

RSA CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Effects-based Targeting for Critical Infrastructure

SESSION ID: HT-T09

Sean McBride

Director of Analysis
Critical Intelligence
www.critical-intelligence.com

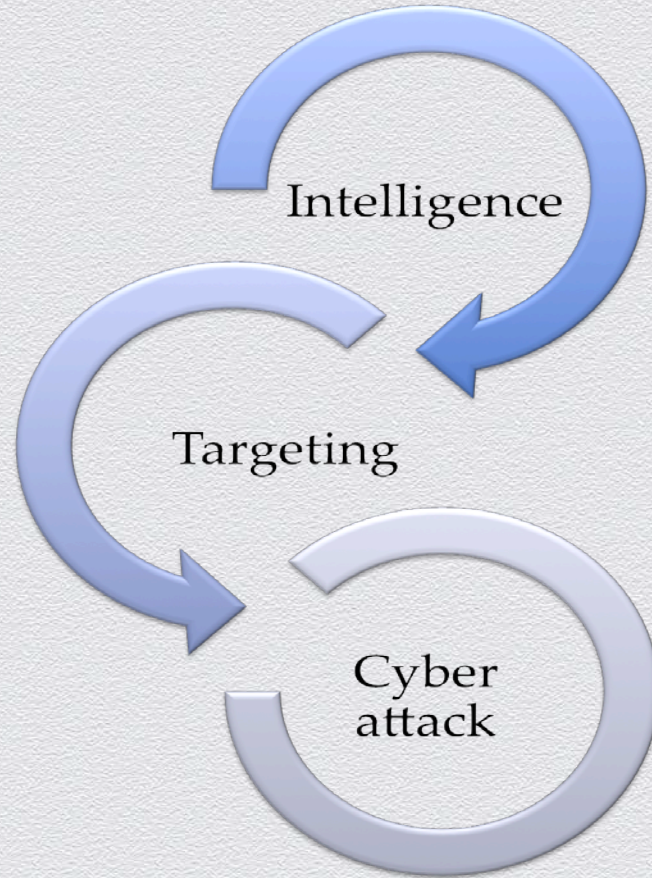


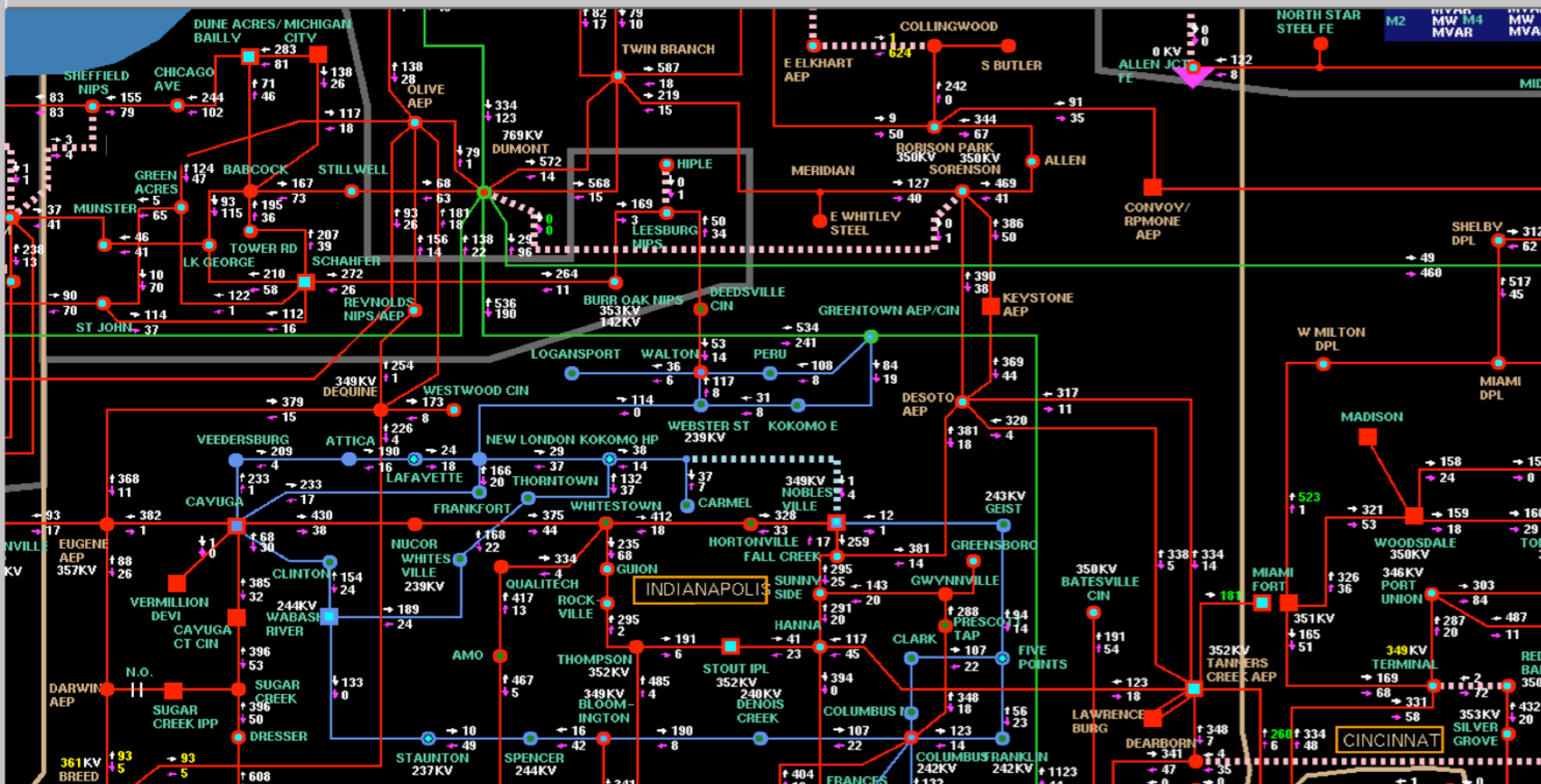


RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**How would you
infiltrate/attack/affect
a wide swath of
critical infrastructure
facilities in the United
States?**



