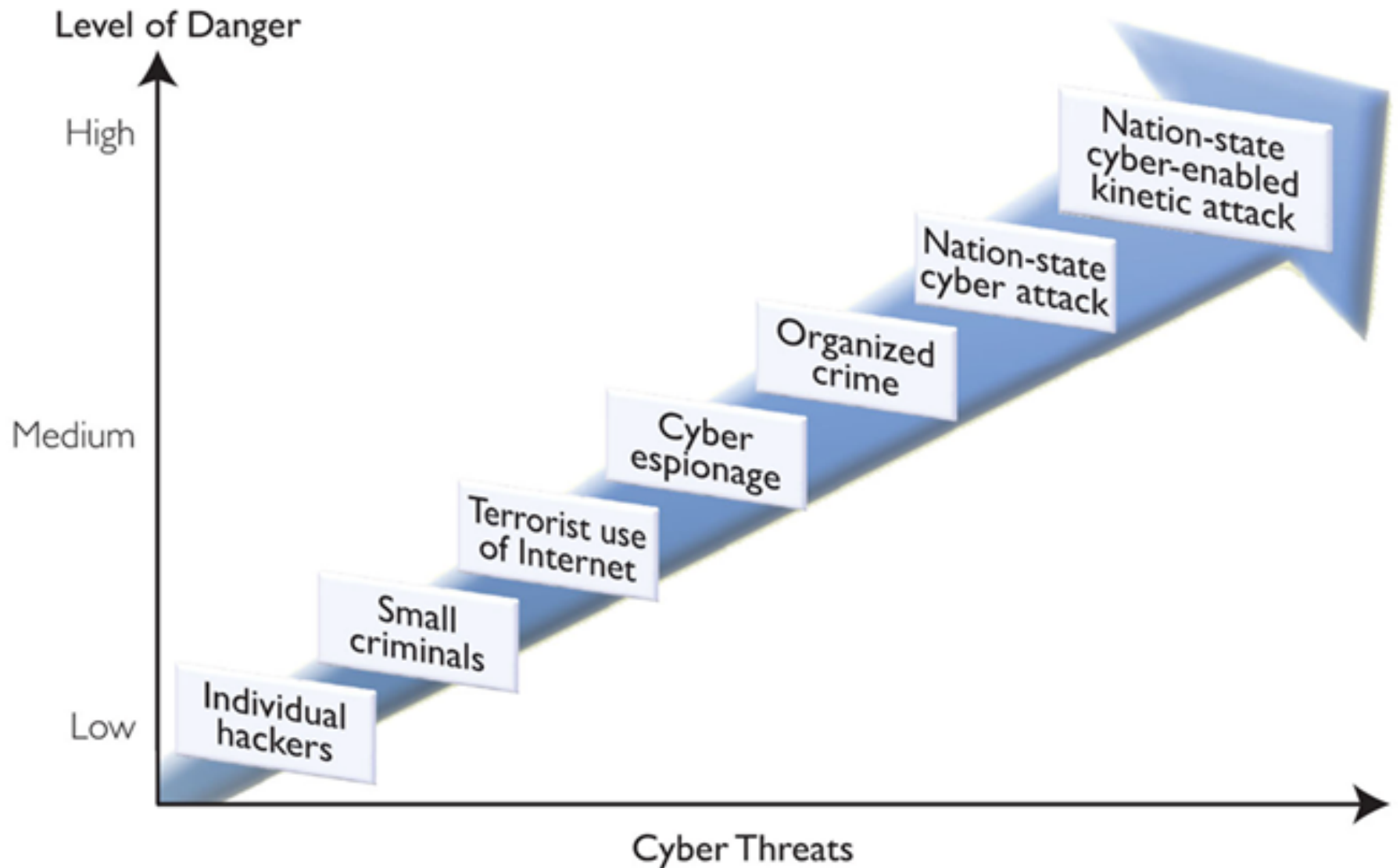


- Churches
- Libraries
- Bars / Nightclubs
- Theaters / Cinemas
- Sports Facilities
- Town Hall
- Post Office
- Public Works
- Chamber of Commerce
- Local Telecoms
- Real Estate Brokers
- Local Banks
- Law Offices
- Schools
- ...

