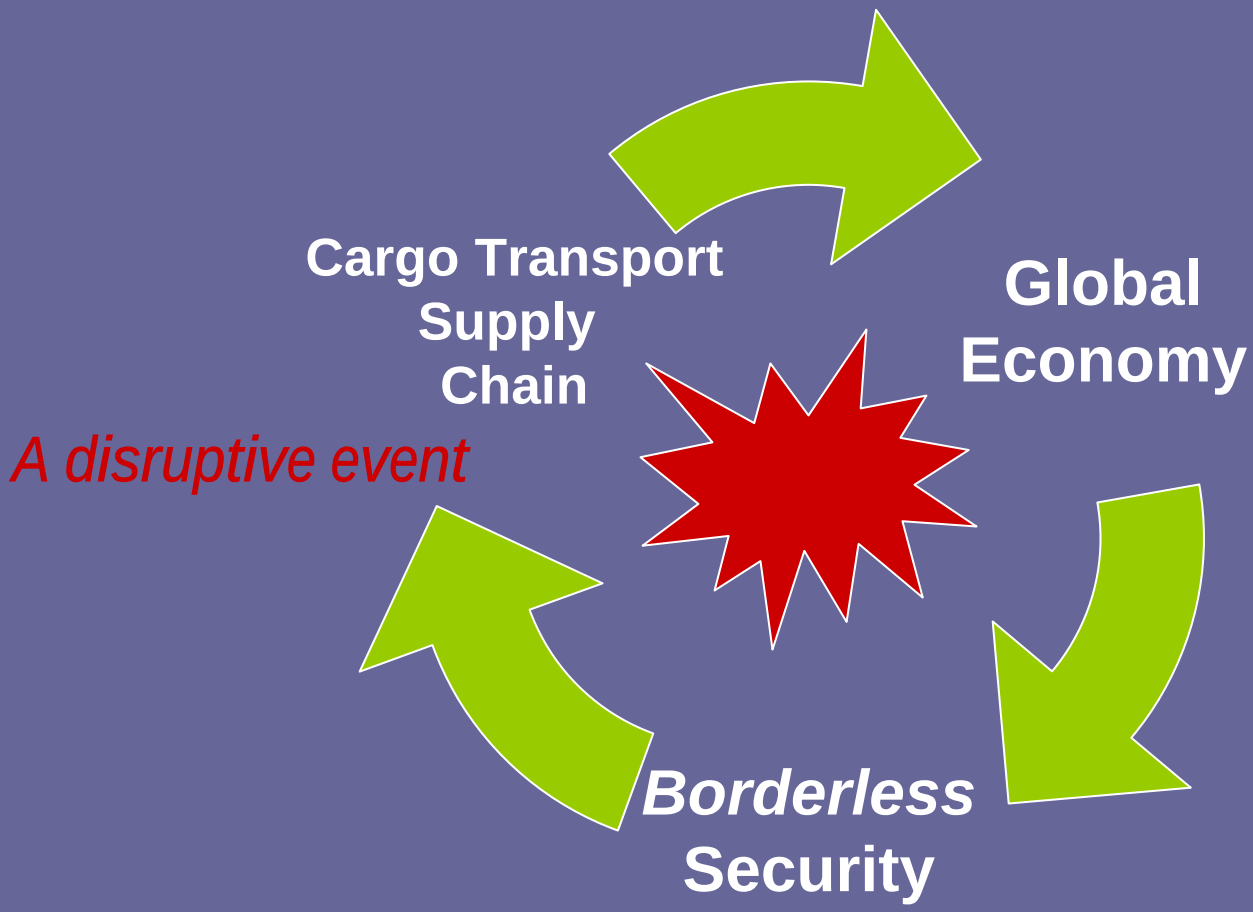
Network Centric Principles and World Cargo Security

Salvatore Fiorillo
TheoSecurity
Email: sfiorillo@theosecurity.com
Barbara Torell
Leibniz Open University
Email: batorell@tin.it

The Maritime Security Dilemma:

supply chain efficiency in a borderless environment



McLean's '*Container Revolution*' in 1956

- Malcolm McLean, an American trucking magnate, concluded that ports were disorganized, chaotic places
- He created a standardized container:
  - *the basis for today's global supply chain*

» *Fifty years later:*

Maritime trade has increased 220%

Should the supply chain layout be reviewed?

What has changed since 1956?

