



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

David Raymond

Greg Conti

Drawbridge Networks

Virginia Tech

West Point

@_decius_

@dnomyard

@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



- **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*?

Google:

city

/'sɪdē/

noun

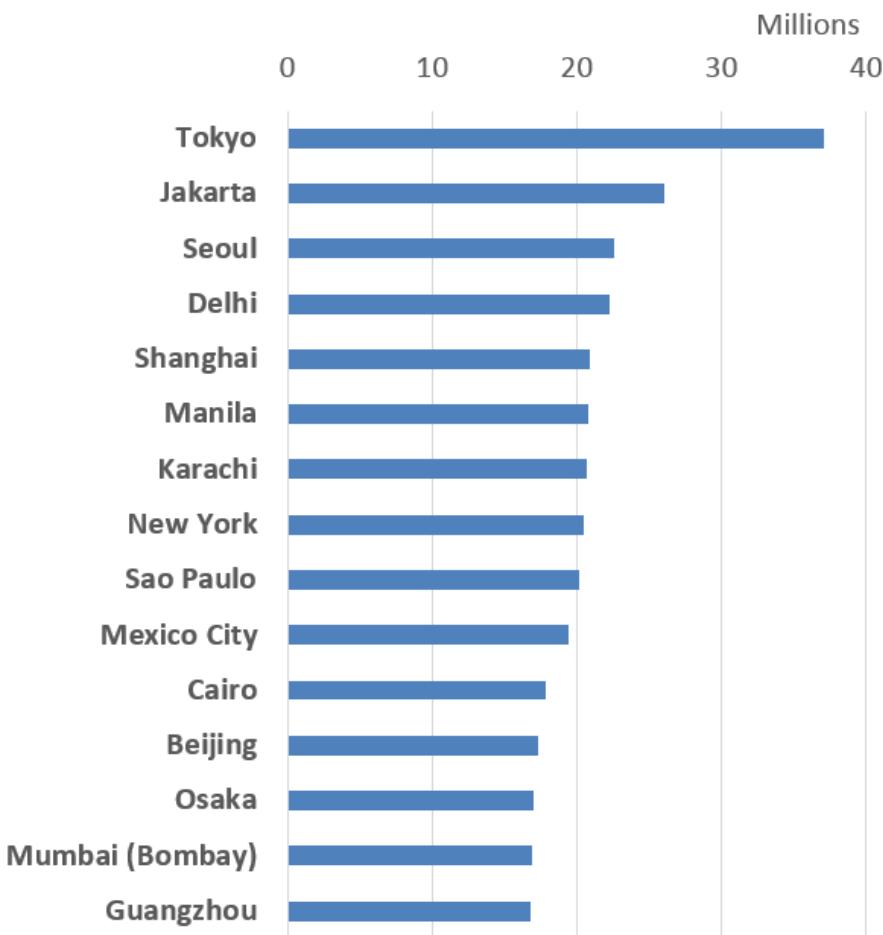
1. a large town.
“one of Italy’s most beautiful cities”
2. informal
a place or situation characterized by a specific attribute.
“panic city”

Attributes:

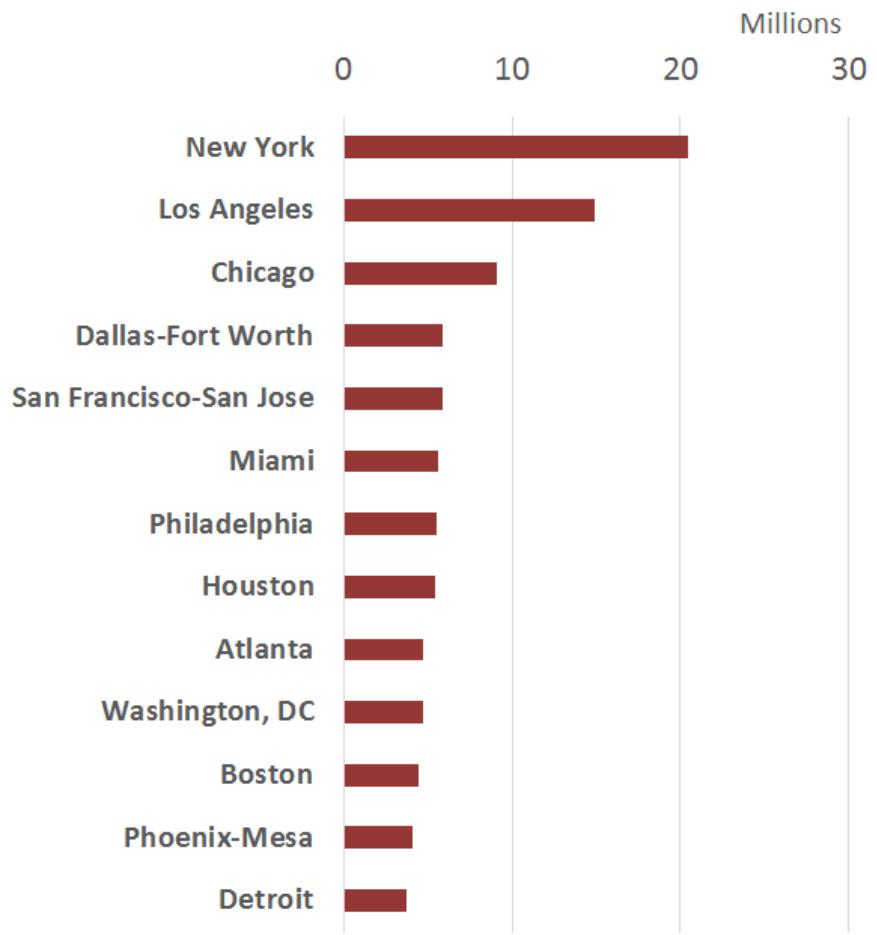
- A center of population, commerce, and culture (*thefreedictionary.com*)
- Incorporated municipality, usually governed by mayor and council (*Dictionary.com*)
- Has complex systems for sanitation, utilities, land usage, housing, and transportation (*Wikipedia*)

Largest Cities

Global

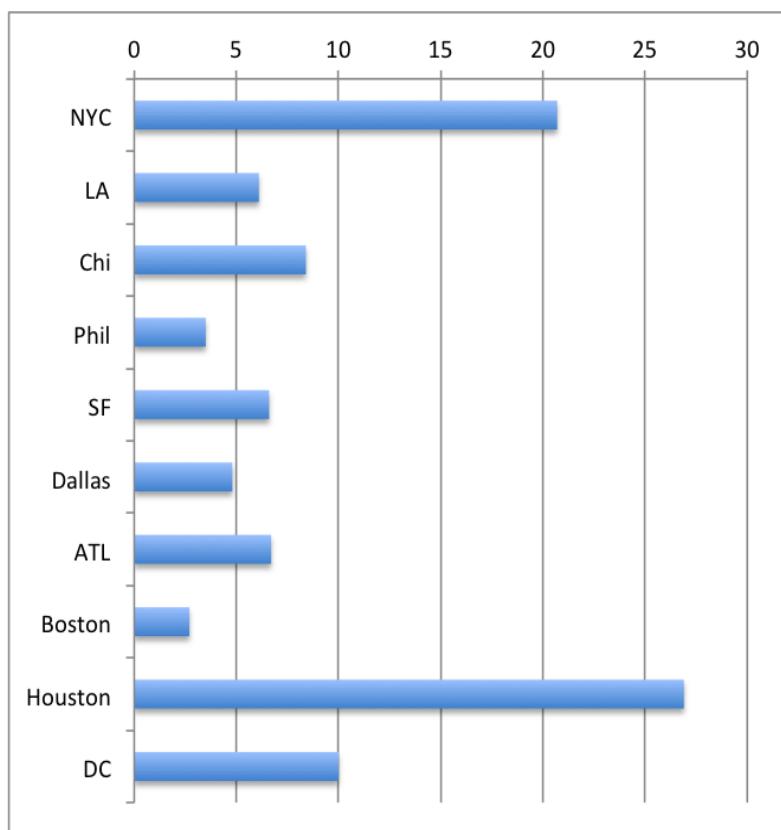


US



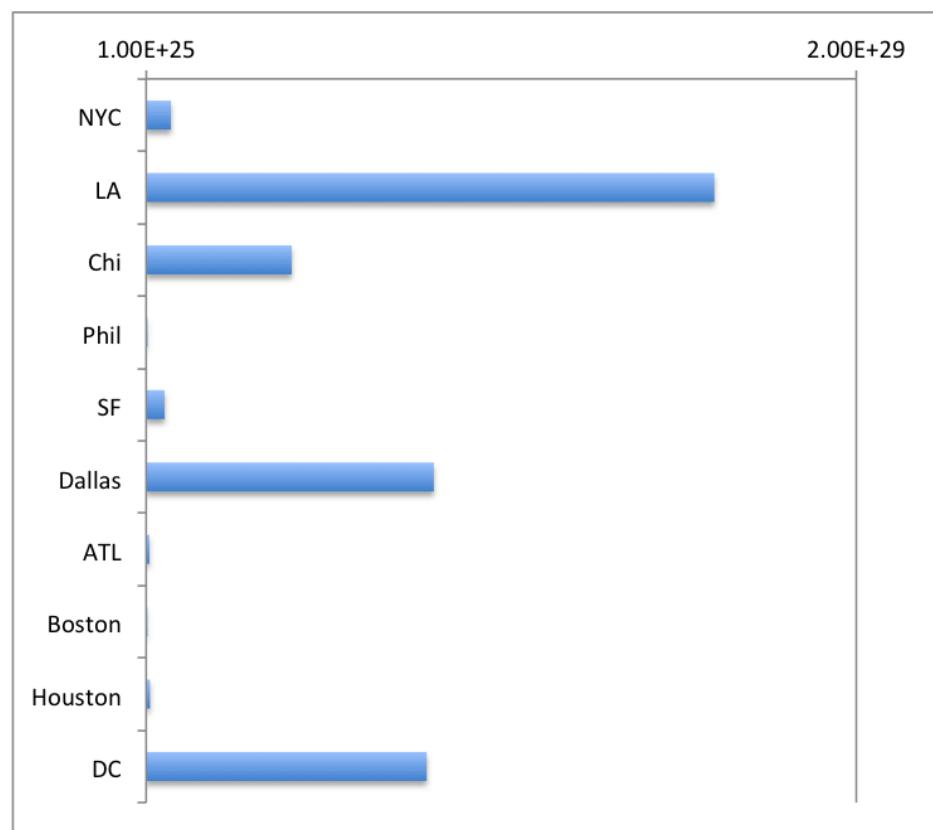
IP Addresses per Metro Area DMA Code

IPv4 (millions)

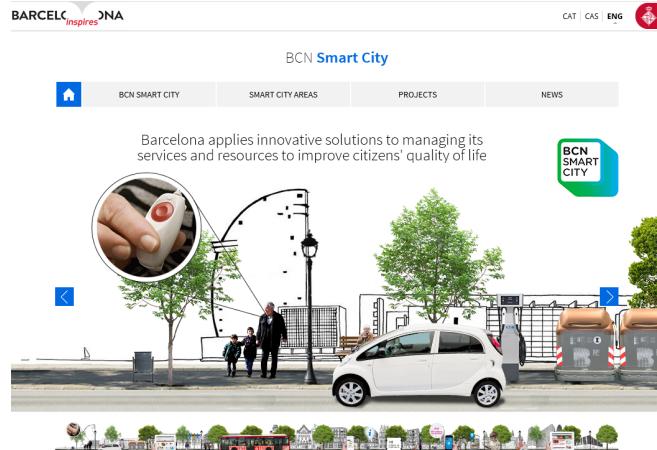


IPv6

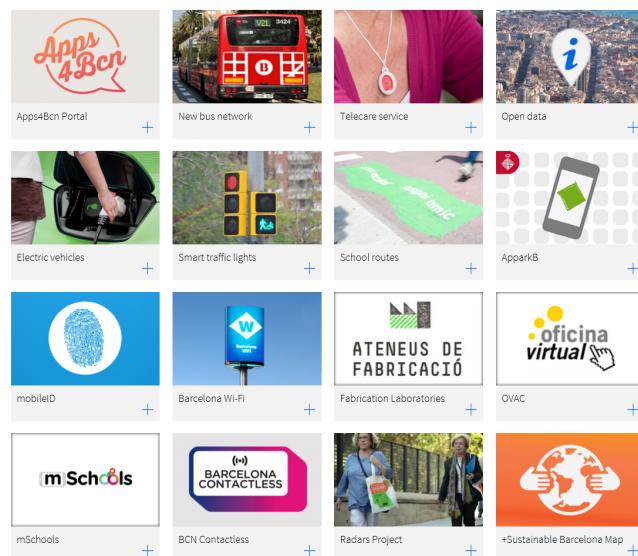
(Illustrates relative adoption, but baseline is e^{25} .)