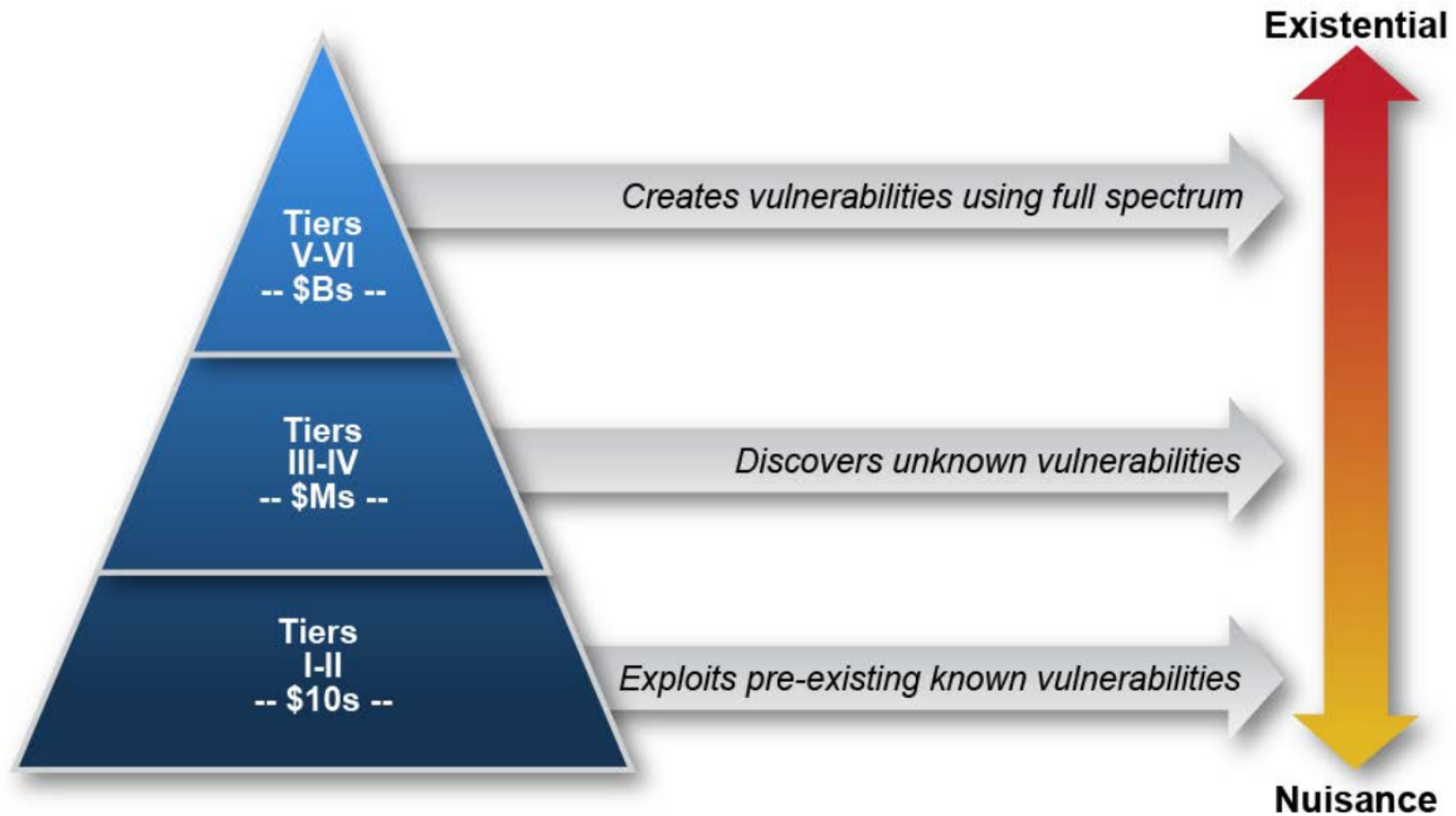


- Introduction
- Pen Testing
- Dissecting a City
- Cross Sectioning
- Pressure Points
- **Risk Analysis**
- Solutions

