

Innovative Technologies for a Resilient Marine Transportation System
3rd Biennial Research and Development Conference - June 24–26, 2014
The National Academy of Sciences Building, Washington, D.C.

Ensuring Optimum Resilience in Marine Transportation: Extended Applications of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model

By:

Prof. Maria G. Burns

Director, Center for Logistics and Transportation Policy
College of Technology, University of Houston
mburns2@uh.edu - Tel: 713-743-1194





Ensuring Optimum Resilience in Marine Transportation: Extended Applications of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model

MSRAM (Maritime Security Risk Analysis Model):

“Because it is not feasible to secure our homeland against every conceivable threat, we have instituted **risk management** as the primary basis for policy and resource allocation decision making.”

-DHS Strategic Plan 2012-2016

- Mission 1: Preventing **Terrorism** And Enhancing **Security**
- Mission 2: Securing And Managing Our **Borders**
- Mission 3: Enforcing And Administering Our **Immigration Laws**
- Mission 4: Safeguarding And Securing **Cyberspace**
- Mission 5: Ensuring **Resilience To Disasters**





MSRAM MISSION :

AIM :

- Alleviate terrorist attacks within the USA;
 - Reduce the Nation's vulnerability to terrorism;
 - Eliminate the resulting consequences, i.e. damages;
 - Recuperate from potential threats / attacks, while ensuring socioeconomic security and sustainability;
-
- **MSRAM is a security risk analysis tool** used to assist in the prioritization and protection of Critical Infrastructure and Key Resources (CIKR).
 - **DRMM = Develop risk management for optimum decision making**
 - **Critical Infrastructure Protection (CIP)** Federal departments will identify, prioritize, coordinate protective measures through **Shifting from a consequence based system to a risk based system.**

shifting from a consequence based system to a risk based system.
prioritize, coordinate protective measures through
critical infrastructure protection (cip)





MSRAM & DRMM

MSRAM = Risk Assessment :

DRMM = Develop risk management for optimum decision making:

- **Security Vulnerabilities to anthropogenic disasters (*natural);**
- **Resource restrictions & sensible allocation;**
- **Infrastructure precedence;**
- **National priorities (socioeconomic);**
- **National planning scenarios, funding (local, state, national, tribal).**



2. MSRAM Methodologies:

Achieving Risk Reduction; Alleviating Risks : Protective measures; Estimating Primary & Secondary Security Consequences.



*MSRAM Risk Assessment per target / attack mode.
MSRAM data analysis enhances decision making
throughout the chain of Command:*

1. STRATEGIC
LEVEL

2. TACTICAL
LEVEL

3. OPERATIONAL
LEVEL





MSRAM RISK INFORMATION & SCENARIO ASSESSMENT

Target Risk Data

- **Target Name**
- Area (port, waterway, lat/long, county,
- DHS MCI/KR Station
(Maritime Critical Infrastructure/Key Resource)
- DHS Critical Port Infrastructure.
- USCG Station

- **Risk Assessment/Mitigation**
- USCG role (lead, support, other)
- Maritime Transportation Security Act (MTSA 2002) Equiv. to ISPS.
- Port Captain

Scenarios= Target & Attack Mode

- **Threat**
 - Ideology Intent
 - Capability
 - Geographic Intent.

- **Vulnerability**
 - Feasibility
 - Target vulnerability
 - **Max Consequence**

Consequences

- **Primary consequences:**
 - Death/Injury
 - National Security
 - Symbolic
 - Economic, direct
 - Health & Environmental, direct

- **Secondary consequences**
 - Economic, indirect
 - Health & Environmental, indirect.



MSRAM & DRMM serve as "Risk Based Decision Making tools" for terrorism;

- Risk Assessment & Risk Management tool;
- Helps consolidate and **allocate resources**, capabilities & competencies. Enables **communication & coordination** between federal – state – private sectors.
- Helps develop **risk management & contingency plans**;
- Prioritizes **investment**, helps develop **risk reduction strategies**;
- Helps carry out **in depth risk assessment scenarios**.
- **Justifies risk management decisions** at the tactical, operational and strategic levels.





The role of MSRAM (Maritime Security Risk Analysis Model):

MSRAM architecture facilitates contrast & comparison of targets.

Aims to reduce risk by prioritizing security resources, measures, and potential impact to over 28,000 maritime targets.

MSRAM SCENARIOS : TARGET TYPES AND ATTACK MODES .

TARGET TYPES	ATTACK MODES
•Targets in the vicinity of military outloads.	•Boat Attack
•Strategic assets: Nuclear power plants.	•Attack by hijacked aircraft
•Infrastructure (Bridges, pipelines, tunnels, dams).	•Attack by hijacked vessel.
•Offshore Platforms, MTSA-regulated facilities.	•Assault team / Suicide Attack
•HAZMAT Carriers, Barges and Ships.	•Sabotage
•High rise buildings and non-regulated high consequence targets in the port & waterway vicinity.	•Bomb (Boat, Truck, Aircraft, Submarine). •Bomb (Swimmer/Diver)
•Historical buildings, monuments and events.	•Mines (Aquatic and Land) •Chemical, Biological, Nuclear weapons.
	•Passenger ship / explosive devices.