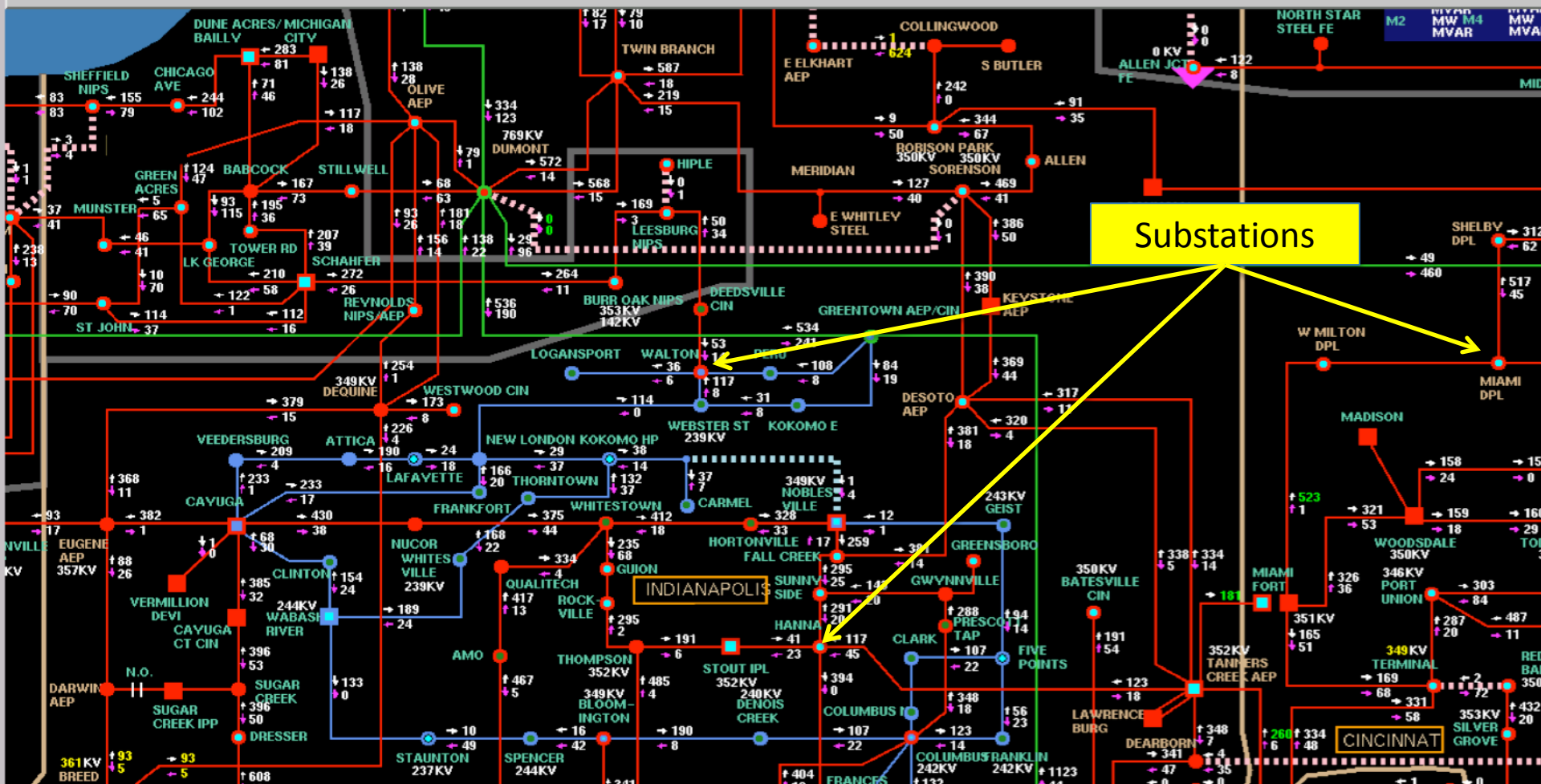


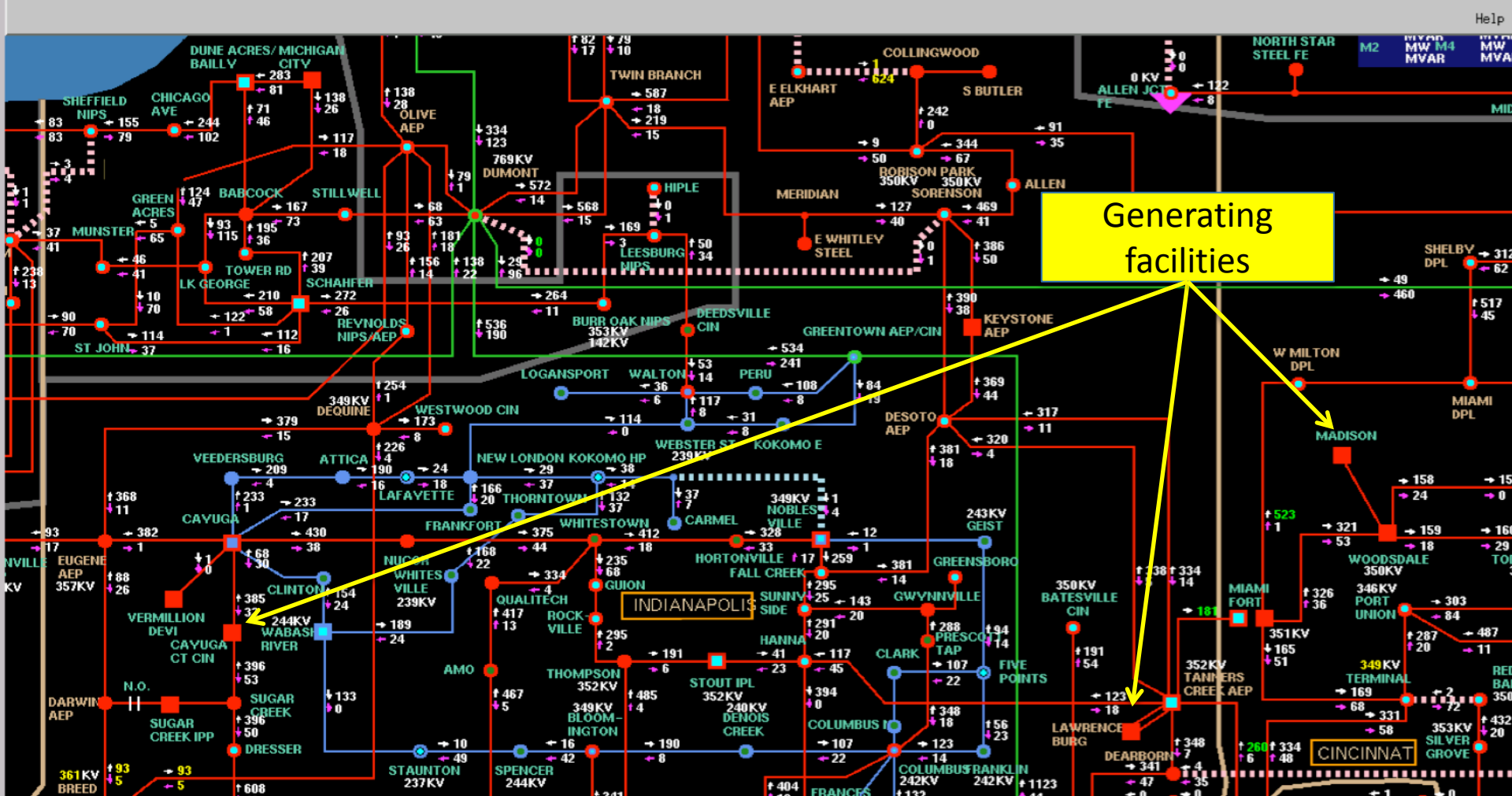
Targeting

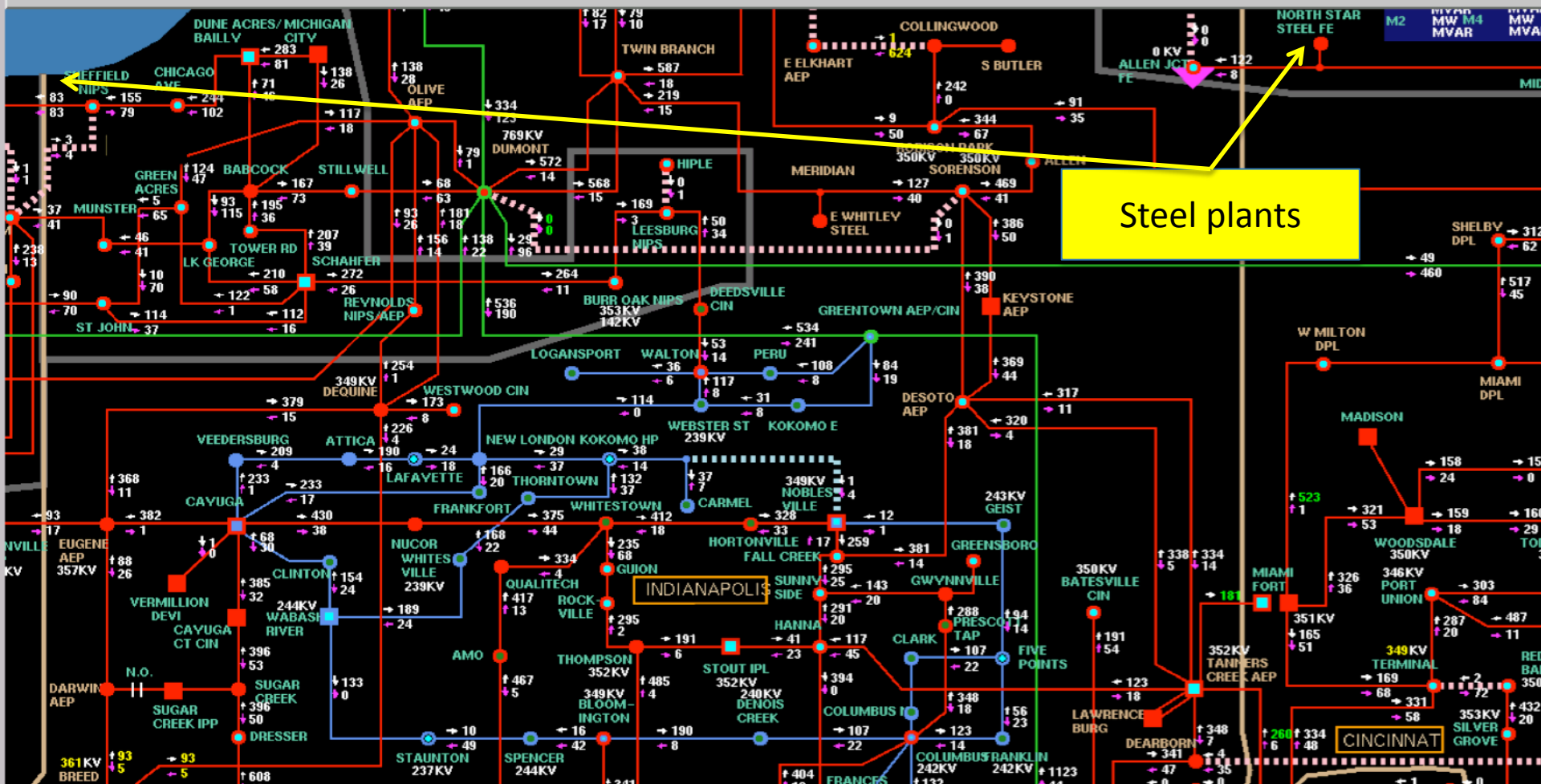
*Targeting is the process for selecting and prioritizing targets and matching appropriate actions to those targets to create **specific desired effects** that achieve objectives, taking account of operational requirements and capabilities.*

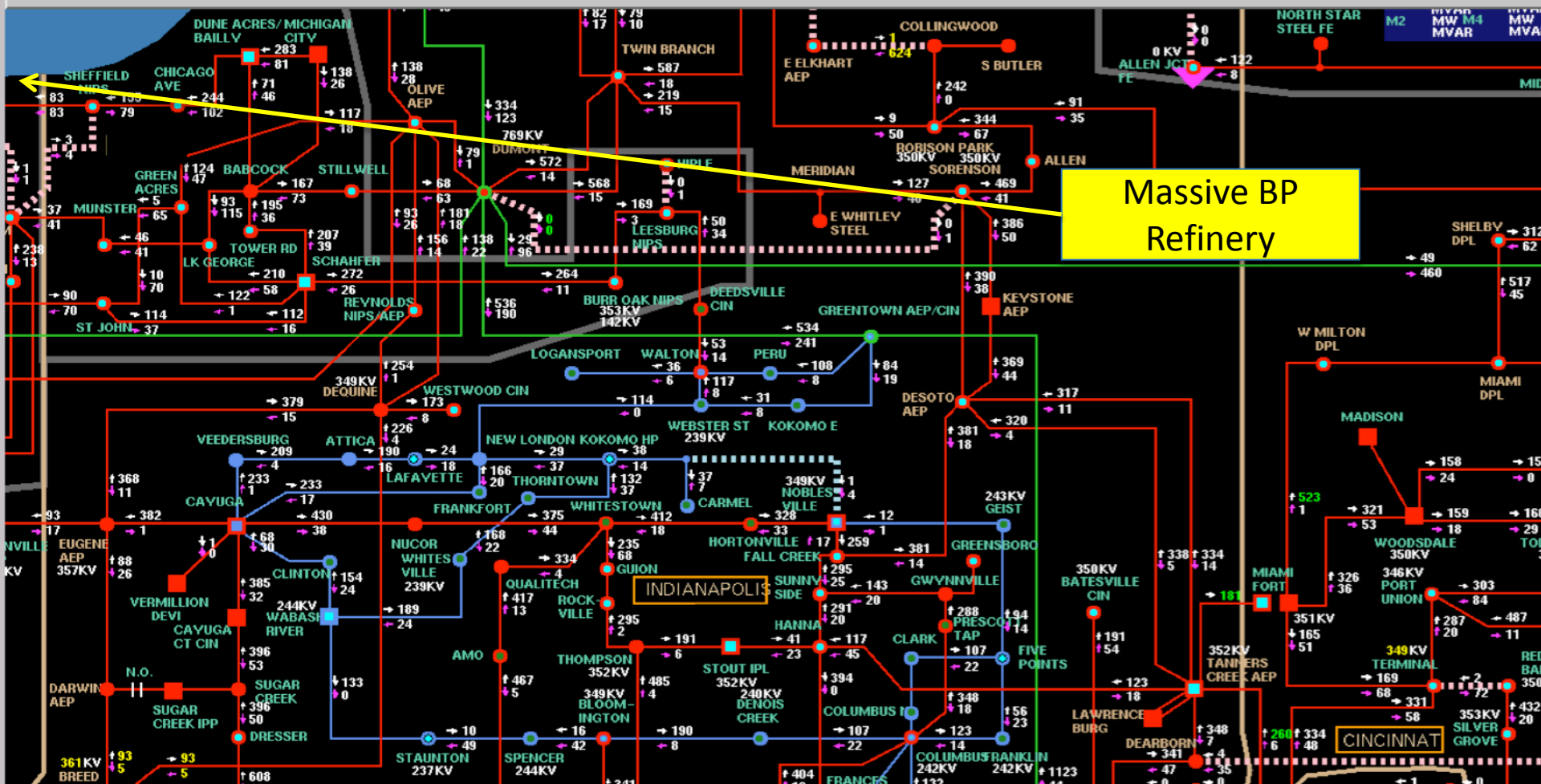
- Targeting: Air Force Doctrine Document

