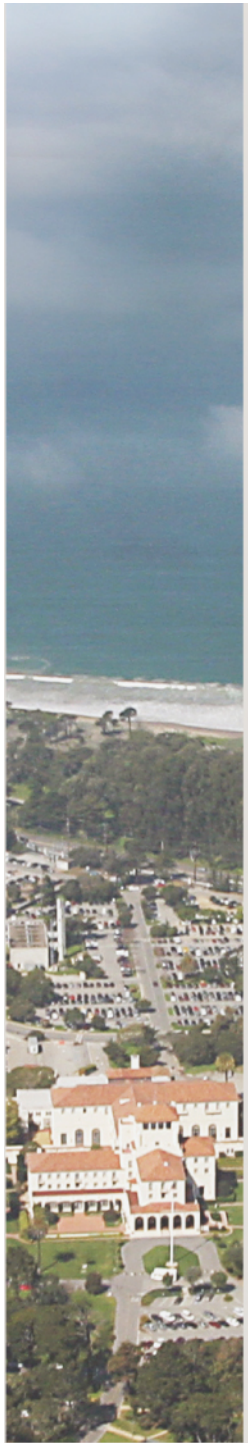


NAVAL
POSTGRADUATE
SCHOOL

Domestic Infrastructure – Critical Vulnerabilities and Protection

Grant Interest Rate Observer Conference

Dr. Leonard A. Ferrari
Provost, Naval Postgraduate School

Monterey, California
WWW.NPS.EDU

Critical Vulnerability

▪ Cyber Security at crisis proportions

- There is a wide scope of computers and networks in the economy, national security and government. But… most security is an afterthought
- Host security is a major weak link today.
- Network attacks can result in denial of service, spoofing, router infrastructure compromise
- Cyber Attacks can render information unavailable, modify critical information, and leak sensitive information

Worst Case Scenarios Are Easy to Imagine

- **Cyber Attacks**

  - Attackers target specific systems
  - Attractive business targets are those:
    - Essential for operations and are widely used systems
    - Keys to asset creation such as a buy-sell simulator
    - That could create a liability such as explosions, chemical leaks, collisions, etc.
  - "PC World – CIA Says Hackers Have Cut Power Grid"

Protecting Cyber Security

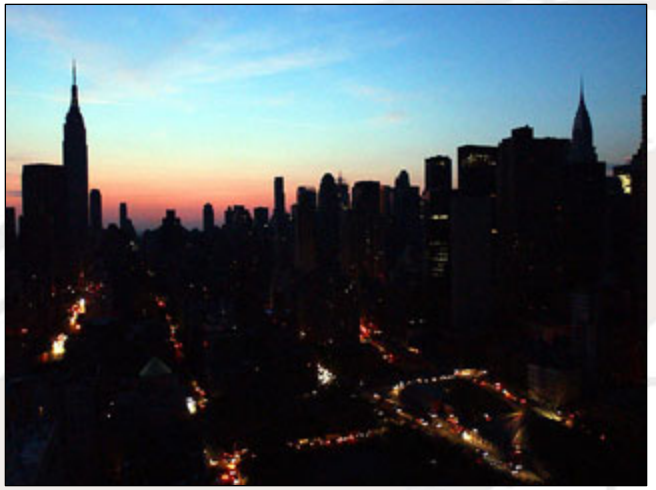
▪ Security Through Engineering

- Secure by Design by eliciting security requirements, building a system to be inherently secure, and validate that requirements are met.
- Secure out of the box by configuring security by default, minimize user privileges, and make available only well-defined interfaces.
- Secure in Operation by make recommendations for secure use tools to support secure system administration, and give management a clear view of the system security

Security = Technology + Assurance

Worst Case Scenarios Are Easy to Imagine

▪ Power Grid Network Infiltration



- A group of sophisticated, knowledgeable hackers gain access to the New York City power grid through commonly used supervisory control and data acquisition (SCADA) systems.
- The grid, already strained by consumer demand nearing its capacity, is an easy target for knowledgeable rogue groups.
- Within seconds, the group disrupts power to millions of resident and business customers, including financial markets.
- With the financial district down, Wall Street goes dark and more than $100 billion a day in Federal Funds trading, and billions more in private transactions, is frozen.