# Cyber Threat Spectrum

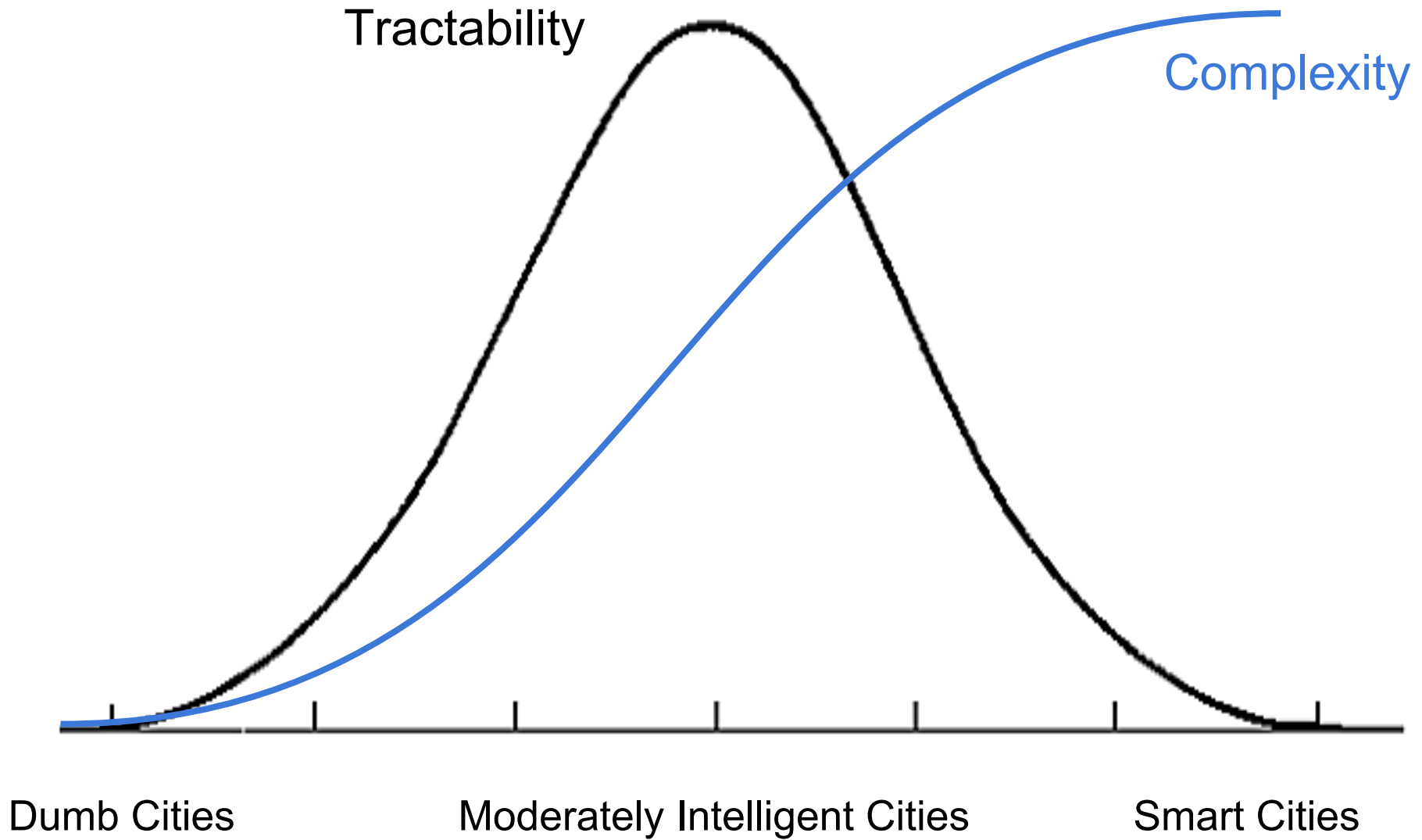


# Threat Hierarchy





- Introduction
- Pen Testing
- Dissecting a City
- Cross Sectioning
- Pressure Points
- Risk Analysis
- Solutions