Smart Cities = Larger Attack Surface



Barcelona, Spain



Representative Projects

“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

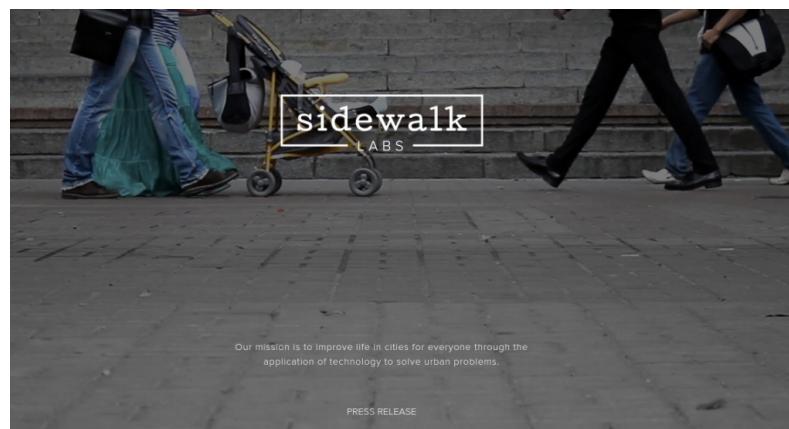
Major Industry Initiatives

The screenshot shows the Cisco website's "Smart+Connected Communities" section. At the top, there's a navigation bar with links for Worldwide [change], Log In, Account, Register, and My Cisco. Below the navigation is a sidebar with categories like HOME, SOLUTIONS, INDUSTRY SOLUTIONS, and various industry-specific sections such as Automotive, Consumer Packaged Goods, Education, Energy, Financial Services, Government, Healthcare, Hospitality, Life Sciences, Manufacturing, Materials and Mining, Public Sector, and Retail. The main content area features a video player titled "Transforming the Urban Experience" with a thumbnail of a city street. To the right of the video are links for Let Us Help (Email, Find a Local Reseller, Call 1-866-428-9596), View the demo (0000436), and Other Countries. Below the video is a section titled "Addressing the Challenges of a Changing World" which discusses urban challenges like traffic jams, pollution, and economic growth. It mentions Cisco Smart+Connected Communities solutions. Further down are sections for "Smart+Connected City" and "Smart+Connected Transportation". Social media links for Facebook, Twitter, YouTube, LinkedIn, and Flickr are also present.

Cisco's Smart Connected Communities

The screenshot shows the IBM Intelligent Operations Center website. The header includes links for Features and Downloads. A banner at the top states "Operational insight helps city leaders manage a safer, smarter city." Below the banner is a section for "Intelligent Operations Center for Smarter Cities" with a "View the demo" link (0000436). The main content area discusses the IBM Intelligent Operations Center's capabilities for managing complex city environments, including integrated data visualization, real-time collaboration, and deep analytics. It lists several key features: monitoring resources and incidents through situational awareness; optimizing city growth and operations through deep analysis of the city environment and resources; connecting citizens and addressing their concerns through citizen collaboration tools and services; keeping citizens safer with crime risk-spot analytics; and integrating data from various departments and agencies through a common platform. On the right side, there are sections for "Not in United States?", "Considering a purchase?", "Contact IBM" (with links for Chat now, Email IBM, Request a quote, or call 1-877-426-3774), and "Product support". A video player on the right shows a video titled "Video: An Intelligent Operations Center for emergency management in the Philippines".

IBM's Intelligent Operations Center



Google's Sidewalk Labs

But Don't Forget Dumb Cities





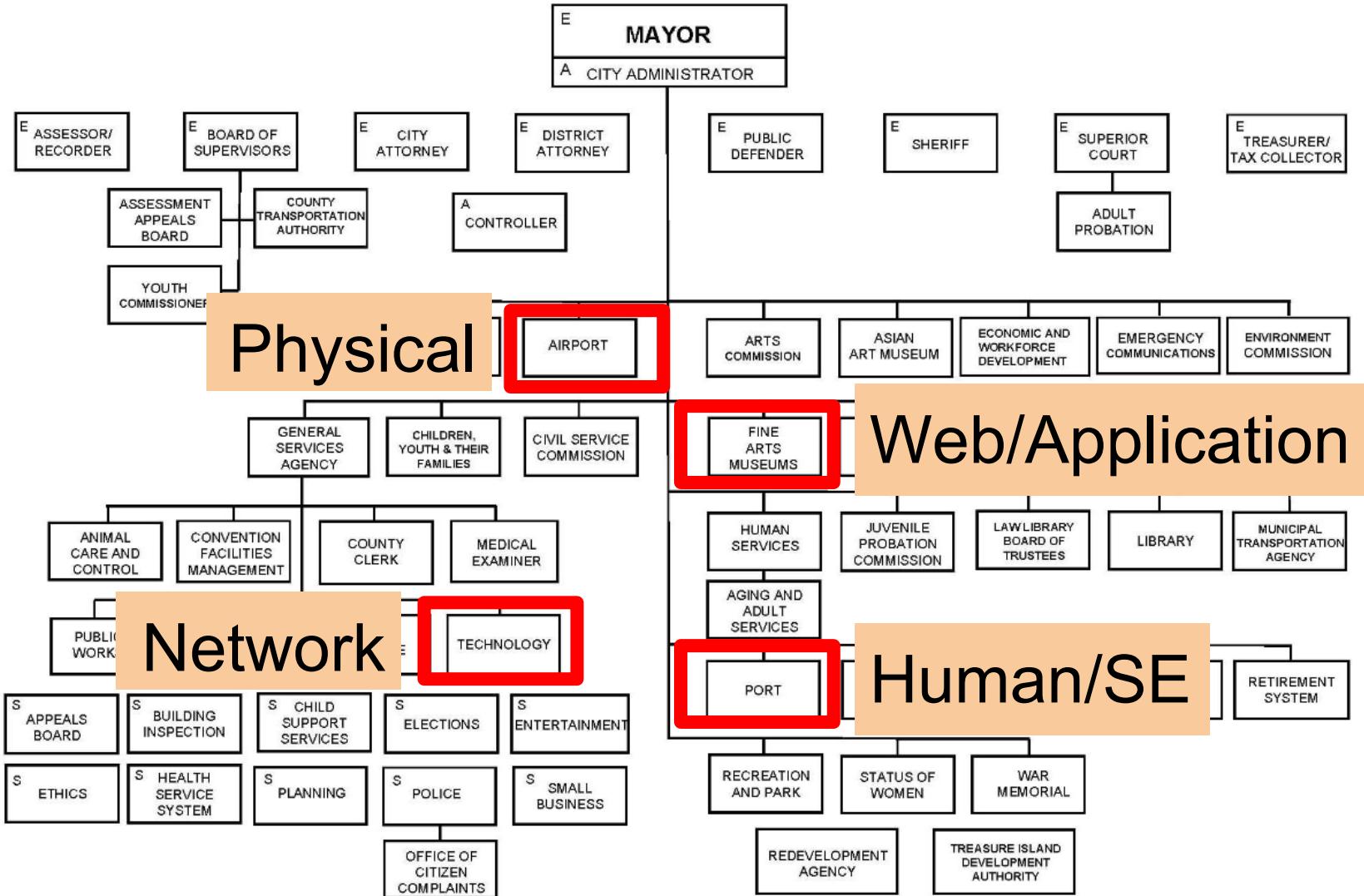
- Introduction
- **Pen Testing**
- Dissecting a City
- Cross Sectioning
- Pressure Points
- Risk Analysis
- Solutions

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

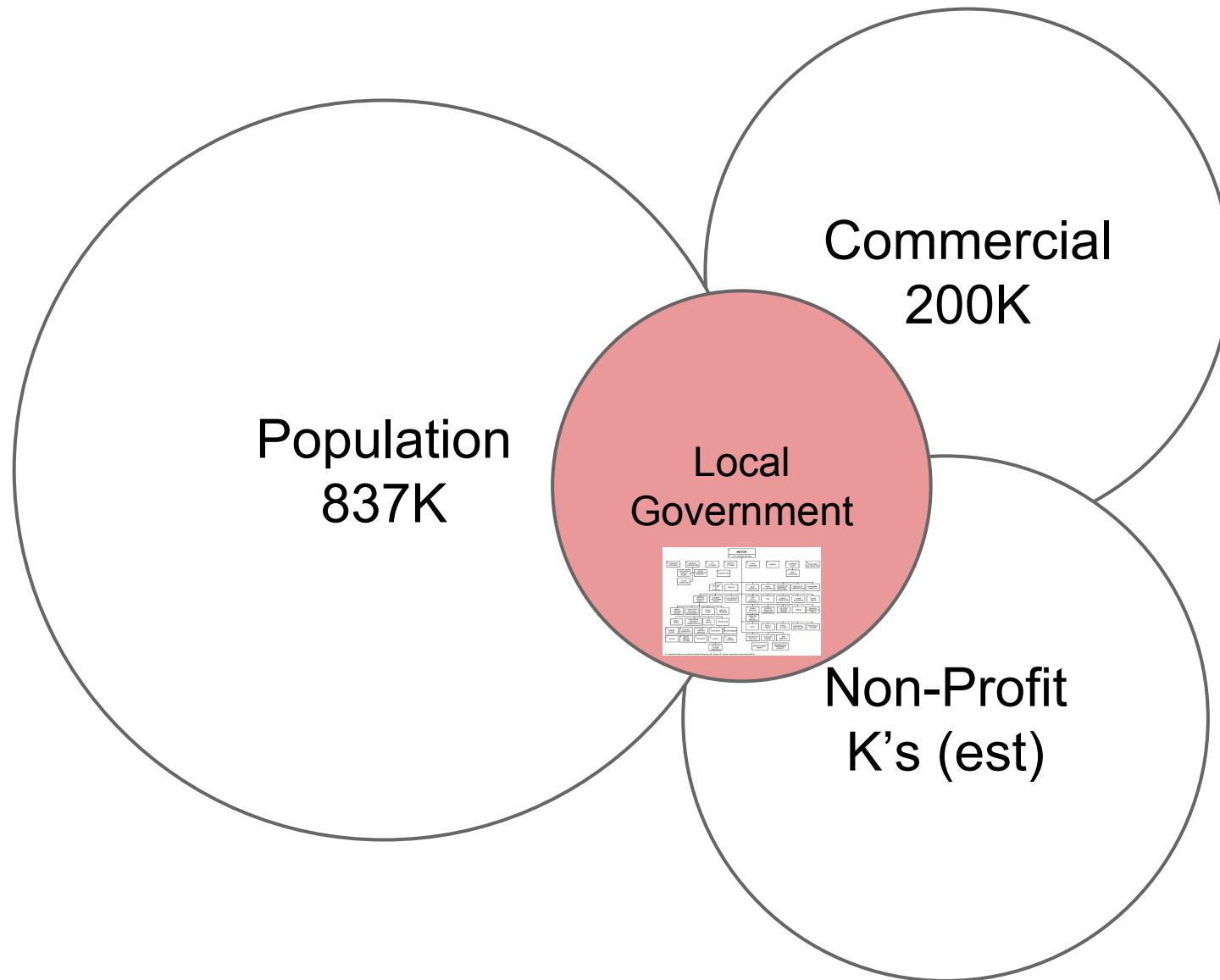
- | | |
|---|--|
| <ol style="list-style-type: none">1. Preparation<ol style="list-style-type: none">a. NDA/permission memob. Scoping and ROE2. Testing<ol style="list-style-type: none">a. Reconnaissanceb. Scanningc. Exploitationd. Password attackse. Wireless attacksf. Web app attacks3. Conclusion<ol style="list-style-type: none">a. Analysis and retestb. Pen test report | <p>VS.</p> <ol style="list-style-type: none">1. Define “City” (Scope)2. Determine audit surface area @ each level of abstraction<ol style="list-style-type: none">a. Determine how to collect information @ each level3. Cross sectional analysis4. Pressure point analysis5. Risk analysis of threat actors<ol style="list-style-type: none">a. Most likely courses of actionb. Most dangerous courses of action |
|---|--|

ANATOMICORVM INSTRVMEN-
TORVM DELINEATIO.

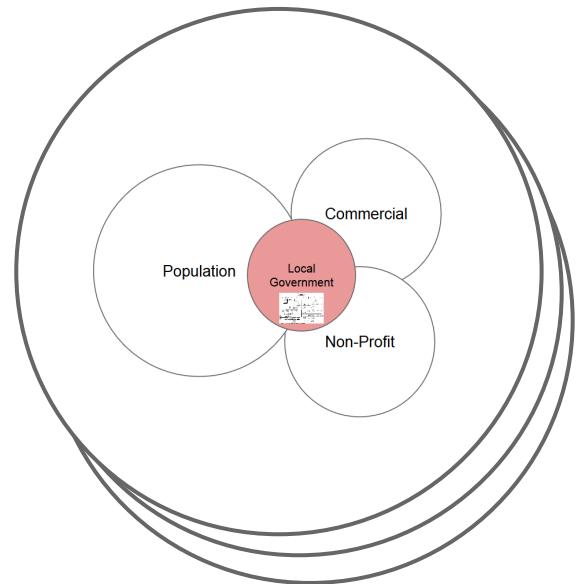


- Introduction
- Pen Testing
- **Dissecting a City**
- Cross Sectioning
- Pressure Points
- Risk Analysis
- Solutions

A Quick Look at San Francisco



A Quick Look at the United States

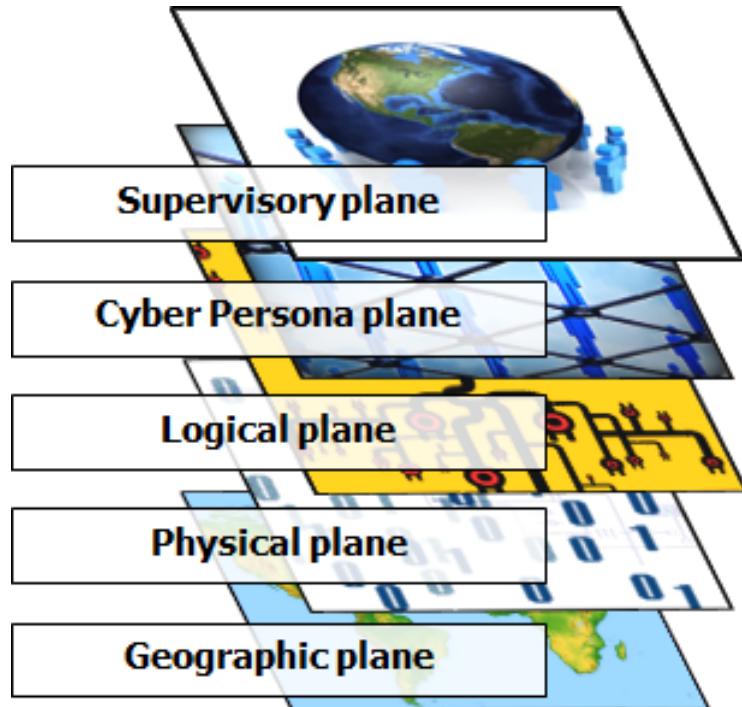


“Cities”