Worst Case Scenarios Are Easy to Imagine

▪ Subway Attack

- During a peak commuter period, a terrorist group detonates a small explosive on a forward subway car, injuring several passengers while also disabling the train trapping hundreds more.

- Moments later, the same group releases a chemical agent throughout the subway tunnels through a series of coordinated dispersal points and apparatuses.

- The invisible poison creeps forward through every crack and crevice, killing hundreds and sickening countless more as it diffuses throughout the network of underground tunnels.

Worst Case Scenarios Are Easy to Imagine

▪ Oil Supply Disruption

- "By hitting oil targets overseas, terrorists can hit us here at home, achieving the same destabilizing effect as an attack on American soil. Dependence on foreign oil is America's Achilles heel."

  Dr. Gal Luft, Executive Director
  Institute for the Analysis of Global Security

- Two car bombs infiltrate and explode inside Abqaiq, a Saudi Arabian oil processing facility that is the largest in the world.

- The resulting toxic inferno kills hundreds and sickens thousands surrounding the enormous facility.

- Approximately 4-6 million barrels of oil daily is removed from an already tumultuous market, causing incredible turmoil throughout domestic and international marketplaces.

Protecting the Power Grid

▪ Challenges

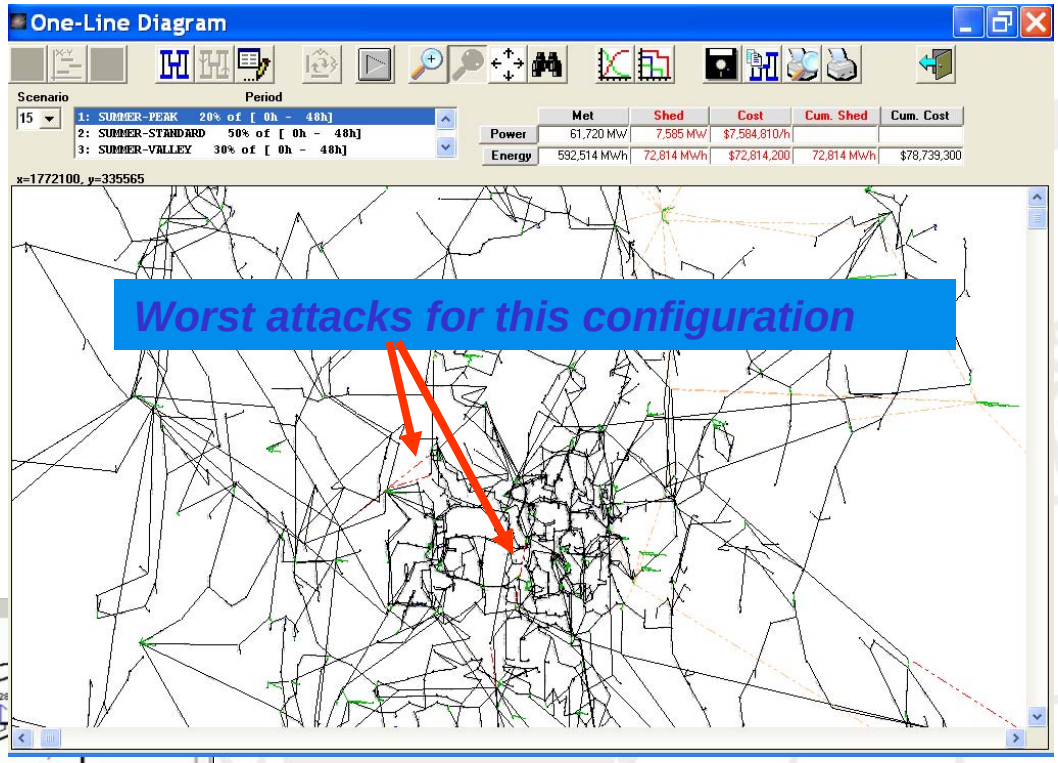
- ▫ Large-scale electric power grids are impossible to protect in their entirety.
- ▫ Supervisory Control and Data Acquisition systems are required for a utility to function in the marketplace, but allow hackers access points into the grid.