- The maritime industry's growth rate doubles every 5 years
  - 90% of which goes by standardized containers
  - U.S. ports move 45,000 containers daily
  - By 2010, estimated increase: 75,000
  - 23 million containers enter US yearly
- Over 6 billion tons and 60% by value of total world trade goods
  - **carried by sea**
- Millions of containers are moved worldwide annually
  - Yearly=40% of the world's crude oil passes through
    - The Strait of Hormuz and will rise to 60% of oil traffic by 2025
  - Daily=37 million oil barrels pass through 6 sea straits ($2557 M/d)

Vulnerabilities-Risks-Threats

- **Vulnerabilities**
  - Crucial trade routes [Straits of Malacca, Hormuz, Bosporus, and Suez]
  - Bulk cargo vessels [sub-standard and aged]
  - LNG\LPG carriers **[liquefied natural gas & liquefied petroleum gas]**
  - Non-responsible ownership [unknown, opaque and potentially open to piracy or terrorist organizations]

- **Risks**

  Potential danger:
  - Bulk vessel cargoes as missile or chokepoint barrier to Straits

  Potential for rogue collaboration:
  - Criminal gangs, pirates and terrorist in Southeast Asian waters disrupting crucial passages:
    - **Affecting Middle East oil exports to Asia**
    - **Causing huge trade breakdowns**

- **Threats** [mostly unfulfilled]
  - Potential to disrupt world trade and inflict economic slowdown
  - Potential to disable the geopolitical structure

Why is maritime cargo security so vulnerable to terrorism?

- Maritime global trade benefits from *"relaxed"* regulations:
  - through the use of *Flags of Convenience*
- Maritime transports have a history of:
  - Trafficking in arms, WMD, human beings, stolen goods and narcotics
- Maritime threats form a composite:
  - *pirate/criminal /terrorist*

Scenario Actors

- State Actors
  - Iran ?
  - North Korea ?
- Non-State Actors
  - Pirates
  - Criminals
    - Organized crime
  - Terrorists

The Exploiters:

Unknown Actors

- Untraceable “shell” companies
- “Ghost” fleets [leased or owned]
- ***Flags of Convenience*** [FOC]

  --purchased from sovereign states:

  [e.g. Liberia, Cambodia, Cyprus, Slovakia etc.]

U.S. Initiative Agreements-
"Are they mere Band-aids?"

"Some deter but all remain vulnerable to security breaches"

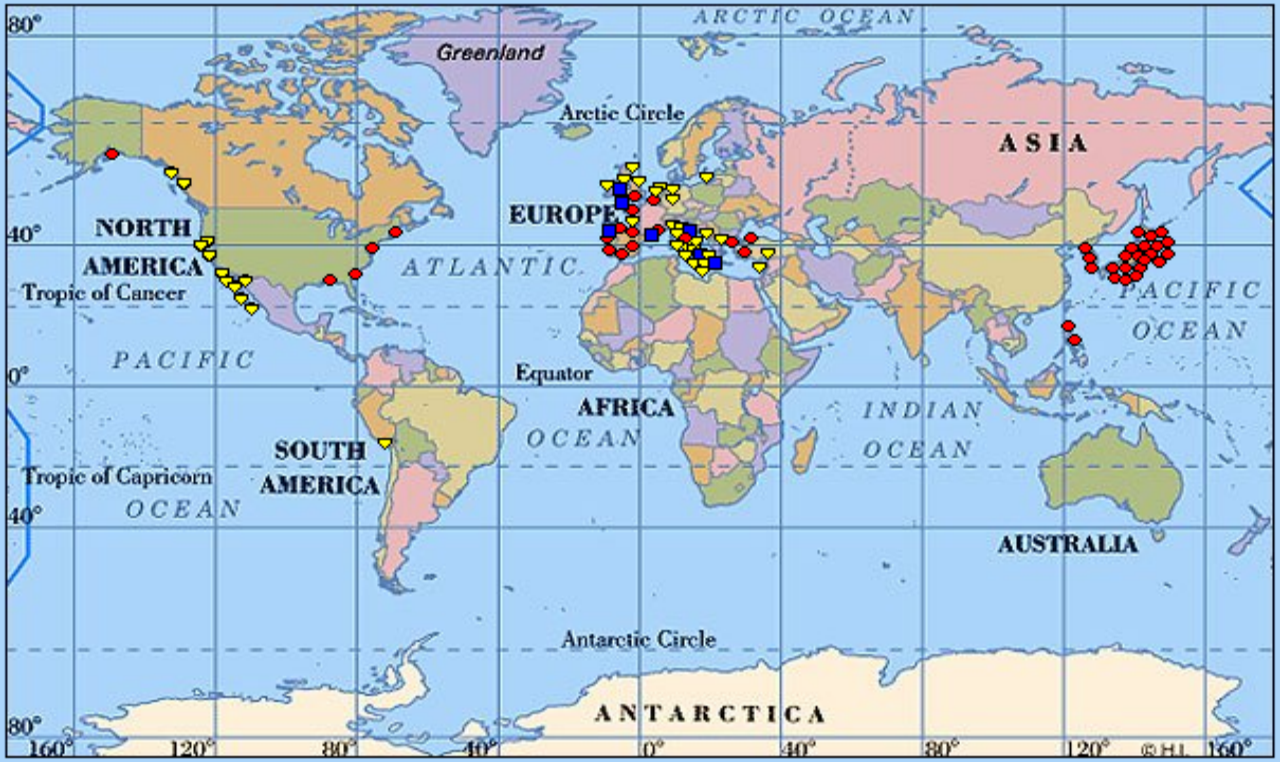
- CSI — *Container Security Initiative*
  - Voluntary cooperation with few guarantees
  - 'Many competing technologies'
  - Too early to estimate whether "smart and secure" containers will deliver the "goods" without incident
- C-TPAT — *Customs Trade Partnership Against Terrorism*
  - Multi-layered program to detect & prevent weapons entering U.S. through containers
  - Technology & other resources cannot keep up with security breaches
- PSI — *Proliferation Security Initiative*
  - Violates International Law of the Sea
  - Useless since FOCs *(Flags of Convenience)* defy detection