X 39K =

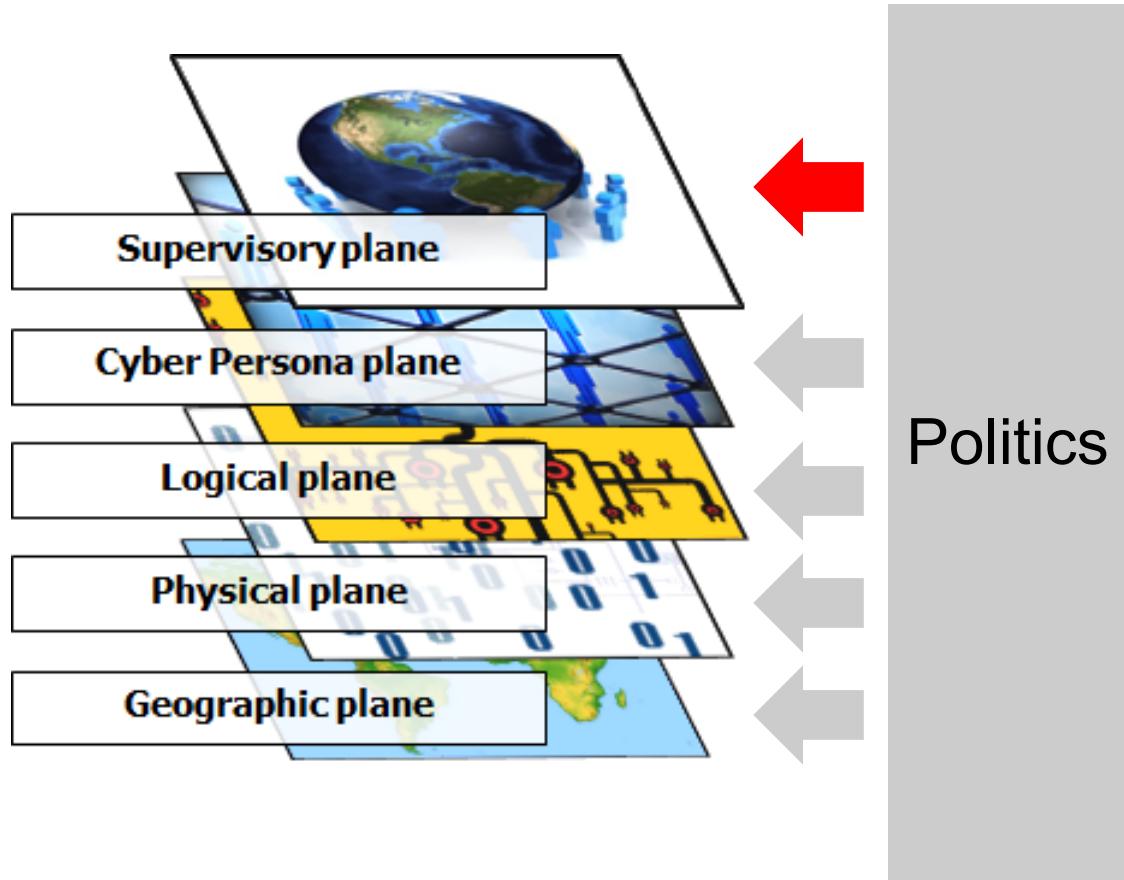
- 1 Country
- 50 States
- 18K Large Businesses
- 39K Local Govts
- 1.5M Non-profits
- 27M Small Businesses
- 182M Smart Phones
- 310M Personal Computers
- 318M People
- Bs IoT

Cyberspace Planes

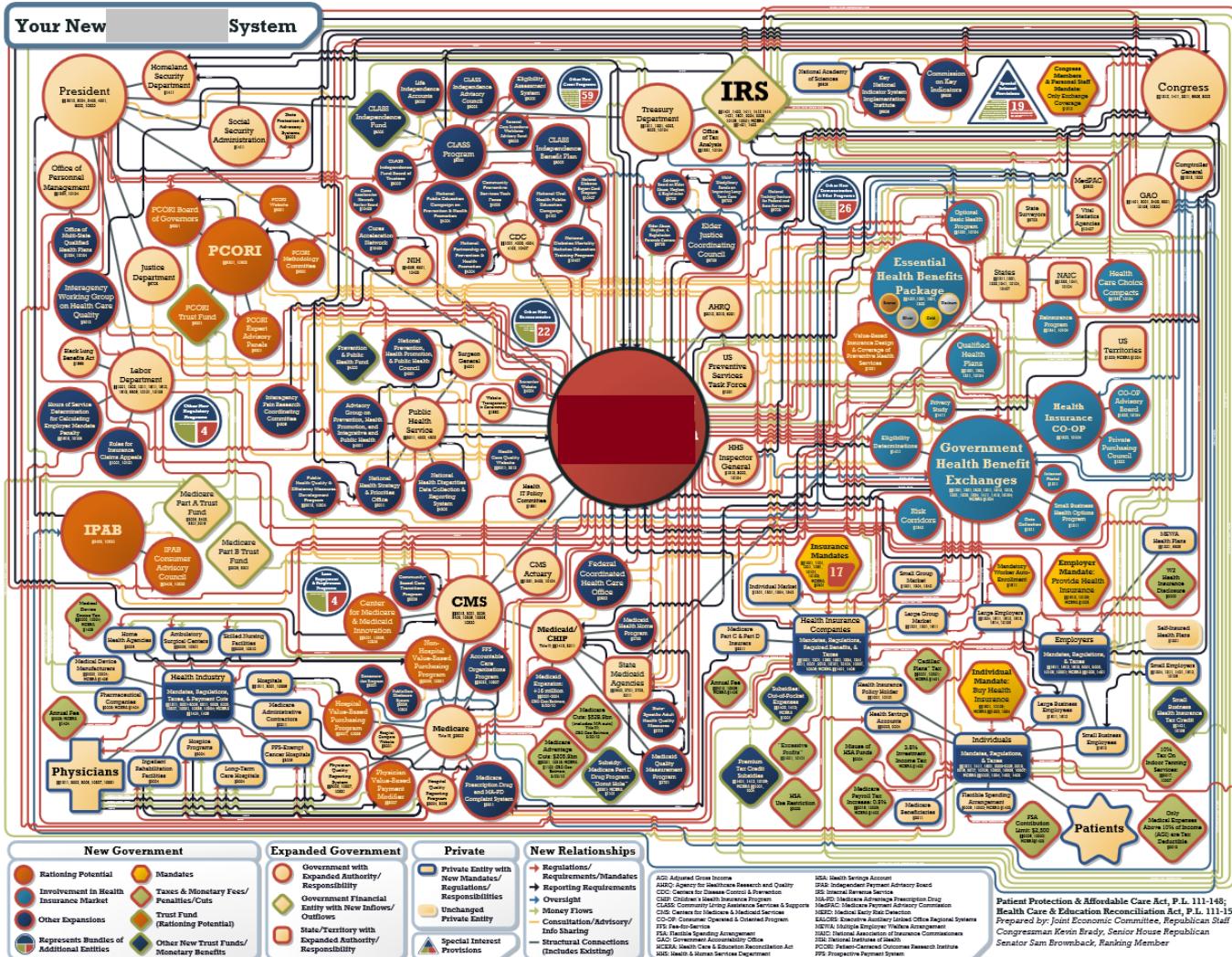


- **Supervisory** - Often siloed/compartmentalized between sectors
- **Persona** - Relevant identities or accounts; do you know who to contact in other sectors?
- **Logical** - System compatibility; how do various networks and systems communicate?
- **Physical** - Redundancy; can connectivity be compromised?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

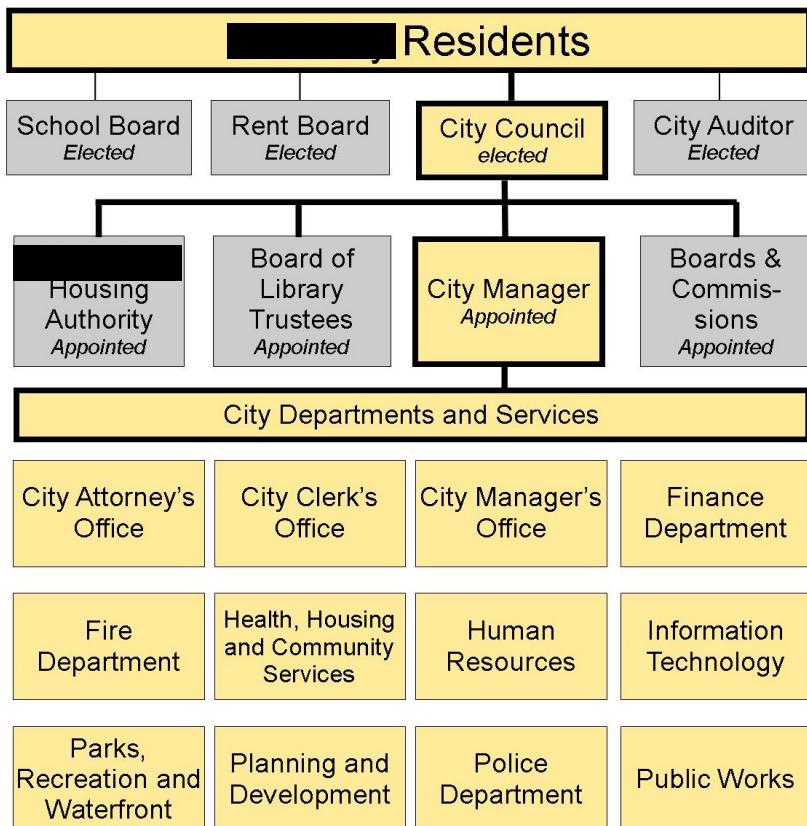
Cyberspace Planes



“Silos of Excellence”