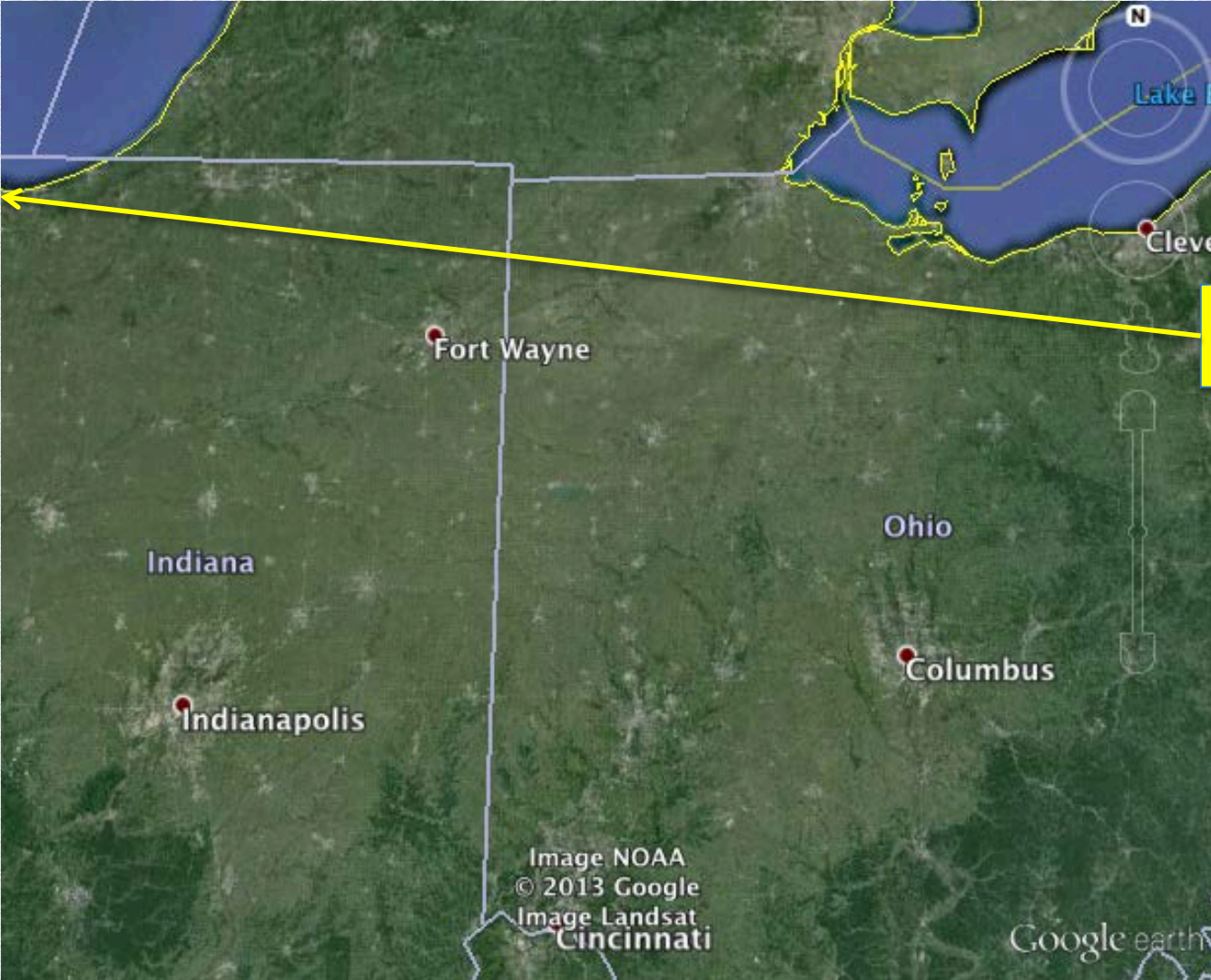








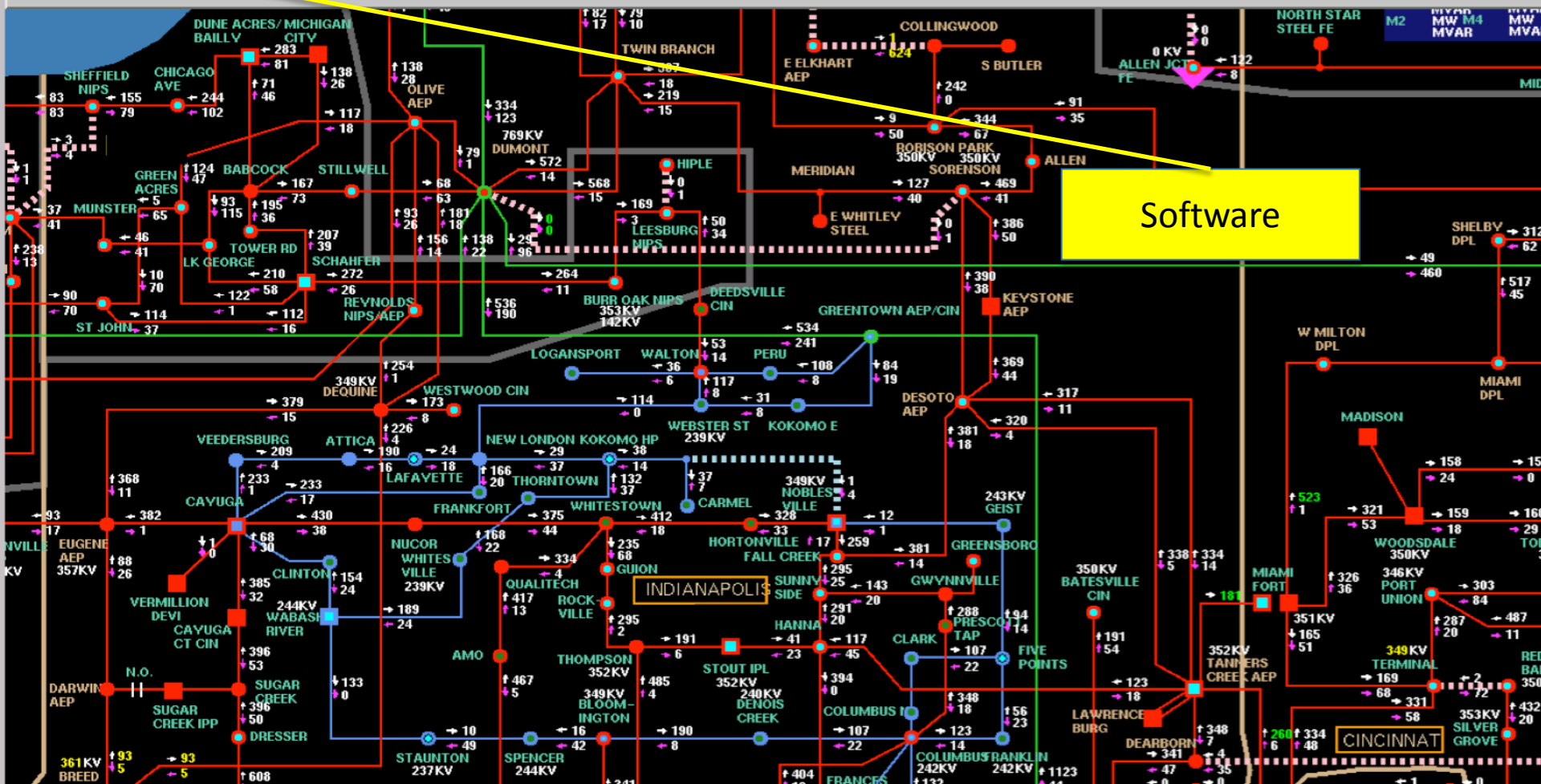


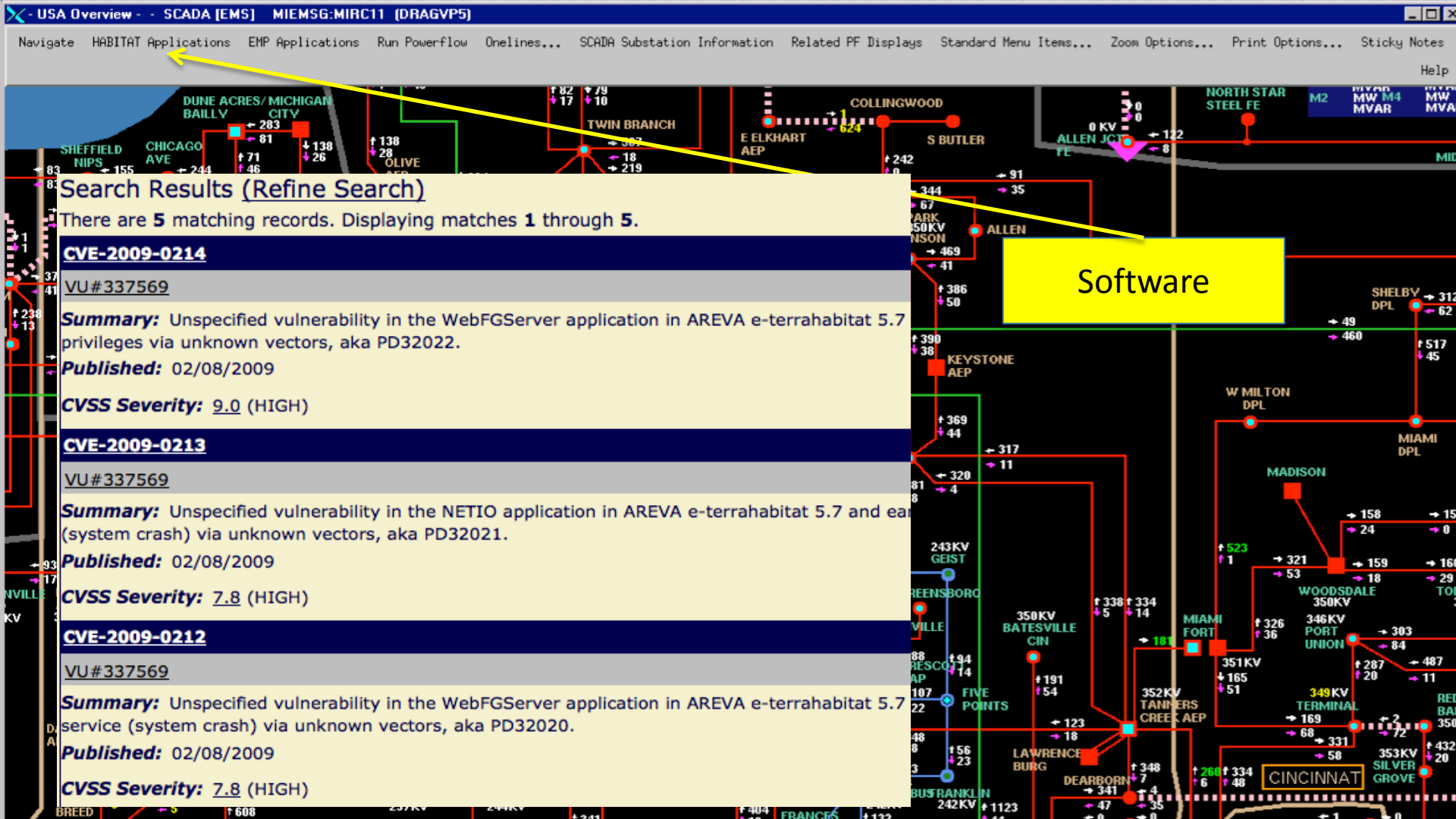


Massive BP
Refinery

Image NOAA
© 2013 Google
Image Landsat
Cincinnati

Google earth





Search Results (Refine Search)

There are 5 matching records. Displaying matches 1 through 5.

CVE-2009-0214
VU#337569
Summary: Unspecified vulnerability in the WebFGServer application in AREVA e-terrahabitat 5.7 privileges via unknown vectors, aka PD32022.
Published: 02/08/2009
CVSS Severity: 9.0 (HIGH)

CVE-2009-0213
VU#337569
Summary: Unspecified vulnerability in the NETIO application in AREVA e-terrahabitat 5.7 and ea (system crash) via unknown vectors, aka PD32021.
Published: 02/08/2009
CVSS Severity: 7.8 (HIGH)

CVE-2009-0212
VU#337569
Summary: Unspecified vulnerability in the WebFGServer application in AREVA e-terrahabitat 5.7 service (system crash) via unknown vectors, aka PD32020.
Published: 02/08/2009
CVSS Severity: 7.8 (HIGH)

Software

Carmel



#RSAC

RSACONFERENCE2014

Carmel

Manager, Network & Telecommunications at MISO
Indianapolis, Indiana Area | Utilities

Previous MISO, Core BTS, Inc., Broadwing Technology Solution
Education Purdue University

Connect

Send InMail



What if I had:

- Photo
- Work location
- Email address
- Job description
- Professional history

Targeting

Targets are areas, complexes, installations, forces, equipment, capabilities, functions, individuals, groups, systems, or behaviors identified for possible action to support the commander's objectives, guidance, and intent.

- Targeting: Air Force Doctrine Document



Target Development

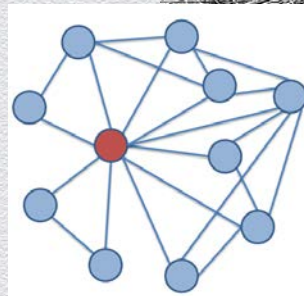
Target development is the systematic evaluation and analysis of target systems, system components, and component elements to determine high value targets (HVTs) for potential lethal or non-lethal attack.