MARITIME

“BATTLESPACE”

Potential Scenarios

THE BATTLESPACE



Major Liquified Natural Gas [LNG] World Facilities

What to do?

Command and Control in a networked era

From a Monitoring Point of View:

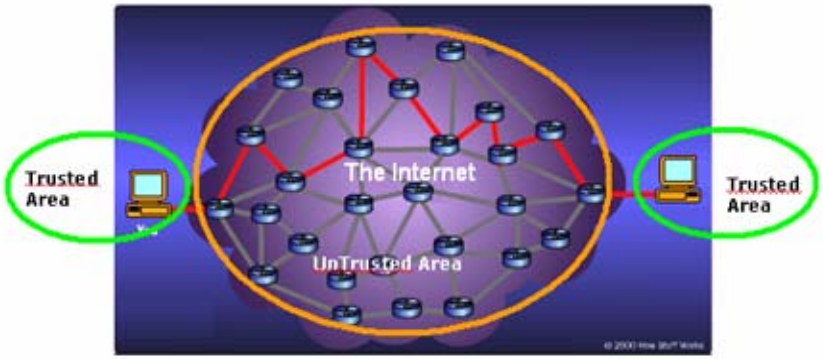
- There are few differences between physical and information goods
- Both share common principles:
  - The Security Chain: *Confidentiality, integrity, and Availability*

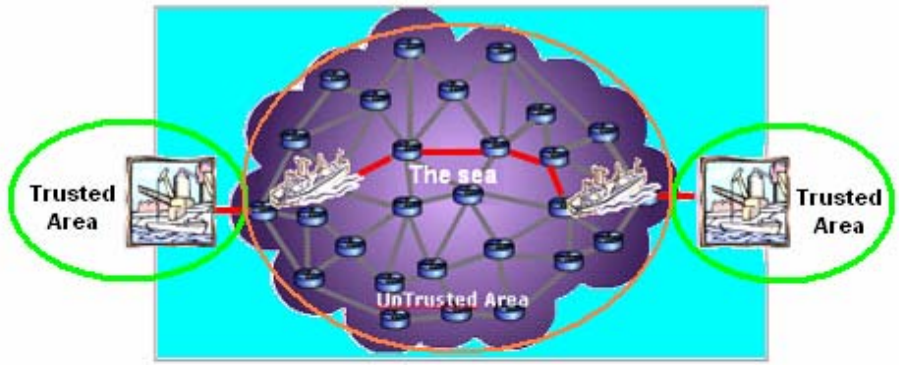
Universal Security Principles

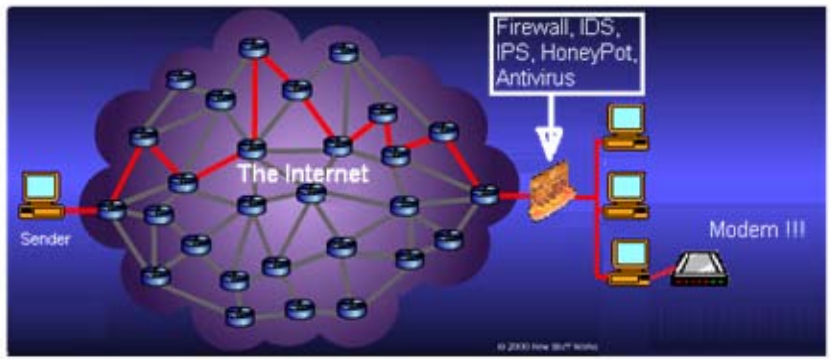
- **Confidentiality =**
  - **Hacking into the 24-hour-cargo manifest database presents opportunities for gaining intelligence on maritime transport movements and company relations**
- **Integrity =**
  - **A malicious payload (WMD, chemicals etc.) in a *legitimate* container, allows for the unauthorized cargo delivery behind secure borders**
- **Availability =**
  - **Directed to vessels (motive= hijacking or disruption)**
  - **Directed to the receiving facility**
    - **leading to an explosion of WMD, dirty bombs, or LNG tanker/ crude oil vessel**