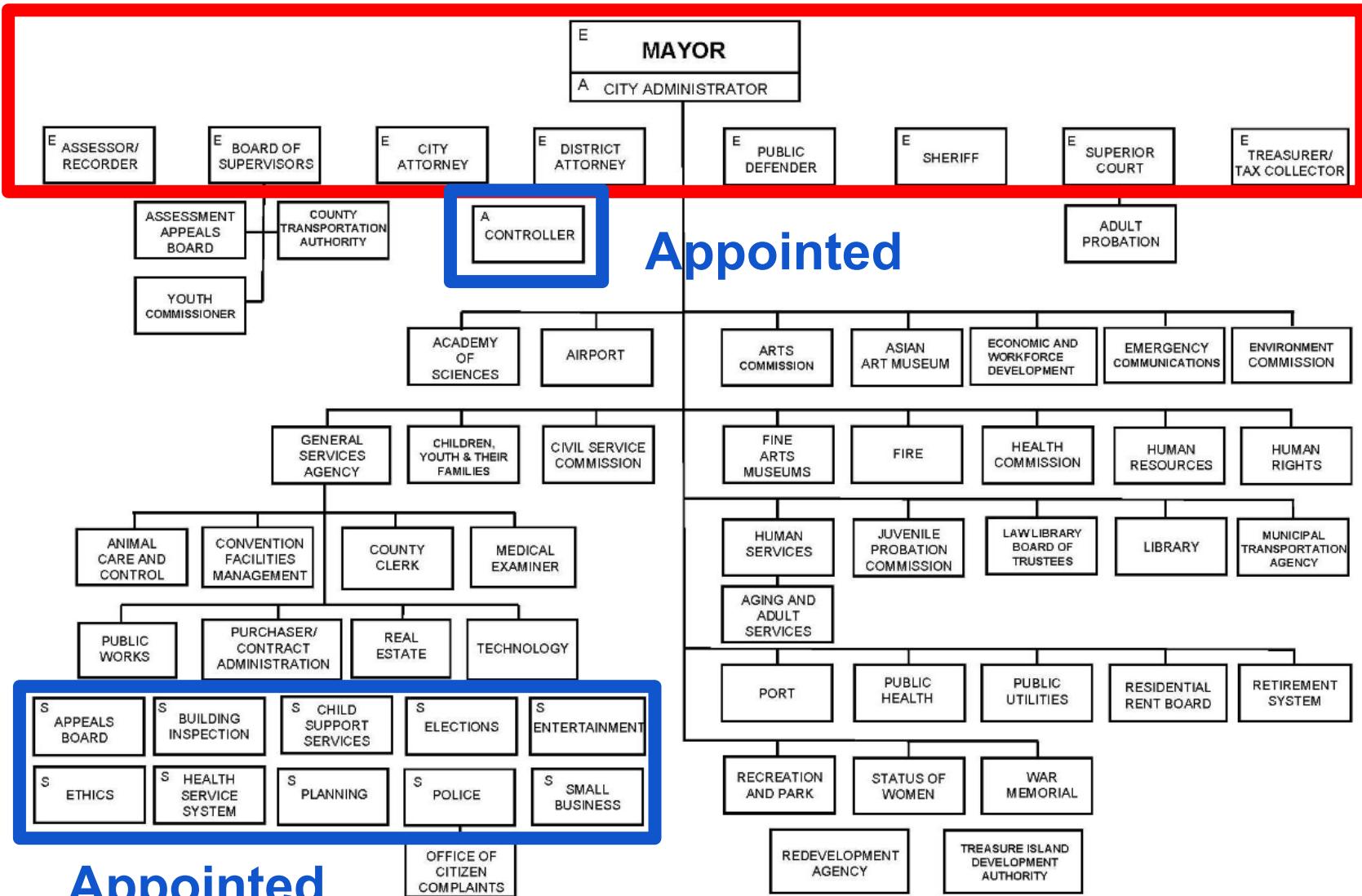
Supervisory Plane



- **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



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



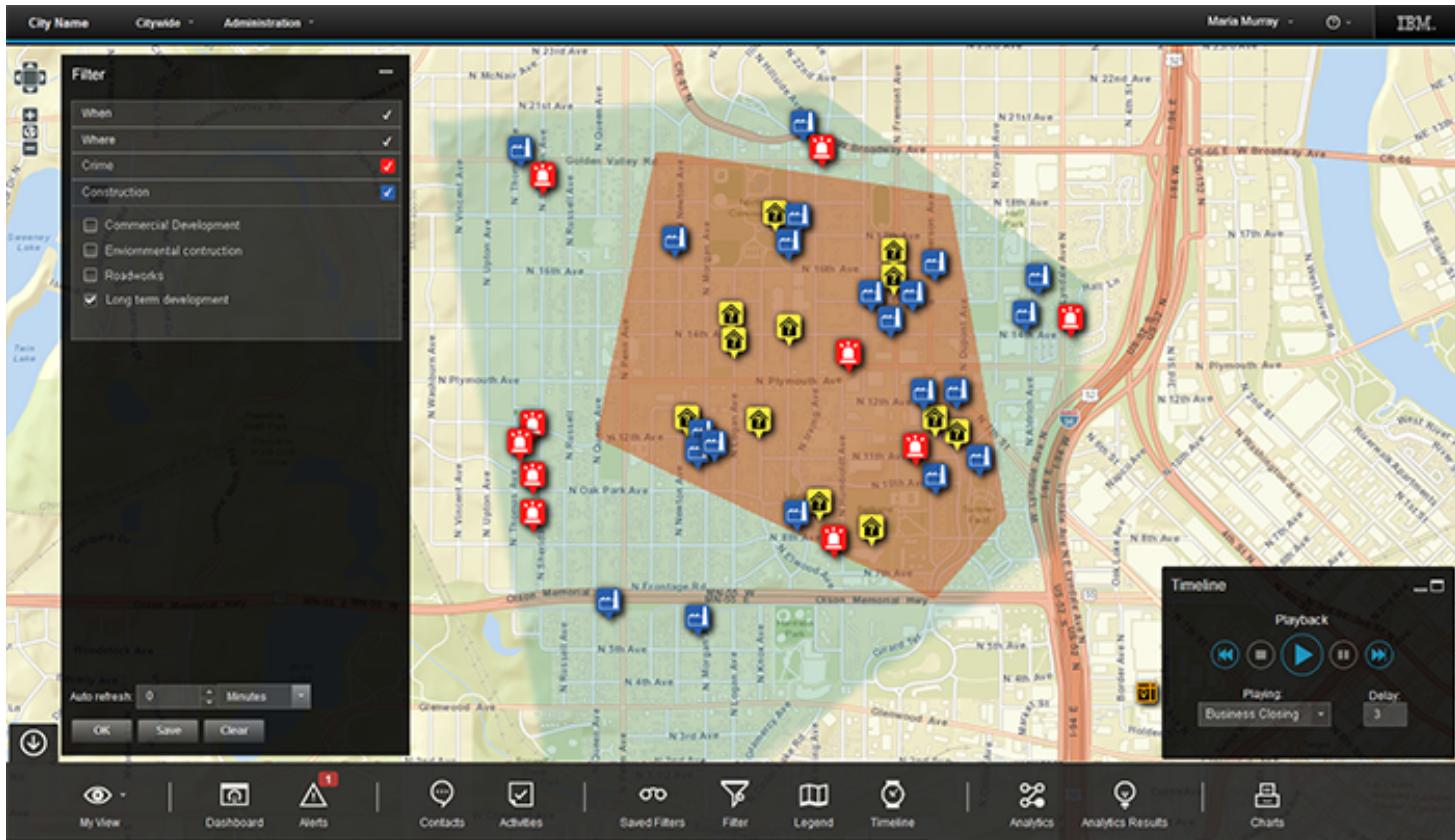
IBM Intelligent Operations Center

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

This screenshot shows the FAST Dashboard's map interface. On the left is a sidebar with a table of locations for I-15 SB. The main area shows a map of the Las Vegas and surrounding areas with numerous blue and yellow dots representing traffic cameras. A callout box shows a live feed from CCTV #5004.

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 NB at Flamingo
109	I-15 NB at Tropicana
110	I-15 SB at Hacienda
111	I-15 SB S of Russell
112	I-15 NB at Sunset
113	I-215 at I-15
114	I-15 NB at I-215
115	I-15 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



Many City governments have provider independent IP addresses

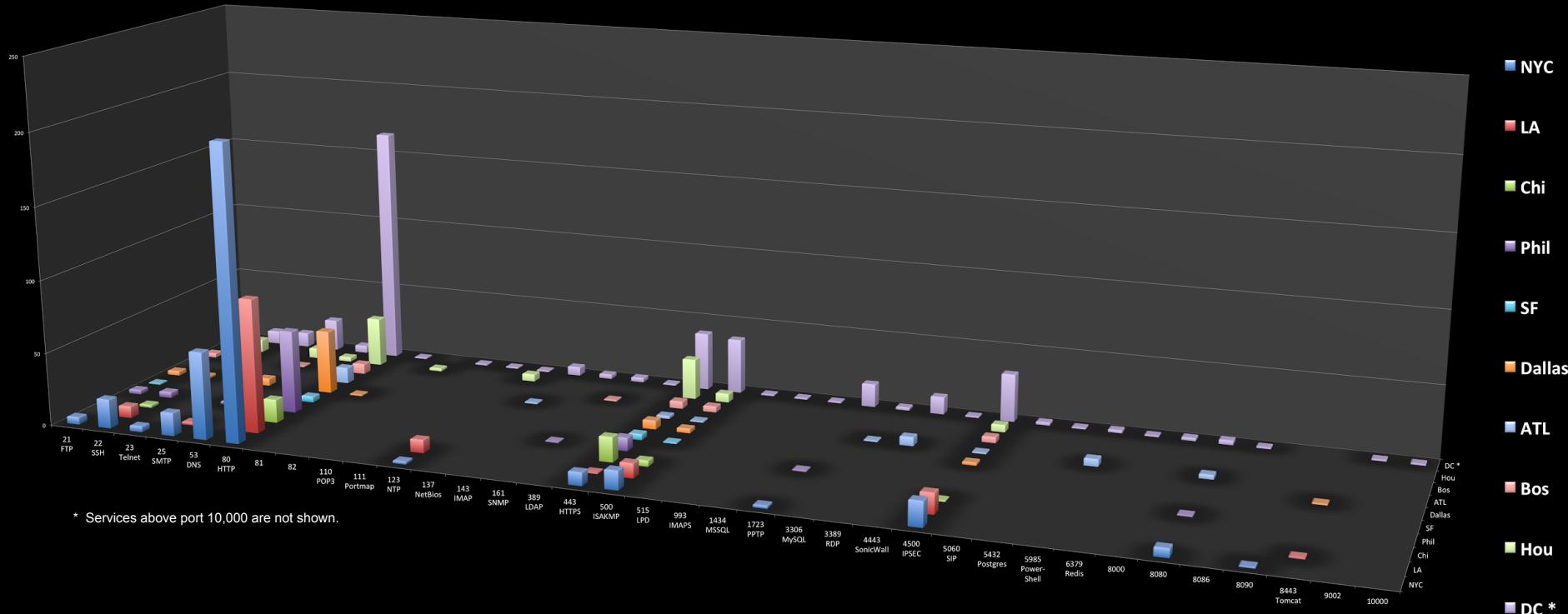
The screenshot shows the ARIN website's Whois-RWS search results for a specific network range. The page has a red sidebar on the left with a blue button labeled "ARIN Online enter". The main content area has a light blue header bar with the text "WHOIS-RWS". The search results table is titled "Network" and contains the following information:

Network	
Net Range	205.153.112.0 - 205.153.115.255
CIDR	205.153.112.0/22
Name	CLNVN-2
Handle	NET-205-153-112-0-1
Parent	NET205 (NET-205-0-0-0)
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	http://whois.arin.net/rest/net/NET-205-153-112-0-1
See Also	Related POC records.
See Also	Related organization's POC records.
See Also	Related delegations.

To the right of the table is a "RELEVANT LINKS" sidebar containing the following links:

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

Internet facing services hosted by the ten largest U.S. City governments.