- U.S. Army Open Source Intelligence Manual



High Value Targets

- ◆ HVT – points that maximize payoff for attacker
- ◆ Defenders often at disadvantage due to differing perceptions of risk:
 - ◆ Subsidiary: Utility of an energy holding company
 - ◆ Enterprise: Entire organization
 - ◆ Nation: Entire country
 - ◆ Community/location: national capital area
 - ◆ Up and down-stream dependencies

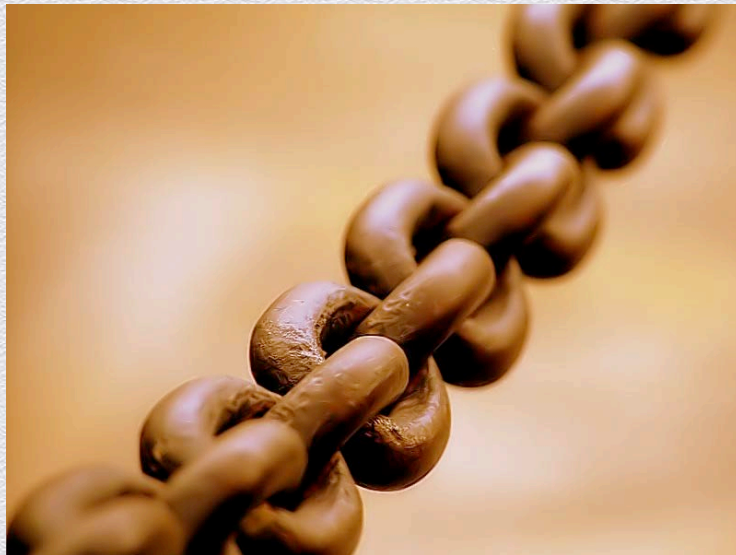


HVT victim vs vector

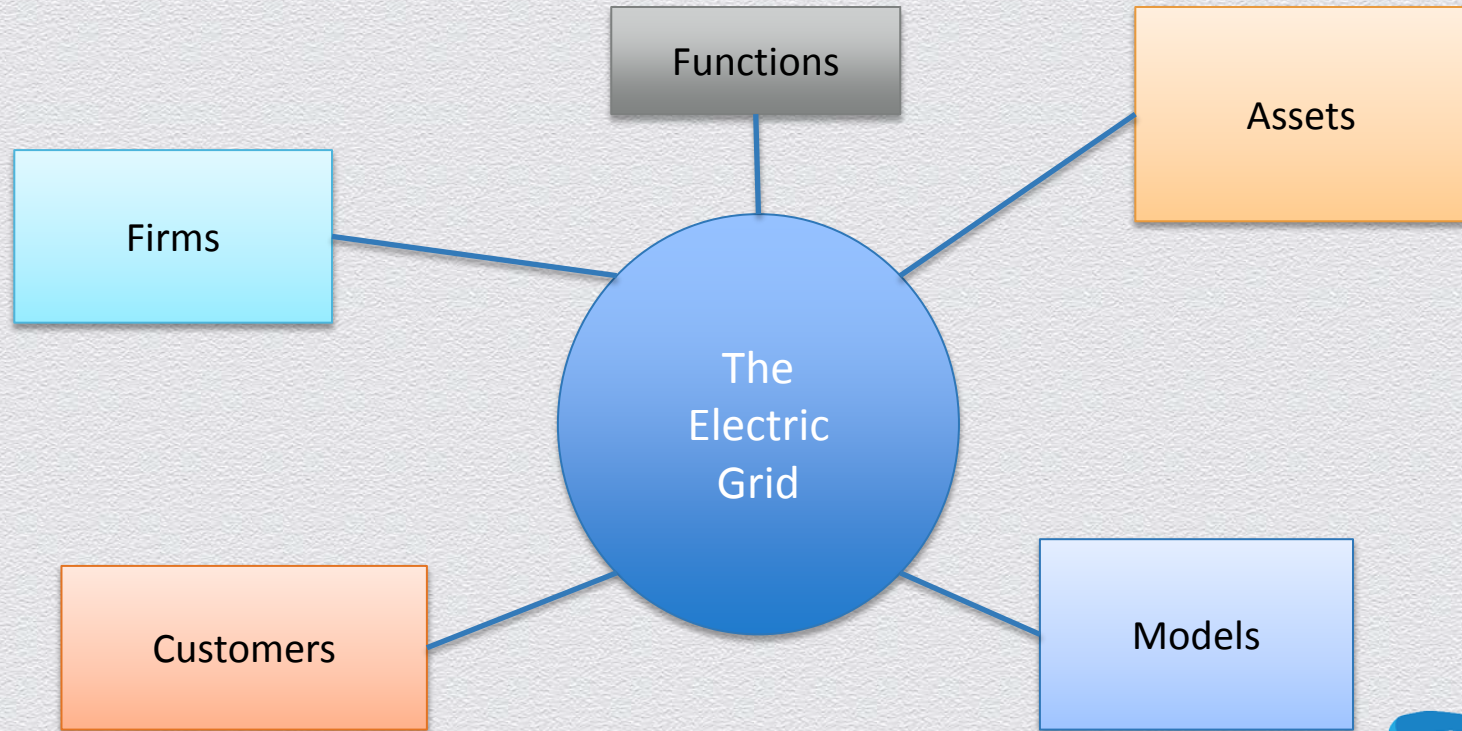
- ◆ Utility as victim
 - ◆ Desired effect: make money
 - ◆ Means: power outage to extort utility
- ◆ Utility as vector
 - ◆ Desired effect: greater economic influence
 - ◆ Means: power outage affecting major competitive export sector (steel, automotive, oil, etc.)

Target Chaining

- ◆ Each piece of information may be used to achieve an objective in another campaign
- ◆ What do you *need* to exploit in order to exploit what you ultimately *want* to exploit?
- ◆ Example: RSA SecureID compromise rumored to be used against LMCo, Northup, L3



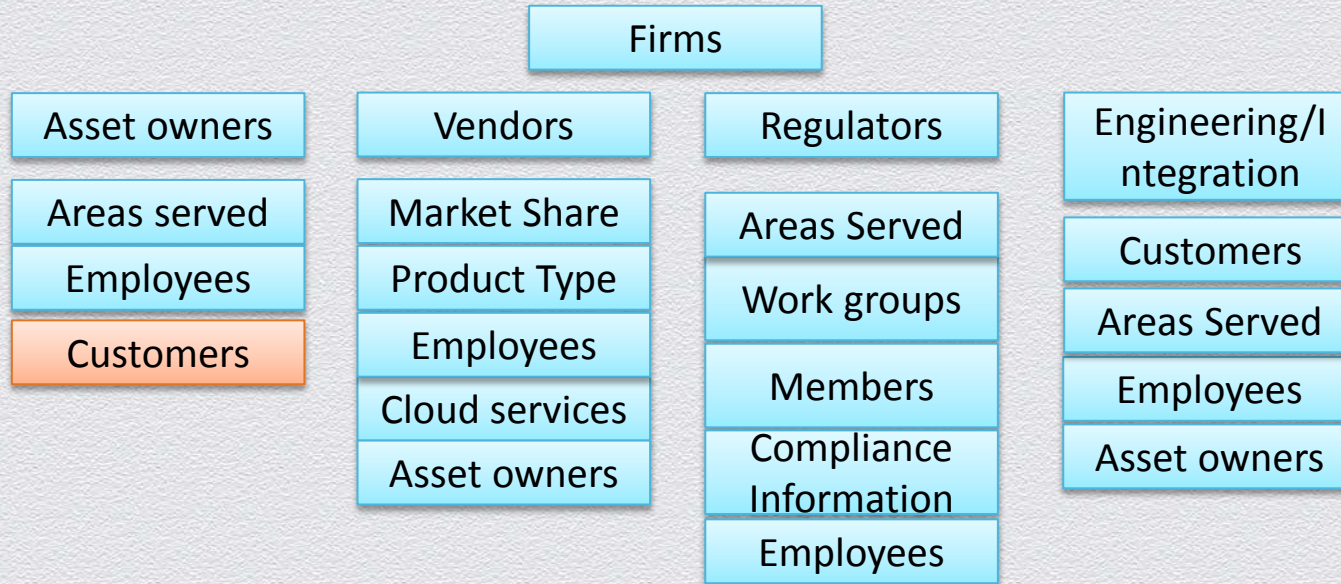
System of Systems Analysis



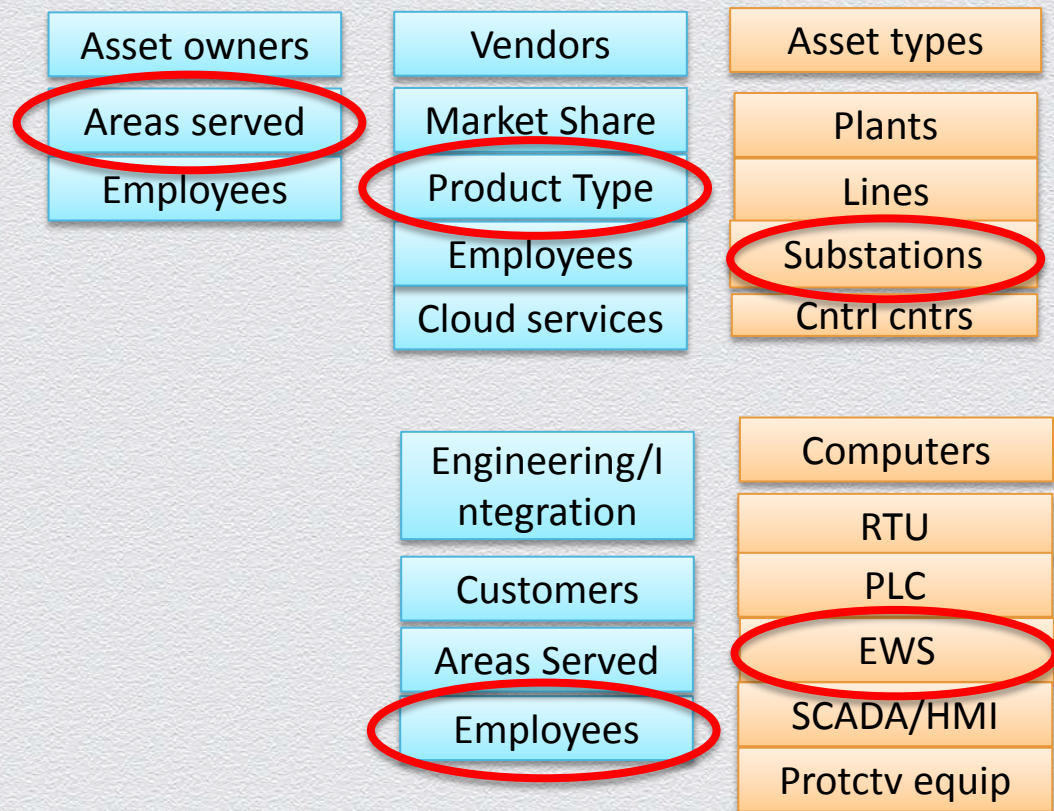
SOSA – Simplification of Electric Grid



SOSA – Simplification of Electric Grid

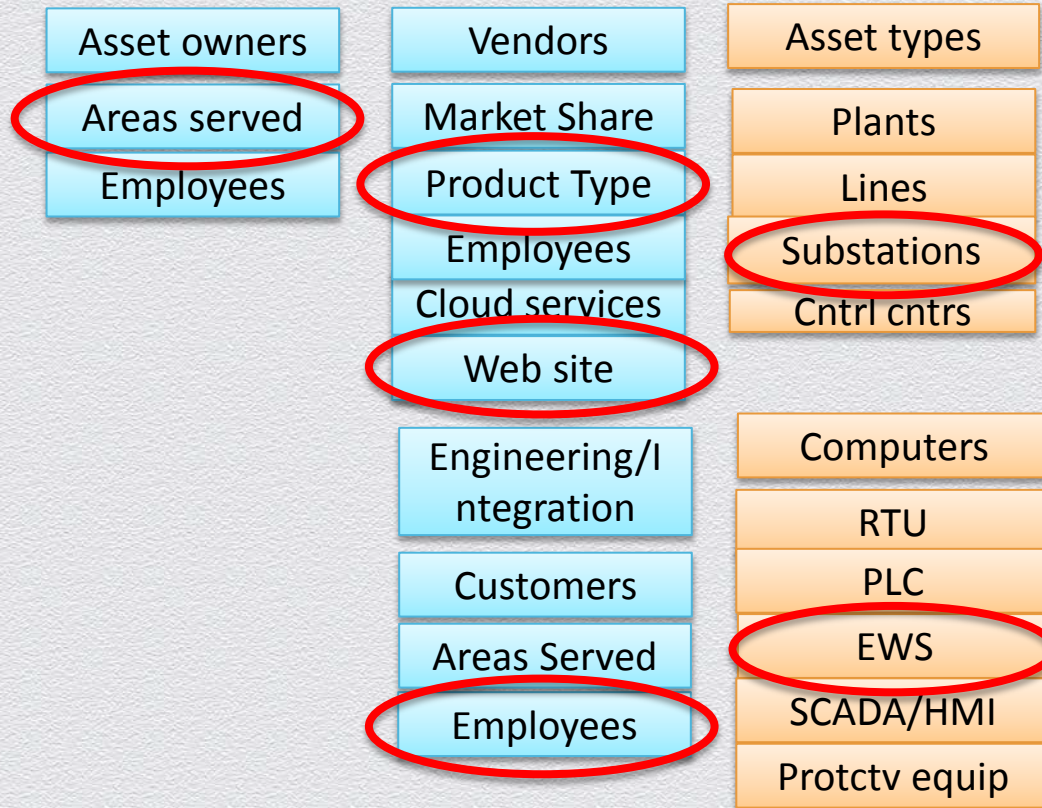


SOSA leads to HVT identification



What
Integration
firm employee
has access to
the EWS used
to configure
the protective
equipment for
the target
area served?