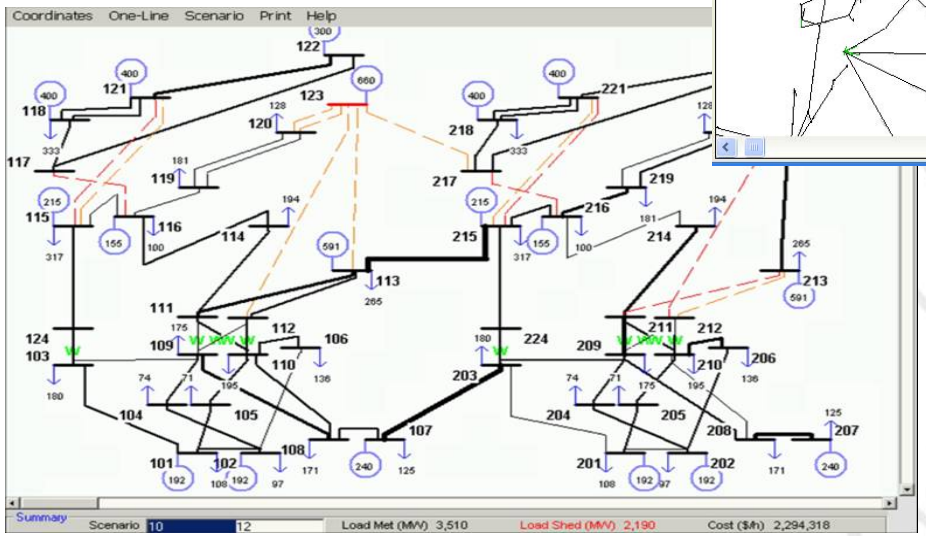
▪ Solutions

- ▫ NPS has developed elaborate models that can assist in determining the vulnerabilities of our systems.
- ▫ Developed models can also determine and evaluate the best possible defense plans, protecting as much of the infrastructure's function as possible from any given attack.
- ▫ By assuming the enemy will find the worst possible attack for a given defense, these models can provide accurate performance guarantees for potential defense solutions.

Protecting the Power Grid

- **The VEGA Project – Vulnerability of Electric Power Grids**
  - Developed jointly by NPS and University of Texas.
  - Determines the worst possible disruption caused by a terrorist attack.
  - Compares multiple attack plans terrorists may undertake given difference resource constraints.

