Inter-Agency Cooperation in Securing the Port of New York and New Jersey: A Network-Centric Operations Approach

Dr. Rashmi Jain
Associate Professor of
Systems Engineering and Engineering Management
Stevens Institute of Technology

State of New Jersey Symposium on Homeland Security Research
October 29, 2003

STEVENS
Institute of Technology

Overview

- Network-Centric Approach
- Network-Centric Operations
- Information Superiority
- Essential Elements of Network-Centric Systems
- Case of Port of New York and New Jersey
- Agencies Participating in our Research
- Some Major Port Security Initiatives
- Some Preliminary Findings on Port Security Issues

Network-Centric Approach

- Create assured, dynamic, shared information environment that enables the agencies involved in port security to better integrate and transform their capabilities to investigate, analyze, prepare, respond to threats, and manage consequences.

STEVENS
Institute of Technology

Network-Centric Operations

Information-based operations that use interconnected information processing, networks, and data from three perspectives:

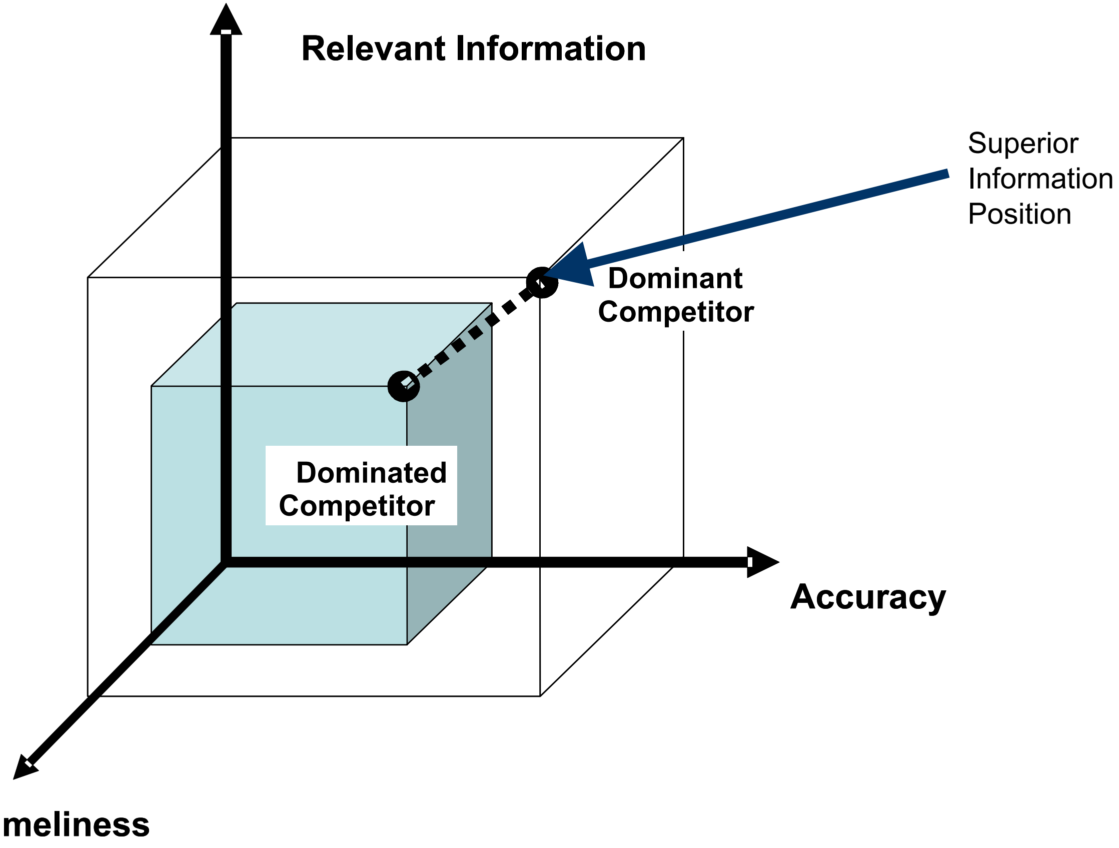
1. Leveraged User Functionality
   - Capability to adaptively perform assigned operational roles.
   - Increasing use of system-provided intelligence.
2. Interoperability
   - Standard means to provide/acquire information, services, application logic, and resources;
   - Common approach to assemble and interact with interoperable operational capabilities;
   - Information integration and process integration
   - Standard approaches to metadata and data management
3. Net-Centric-Induced Operational Effects
   - Shared Situation Understanding
   - Compression of Time thru simultaneity
   - Agility - Distributed, Self-synchronization