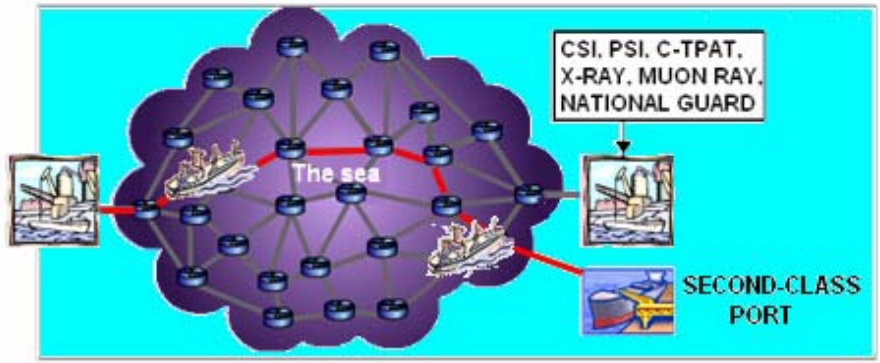
Cyberspace and open sea

- Some analogies between the internet and the open sea: both are *un-trusted—un-trustable* mediums









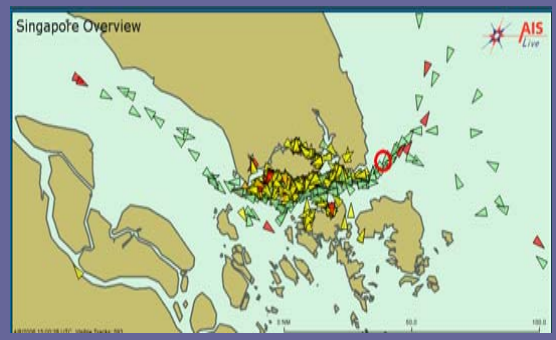
Some examples of adapted attacks

- *Reconnaissance*
  - Profiling the enemy and gaining intelligence
- *Covert Channel*
  - Communicating secrets in open space
- *Spoofing Attack*
  - Masquerading and pretending
- *De-fragmentation*
  - Small seemingly innocuous parts reassembled as in a puzzle

Reconnaissance with free monitoring tools

New York

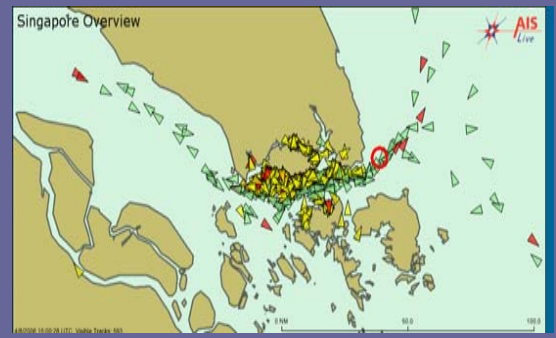
Strait of Hormus



Rotterdam

Shanghai

Kobe



Singapore

MMSI	563174000	Last seen at	4/8/2006 15:44:47 UTC
Name	GOLDENSARIINDAH	Latitude	N 40°35.320'
Callsign	9VVB	Longitude	W 74°01.990'
IMO number	8408715	Heading	2°
Length	197 m	Speed	1.8 knots
Beam	30 m	Destination	NEW YORK
Draught	7.0 m	ETA	4/8/2006 9:00:00 UTC
Vessel Type	Cargo	Status	Under way using engine
Extra Info	N/A		

Covert Channel

Covert messaging

Without the use electronic devices

A useful technique based on location and color of a particular container

"Arriving with stolen goods"

"Something is wrong. Goods not loaded"

"Warning!" "Police on board"

A Van Riper-type project

Spoofing/Masquerading Attack

“What you see is NOT what you get”