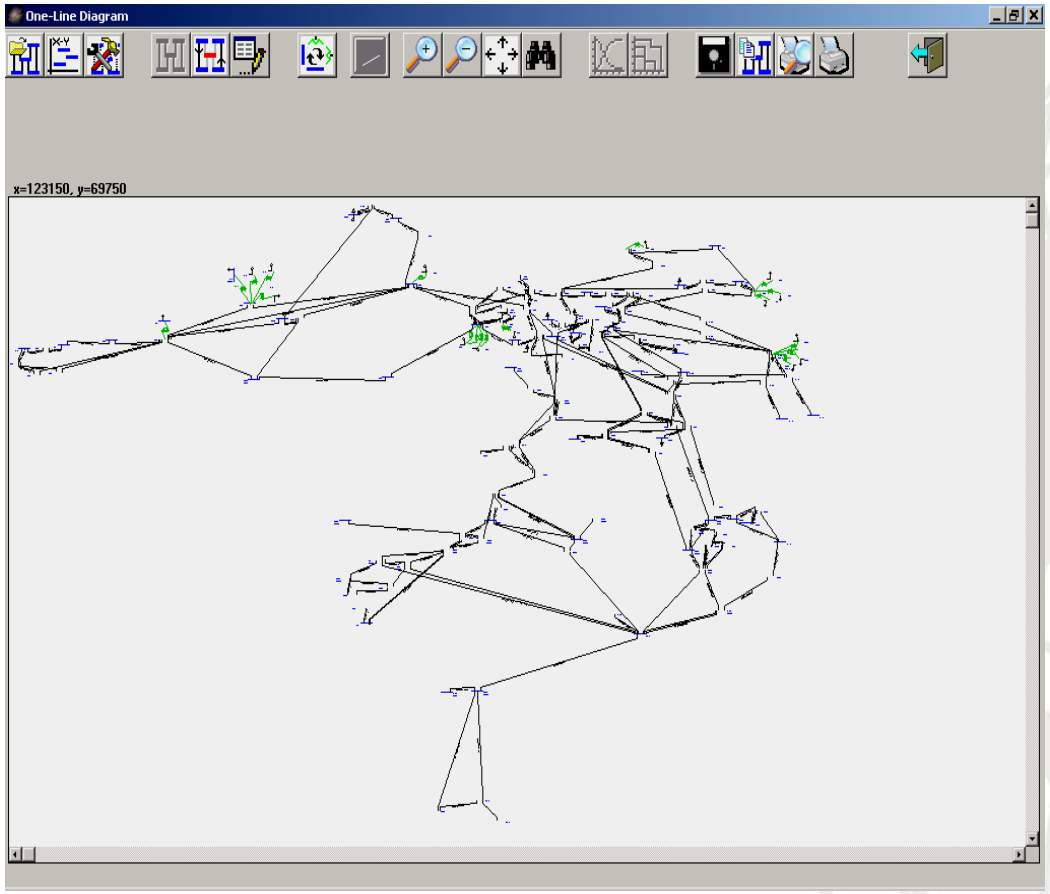


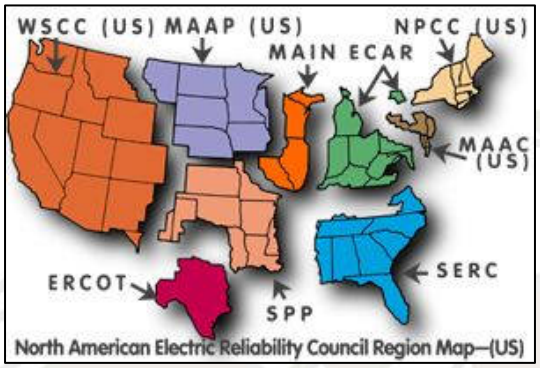


- Accurately models all high-voltage components of a major power grid.
- Methods and results are easily scalable without aggregation.

Protecting the Power Grid

- **U.S. Regional Grid Case Study**
  - North American Electric Reliability Council region
  - 5,400 buses / 6,500 lines / 500 substations
  - Summer 2005 / Peak load 69 GW, Gen. Cap. 91 GW





- **Computational Results**
  - No single "Achilles heel" in this grid. A single failure does not disrupt the system.
  - Increasing attacker effort yields a steady reduction in grid function.
  - Protecting a small number of key substations can reduce the overall vulnerability of the entire regional grid.

Defending Public Transportation Networks

▪ Challenges

▫ Major metropolitan subway networks are difficult to protect given their size.

▫ With thousands entering and exiting train stations daily, timely screening of passengers is near impossible.