STEVENS Institute of Technology

Information Superiority

- The need for information superiority and the capability to immediately and appropriately respond to such information is the driver towards more sustainable, interoperable, and pervasive collections of network-centric systems.
- Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.
- It is a state that is achieved when a competitive advantage is derived from the ability to exploit a superior information position

Superior Information Position



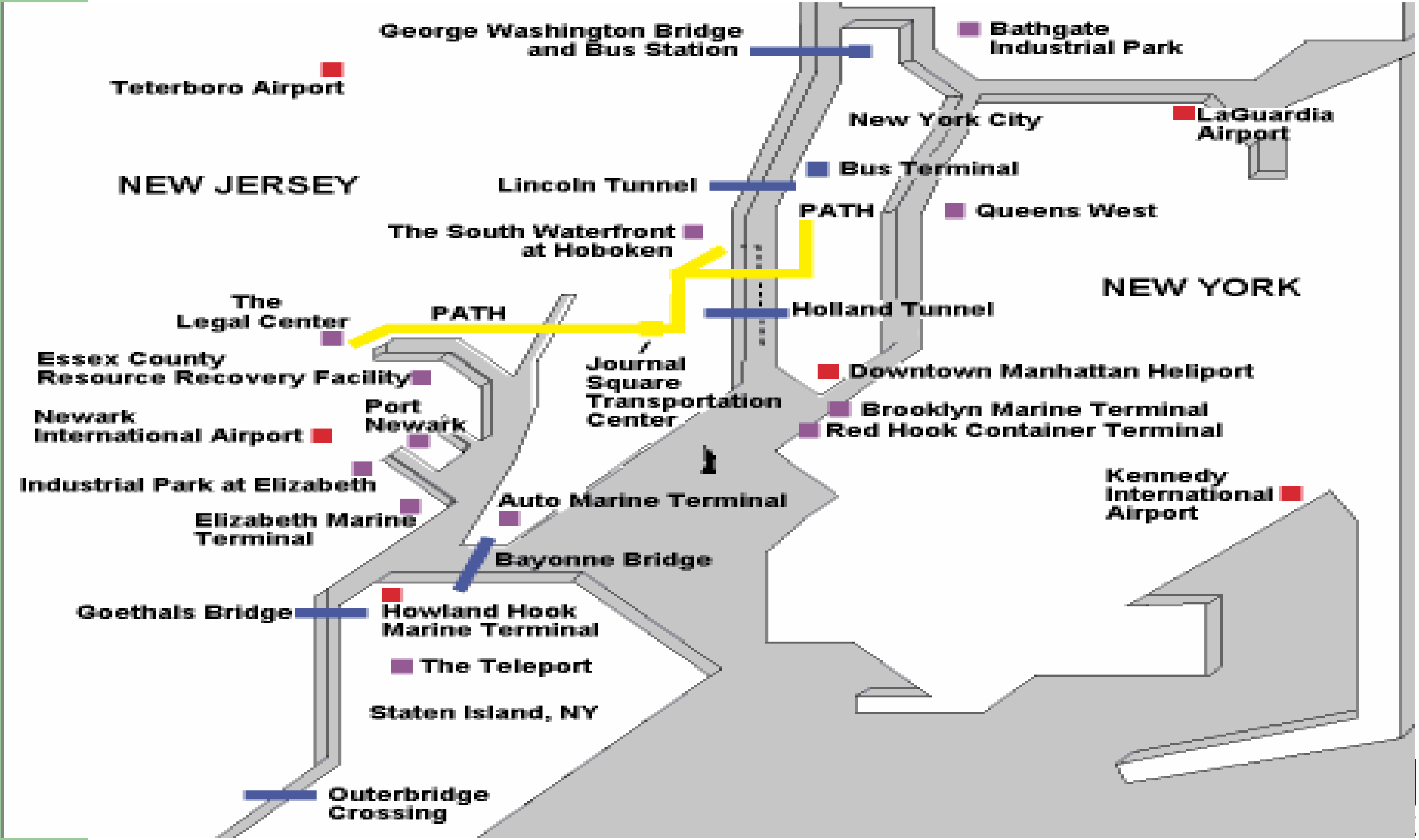
Source: Network Centric Warfare: Department of Defense Report to Congress, Department of Defense, Washington, D.C., 27 July, 2001

Essential Elements of Network-Centric Systems

- **Shared Awareness** is a key tenet of network-centric systems. Situation awareness or "Common Operating Picture" (COP) is shared across the network and is available to all the nodes. The COP comprises of three domains in which the nodes operate: physical, information, and cognitive.
- **Self-synchronization** is the ability of all the elements of the system to organize and synchronize information bottoms-up.
- **Speed of command** is the process by which superior information is turned into a competitive advantage. It is the process of making major decisive changes to the initial conditions to prepare for taking actions based on the superior information.