The *real Kono*
a trusted vessel

The *spoof Kono*
a masqueraded vessel

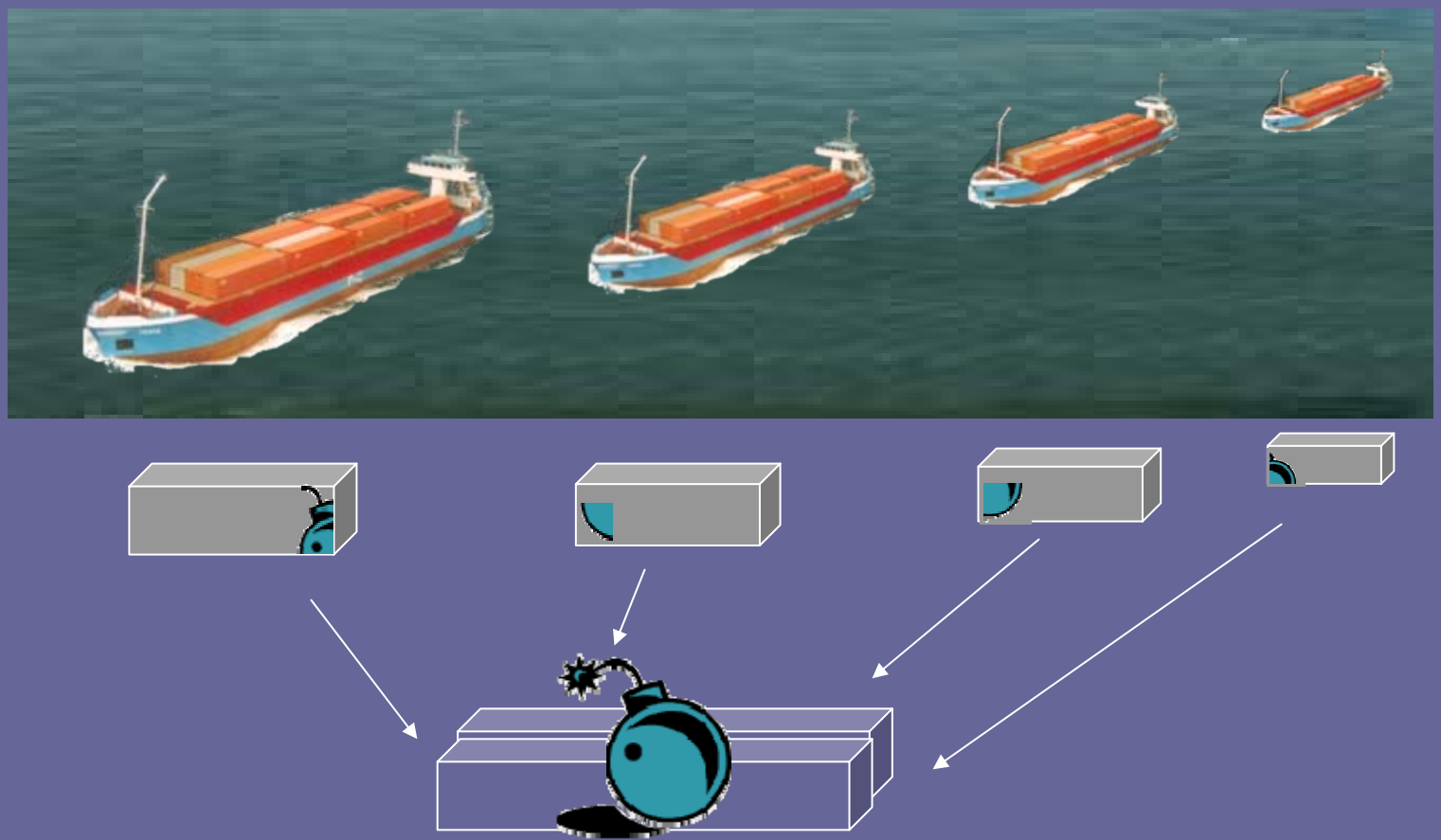
The Flags Of Convenience (FOC) variant

Kono: A French vessel

Kono: A Dutch vessel*

Extension of Defrag attack

Multiple ships carrying rogue payloads that only become visible when all parts are assembled



The De-Militarized Zone (DMZ)

- Few maritime receiving infrastructures are designed to protect the surrounding area from the most recent types of attacks
- As a security zone, a DMZ provides a buffer between the un-trusted outside and the trusted inside area (reflecting the Defence-in-Depth principle).
- LNG receiving facilities (usually set miles from a coastline) are credible examples of such implementation

The "Curse" of Probabilities

"The terrorists only have to get lucky once,

-- we have to get lucky every time"

[Intelligence officer quoted in Flynn 2006]