Source : USCG 2012

The role of MSRAM (Maritime Security Risk Analysis Model):

Post - September 11, 2001:

- Protect US potential targets of attack: seaports, waterways, ships and refineries.
- USCG (DHS) federal agency for maritime security, encompassing the protection of U.S. ports, coasts, and inland waterways as part of its Ports, Waterways, and Coastal Security (PWCS) mission.
- Economic impact: cargoes of \$700 billion / annum (DHS 2012).
- Impact on global trade, transport, society.





The role of MSRAM (Maritime Security Risk Analysis Model):



2004 : USCG commitment to design & implement risk management & risk assessment.

•Progress in assessing maritime security risks using MSRAM.

2005:

MSRAM development: the Coast Guard had begun to address the limitations of its previous port security risk model.

2012: USCG risk management is implemented through MSRAM:

- ✓ Prioritizing port security resource allocation;
- ✓ Recognizing competences essential to alleviate potential threats;
- ✓ Identifying key targets.

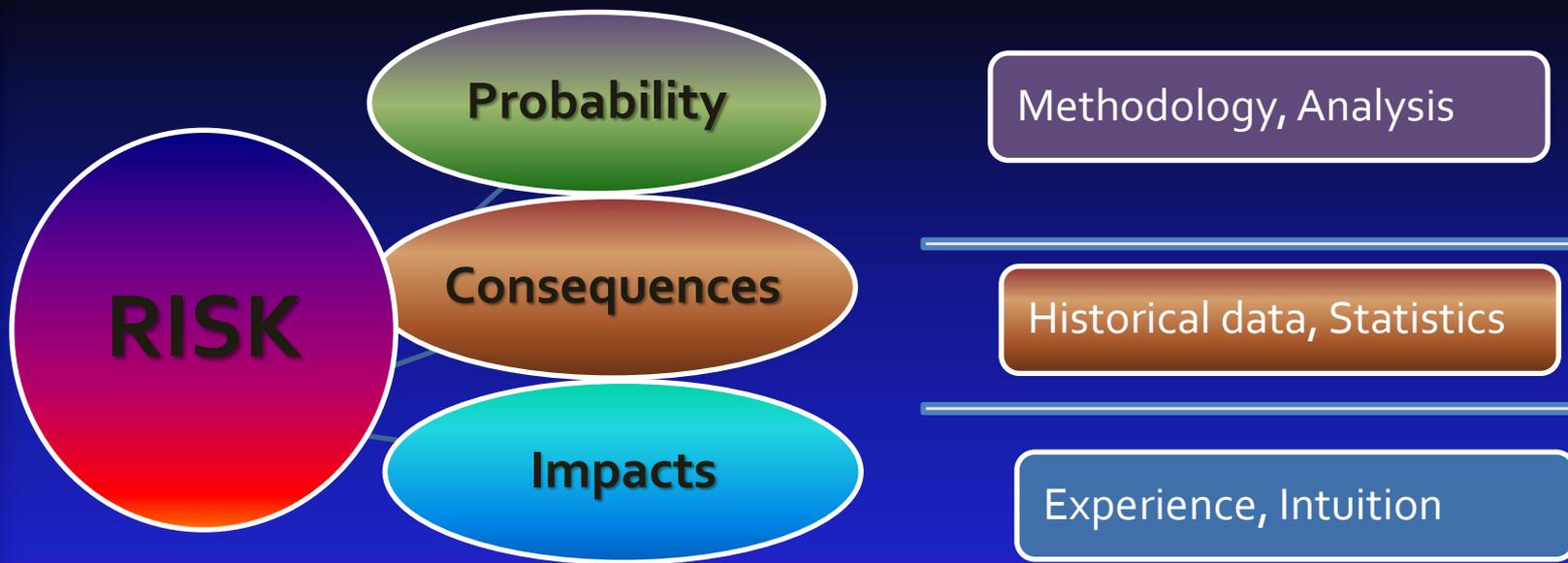


2001-2005 PSRAT	2006 – MSRAM 1	2007 – MSRAM 2	2008 – 2015 – MSRAM +
<p><u>AIM:</u> enhancing Captain of the Port (COTP) Risk security management. Improve =</p> <ul style="list-style-type: none"> consistency + threat Consequence data to support ONS (Operation Neptune Shield). Port Risk data supported port security risk assessment. Government Accountability Office (GAO) = Good start – improvements needed. 	<p><u>AIM:</u> sustain field + headquarters. Addresses threat element from USCG Intelligence Coordination Center (ICC) + consistency issues. Supported=</p> <ul style="list-style-type: none"> COTP/Sectors. Operation Neptune shield. TWIC card. Fight maritime terrorism. GAO= Address concerns. Addresses 13 of 18, critical infrastructure and key resources. 	<p><u>AIM:</u> advance training, support & information assessment.</p> <ul style="list-style-type: none"> Expanded range of scenarios. Supported= COTP/SECTORS Operation Neptune shield. Special training for port security teams. TWIC Card, transportation worker identification card. Combatting maritime terrorism. Mounted automatic weapon project. GAO = Most efficient tool for risk management in DHS. 	<p><u>AIM :</u> Address full scope of CBRN Threat) (Chemical, Biological, Radiological, And Nuclear Risk Assessments). Improve = consequence/vulnerability analysis. Address 18 of 18 CIKR (Critical Infrastructure and Key Resources). Support DHS, OGA, states and other nation’s risk analysis. GAO = Maritime security is the only are to receive the grade of substantial progress. (*GAO= government</p>