SOSA leads to HVT identification



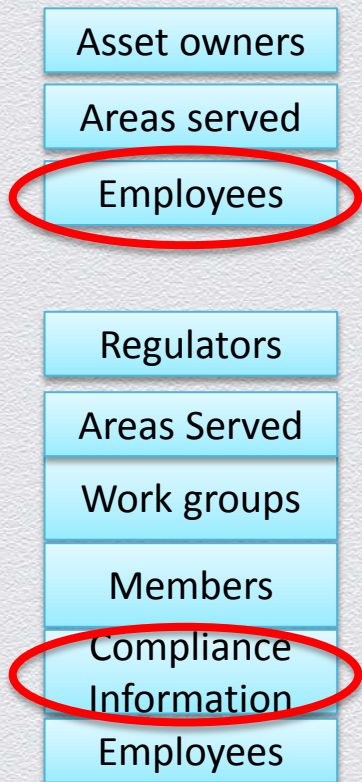
What Web site is he likely to visit?
(maybe to get the latest firmware from the vendor?)

SOSA leads to HVT identification

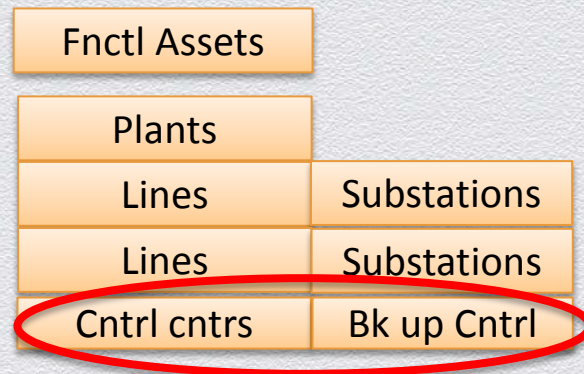


What vendors have
cloud services for
market operations?

SOSA leads to HVT identification



What regulator maintains information about asset owner control centers, and employees who work there?



Internet-Derived Targeting

- ◆ Using the Internet as a targeting platform
 - ◆ Base target lists off what information is readily available
 - ◆ Benefits: low cost, low risk approach, favorable for cyber operations
 - ◆ Drawbacks: information may be dated or misleading, not as favorable for kinetic operations
- ◆ Not necessarily exclusive of other intelligence/targeting methods
 - ◆ Example: IDT can inform HUMINT targeting; multiple intelligence collection methods can be used as “sanity checks”



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**How would you infiltrate
an Iranian nuclear
enrichment facility?**

Army War College: *Checking Iran's Nuclear Ambitions* – Jan. 2004

Covert action would probably be the most politically expedient way for the United States to disrupt Iran's nuclear program. It might include one or more of the following:

- ◆ *harassment or murder of key Iranian scientists*
- ◆ *disruption or interdiction of key technology or material transfers... on land, in the air, or at sea*
- ◆ *introduction of destructive viruses into Iranian computer systems controlling the production of components or the operation of facilities*

"The challenges of U.S. Preventative Military Action" Michael Einstadt



 #RSAC

RSACONFERENCE2014

NYT Article – Jan. 2009

The covert American program, started in early 2008, includes renewed American efforts to penetrate Iran's nuclear supply chain abroad, along with new efforts, some of them experimental, to undermine electrical systems, computer systems and other networks on which Iran relies. It is aimed at delaying the day that Iran can produce the weapons-grade fuel and designs it needs to produce a workable nuclear weapon.

The New York Times

Aviation Week Article – Feb. 2010



*The vanguard of Israel's cyber-warfare efforts is focused on blocking Iran's nuclear ambitions. A U.S. expert said recently that malware could be inserted, disrupting the controls of sensitive sites like uranium enrichment plants. ... Israeli intelligence has tried to insert malware that can damage information systems within Iran's nuclear program. The systems are not connected to the Internet, **but to equipment sold to the Iranian government***

Q1 2011: Stuxnet “Consensus”



NYT article:

Tested at Oak Ridge and Dimona

INL: Siemens portion?

USB vector

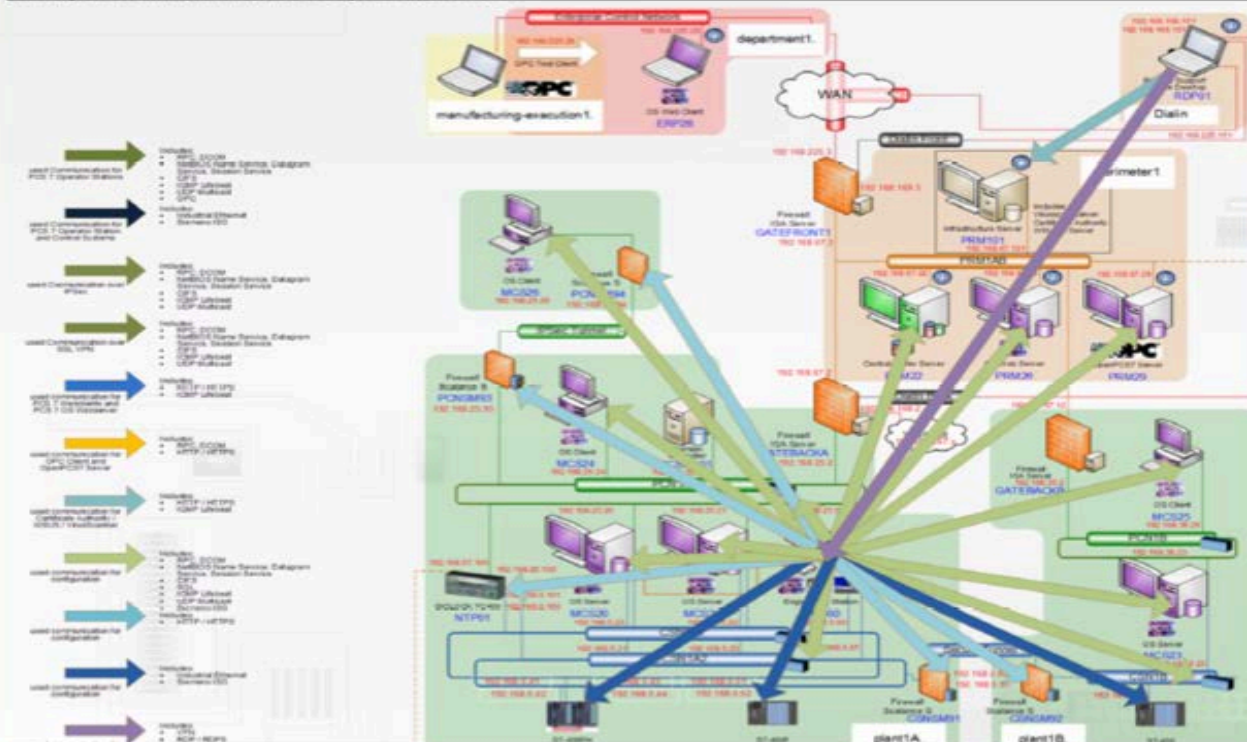
TOE 2: Unauthorized Access to the Engineering Station – Goal is for attacker to gain interactive login to PCS 7 ES

SIEMENS

Mittwoch, 14. Mai 2008

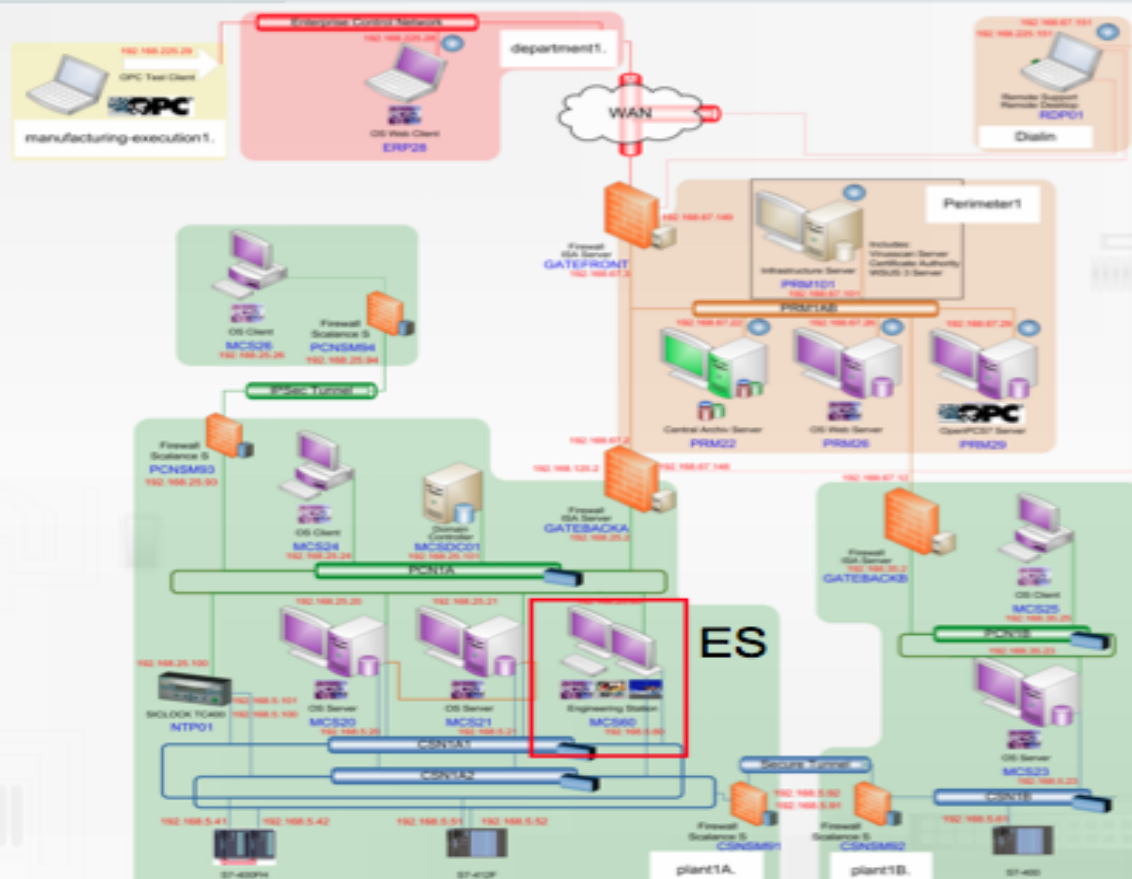
scen engineering and remote support

Security Assessment of SIMATIC PCS 7 by Idaho National Labs



The ES is used for development, maintenance and troubleshooting of the Basic Process Control System (BPCS) and for the Process Safety System (SIS).

TOE 6: Unauthorized Configuration Database Access – Goal is to modify configuration from the PCS 7 ES



Objectives

- Infiltrate PCS 7 ES and modify configuration
- Access / modify control system configuration without being detected
- Compromise controller configurations in BPCS (AS6) and SIS (AS4 – AS5)

Hacker modifying a controller configuration would be a significant security breach

Was it really (just) via USB?