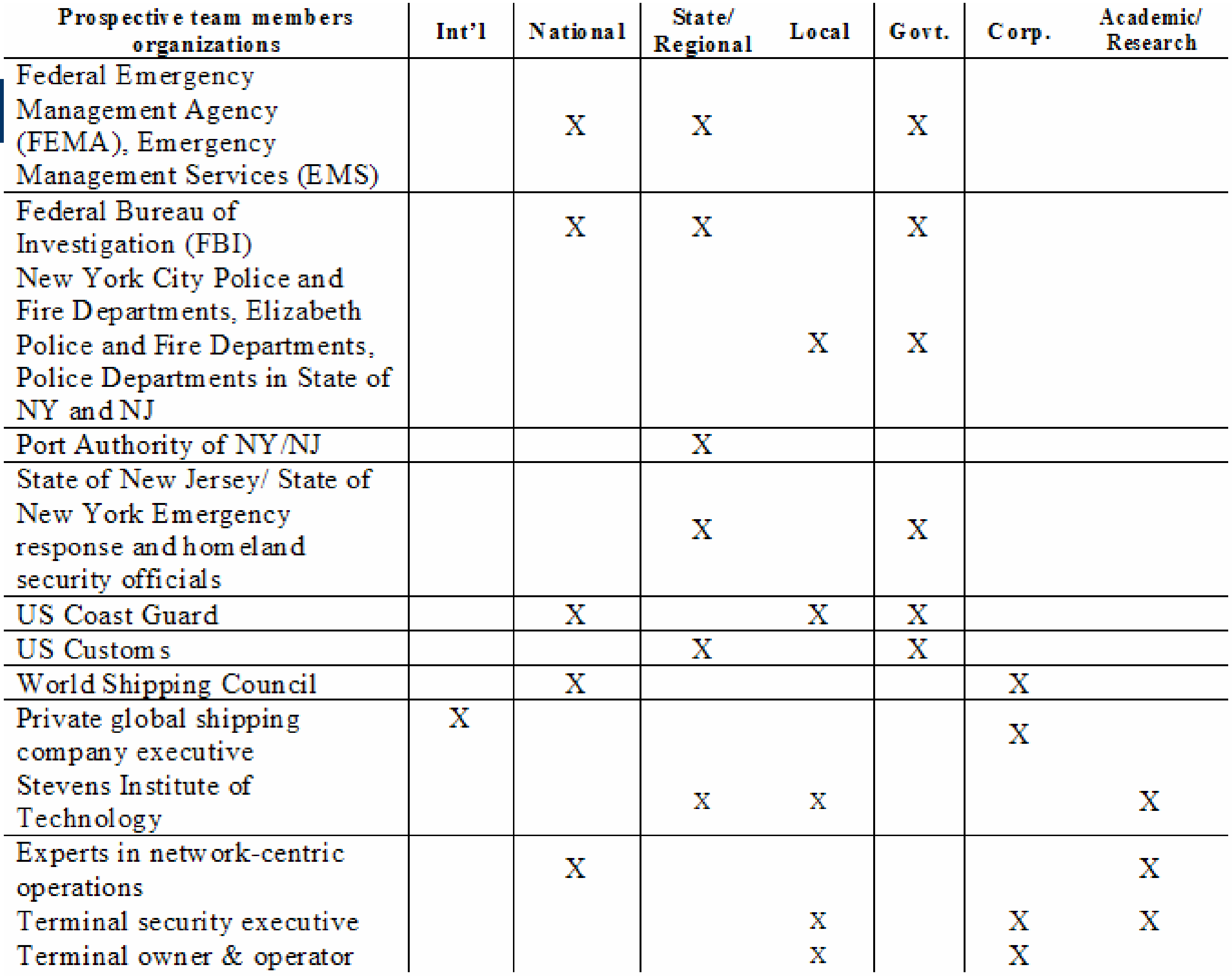
STEVENS
Institute of Technology

Facilities Map of Port Authority


George Washington Bridge and Bus Station
Bathgate Industrial Park
Teterboro Airport
New York City
LaGuardia Airport
Bus Terminal
NEW JERSEY
Lincoln Tunnel
PATH
Queens West
The South Waterfront at Hoboken
NEW YORK
The Legal Center
PATH
Holland Tunnel
Journal Square Transportation Center
Downtown Manhattan Heliport
Essex County Resource Recovery Facility
Port Newark
Brooklyn Marine Terminal
Newark International Airport
Red Hook Container Terminal
Industrial Park at Elizabeth
Kennedy International Airport
Auto Marine Terminal
Elizabeth Marine Terminal
Bayonne Bridge
Goethals Bridge
Howland Hook Marine Terminal
The Teleport
Staten Island, NY
Outerbridge Crossing

Source: Port Authority website

Agencies Participating in the Research



Prospective team members organizations	Int'l	National	State/ Regional	Local	Govt.	Corp.	Academic/ Research
Federal Emergency Management Agency (FEMA), Emergency Management Services (EMS)		X	X		X		
Federal Bureau of Investigation (FBI)		X	X		X		
New York City Police and Fire Departments, Elizabeth Police and Fire Departments, Police Departments in State of NY and NJ				X	X		
Port Authority of NY/NJ			X				
State of New Jersey/ State of New York Emergency response and homeland security officials			X		X		
US Coast Guard		X		X	X		
US Customs			X		X		
World Shipping Council		X				X	
Private global shipping company executive	X					X	
Stevens Institute of Technology			x	x			X
Experts in network-centric operations		X					X
Terminal security executive				x		X	X
Terminal owner & operator				x		X	

Some of the Officials Interviewed..

President	New York Shipping Association
Commanding Officer	U.S. Coast Guard, Actvities NY
Director, Operations and Emergency Management	Port Authority of New York and New Jersey
Division Director, Response and Recovery Division	Federal Emergency Management Agency (FEMA)
Assistant Director in Charge	Federal Bureau of Investigations
Director of Field Operations for the New York Customs Management Center	US Customs and Border Protection
Director	State of New Jersey - Dept of Law & Public Safety

Agencies Involved

- US Coast Guards
- Port Authority of NY/NJ
- Bureau of Customs and Border Protection