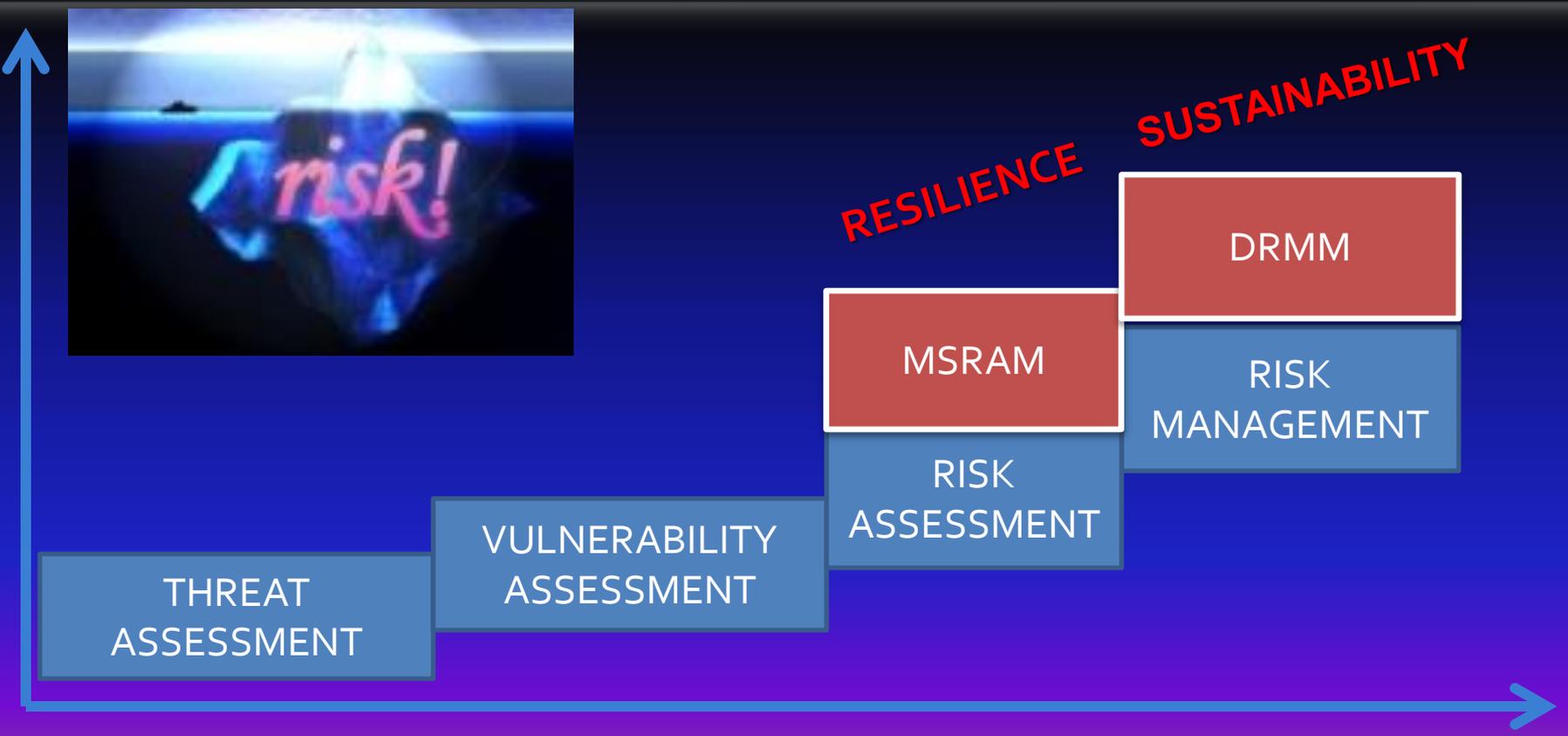
Ensuring Optimum Resilience in Marine Transportation: Extended Applications of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model

The role of MSRAM (Maritime Security Risk Analysis Model):
Supporting U.S. Coast Guard's mission to forecast and alleviate "generic attack" security risks within U.S. ports and waterways.
Evaluating threats, consequences and key vulnerability areas.





The role of DRMM (Dynamic Risk Management Model):
To utilize MSRAM's risk assessment data and methodology in likely scenario-based drills that reflect likely threats and expose vulnerabilities. It accurately evaluates timelines, investment needs, and prioritizes risk.



Federal Emergency Management Agency

FEMA's National Planning Frameworks: (2nd edition, May 2013).