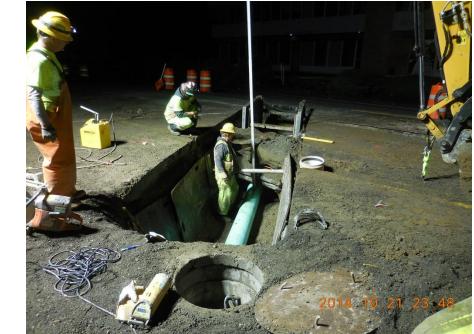
Physical Plane



Wireless Sensors



Shodan Maps



Buried Fiber

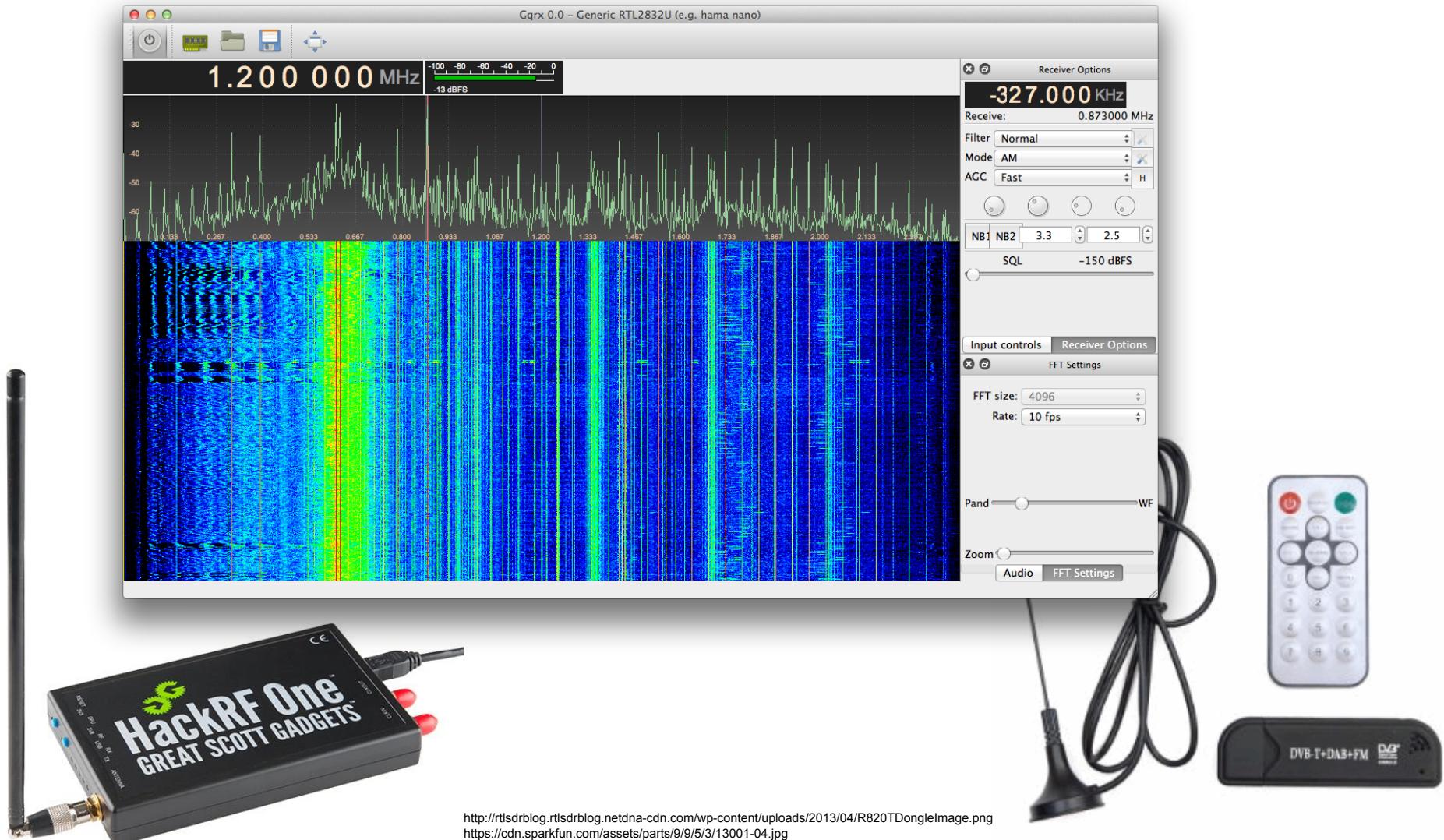


Emergency
Broadcast
System

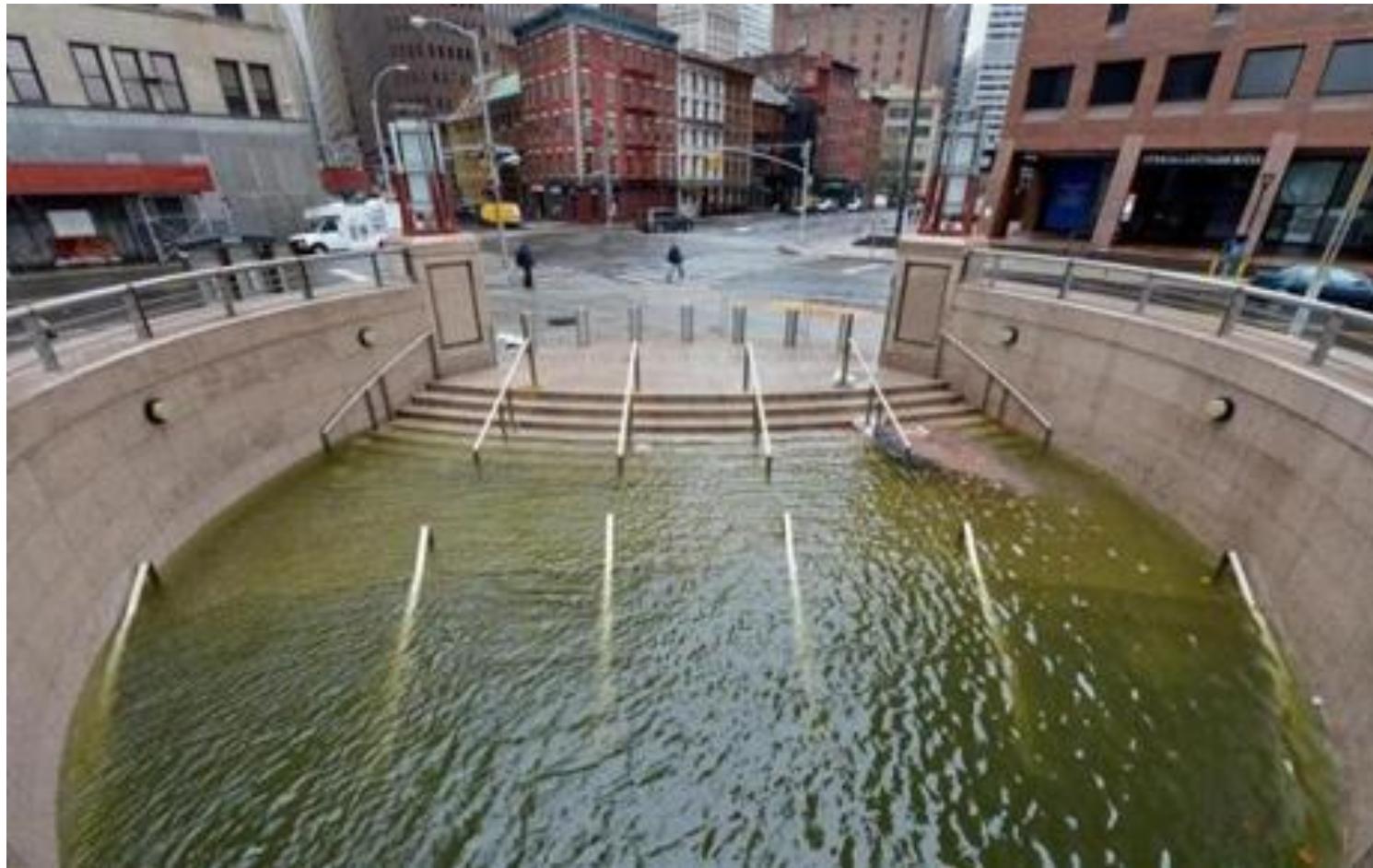


Municipal Wifi

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



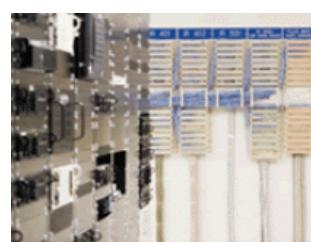
Critical Manufacturing



Healthcare and Public Health



Dams



Information Technology



Defense Industrial Base



Nuclear



Emergency Services



Transportation Systems



Energy



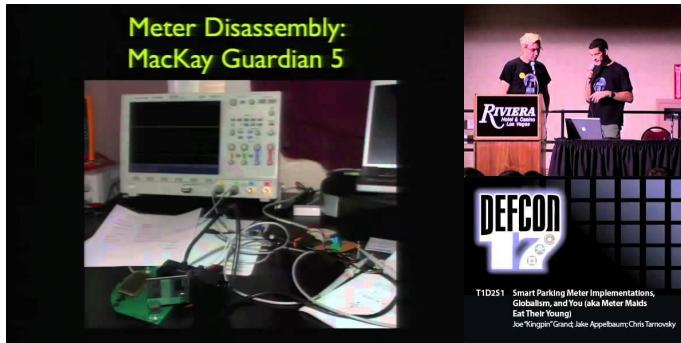
Water and Wastewater

<http://www.dhs.gov/critical-infrastructure-sectors>

InfoSec Community Research



Hacking Traffic Control Systems DEFCON 22



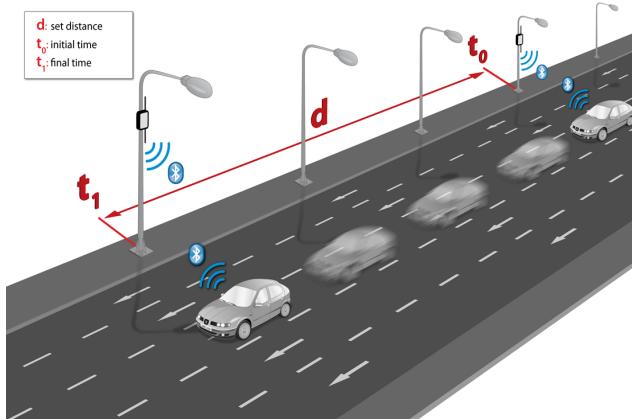
Smart Parking Meters
DEFCON 17



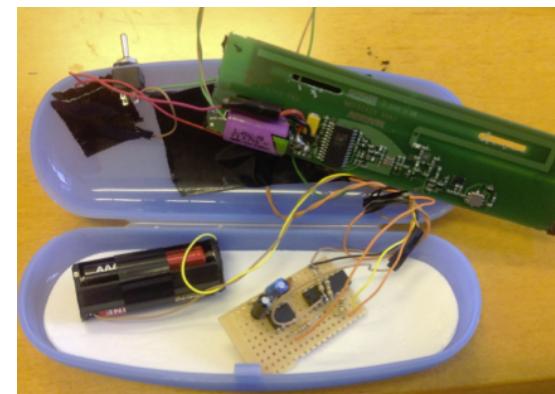
Electronic Road Signs



Gas Stations



Bluetooth Traffic Monitoring
DEFCON 22



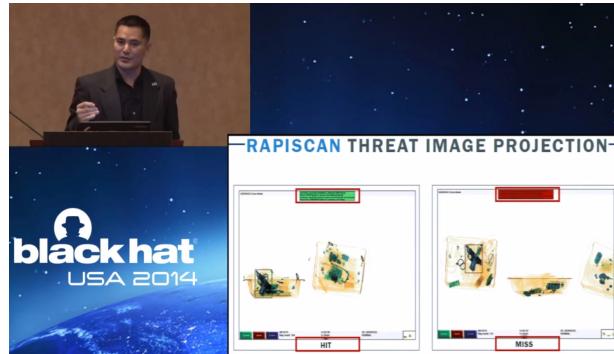
Toll Collection Systems
DEFCON 21

InfoSec Community Research



Power Meters

DEFCON 20



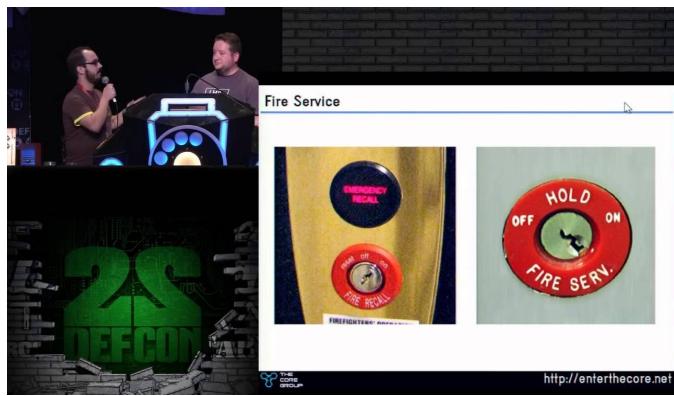
Airport Security & Air Traffic Control

BH 2014 / DEFCON 18



Water Plants

DEFCON 18



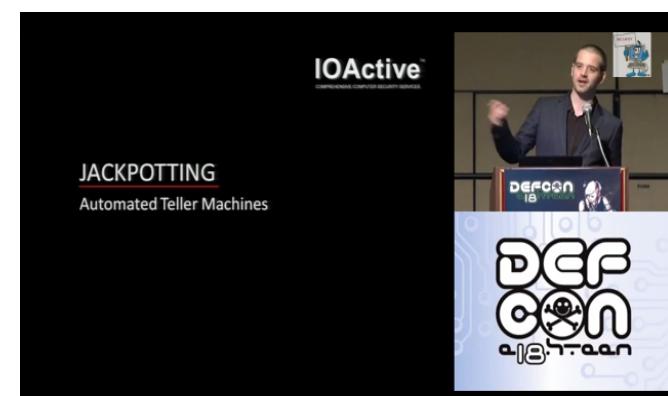
Elevators

DEFCON 22



Municipal Surveillance

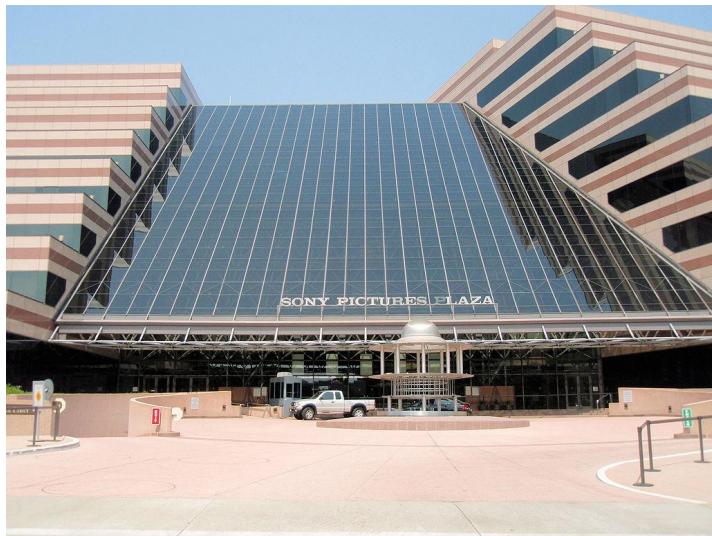
DEFCON 22



ATMs

DEFCON 18

and It Isn't All Just Researchers...



Sony Hack (2014)



Saudi Aramco

Saudi Aramco Hack (2012)



Sands Casino (2014)



Sands Casino (2010)