Leveraging existing capabilities: Customs – Nov. 2008

92. [REDACTED] We want to share with German officials information indicating that in November 2008, a representative of the Iranian firm Texofin expressed interest in acquiring a computer numerical control (CNC) system manufactured by the German firm Siemens. The Texofin representative sought the system, a SINUMERIK 810 or 802, for use with a six-axis filament winding machine. Such a filament winding machine could be used in a missile program to produce rocket motor cases and pressure vessels, or in nuclear fuel enrichment applications for manufacturing components of centrifuge assemblies. Filament winding machines having three or more axes are controlled by the Missile Technology Control Regime (MTCR), Nuclear Suppliers Group (NSG), and Wassenaar Arrangement. The control systems used with them - including the Siemens SINUMERIK 810 and 802 - are controlled by the NSG.



Leveraging existing capabilities: Customs – Apr. 2009

92. [REDACTED] SUMMARY: Germany delivered two non-papers on April 1 to United Arab Emirates (UAE) MFA Deputy Director General Al-Absi, and UAE MFA Director General (for European Issues) Kazim, expressing Germany,s request for the UAE to interdict the IRISL vessel M/V Sabalan. The papers also asked the UAE to inspect its cargo for Siemens computers and accessories - possibly intended for use with Iranian centrifuge cascades. Germany informed us that the M/V Sabalan has been identified and secured and that they expect that the crate contents will be inspected on Sunday, April 4, likely in Jabel Ali. Germany did not indicate if a German official would be present, supervising the inspection. Germany gave no further details about the inspection other than to say "this is a positive development" and "we'll wait and see what we find out." END SUMMARY



Siemens support forum – Jul. 2009

SIEMENS

Behrooz

☐ Member



Joined 12/1/2007

Last visit: 9/4/2010

Posts: 19

Rating:

☆☆☆☆☆☆ (0)

Unfortunately, I have the Similar Error (Please find the attachment),

And with your Solution I could not get any result.

When I create a new project this error prevent me from downloading the CFCs.

I think, it causes from any viruses, because when I used My Flash to transfer my program to another PC, That PC Showed that Similar Error while before that it works normally.

All of my PC in my Company encounter with this Error, We used Symantec and Nod 32 Antiviruses, But I have not get any result.

Please let me be informed, if you know anything about it. 🤖🙄

Attachment: @CFC_ERR.JPG (47 Downloads)

M.R.Tajalli

#RSAC

RSACONFERENCE2014

Blog and Resume



PersianControl



About Me



Mohammad Reza(Behrooz)
Tajalli

[View my complete profile](#)

3. Experiences:

- Industrial automation engineering for Gas & Oil and other projects with SIEMENS automation systems in **NEDA** Company (www.nedaco.com). Tehran , Iran.(Sept.2006 till now):
 - i. Chiller Project: Commissioning.(Kashan, Iran)
 - ii. HVAC Project: PLC Programming & Commissioning.(Kashan , Iran)
 - iii. Sulfiran Project: Commissioning.(Fajre Jam Refinery, Asalooeyeh , Iran)
 - iv. Momtazan Cement Project: Commissioning.(Kerman, Iran)
 - v. Gas Pump Station (IGAT 4) Project: DCS Programming & Commissioning. (Khonj, Iran).



Oil & Gas



Power Plant



Mineral Ind.



Commercial

NEDA Industrial Group

Introduction

About us

Contact us

Technologies

Our projects

Workshop

Our projects

List of projects completed by **NEDA** Industrial Group in the recent past

Date of Contract		
Feb. 2011	Project	Renovation of Gas Turbines Control System, Kangan Gas Fields
	Client	Fars Regional Electric Co.
	EndUser	Fars Regional Electric Co.
Feb. 2011	Project	Renovation of Gas Turbines Control Systems
	Client	Karoun Oil & Gas Co.
	EndUser	National Iranian South Oil Company
Feb. 2011	Project	Boiler Burner Management Systems
	Client	Borna Tadbir Behta Co.
	EndUser	South Pars Oil Fields- phases 17 & 18

NEDA & Siemens



NEDA Industrial Group

About us

NEDA's 26 years of presence in Industrial Automation in Iran

Neda Industrial group was established in 1984. In 1985, Neda developed "NEDACOM" the first Iranian made PLC. This product was used in more than 40 monitoring projects in cement industries throughout the country. So many years later, today considerable number of those PLCs are still in service for scanning systems of furnaces in scores of cement plants in Iran.

In 1996 using S5 series of Siemens PLCs, **Neda** succeeded in design and commissioning of the control & monitoring system for Isfahan Steel complex. A plant with manufacturing capacity of over 600,000 tons of steel per annum. That was the first time that this type of project was attempted by an Iranian company. Before then, this type of control systems were wholly imported from abroad. The proto-type for that system was initially designed by **Neda**, using Nedacom PLCs.

In 1999 Neda acting as Siemens local partner in Iran, embarked on designing the control system for 14 modules of combined cycle power plants in 6 different power stations. The control system was designed using Siemens DCS system known as Teleperm XP. By year 2000 the first unit was commissioned in **Montazer Qaem** power plant.

Transfer of technical know-how on this scale, not only was unprecedented in Iran, but it was also a first for Siemens to be carried out outside Germany and under its supervision.

Few years later, Neda as part of Siemens's plan for local manufacture of DCS, completed two projects for **MAPNA**, consisting of design, manufacture and supervision for installation and commissioning of the control systems for 23 combined cycle units for 4 power plants around the country.

 #RSAC RSACONFERENCE2014

Workshop

Workshop

The new factory of **NEDA Industrial Group** was founded in 2005 in Hashtgerd city in 70 Km near Tehran. All of Control, F&G, Protection and electrical Panels are manufactured and tested in this factory.

Experience

Neda commitment to remaining at the forefront of innovative panel design and a dedication to customer satisfaction has developed our involvement with all major industry sectors including:

- Oil and Gas
- Petrochemicals
- Power Generation and Distribution
- Mining and Metals

Certificates

- From Siemens Company for manufacturing of control and Distribution panels of TXP system.
- From Autronica Company for manufacturing of F&G panels.
- From Siemens company for manufacturing of control panels with S7 plc families including DCS & ESD.

Neda article in Control Magazine – Jul. 2012

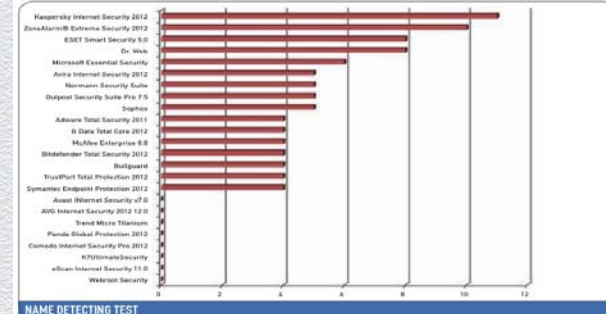
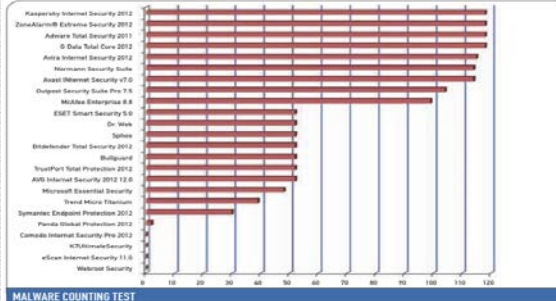
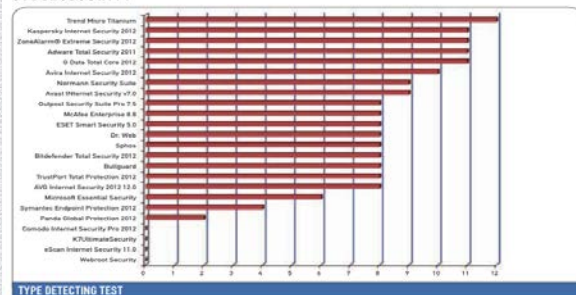
CYBERSECURITY

What's the Best Defense against Stuxnet?

A comparison of which tools are the best for finding Stuxnet in a system.

by Morteza Rezaei

CYBERSECURITY



Morteza Rezaei is an automation expert at **NECA** Industrial Group, a manufacturer of PLCs and a Siemens local partner in Tehran, Iran. He is experienced in Siemens PLC programming and cybersecurity in industrial plants. He can be reached at morteza.rezaei@gmail.com.

#RSAC

RSACONFERENCE2014

NEDA added to Department Of Commerce Entity list – Sep. 2008



Neda Industrial Group, No. 10 and 12, 64 th St. Jamalodin Asadabadi Avenue, Tehran, Iran.	For all items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.	73 FR 54507, 9/22/08.
Nedayeh Micron Electronics, No. 34 Mansour St., Tehran, Iran.	For all items subject to the EAR. (See §744.11 of the EAR).	Presumption of denial.	73 FR 54507, 9/22/08.

Indictments link NEDA to Iran's Military Procurement

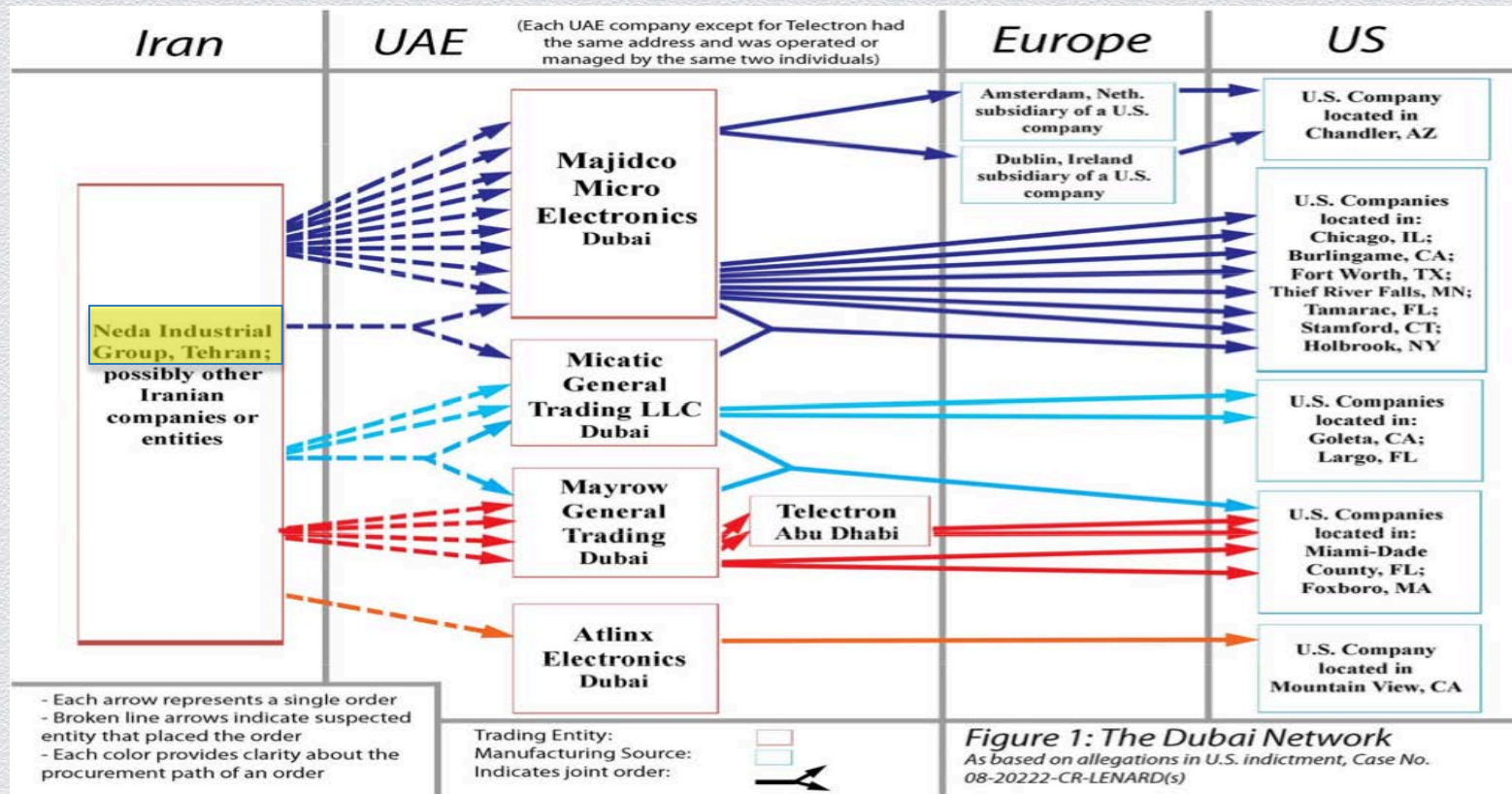


Figure 1: The Dubai Network

As based on allegations in U.S. indictment, Case No. 08-20222-CR-LENARD(s)