PREVENTION: prevent security threats within USA.



PROTECTION: reducing vulnerability to terrorism.



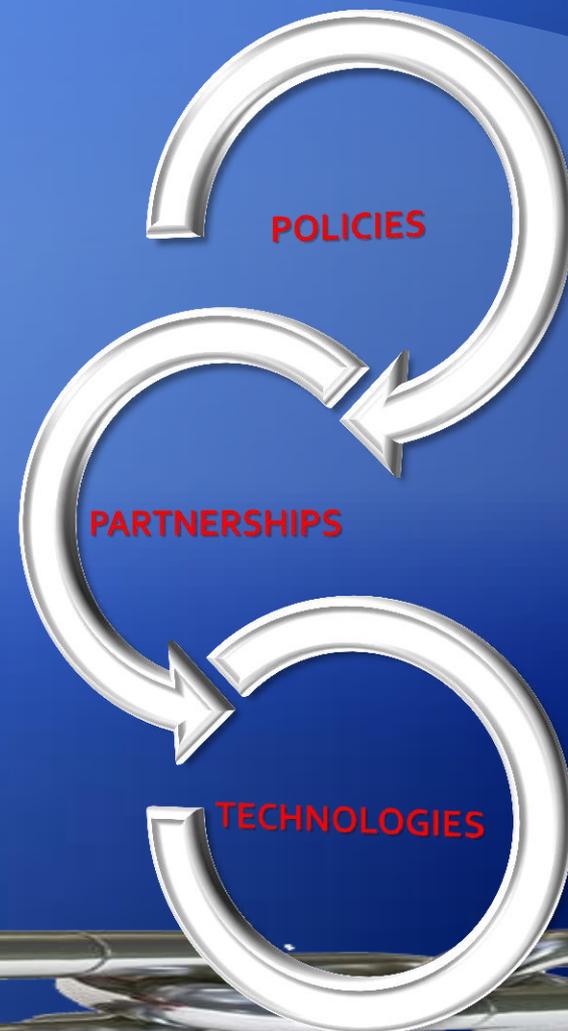
MITIGATION: Averting danger



RESPONDING: eliminating damage



RECOVERING: after attack, ensuring socio-economic security.





EXTENDED APPLICATIONS

DHS Strategic Plan, 2012-2016

VISION

A homeland that is safe, secure, and resilient against terrorism and other hazards.

MISSION

We will lead efforts to achieve a **safe, secure, and resilient homeland**. We will counter terrorism and enhance our security; secure and manage our borders; enforce and administer our immigration laws; protect cyber networks and critical infrastructure; and ensure resilience from disasters. We will accomplish these missions while providing essential support to national and economic security and maturing and strengthening both the Department of Homeland Security and the homeland security enterprise.

SECURITY THREATS: NEW SCENARIOS AND APPLICATIONS



TERRORISM



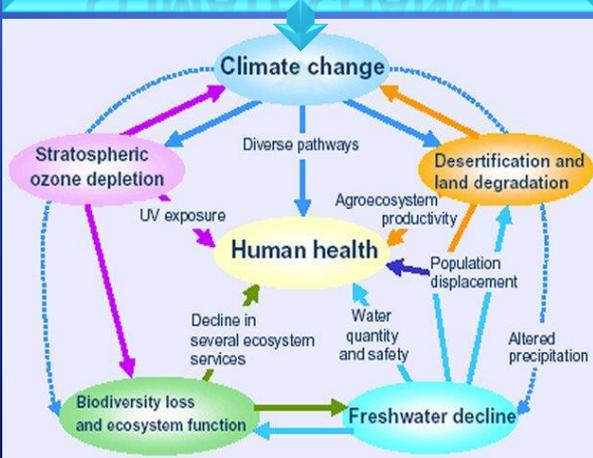
SEA PIRACY



CYBERSECURITY



CLIMATE CHANGE



HURRICANES



FLOODING



Ensuring Optimum Resilience in Marine Transportation: **Extended Applications** of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model



RISK
ASSESSMENT
TOOL

RISK
MANAGEMENT
TOOL

RESOURCE
ALLOCATION

INVESTMENT
OPTIMIZATION

PUBLIC-
PRIVATE
SECTOR
COALITION

ACCURATE
CONTINGENCY
PLANS

HARMONIZE SECURITY
POLICIES & PROTOCOLS

FURTHER ALIGN
PUBLIC & PRIVATE
SECTOR

RESOURCE INVESTMENT
& MANAGEMENT

- SEA, LAND, AIR TRANSPORTATION
- ENERGY & INDUSTRY
- PUBLIC, PRIVATE AND COMMUNITIES

COMMUNICATION

EDUCATION

CULTURE

TECHNOLOGY



Impact of a terrorist attack



Logistics companies lose **US\$3 - US\$4 million a day** while the ports are closed, while producers/manufacturers suffer disruptions to their assembly lines. ("just in time").



SUPPLY CHAIN FINANCIAL LOSS due to terrorist attack threat
Half a Billion dollars per week per major port, e.g. LA, Long Beach
- supply chain: industrial & transportation disruptions.