- Joint Terrorism Task Force
- Office of Counter-Terrorism
- Federal Emergency Management Agency
- …….Others

STEVENS
Institute of Technology

JTTF

- All agencies participating in the JTTF sign a formal memorandum of understanding that clearly states the task force's two objectives:
  - reactive: to respond to and investigate terrorist incidents or terrorist-related criminal activity; and
  - proactive: to investigate domestic and foreign terrorist groups and individuals targeting or operating within the New York metropolitan area for the purpose of detecting, preventing, and prosecuting their criminal activity.

STEVENS Institute of Technology

Container Security Initiative

- The U.S. Customs launched the Container Security Initiative (CSI) in January 2002 to reduce the risk of global containerized cargos being exploited by terrorists.
- CSI consists of four core elements:
  - Establish security criteria for identifying high-risk containers based on advance information.
  - Pre-screen containers at the earliest possible point.
  - Use technology to quickly pre-screen high-risk containers.
  - Develop secure and "smart" containers.

STEVENS
Institute of Technology

Customs-Trade Partnership Against Terrorism (C-TPAT)

- C-TPAT is a voluntary program modeled on the U.S. Custom’s narcotics smuggling prevention programs - "Carrier Initiative Program" and "Super Carrier Initiative Program". The intent of C-TPAT is for businesses participating in the supply chain to partner with U.S. Customs in their efforts to improve security. C-TPAT and CSI are part of the international initiatives to improve and enhance security arrangements throughout the supply chain.

Issues

- Many committees and task forces with much overlap.
- There is no singular coordinating body looking at the security issues together.
- No well-defined command and control structure.
- Issues being addressed in “modal” stovepipes (port security, surface transportation, airport security etc.)
- Planning activities not reflected at operational levels.
- Lack of interoperable communications.
- Need for flexible networks for situational response.
- More focus on sensors than on information sharing/dispersion.
- Need for a regional communications network to link local, state and fed agencies with a common agreed technology.