# One approach: Treat like a *company*

## How is a city different?

- Politics!
- Governmental inertia
- Limited budget
- Complex legal authorities



## How is it the same?

- Security is a cost center
- Can (usually) be partitioned into business units
- *Some city CISOs approach it like they would a company!*

# Securing Smart Cities Initiative



Activities Include:

- Educating smart city planners and providers on the importance and cost benefits of security best practices
- Collaborating with partners to share ideas and methodologies
- Endorsing the significance and benefits of introducing security early into the development lifecycle of a project or plan
- Fostering partnerships between cities, providers, and the security community
- Creating standards, guidelines, and resources to help improve cybersecurity across all areas related to smart cities

**IOActive**®

**KASPERSKY**®

**Bastille**

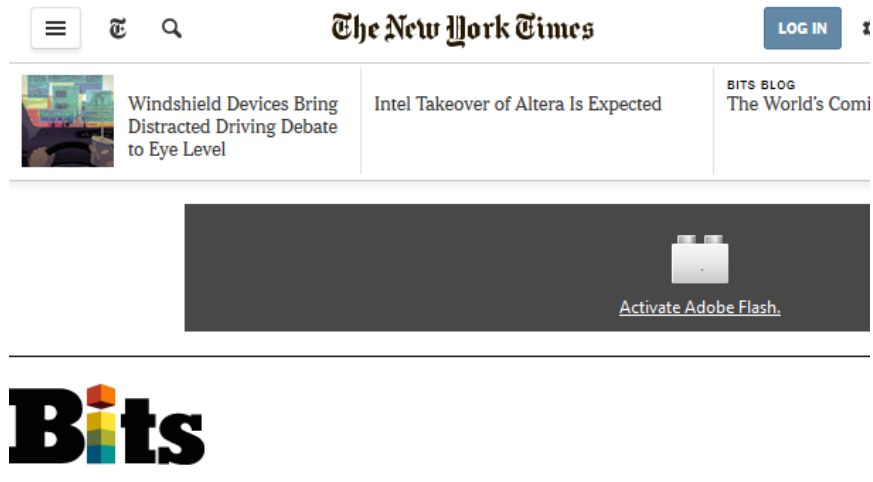
**CSA** cloud security alliance®

**XIPITER**

**securingSMARTCITIES.org**



# Solutions Proposed by the Initiative



The screenshot shows the top navigation bar of The New York Times website. On the left, there is a menu icon, a search icon, and the site name "The New York Times". On the right, there is a "LOG IN" button. Below the navigation bar, there are three article thumbnails. The first one is titled "Windshield Devices Bring Distracted Driving Debate to Eye Level" and features a photo of a car's interior. The second is titled "Intel Takeover of Altera Is Expected". The third is titled "BITS BLOG The World's Comi" and is partially cut off. Below these thumbnails is a dark grey banner with a white Adobe Flash logo and the text "Activate Adobe Flash." Below the banner is the "Bits" logo, which consists of the word "Bits" in a bold, black font with a colorful bar (red, orange, yellow, green, blue) under the "i".

## SECURITY

### Security Researchers Start Effort to Protect 'Smart' Cities

By NICOLE PERLROTH MAY 26, 2015 3:00 PM 5 Comments

Email

Share

Tweet

Save

More

It's a brave new world when hackers step in to protect citizens because regulators are not getting the job done.

Two years after President Obama [signed an executive order](#) setting voluntary guidelines that companies could follow to prevent cyberattacks — especially on critical infrastructure like dams and water treatment facilities — security experts have found that



Cesar Cerrudo, chief technology officer at IOActive Labs. IOActive Labs

- Cyber Security Checklists for Smart Cities
- Properly Installed Encryption
- Strong Passwords
- Structured Patching Regimes
- Security requirements and approval process
- Track access to city systems
- Run regular tests
- Emergency response teams
- Information sharing with other cities
- Create manual overrides for all smart city systems