9/11 terrorist attack LOSSES:

3,000 lives + 60 billion: (direct + indirect losses)

Direct losses: (physical assets) **\$28 billion.**

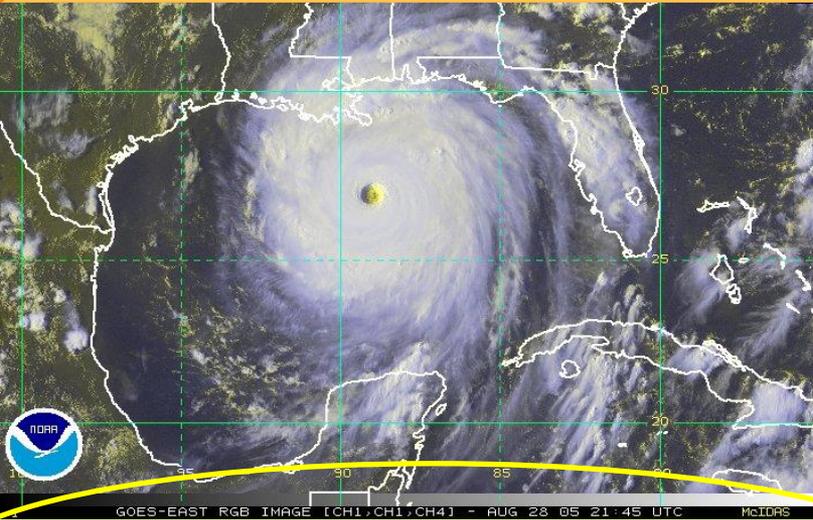
Indirect losses (insurance for loss of life, business collapses, jobs lost, infrastructure and other liabilities amount to **\$32 billion**)

9.11.01

The Socio-Economic Impact of a Natural Disaster:

Hurricane Katrina – NOLA, USG

August 2005



1,833 people died & Thousands in distress;
USD 108 billion in damages

The Gulf of Mexico: destruction of rigs and refineries brought on by the hurricane, over **91% of oil production and 83% of gas production** was shut down. **6 months after Katrina 85% of daily gas and 76% of daily oil production** were restored.

Earthquake in Kobe, Japan,

January 2005

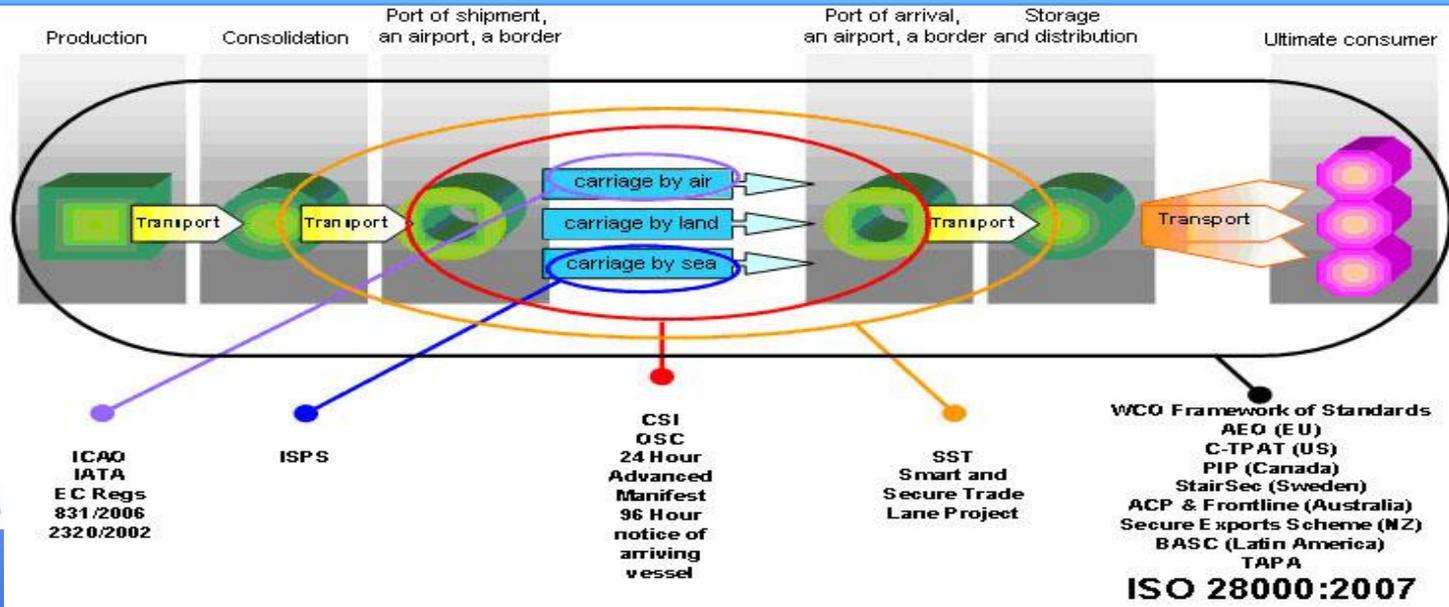
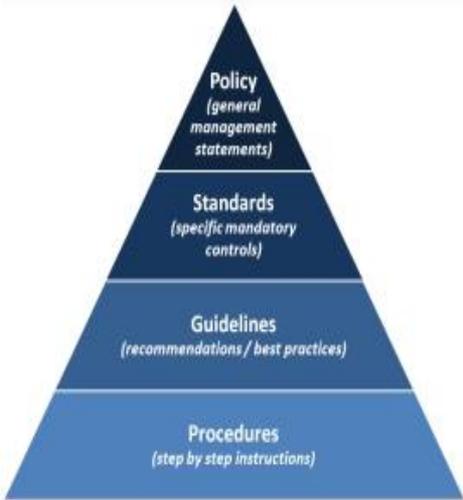