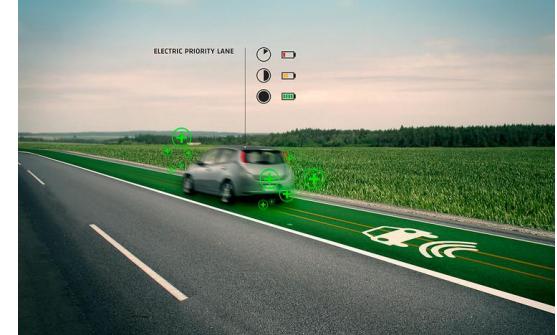
At Next Year's Black Hat



Roadway Sign Networks



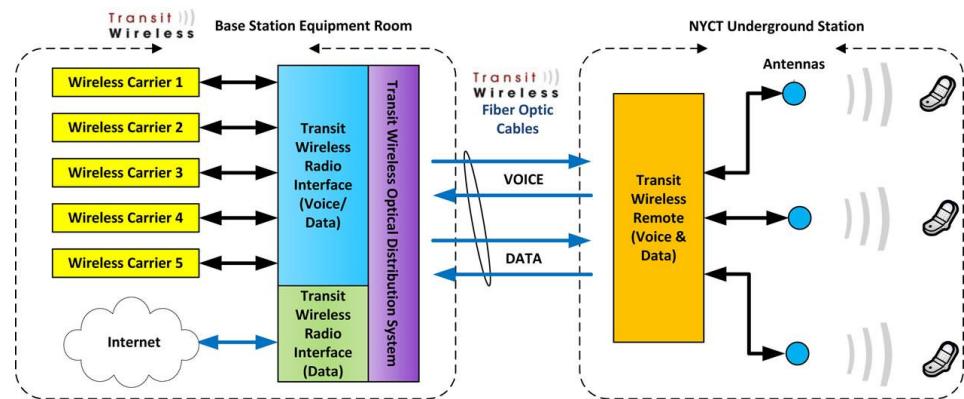
Electronic Billboards



Smart Highways



Traffic Reporting Systems



Mass Transit Wireless Networks

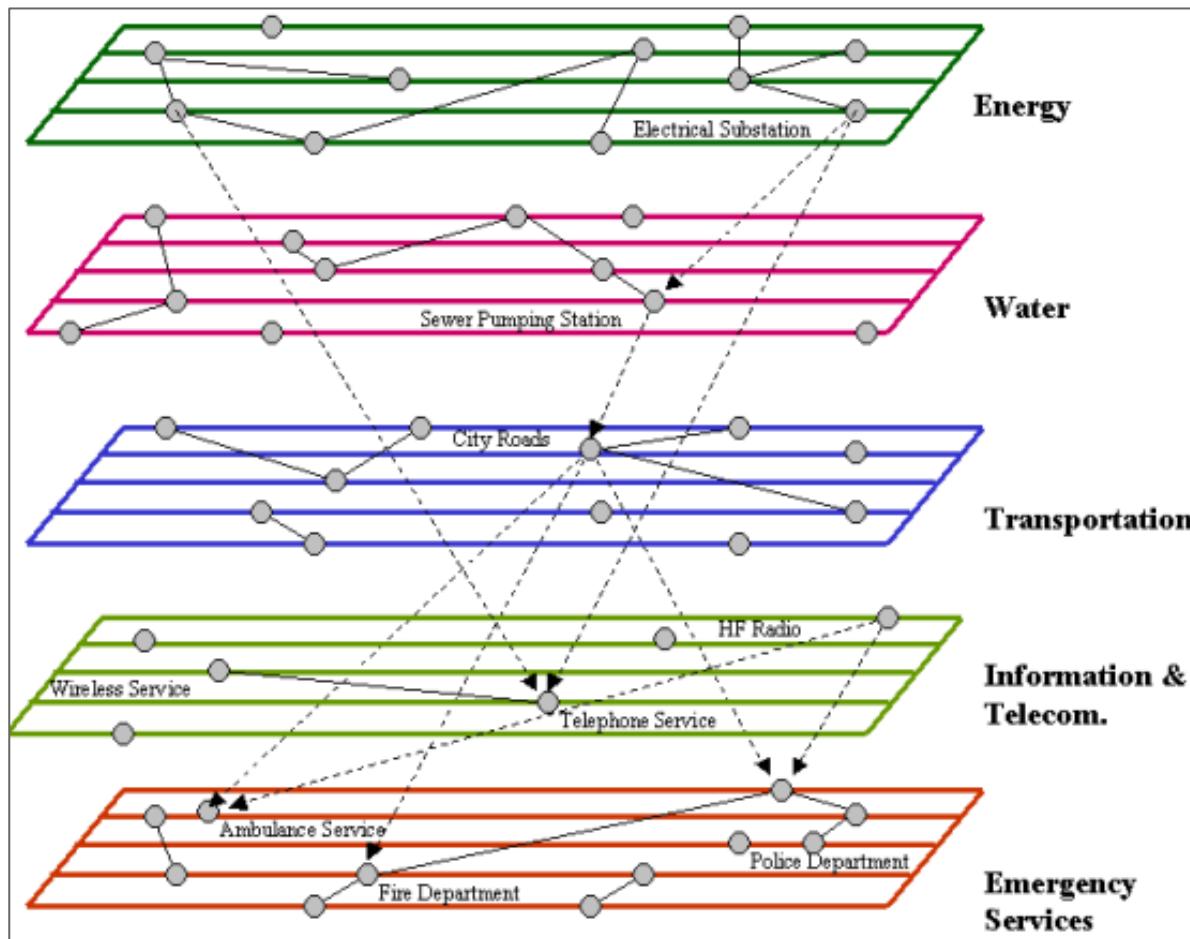
Effects



- **Deceive** - Cause a person to believe what is not true
- **Degradate** - 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)



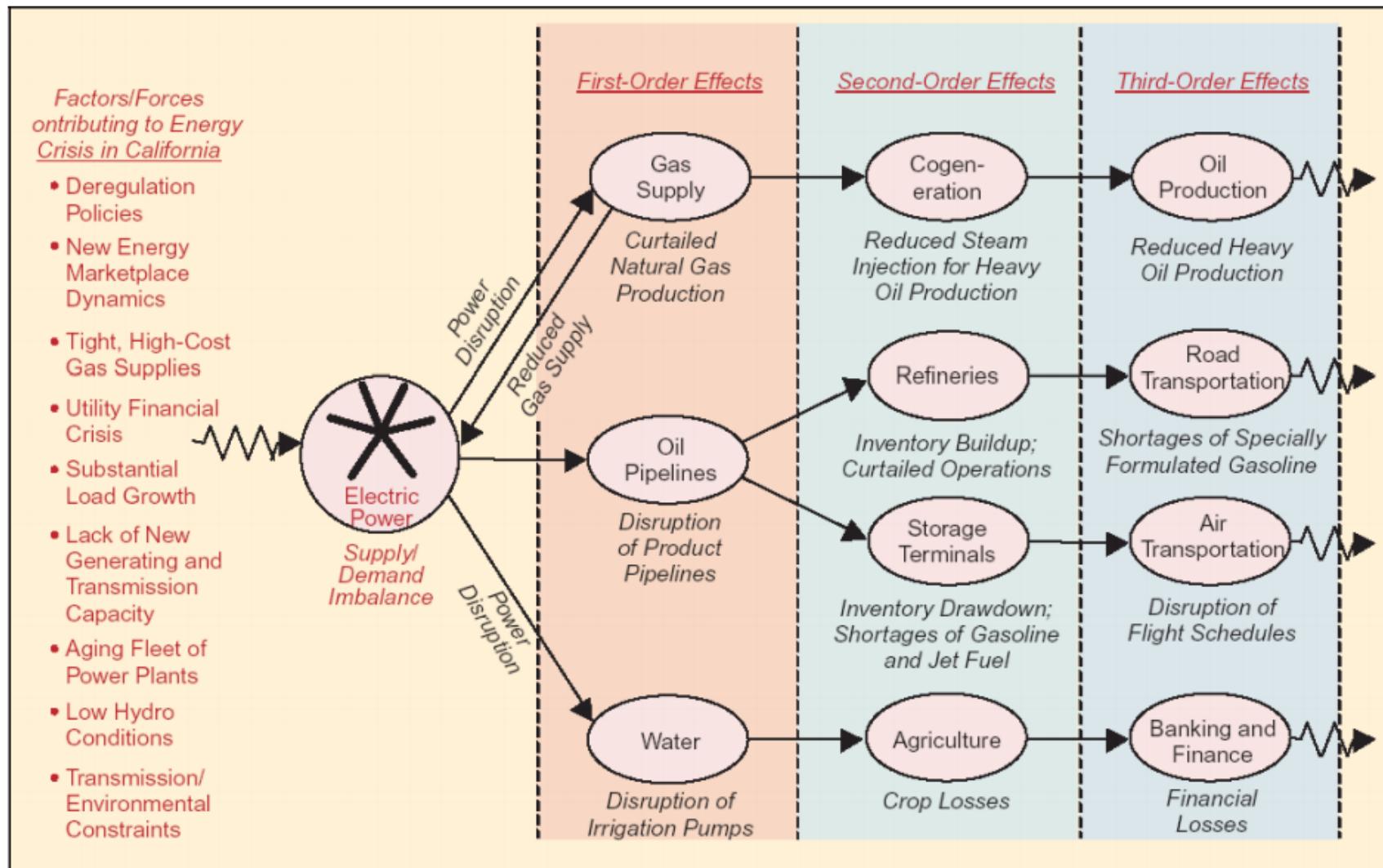
- Individual infrastructures are represented on a single plane
- Parallel lines represent subsets of infrastructure
- Nodes represent key infrastructure components
- Dotted lines indicate interdependencies

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
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

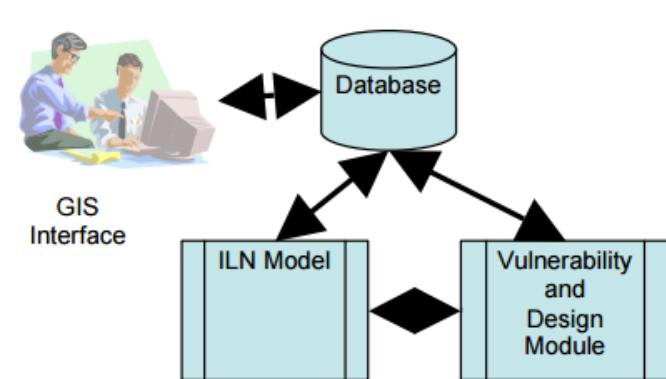
Key: H High M Medium L Low

Cascading Consequences

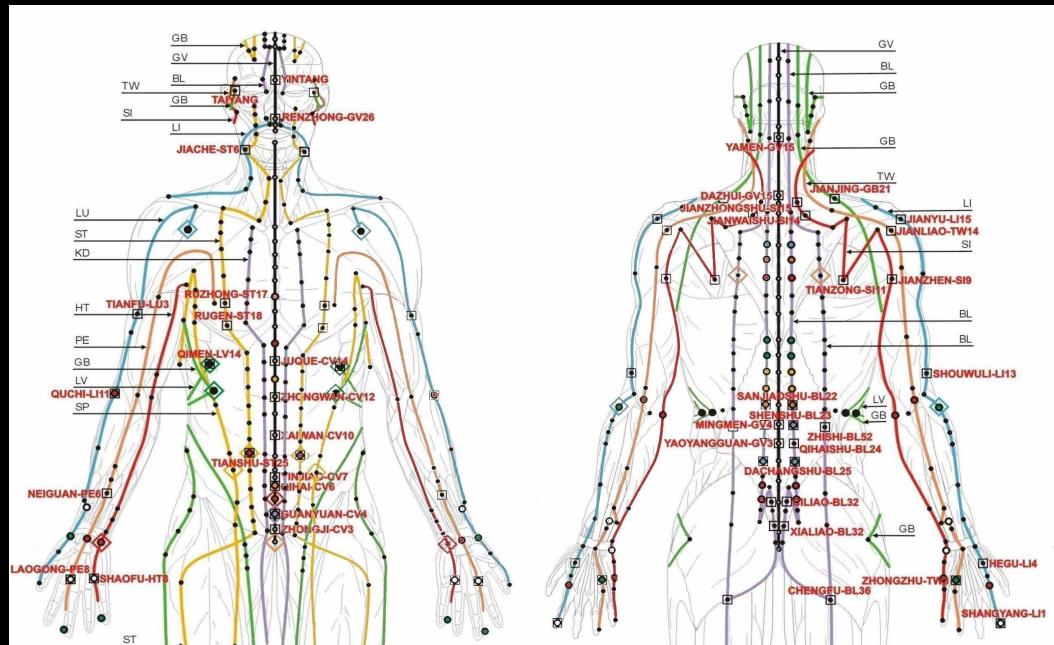


Modeling Interdependencies

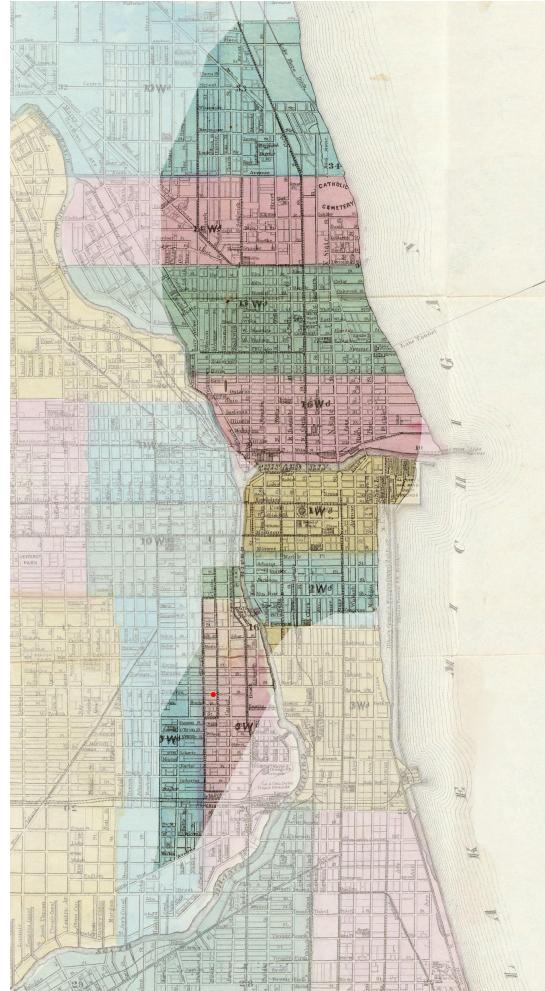
- National Infrastructure Simulation and Analysis Center (NISAC)
 - <http://www.sandia.gov/nisac/>
 - Suite of tools for analyzing interdependencies between sectors
- Multi-network Interdependent Critical Infrastructure Program for Analysis of Lifelines (MUNICIPAL)
 - RPI/NSF
 - Uses Interdependent Layered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



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



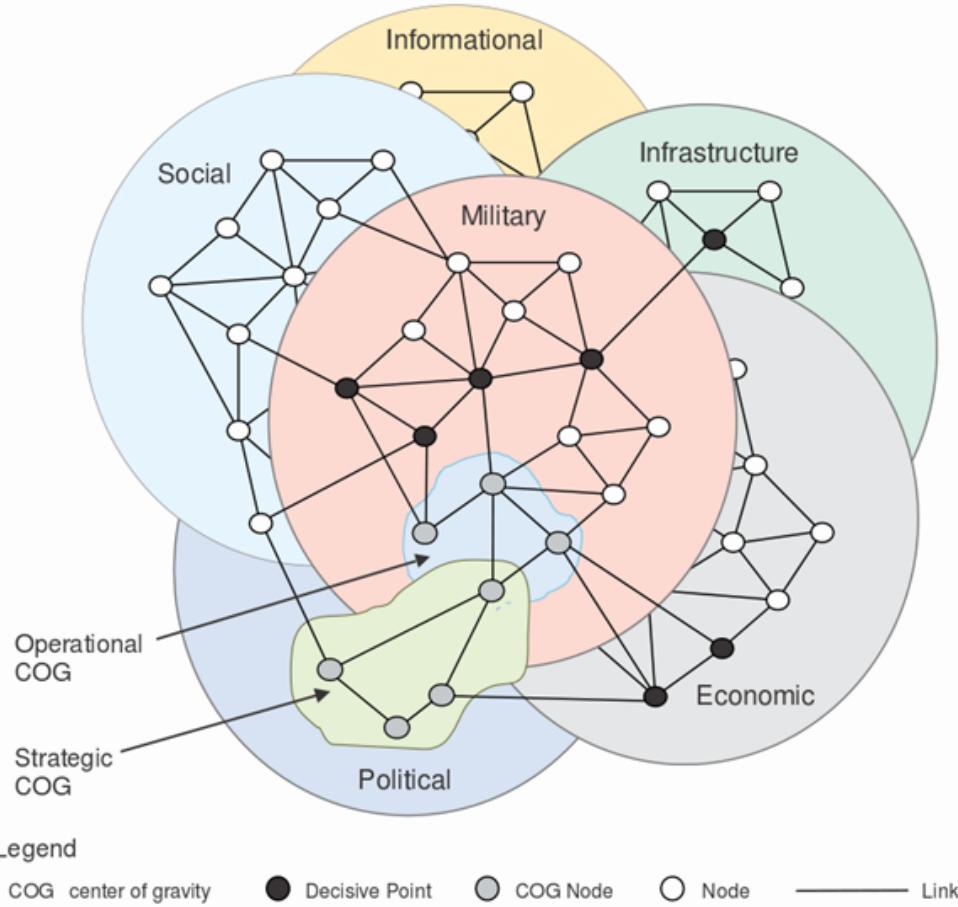
A Small Barn Fire...