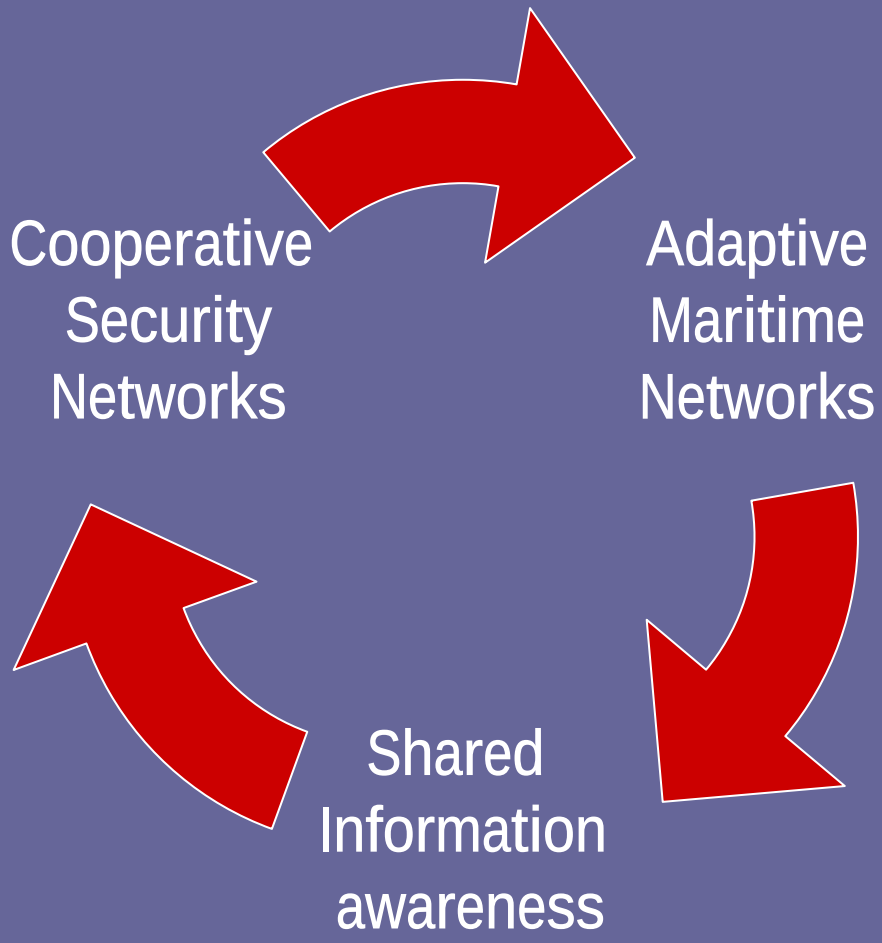
Reality Checks:

A borderless world does not deliver "borderless security"

- Stop expecting security guarantees
  - ***There are none***
- "If you look at everything,
- ***you will see nothing"***
- "Treating every case equally is yielding the statistical advantage to terrorists"

How do we improve the odds?

A Way out
of the Security Dilemma



Part Two

Entropy of systems

An Analysis of Actors:

A focus on how to manage the inner force

With

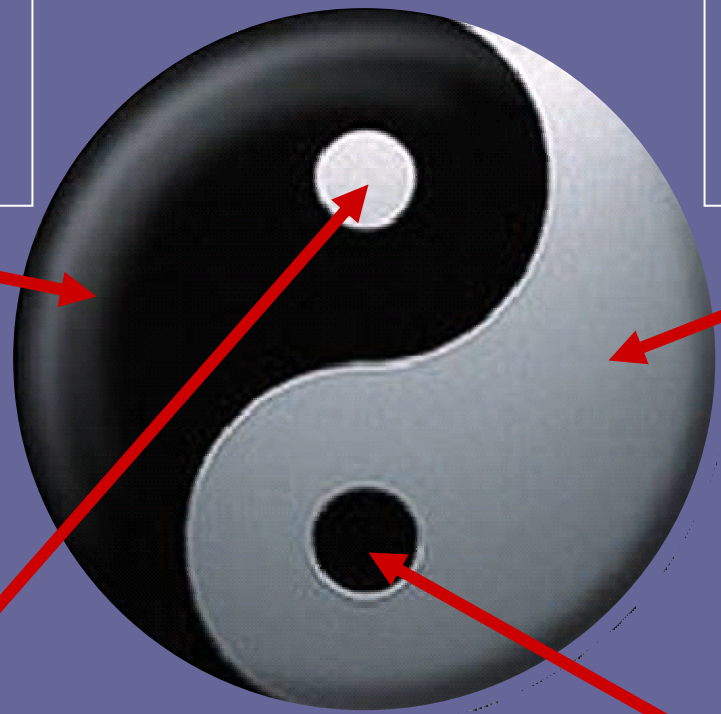
Complex Adaptive Systems

A Complex Adaptive System

Unreliable & Un-trustable Components (Low Doctrine)