6,400 people died, 30,000 injured & Thousands in distress;

US\$ 200 billion in damages
100,000 buildings destroyed
300,000 homeless
KOBE - Japan's major port closed for 2 months;
20,000 Toyota cars – production off-schedule (NIST SP 901)



MSRAM, DRMM & POLICIES



Compulsory programs



1) Compulsory today
2) Compulsory soon

Supply Chain growth is directly proportional to Security risks,

Whereas targets shift to the six key components of a Supply Chain, i.e.

- 1) Production** (Industrial Zone, Refineries),
- 2) Supply** (key-components i.e. spare parts for value-added goods),
- 3) Mass Storage Areas** (Warehouses, Distribution Centers)
- 4) Transportation** (Hub Ports, Sea Ports, Airports),
- 5) Decision-Making Centers** (Areas of Political, Economical and Military significance) and
- 6) Cyber Security** (access to sensitive data via IT).

Source: M.Burns, JTRS 2013





HIGH SECURITY RISK TENDS TO SHIFT TO AREAS OF GROWTH

**POLITICAL,
MILITARY,
ECONOMIC
CENTERS**

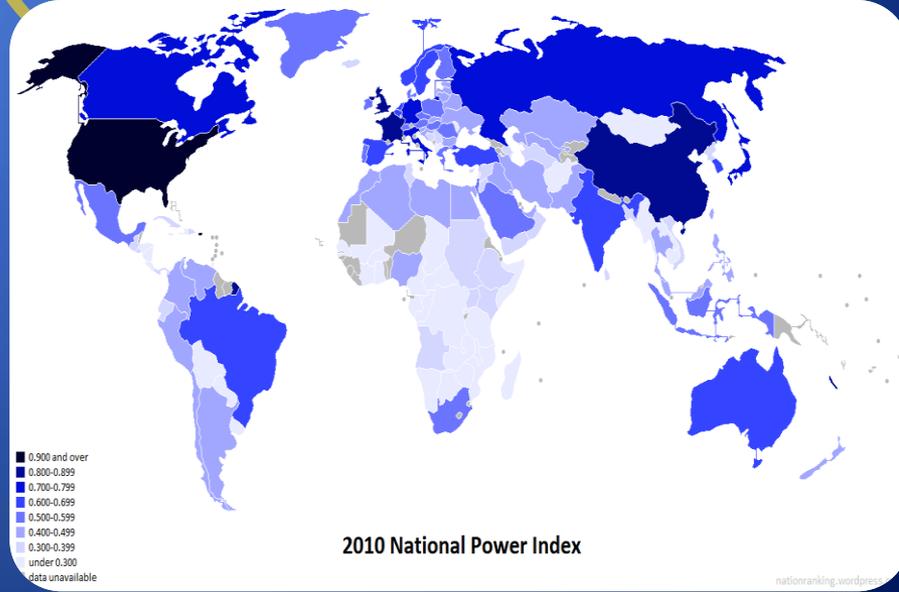
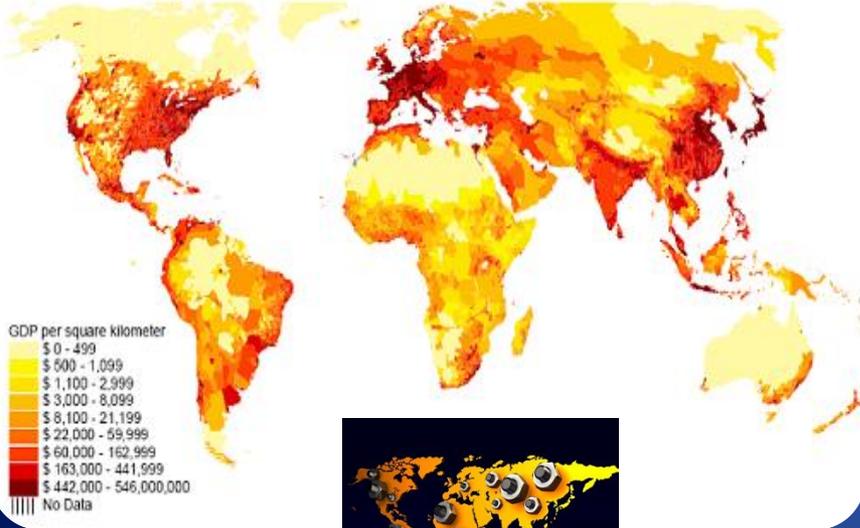
PRODUCTION :
industrial zone,
refineries.