TABLE 1: DUBAI NETWORK – TIMELINE OF ALLEGED PROCUREMENTS

Date of order placement or purchase (on or about)	Trading company	Intermediary company or entity	Intermediary company or entity	United States supplier location	Item(s) procured	Iranian recipient	Date received (on or about)
January 14, 2004	Majidco Micro Electronics (Dubai)	Amsterdam, Netherlands office of Chandler, AZ company	-	Chandler, AZ	7500 Microchip brand microcontrollers	Neda Industrial Group (Tehran)	May 31, 2004
January 21, 2004	Atlinx Electronics (Dubai)	-	-	Mountain View, CA	120 field-programmable gate arrays	Unknown Iranian entity (claimed end user: located in Heliopolis, Egypt)	March 9, 2004
March 14, 2004	Majidco Micro Electronics (Dubai)	-	-	Chicago, IL	89 Motorola computer chips	Neda Industrial Group (Tehran)	April 17, 2004
March 15, 2004	Majidco Micro Electronics (Dubai)	-	-	Burlingame, CA	2000 MHS microprocessors	Neda Industrial Group (Tehran) (claimed end user: Majidco)	April 1, 2004

NEDA sanctioned for Natanz – Dec. 2012

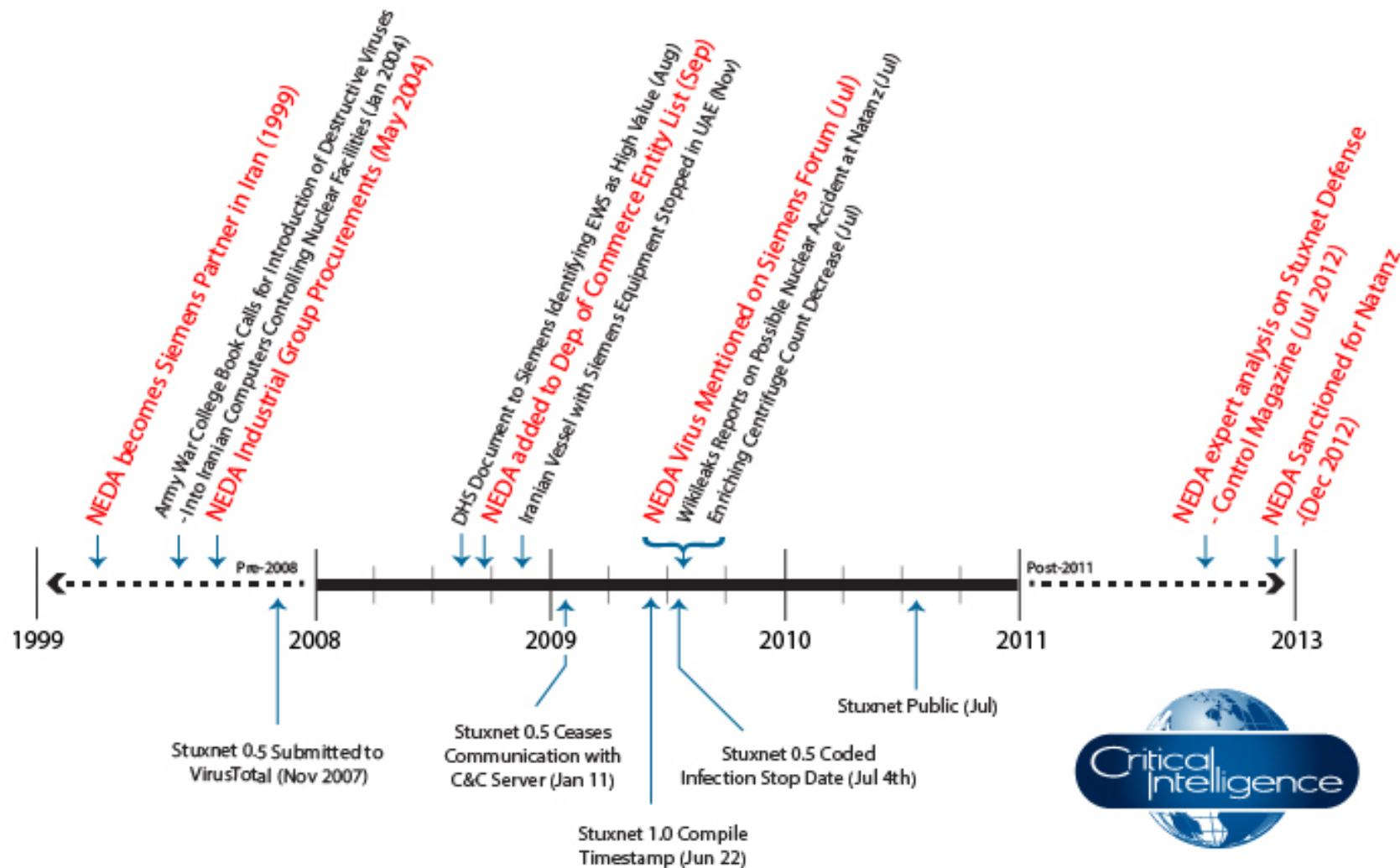


Neda Industrial Group (Neda) is an Iranian entity with strong links to the Iranian nuclear program, including the manufacture and procurement of proscribed equipment and material for use at Iran's Natanz Uranium Enrichment Facility. Since at least 2011, Neda has attempted to procure from foreign entities sensitive centrifuge-related components that have direct application in Iran's nuclear program.



Victoria Nuland

The companies placed under sanctions were Pouya Control, Iran Pooya, Aria Nikan Marine Industry, Faratech, Neda Industrial Group, Tarh O Palayesh and Towlid Abzar Boreshi Iran.



(Dashed line indicates time in a condensed not-to-scale format)

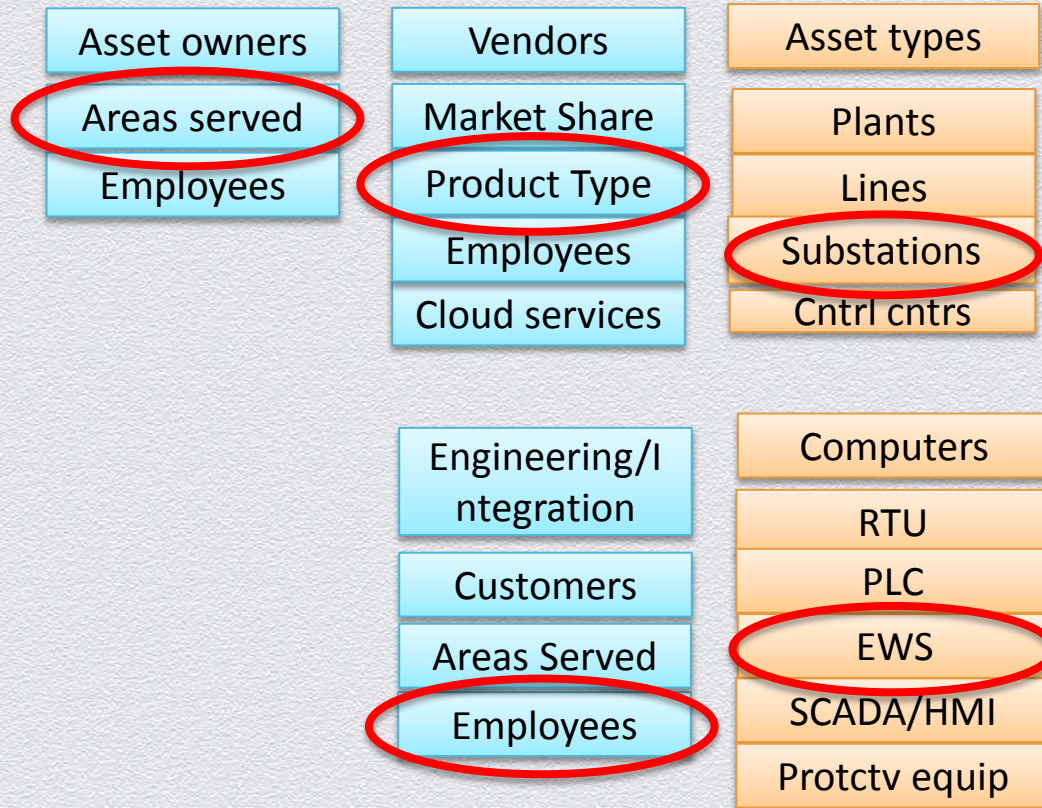


RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**How would you
infiltrate/attack/affect
a wide swath of
critical infrastructure
facilities in the United
States?**

SOSA leads to HVT identification



What Integration firm employee has access to the EWS used to configure the protective equipment for the target area served?

Internet Derived Targeting: Major Integrators in USA

2013:

Wood Group Mustang; SI revs: \$95 MM

Maverick Technologies: \$ 65 MM

Prime Controls: \$46 MM

2012:

Mustang Engineering; SI revs: \$90 MM

Keller Technology; SI revs: \$65 MM

Maverick Technologies; SI revs: \$58 MM



Customer Lists!

Automation and Control Projects

BP GOM Deepwater Development Program



Mustang was selected in March 2000 to provide engineering services for the BP GOM Deepwater Development Program in the Gulf of Mexico. MAC provided development of engineering tools and standards for Mustang, and Mustang provided engineering services for Mustang, and Mustang provided engineering services for Mustang.

Chevron Tahiti ICCS



MAC was selected to provide the front-end and data services for all process control and safety instrumentation for the Chevron Tahiti ICCS. MAC was selected from a field of competitors to provide the front-end and data services for all process control and safety instrumentation for the Chevron Tahiti ICCS.

El Paso Rawlins Gas Plant Automation Upgrade

MAC completed a project replacing El Paso's existing gas plant pneumatic control system with a modern, reliable, and secure Wonderware HMI. The project included approximately 560 new I/O signals and the installation of a new control room. MAC executed this work as a turn key project and coordinated with El Paso's Houston based and local resources.

Global Clients

Worldwide, MAVERICK Technologies has helped numerous companies to large, international corporations. Our thorough understanding of best practices and our ability to deliver a high quality solution has earned us a reputation as a leading provider of SCADA and automation solutions.

Click on the links below to learn more about our global clients.

[Abbott Laboratories](#)
[Air Liquide](#)
[AkzoNobel](#)
[Alcon](#)
[Amenon UE](#)
[American Beverage](#)
[Amgen](#)
[ATK](#)
[Aurora](#)
[Bayer](#)

Prime Controls has been awarded a design/build contract by the Dallas Water Utilities to replace the City of Dallas water distribution legacy SCADA system.




Dallas Water Utilities needed a turnkey state of the art solution for a fully redundant SCADA system for the City's water distribution system. The system will be operated from two separate control locations that are synchronized to provide a true 'quad' redundant control system with seamless failover.

Prime Controls scope of work includes: contract management; system design and application engineering; software development and implementation. In addition, Prime Controls will be furnishing and installing the computer system and related products; remodeling the system computer centers; handling the network/communications upgrade, system change-out and commissioning; and all related support services.

Prime Controls solution allows for the remote monitoring and automation of multiple pump stations, elevated tanks, and water meter stations.