▪ Solutions

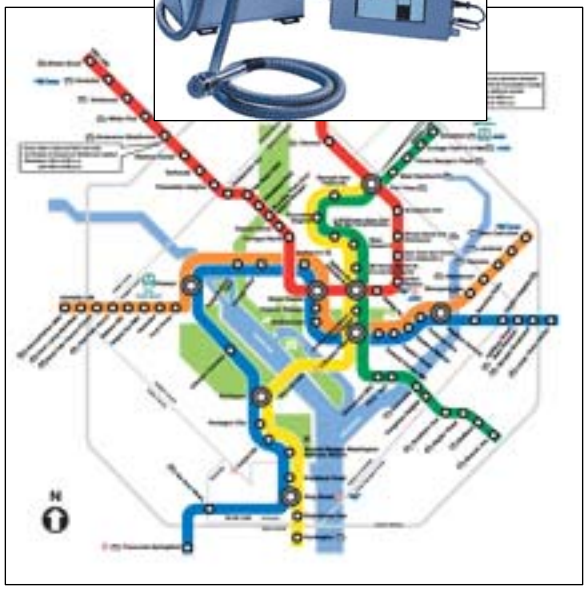
▫ Research the use of fast-acting biological agent detectors placed in tunnels to quickly discover the release of toxic gas.

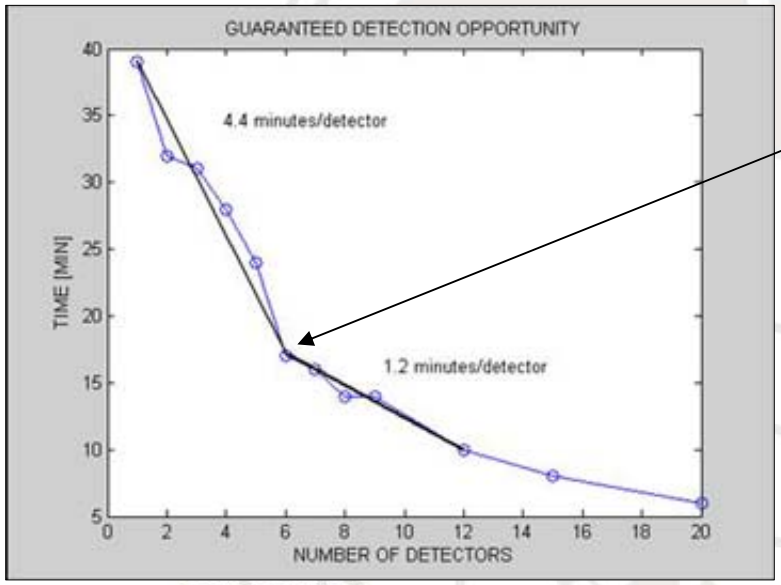
▫ Revived research into methods of securing released agents and fire to contained areas once initiated.

Defending Public Transportation Networks

▪ Optimizing Placement of Bio Agent Detectors

- ▫ Using DC Metro as a model, NPS team determined worst case scenario based on placement of three detectors.
- ▫ Also determined optimal number of detectors to employ to reduce detection time.
- ▫ Proved modeled networks can be useful in making infrastructure protection decisions.





▫ Bend in curve suggests an attractive defense option.

Defending Public Transportation Networks

- **Additional Efforts in Subway, Tunnel Security**

  - Fire, flood as well as chemical and biological agents are all of significant concern in subway network and tunnel safety.

  - Researchers with DHS, West Virginia University and industry have revived an idea using rapidly inflating air bags to seal off dangerous zones.

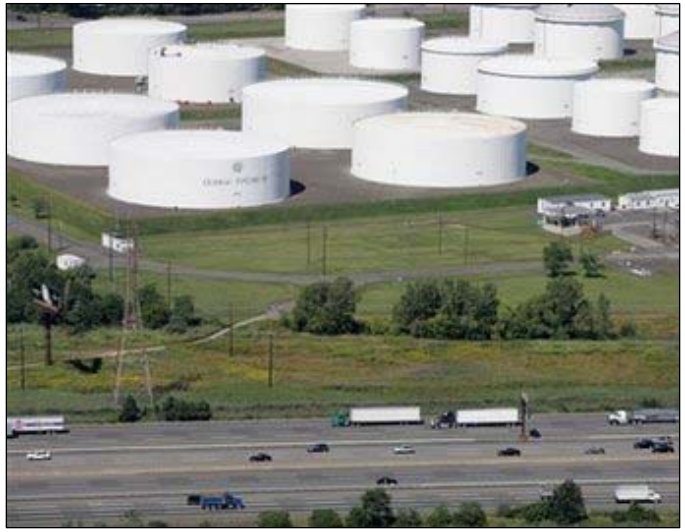
  - Could work with several types of potential subway and tunnel disasters.