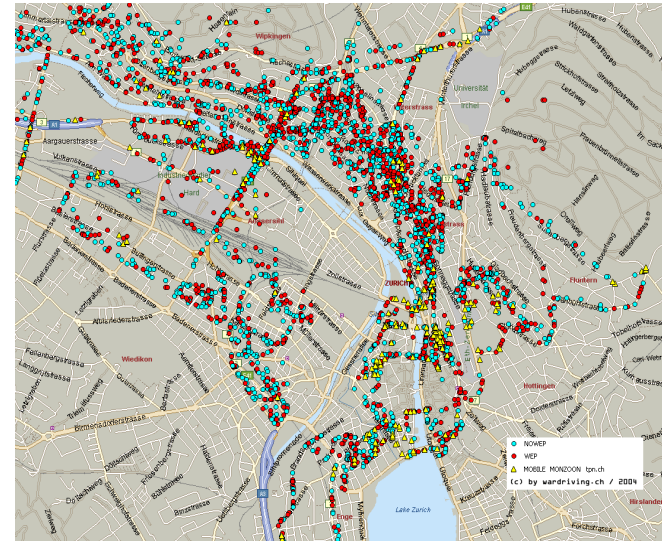
# Solutions

- Executive Support & Buy-in
- Threat intelligence
- Cross functional security assessments
- Develop Metrics
  - Make data public
  - Create a competitive environment
- Robust analytic framework
  - Center of Gravity analysis
  - Interdependency analysis
  - Threat analysis
- Create meaningful city-level exercises and training venues
- Opportunity for a City-level security business model?
- Be ready with a plan when something bad happens
- City-level CERT
- Transparency and Media Attention



# The Need for Broadband Wardriving

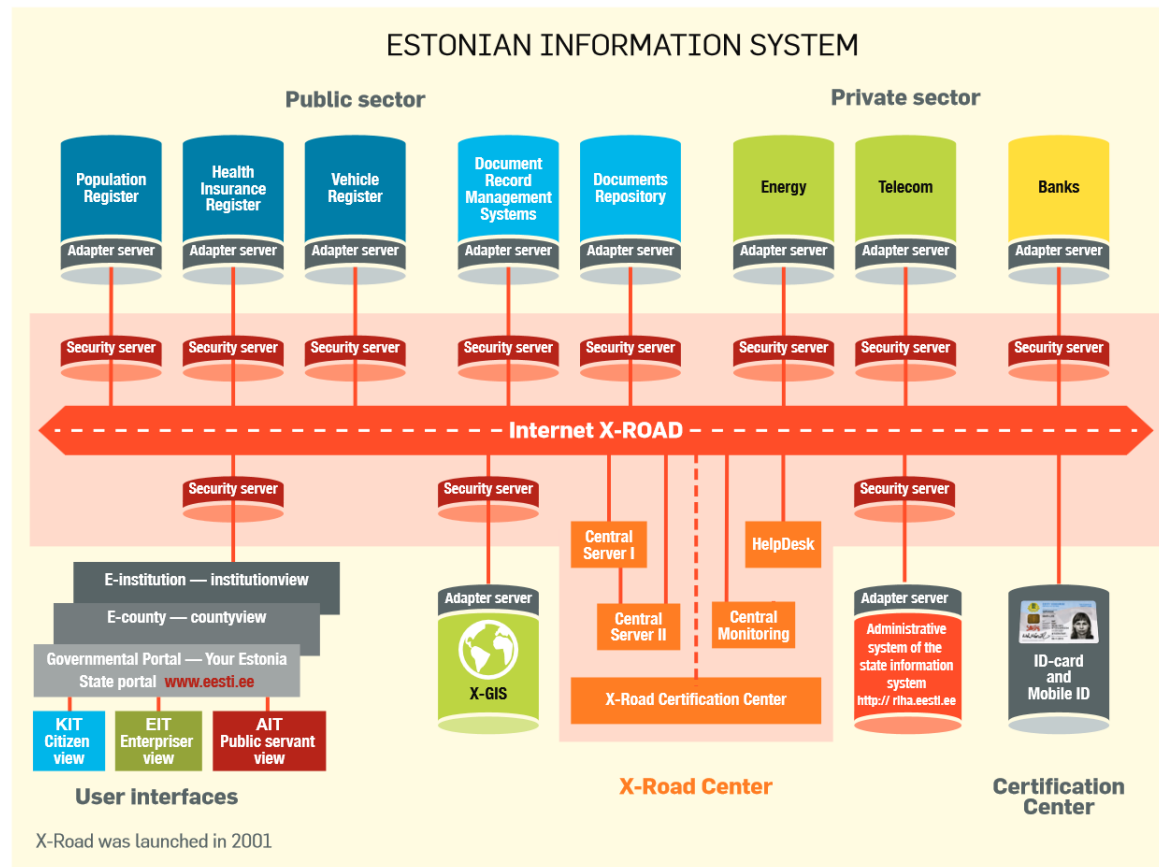
- Spectrum is getting cluttered with potentially vulnerable devices
- We need to know about more than just Wifi
- Auditing large physical spaces for low power transmitters can be a lot of work
- Solutions:
  - Put Wireless Data Collectors in Police Cars
    - Police cars drive everywhere
    - Potential privacy issue? (Device IDs)
  - Crowd Sourcing
    - Better tools are needed
      - Need better mobile phone SDR software for transmitter discovery
      - Some Zigbee hacking projects were written for devices that are now obsolete or are hard to get
      - Websites to report and share data