[Telvent Press Release](#)

Pivoting for employee information



Tom Bedfar
Process Controls Engineer
Paris, Florida | Oil & Energy

[Join LinkedIn and access Tom Bedfar's full profile.](#)

As a LinkedIn member, you'll join 175 million other professionals who are sharing connections, ideas, and opportunities. And it's free! You'll also be able to:

- See who you and **Tom Bedfar** know in common
- Get introduced to **Tom Bedfar**
- Contact **Tom Bedfar** directly

- Validate email addresses
- Craft highly targeted malicious emails
- Wait for “phone home”

Actual results of spear phishing simulation – clicks from these titles:

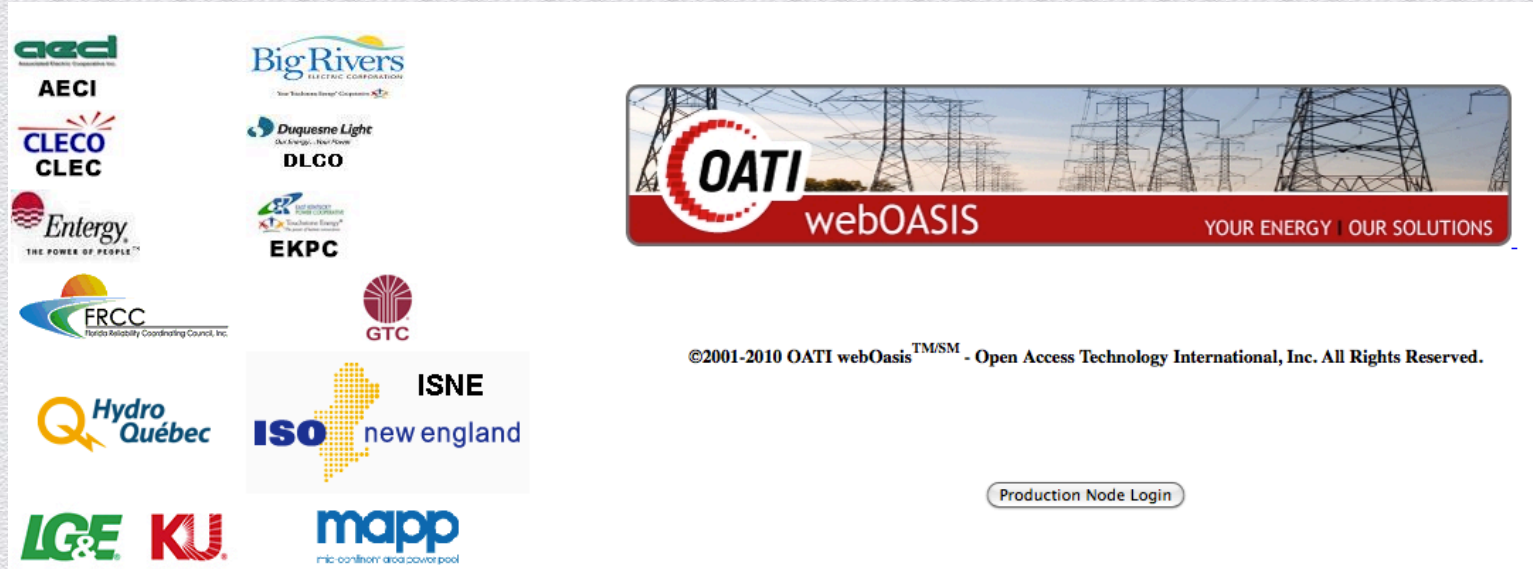
- ◆ Control Room Supervisor
- ◆ Instrument Technician
- ◆ Automation Technician
- ◆ Pipeline Controller
- ◆ Process Controls Engineer
- ◆ Senior VP Operations and Maintenance
- ◆ Equipment Diagnostics Lead
- ◆ 10 other various engineers

SOSA leads to HVT identification



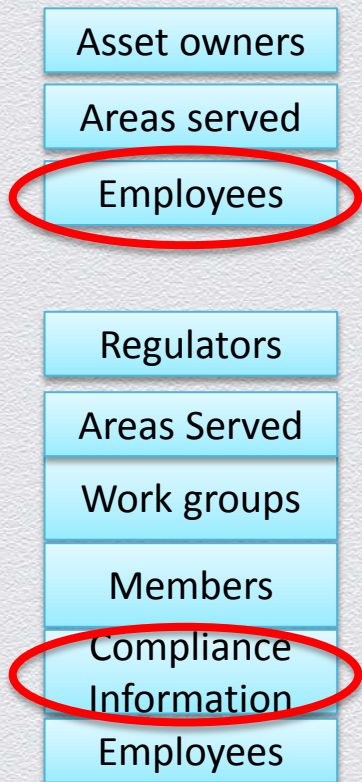
What vendors have
cloud services for
market operations?

Web services for market operations

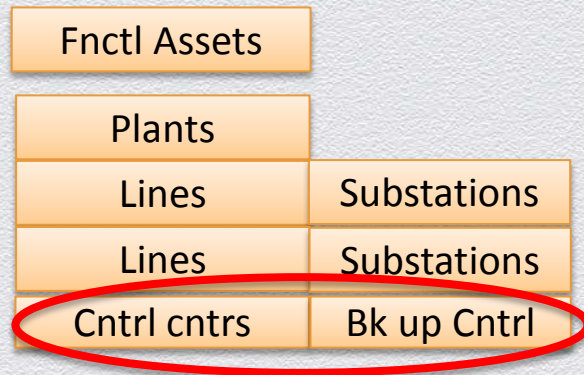


The screenshot displays the OATI webOASIS interface. On the left, a grid of logos for participating utilities is shown, including AECI, Big Rivers Electric Corporation, CLECO CLEC, Duquesne Light, DLCO, Entergy, EKPC, FRCC, GTC, Hydro Québec, ISO new england, LGE, KU, and mapp. The main banner features the OATI logo and the text 'webOASIS YOUR ENERGY | OUR SOLUTIONS'. Below the banner, the copyright notice reads: '©2001-2010 OATI webOasis^{TM/SM} - Open Access Technology International, Inc. All Rights Reserved.' A 'Production Node Login' button is located at the bottom right of the interface.

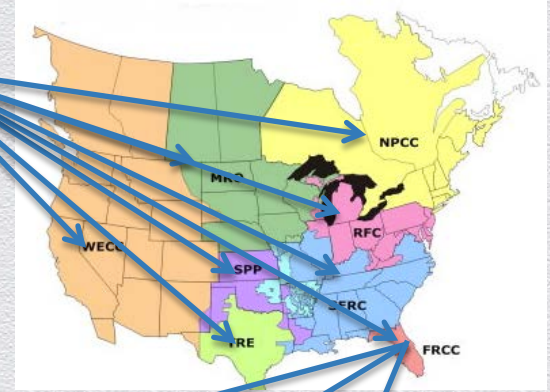
SOSA leads to HVT identification



What regulator maintains information about asset owner control centers, and employees who work there?



Regulatory/Reliability Environment



Just monitor Web pages!



#RSAC

RSACONFERENCE2014

Example: Standards of conduct

- ◆ *FERC Standards of Conduct, Section 358.7(f)(1): A transmission provider must post on its Internet website the job titles and job descriptions of its transmission function employees.*
 - ◆ Organizational charts
 - ◆ Job descriptions
 - ◆ Names, usernames (email), phone numbers of people holding those positions



Example: Info on backup control centers

- ◆ Several presentations from a working group on system reliability were shared to a public Sharepoint site (meant to be shared to privately).
 - ◆ Critical Intelligence noted potential impact to our customers, and reported to offending party, which removed them quickly
 - ◆ Who else grabbed these?
 - ◆ Were other affected parties notified?
 - ◆ What prevents this from happening again? NOTHING! It Did!

Example: State regulatory filings

- ◆ State bodies regulate investor owned utilities
 - ◆ Utilities commissions
 - ◆ Environmental regulators (air and water quality)
 - ◆ Photographs
 - ◆ Engineering diagrams
 - ◆ Employee contact information





RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

**Defense:
Reconnaissance
Surface Management**

Reconnaissance Surface Management Toolset

- ◆ OPSEC
- ◆ Whitewash
- ◆ Honey/canaries
- ◆ Deception
- ◆ Back hacking



Defense: OPSEC

Intelligence collection and analysis is very much like assembling a picture puzzle. Intelligence collectors are fully aware of the importance of obtaining small bits of information (or 'pieces' of a puzzle) from many sources and assembling them to form the overall picture.

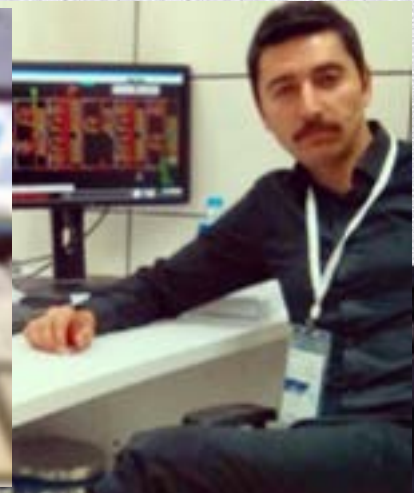
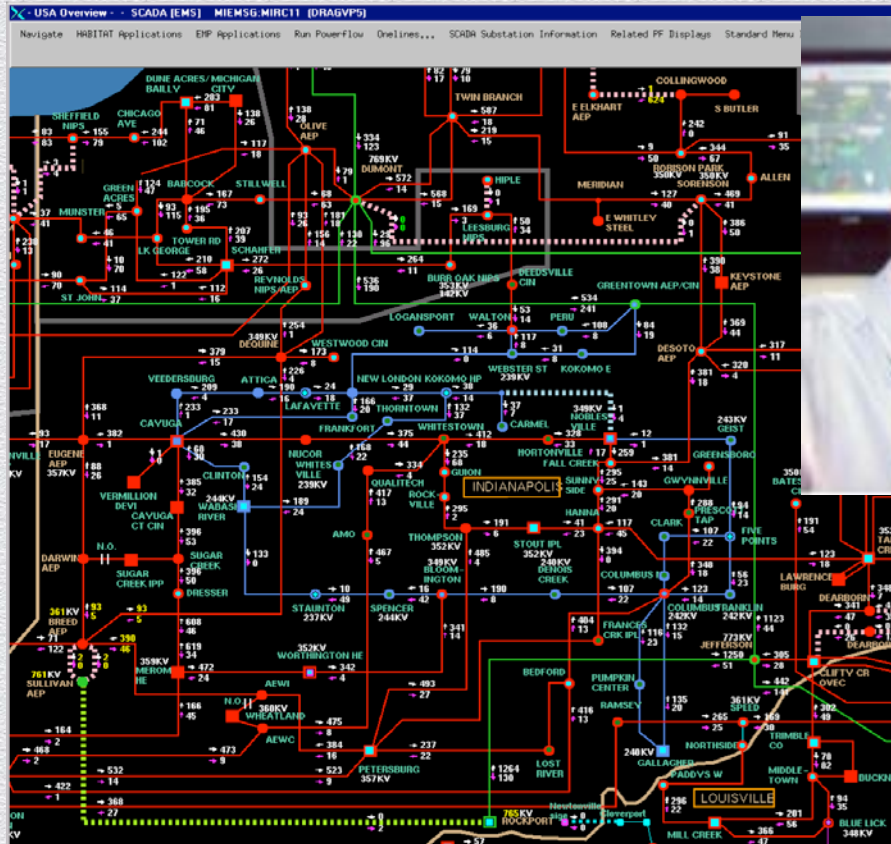


Example information from NERC PSIG

- ◆ Function and physical location of assets
- ◆ Network topology (cyber and physical)
- ◆ Contingency facilities, emergency response plans
- ◆ Communications assets
- ◆ Key suppliers and customers
- ◆ Risk assessment results, audit results, impact assessments
- ◆ Security operating procedures



No SCADA selfies!



RSM operational elements

1. Disclosure Prevention

- ◆ Information classification, Policies, Training, Pre-release “scanning”

2. OPEC Assessment:

- ◆ What have you already disclosed?
- ◆ How do you deal with existing disclosures?

3. Continual Monitoring: What are you (your employees) disclosing now?

- ◆ Regulatory filings, job postings
- ◆ Social media



Anti-IDT Recommendations

- ◆ Obtain threat intelligence with specific ICS focus
 - ◆ These are your crown jewels!
 - ◆ You were getting commercial threat intel for IT stuff but not for ICS stuff ???
 - ◆ Government-provided intel is good, but insufficient
- ◆ OSINT black box Internet-derived targeting for all critical infrastructure asset owners
 - ◆ More than standard penetration test – must consider possible operational ****kinetic**** impacts