Reliable and Trustable Components (High Doctrine)

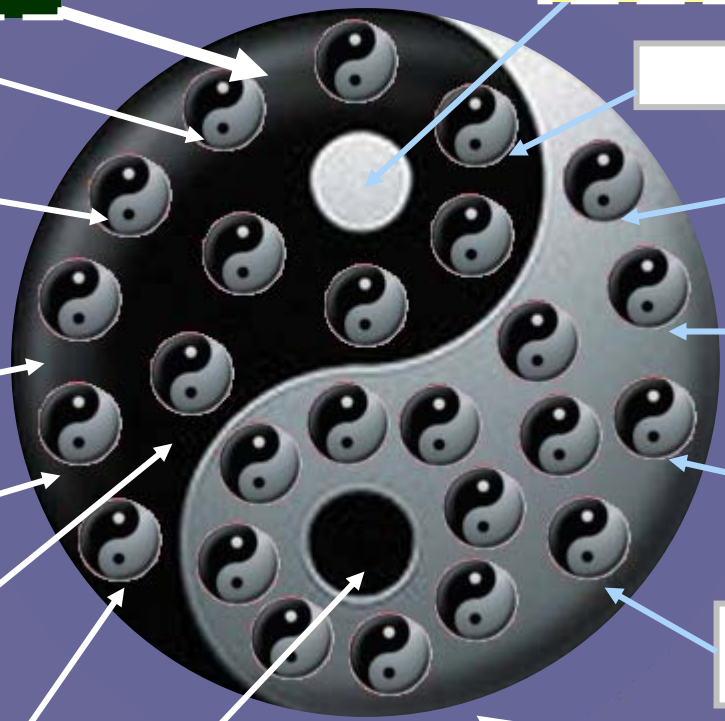
Bureaucracy



Efficiency

Wrongly Estimated Resources – Under Cover Entities (Entropy of CAS)

CAS versus CAS



Black-Hat Complex Adaptive Systems (BH-CAS)

National Set & Prison Gangs

Hawala & Money Services Business

Immigrant Smuggling Networks

Front and Shell Companies

Transnational Criminal Organizations

Terrorist Groups

Under Cover Entities Effects of EBO of BH-CAS

Under Cover Entities Effects of EBO of WH-CAS

Police Depts.

Distributed Awareness Programs (i.e. C-TPAT)

Federal Agencies

Military Bodies & Top LEAs

Intelligence Gathering and Disseminating Agencies

White-Hat Complex Adaptive Systems (WH-CAS)

Need to Know - Need to Share

- The ***need to share*** (mainly after 9/11).

- Why is it not happening?
  - Top-Down approach (“*I’m more important than you, so you have to grant more support than I have”*)

  - Bell-La Padula limits (integration with *agility* and *edge empowerment:*
    - *Fixed* by initiatives such as DHS-Information Sharing Act, PCII training, development of ISE-the central fusion role of DHS-IAIP, and some others. (*Good, when they work.)*