Protecting Oil & Gas Infrastructure

▪ Challenges

- Major oil pipelines and reserves are in unsecured locations, and would be near impossible to fully secure.

- In an already volatile market, minor disruptions in supply can have significant effect on several sectors of the domestic economy.



▪ Solutions

- Analyze domestic strategic petroleum reserves and distribution networks for weaknesses.

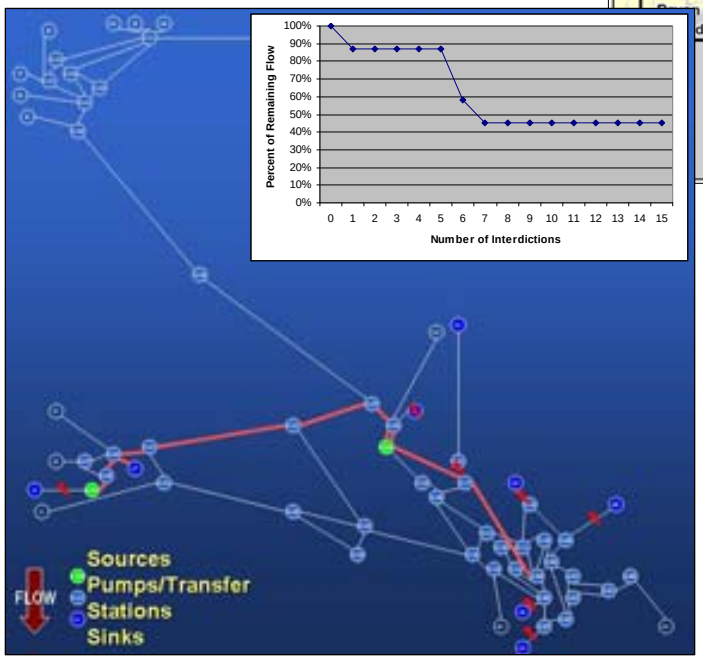
- Determine protection schemes that limit supply disruptions as much as possible.