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

http://upload.wikimedia.org/wikipedia/commons/3/3a/Great_Chicago_Fire_map_with_starting_point.jpg

Center of Gravity Analysis



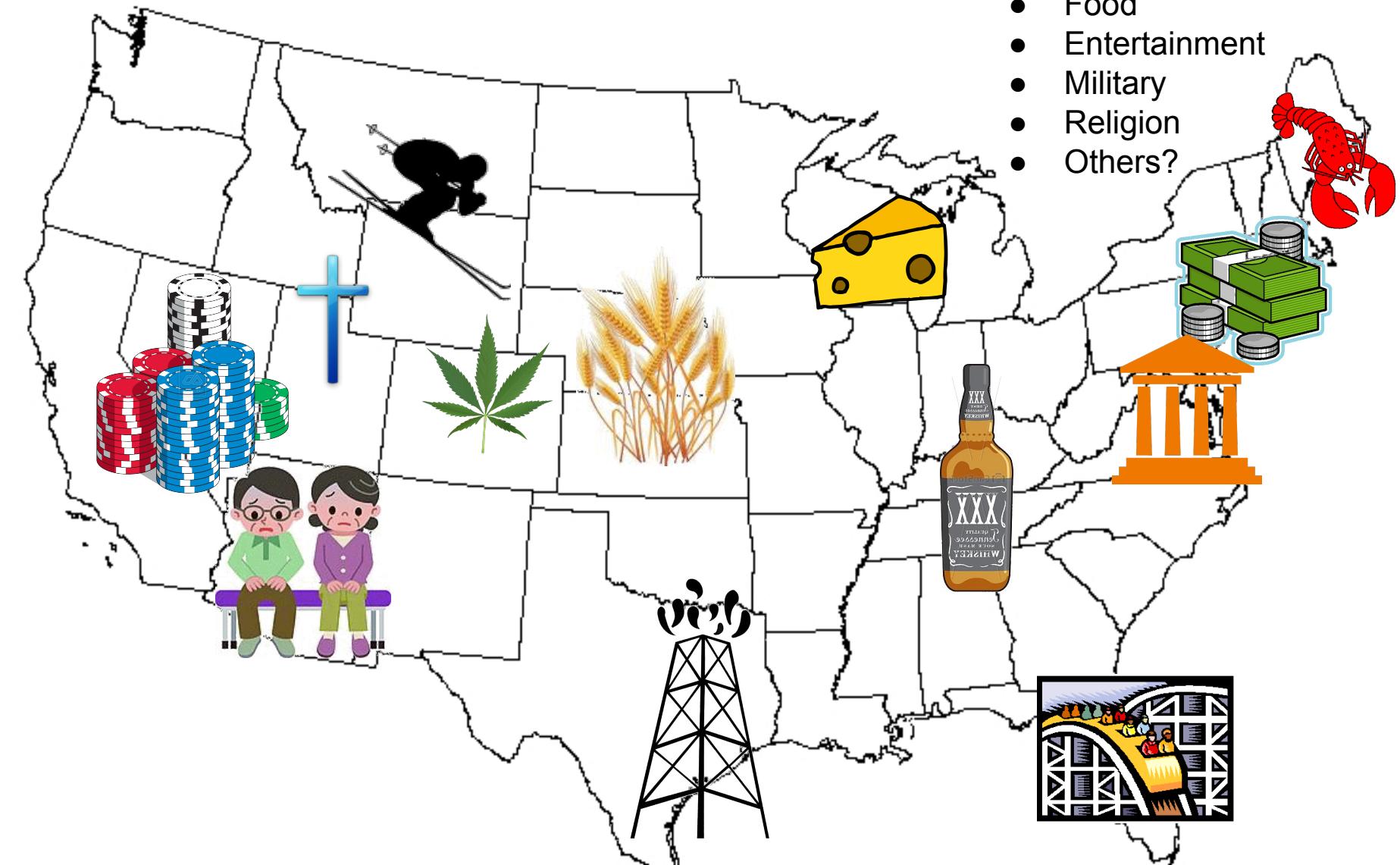
"The source of power that provides moral or physical strength, freedom of action, or will to act."

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

- DoD JP 1-02, 2008

Centers of Gravity

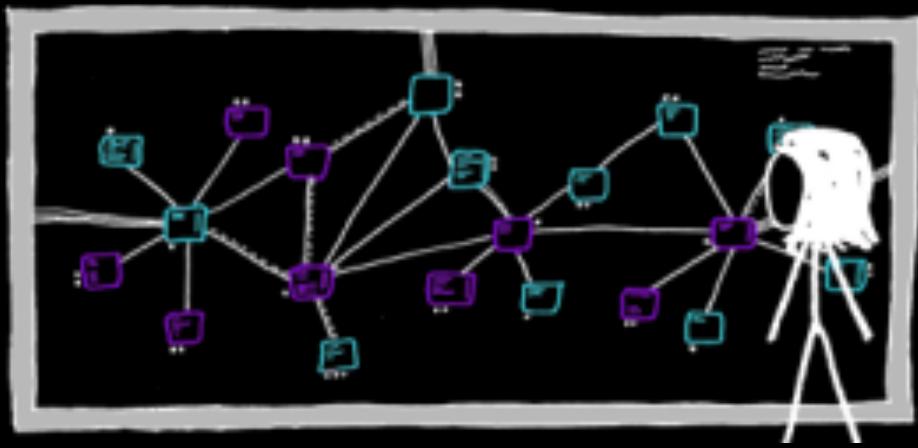
- Government
- Financial sector
- Retired people
- Gaming
- Energy/oil
- Food
- Entertainment
- Military
- Religion
- Others?



“Non-Critical” Sectors

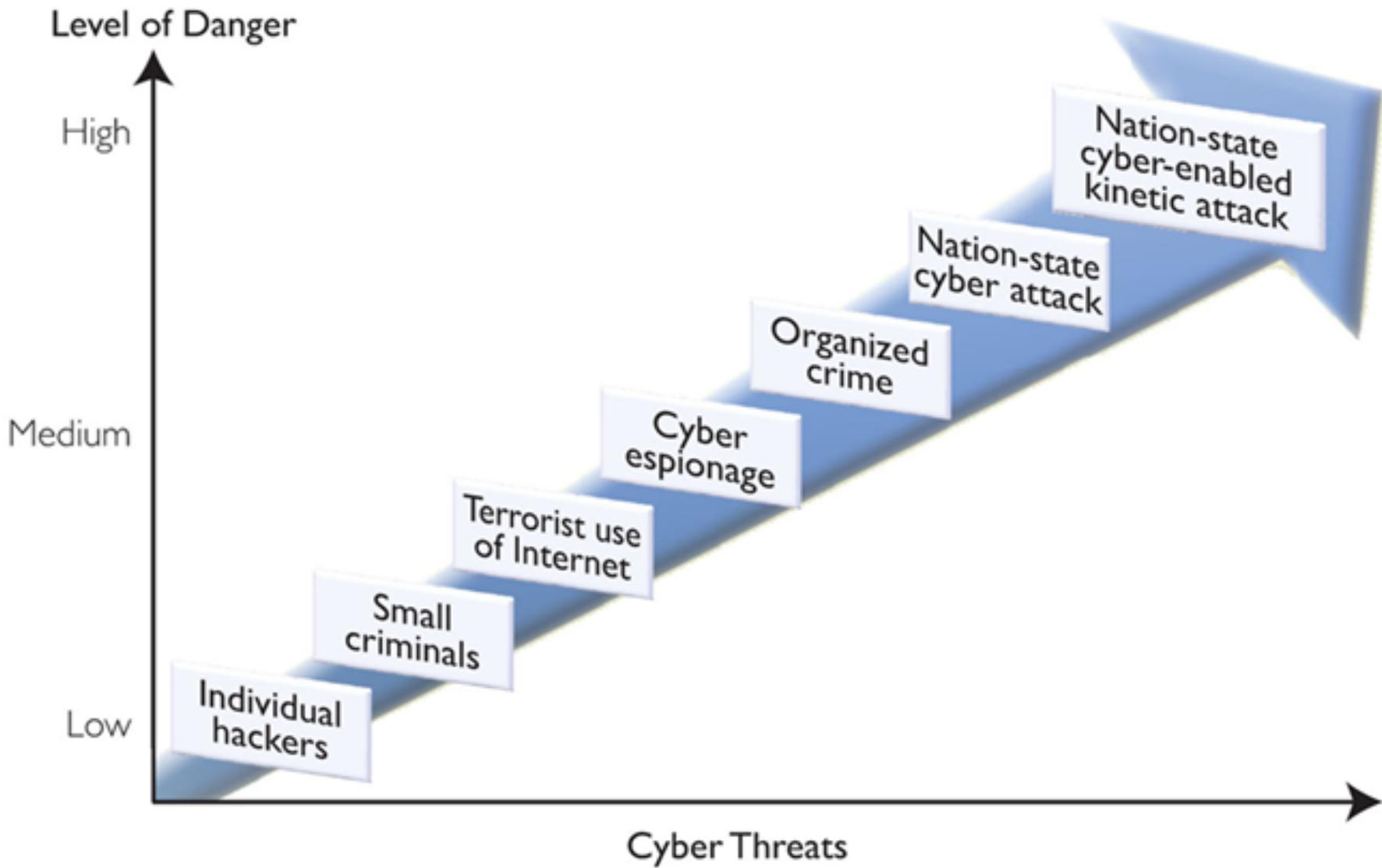


- Churches
- Libraries
- Bars / Nightclubs
- Theaters / Cinemas
- Sports Facilities
- Town Hall
- Post Office
- Public Works
- Chamber of Commerce
- Local Telecoms
- Real Estate Brokers
- Local Banks
- Law Offices
- Schools
- ...

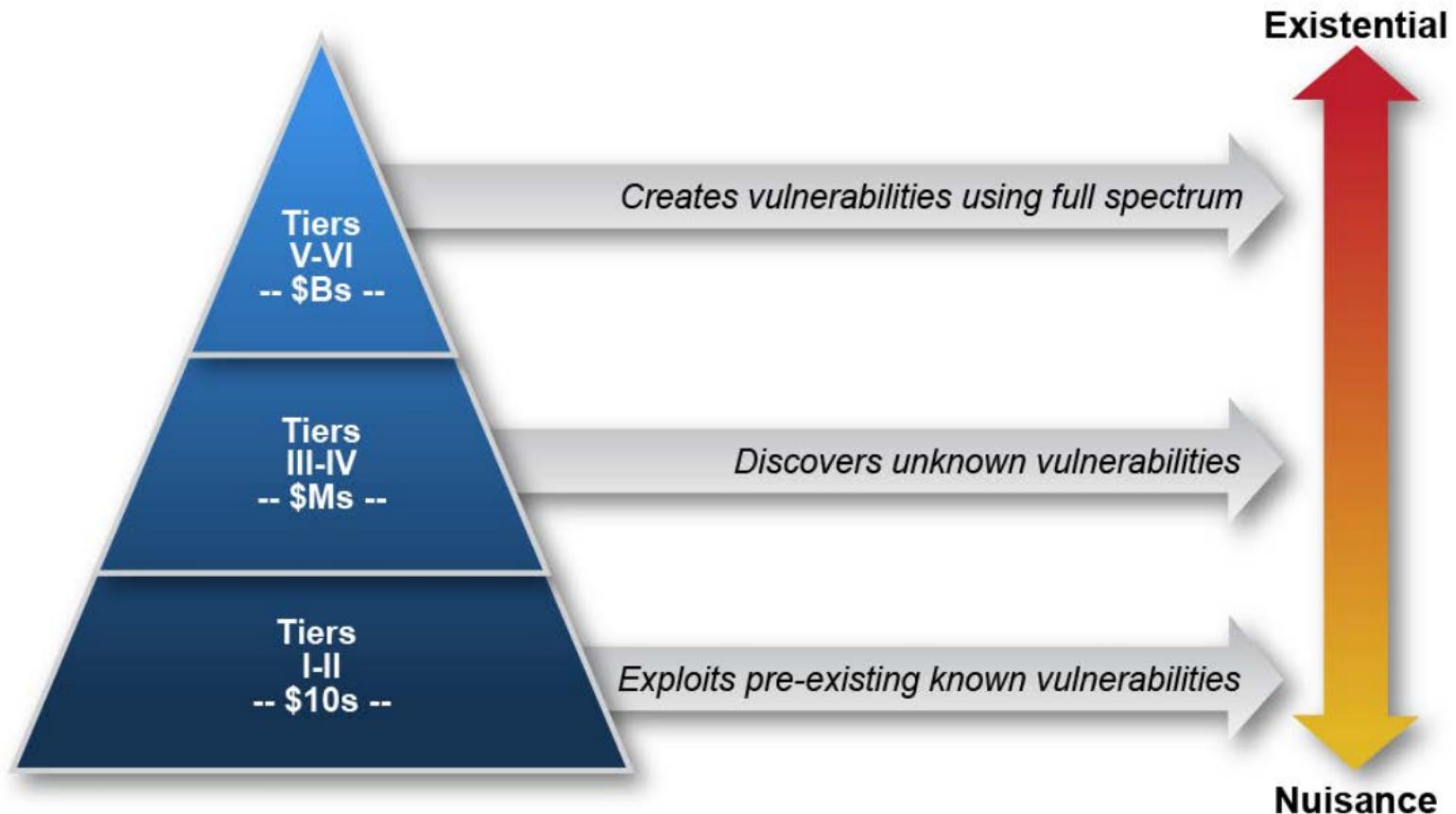


- Introduction
- Pen Testing
- Dissecting a City
- Cross Sectioning
- Pressure Points
- **Risk Analysis**
- Solutions