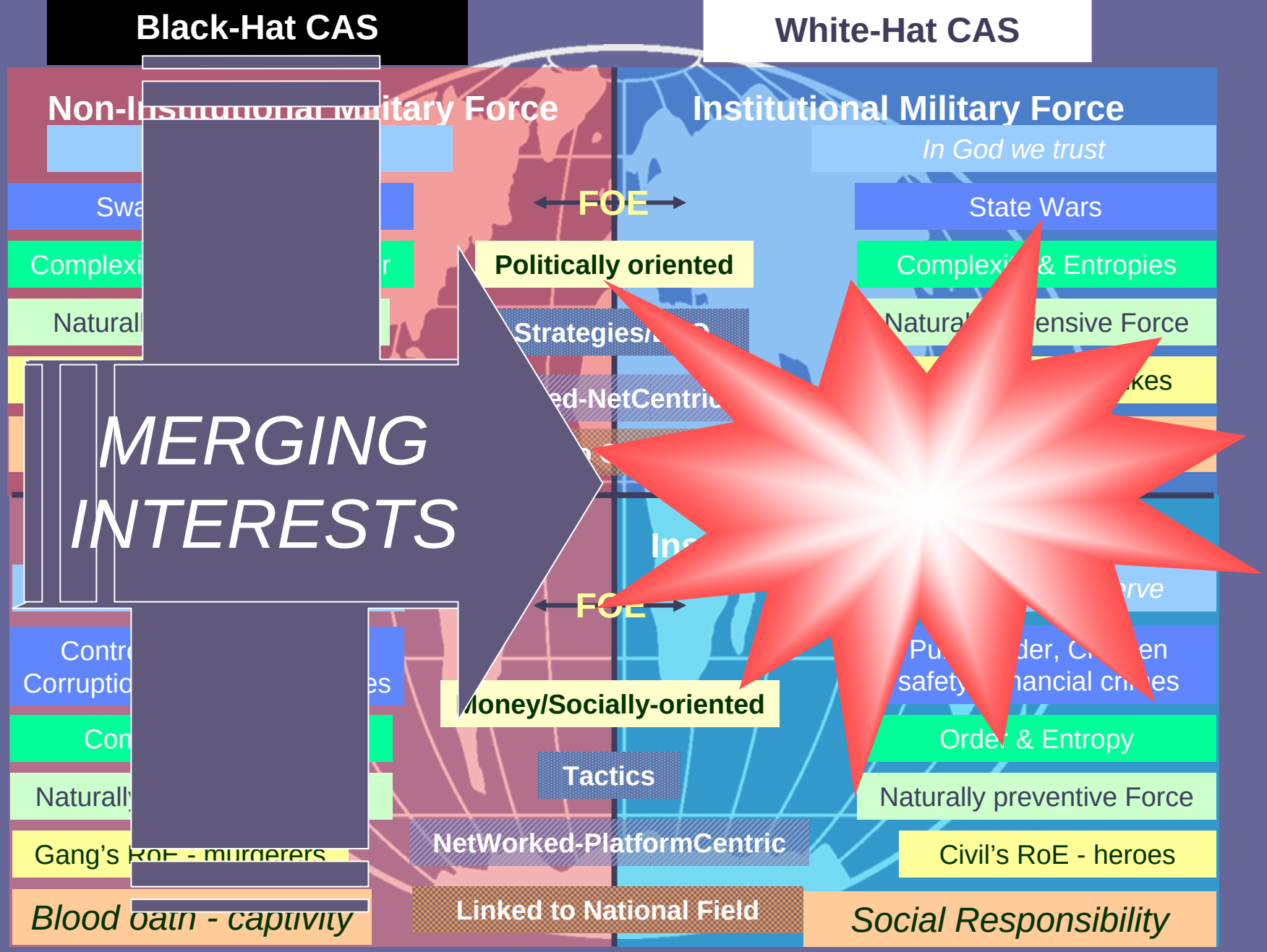
  - Lack of Common Sense-making
    - ***The Need To:***
    - Share more outcomes than outputs **(*avoid information flooding*)**

Demonstrating “The Big Picture”

- ***The Next Slide demonstrates what actors-on-the-ground might look like***

The Black-Hat Community

- Actors setting unconventional time-based or target-based organizations
  - ➢merging their efforts and know-how for faster and better control over their targets


Black-Hat CAS
White-Hat CAS
Non-Institutional Military Force
Institutional Military Force
In God we trust
FOE
State Wars
Politically oriented
Complexity & Entropies
Natural Defensive Force
MERGING INTERESTS
FOE
Money/Socially-oriented
Order & Entropy
Tactics
Naturally preventive Force
NetWorked-PlatformCentric
Gang's RoE - murderers
Civil's RoE - heroes
Blood oath - captivity
Linked to National Field
Social Responsibility
Reason to fight
How they fight
Network Characteristics - 1
Network Characteristics - 2
Rules of Engagement
Personal Motivation

Concluding Remarks

- To be “smart and secure” is hardly an option and maritime transport remains at risk in the following areas:
  - Disruption of cargo supply chain
  - Disruption of major passage ways
  - Disruption of the global market economy

- Responses to Terrorist threats:
  - Respond to changes in registering and monitoring FOCs
  - Respond to the need to re-organizing transport practices
  - Respond to requests for “standardized data transfer protocols”

- Vulnerabilities addressed:
  - External threats: asymmetric attackers will ever foul protecting sensors, but technology can help (us)
  - Internal threats: so long as the entropy of our systems is increased by a lack of cooperative honest and willing efforts, the defending machine will remain vulnerable.

References

- Akimoto, K. (2001) The current state of maritime security Conference paper Institute for International Policy 11-13 December 2001
- Benjamin/Simon (2005) *The Next Attack* New York-Times Books
- OECD (2003) Security in maritime transport: Risk factors and economic impact, *Maritime Transport Committee* July 2003
- Stearman, W.L. (2006) Iranian threat defined, *Iran Focus* 18 Jun 2006
- Timmerman, K.R. (2006) “Iran readies plan to close Strait of Hormuz” www.NewsMax.com March 1.
- Watkins, Eric (2004) Facing the terrorist threat in the Malacca Strait *TerrorMonitor*: Jamestown Foundation
- 2006 GAO reports (www.gao.gov)