**DISTRIBUTION
CENTERS, Mass
Storage Areas.**

TRANSPORTATION

I.T.

GDP Density



GDP, Defense, Technology, Population



Ensuring Optimum Resilience in Marine Transportation: Extended Applications of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model

HIGH SECURITY RISK TENDS TO SHIFT TO AREAS OF GROWTH

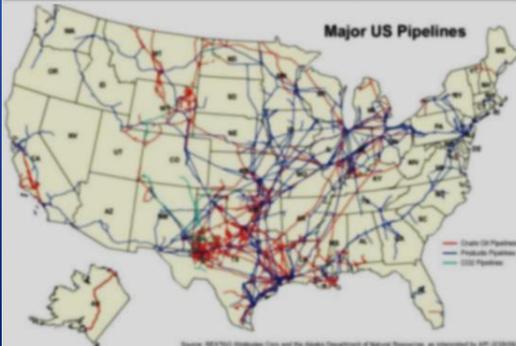
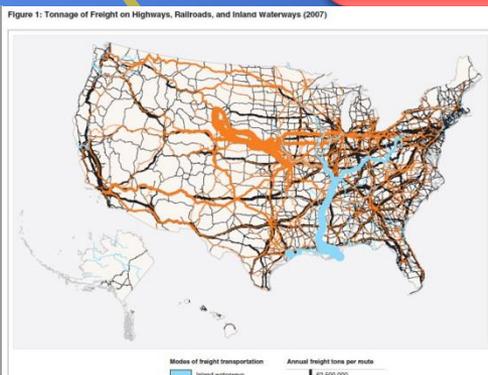
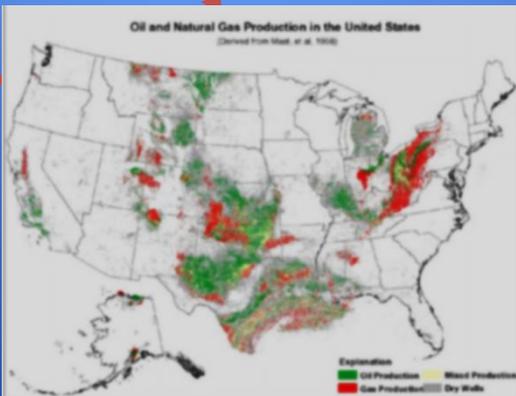
POLITICAL,
MILITARY,
ECONOMIC
CENTERS

PRODUCTION
industrial zone,
refineries.

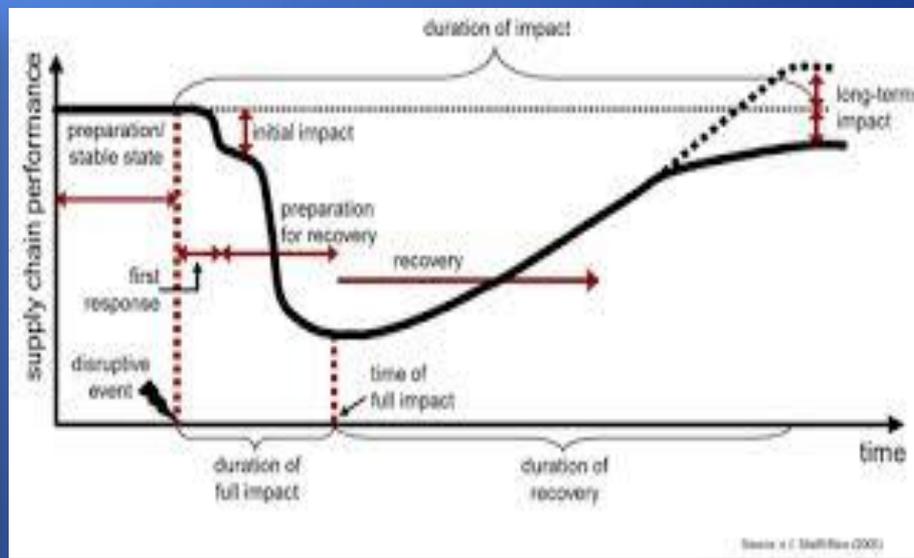
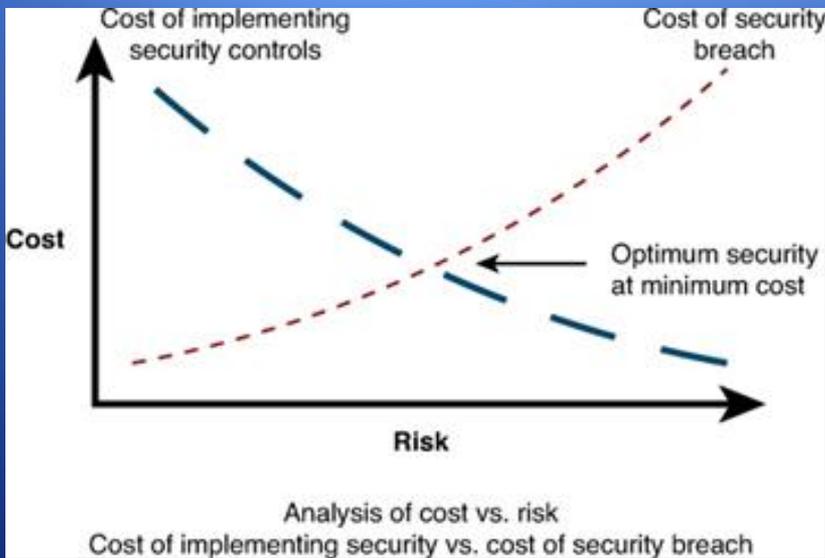
DISTRIBUTION
CENTERS, Mass
Storage Areas.