Cyber Threat Spectrum

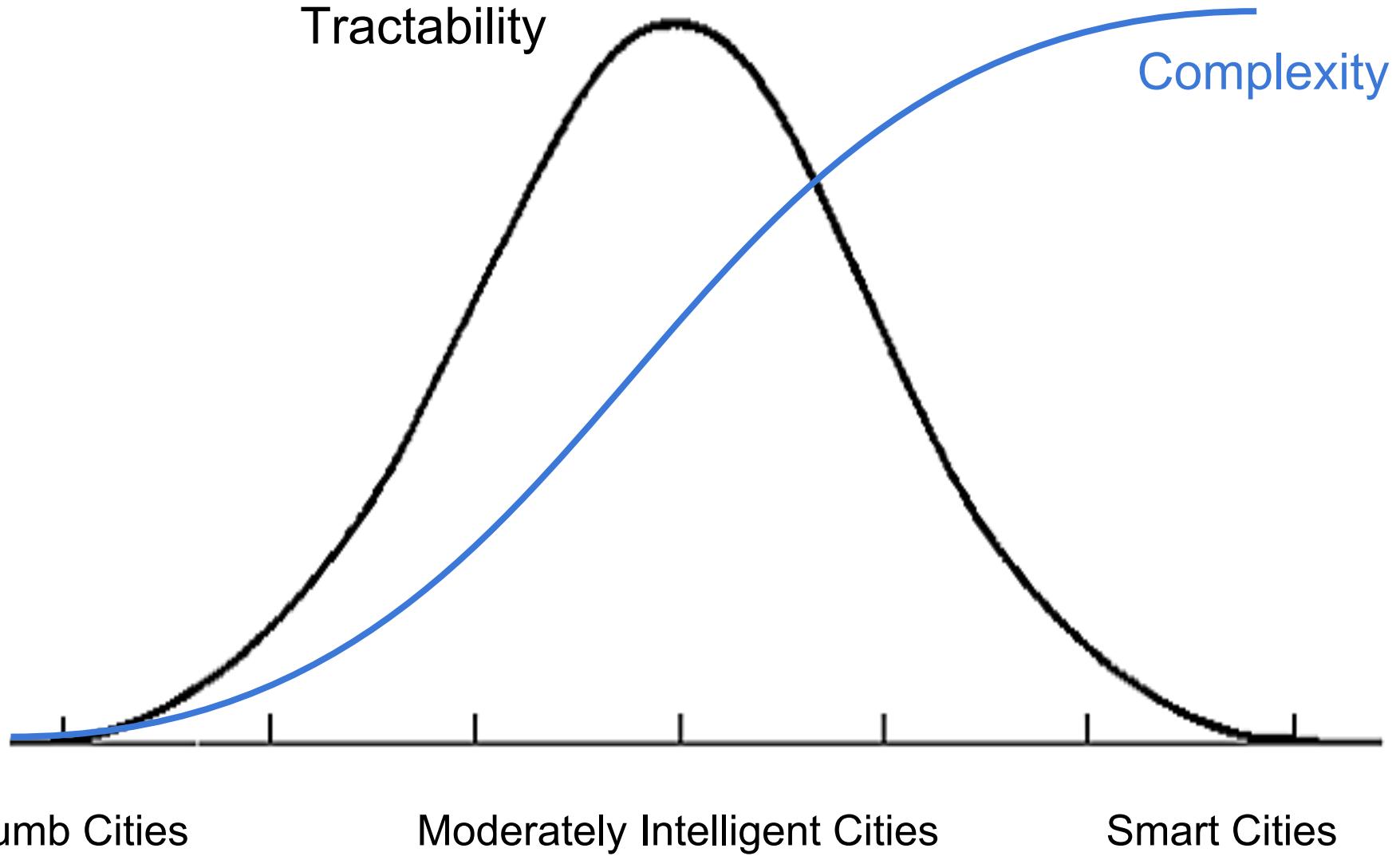


Threat Hierarchy



- 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 header of The New York Times Bits blog. At the top, there are navigation icons for menu, refresh, and search. The title 'The New York Times' is displayed, along with a 'LOG IN' button and a dropdown menu icon. Below the header, there are several news headlines: 'Windshield Devices Bring Distracted Driving Debate to Eye Level', 'Intel Takeover of Altera Is Expected', and 'BITS BLOG The World's Comi'. A large, dark rectangular area in the center contains the headline 'Security Researchers Start Effort to Protect 'Smart' Cities' and a call-to-action 'Activate Adobe Flash.'.

Bits

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

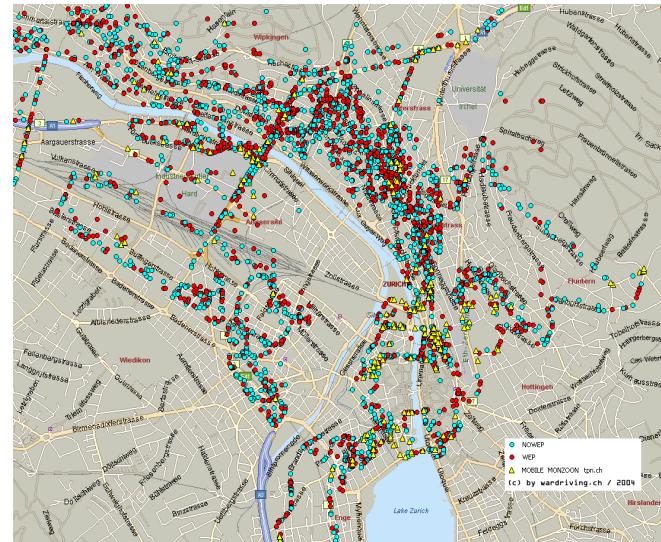
Solutions

- 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

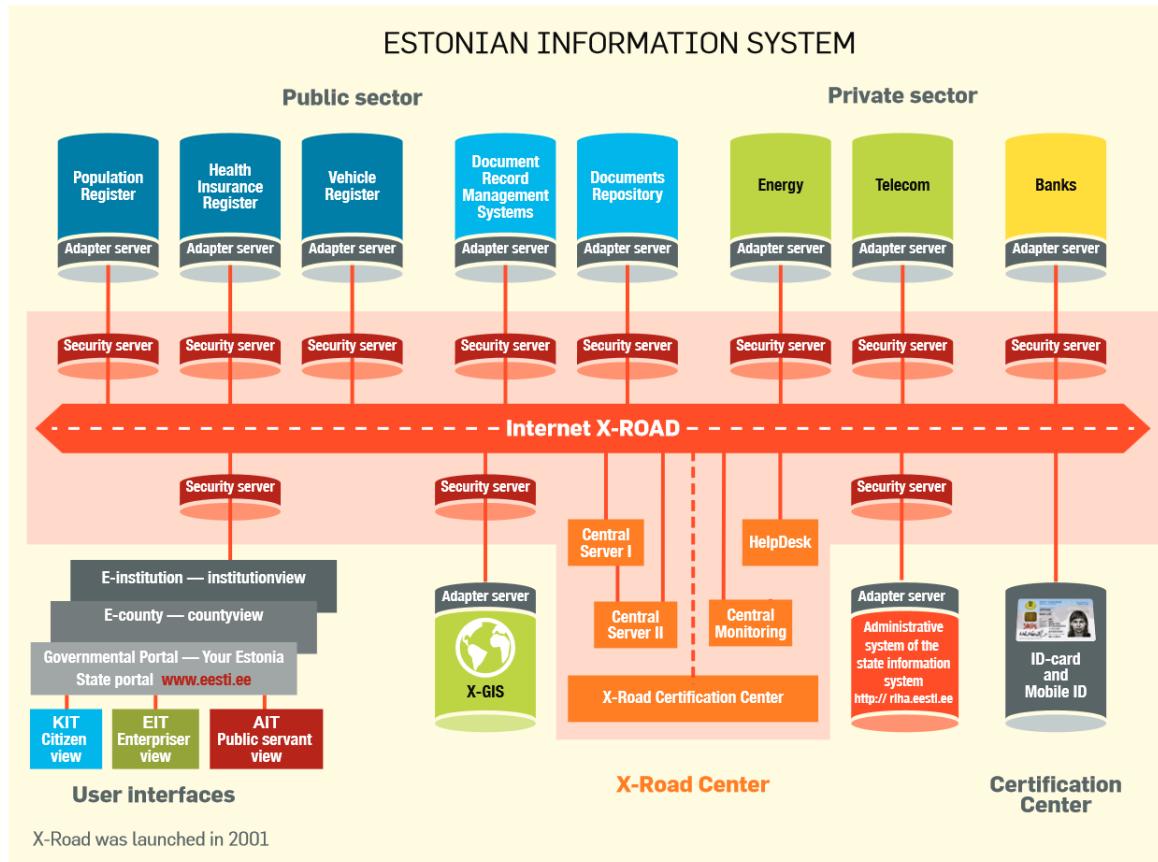
- Spectrum is getting cluttered with potentially vulnerable devices
- We need to know about more than just Wifi
- Auditing large physical spaces for low power transmitters can be a lot of work
- Solutions:
 - Put Wireless Data Collectors in Police Cars
 - Police cars drive everywhere
 - Potential privacy 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 5 - Optimised					
Level 4 - Managed					
Level 3 - Defined					
Level 2 - Repeatable					
Level 1 - Initial		Focus on solution	Focus on long-term solution success	Identify additional value opportunities	Managed 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 established 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



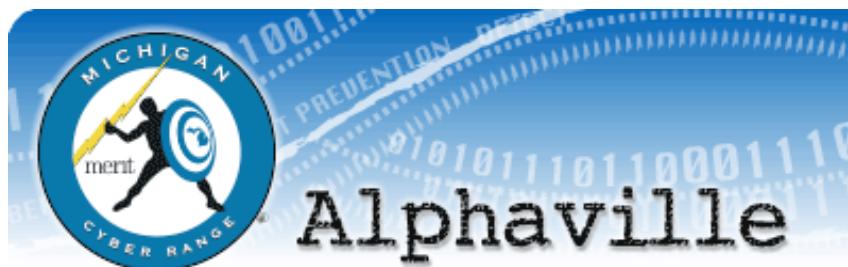
Estonia: A Model for e-Government, CACM June 2015

Simulation and Exercises



SANS CyberCity

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



Michigan Cyber Range: Alphaville

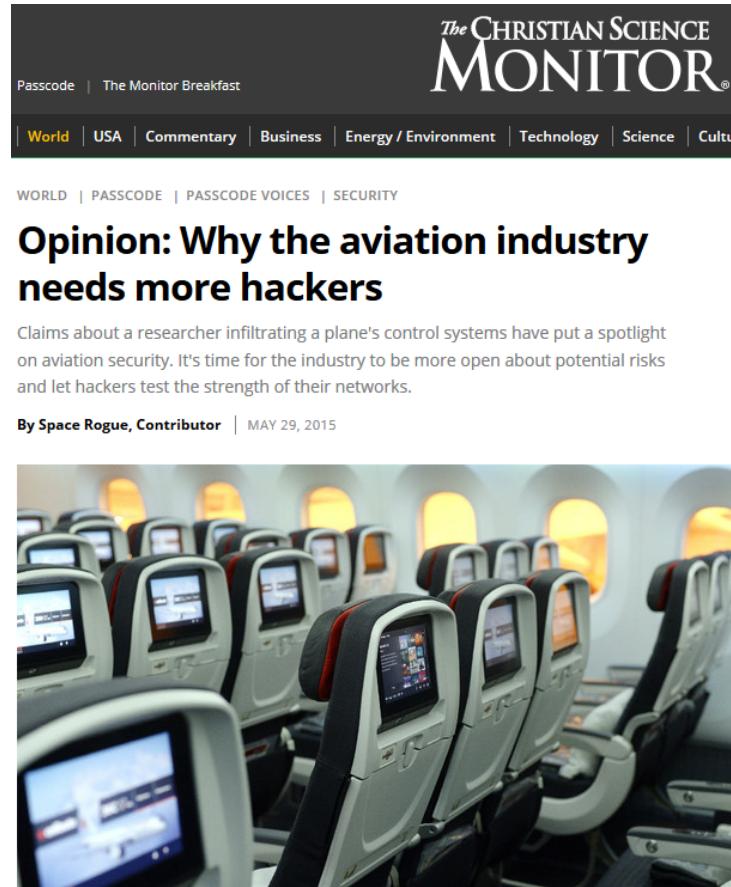
- <http://www.merit.edu/cyberrange/alphaville.php>



EA/Maxis - SIMCITY

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

Media Attention & Public Awareness



The screenshot shows the header of The Christian Science Monitor with navigation links for Passcode, The Monitor Breakfast, World, USA, Commentary, Business, Energy / Environment, Technology, Science, Culture, and a sidebar for WORLD, PASSCODE, PASSCODE VOICES, and SECURITY. Below the header is a large headline: "Opinion: Why the aviation industry needs more hackers". A subtext below the headline reads: "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." At the bottom left is a photograph of an airplane interior showing rows of seats with entertainment screens.

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

- Cities 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