# Capability Maturity Model for Cities?

	Level 1 - Initial	Level 2 - Repeatable	Level 3 - Defined	Level 4 - Managed	Level 5 - Optimised
	Focus on solution	Focus on long-term solution success	Identify additional value opportunities	Managed Architecture	Optimised Enterprise Architecture
Enterprise Architecture	Definitions are agreed	Definitions are available to those who know where to look.	Enterprise Architecture published, communicated and used	Improvements to enterprise architecture framework	Pervasive adoption of the enterprise architecture
Enterprise Architecture Repository	EA team only, while providing services to projects.	Accessed by key content contributors. EA repository first published on EA web site	Loosely connected community of users across the organisation units	Significant EA Assets are documented and modelled, regularly reviewed and updated.	EA assets used for architecture governance and compliance
Enterprise Architecture Development Process	Process only used by Enterprise Architecture	Some use by Solution Architects in Projects. EA Processes integrated with Euroclear	Used by all key projects	Used by all new projects	Continuous improvements to enterprise architecture development process
Target Enterprise Architecture	Some large granularity Service Domains defined. Principles identified.	Service Domains are mapped to existing applications and COTS applications. Business Process reference model establish for core processes.	Reference Architecture in general use for key	Re-use of common application services and Application components Fine granularity services identified	All Reference Architecture models are established and used for all new applications and some legacy

# Look to Estonia



Estonia: A Model for e-Government, CACM June 2015

# Simulation and Exercises



## SANS CyberCity

- <https://www.sans.org/netwars/cybercity>



## Michigan Cyber Range: Alphaville

- <http://www.merit.edu/cyberange/alphaville.php>



## EA/Maxis - SIMCITY

- <http://www.simcity.com/>

# Media Attention & Public Awareness



WORLD | PASSCODE | PASSCODE VOICES | SECURITY

## Opinion: Why the aviation industry needs more hackers

Claims about a researcher infiltrating a plane's control systems have put a spotlight on aviation security. It's time for the industry to be more open about potential risks and let hackers test the strength of their networks.

By Space Rogue, Contributor | MAY 29, 2015



Great example is Space Rogue's article on aviation security in Christian Science Monitor

“Claims about a researcher infiltrating a plane's control systems have put a spotlight on aviation security. It's time for the industry to be more open about potential risks and let hackers test the strength of their networks.”



## **Black Hat Sound Bytes**

- Cites are the backbone of civilization, but are fragile and snarls of complexity and interdependencies.
- Securing our cities would be a major step toward securing nations, but significant obstacles stand in the way.
- Lessons from securing companies can be applied to securing cities, if there is strong leadership, sufficient resources, and politics don't get in the way.



# Questions



Tom Cross  
@\_decius\_

David Raymond  
@dnomyard

Greg Conti  
@cyberbgone