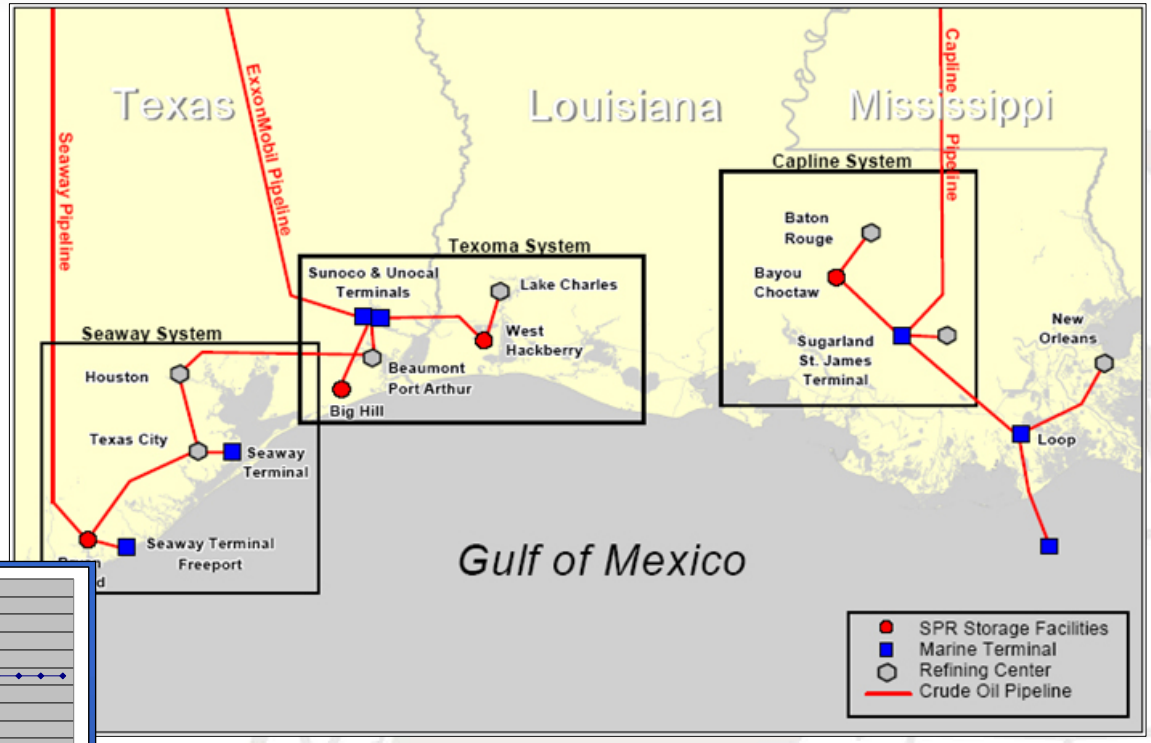
Protecting Oil & Gas Infrastructure

▪ Protecting Strategic Petroleum Reserves

▫ Identify the "critical backbone" connecting sources to the redundant part of the network, and protect that path.

▫ Determine means to fully protect critical backbone.





▪ Key Results of study

▫ Found vulnerabilities in Louisiana component of Strategic Oil Reserves (multiple reservoirs with adjacent piping, East-West flows).

▫ Once protected, Strategic Reserves network can withstand several attacks with minimal loss in overall function.

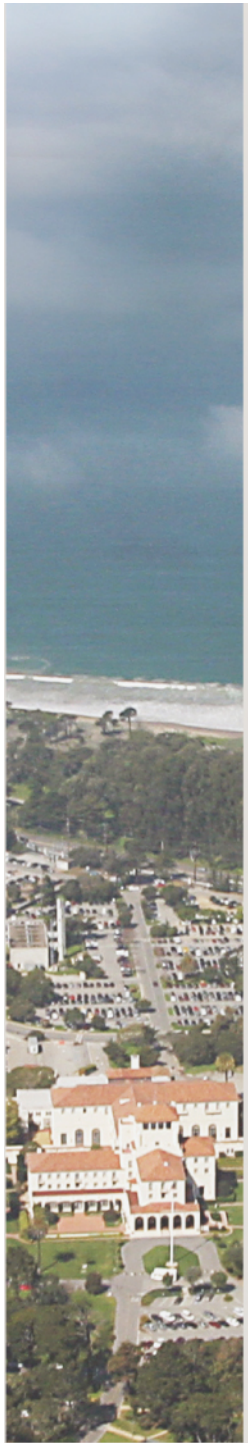
Contributors

Operations Research Department

- Distinguished Professor Gerald Brown
  - gbrown@nps.edu
- Associate Professor Matthew Carlyle
  - mcarlyle@nps.edu
- Assistant Professor Javier Salmeron
  - jsalmero@nps.edu
- Professor Kevin Wood
  - rkwood@nps.edu

Computer Science Department

- Professor Cynthia Irvine
  - irvine@nps.edu



NAVAL
POSTGRADUATE
SCHOOL

Domestic Infrastructure – Critical Vulnerabilities and Protection

Grant Interest Rate Observer Conference

Dr. Leonard A. Ferrari
Provost, Naval Postgraduate School

Monterey, California
WWW.NPS.EDU