TRANSPORTATION

I.T.



Estimating the Economic Impact of Security





Ensuring Optimum Resilience in Marine Transportation: Extended Applications of the Maritime Security Risk Analysis Model & the Dynamic Risk Management Model

**Man-made
and
Natural Disasters**

MSRAM & DRMM Focus

Threat

Vulnerability

Consequences

Plan Attack

Team formation

Attack Resources.
Weapon testing.

Target surveillance.

Penetrating target defense

Weapon Detonation / Release

Primary Impacts

Secondary Impacts

Identify Vulnerabilities

Prevention & Planning

Protection

Response

Primary Consequence Mitigation

Resilience



MSRAM → Risk Assessment → Component of Risk Management.

DRMM → Risk Management = the big picture.



Likelihood	Consequences				
	Insignificant <i>(Minor problem easily handled by normal day to day processes)</i>	Minor <i>(Some disruption possible, e.g. damage equal to \$500k)</i>	Moderate <i>(Significant time/resources required, e.g. damage equal to \$1million)</i>	Major <i>(Operations severely damaged, e.g. damage equal to \$10 million)</i>	Catastrophic <i>(Business survival is at risk damage equal to \$25 Million)</i>
Almost certain (e.g. >90% chance)	High	High	Extreme	Extreme	Extreme
Likely (e.g. between 50% and 90% chance)	Moderate	High	High	Extreme	Extreme
Moderate (e.g. between 10% and 50% chance)	Low	Moderate	High	Extreme	Extreme
Unlikely (e.g. between 3% and 10% chance)	Low	Low	Moderate	High	Extreme
Rare (e.g. <3% chance)	Low	Low	Moderate	High	High

PUBLIC SECTOR

- Federal
- State

PRIVATE SECTOR

- Ports
- Conglomerates
- Transportation
- Manufacturers
- **Medium & Small Companies**

COMMUNITIES

EDUCATION





Thank You!

Any Questions?

Prof. Maria G. Burns

Director, Center for Logistics and Transportation Policy
College of Technology, University of Houston
mburns2@uh.edu - Tel: 713-743-1194





References:

- 1) Burns M., (2008), “ISPS – Maritime Security” Conference, American Bureau of Shipping, Marriott Hotel.
- 2) Burns, M. (2013a) “Effectiveness Evaluation of the Maritime Security Risk Analysis Model And the Dynamic Risk Management Model”. Washington DC: TRB - Transportation Research Board of National Academies, Supply Chain Security Sub-Committee, January 14-16, 2013.
- 3) Burns, M. (2013b) “The economic impact of Supply Chain Security : Financial tradeoffs between Supply Chain Security and Efficiency” Washington DC: TRB - Transportation Research Board of National Academies, Supply Chain Security Sub-Committee, January 14-16, 2013.
- 4) Burns, M. (2013c). Maritime Economic & Transportation Outlook: A New Era Ahead”, “Breakbulk Americas” – Executive Presentation, New Orleans, September 2013.
- 5) Burns M. 2014a. “Port Management & Operations”, Taylor & Francis/CRC, 392 pages, 1st edition.
- 6) Burns M. 2014b. “Logistics and Transportation Security”, Taylor & Francis/CRC, 350 pages, 1st edition.
- 7) Burns M. 2014c. Intermodal Transportation and Marine Transportation Security: Strengths, Weaknesses, Opportunities, and Threats Analysis. Washington DC: TRB - Transportation Research Board of National Academies, Supply Chain Security Sub-Committee, January 14, 2014.
- 8) Department of Homeland Security (2012, 2013) Budget-in-Brief Fiscal Year 2012, 2013. www.dhs.gov.
- 9) Department of Homeland Security (2012) DHS Strategic Plan, 2012-2016, www.dhs.gov.
- 10) FEMA (2013) National Planning Frameworks. 2nd edition, May 2013.
- 11) World Bank 2010-2014
- 12) International Maritime Organization, ISPS, 2014.
- 13) International Standards Organization, ISO, 2014.
- 14) TAPA, 2014
- 15) US CBP, 2014.
- 16) World Customs’ Organization, 2014.
- 17) World Trade Organization, 2010-2014.