Global Maritime Trends and Game Changers

- A recent National Intelligence Council Report identified trends and developments during the next 15-20 years
- The report provided an in depth analysis of megatrends and game changers
- The report identified trends that range from cyber security, and energy independence to an expanding middle class, and a growing food, water, and energy nexus

How Real is the Cyber Threat?

- According to the Repository for Industrial Security Incidents Database the transportation and water and wastewater industries have experienced large increases in reported cybersecurity incidents in recent years – 160% and 60% respectively

Can Cyber Terrorists Kill

- The good news is that this is a low probability
- The bad news is that cyber terrorists can, and have caused significant disruption and damage, particularly to industrial systems
- Because most of these systems are in the private sector and are not yet regarded as national security loopholes, they tend to be less secure than government and military systems.

Industrial Systems are Susceptible

- Although power grids, oil pipelines, dams, and water systems don't present opportunities as nightmarish as nuclear weapons, they nonetheless are capable, under the wrong hands, of causing their own mass destruction.
- In addition, companies increasingly use the Internet to manage such processes as oil-pipeline flow and water levels in dams by means of "supervisory control and data acquisition" systems, or SCADA, which confers remote access.

The Targets

- The targets have primarily been energy companies and the attacks appeared to be probes, looking for ways to seize control of their processing systems
- The attacks are continuing but it is uncertain exactly where they are coming from, or whether they were state sponsored or the work of hackers or criminals

From Espionage to Sabotage

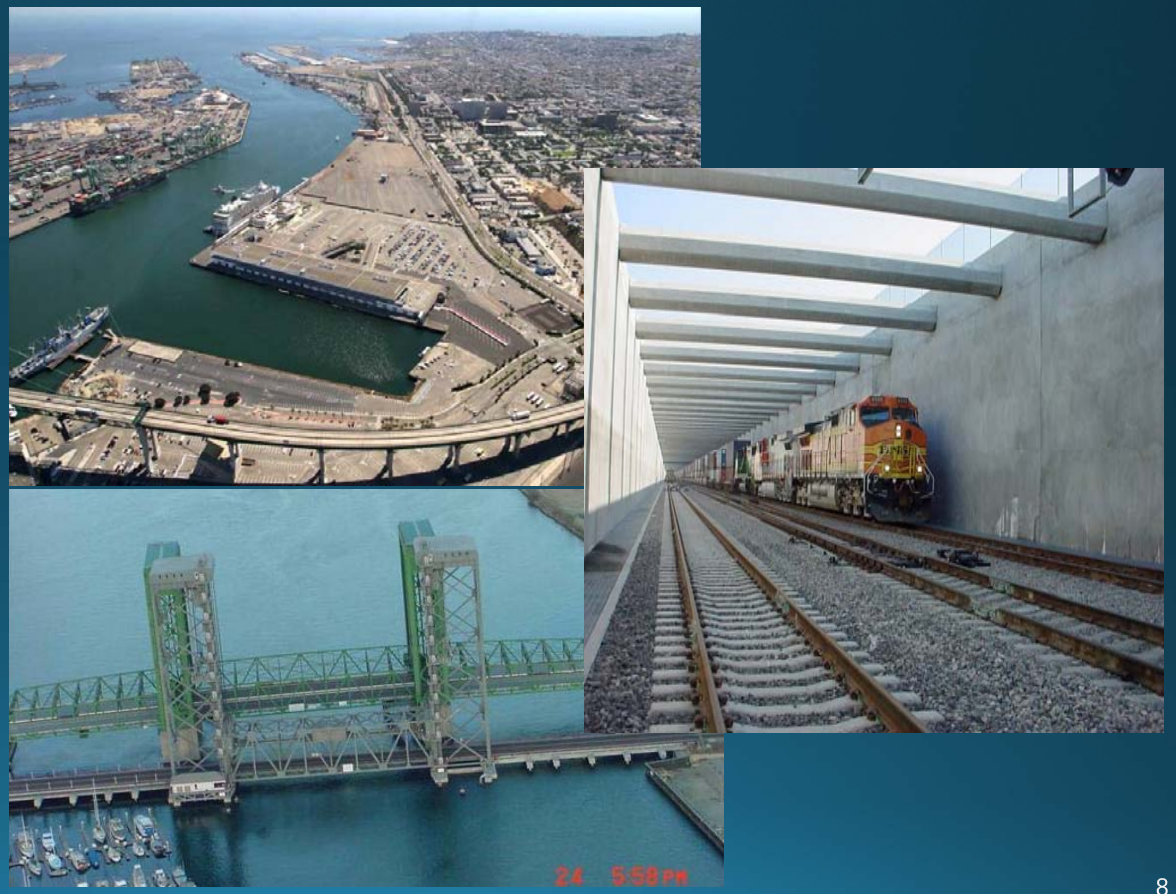
- Earlier attacks on industrial systems focused on gaining information, or probing ways to seize control of processing systems
- Recent attacks seek to destroy data or to manipulate industrial take over or shut down the networks
- This was the case with the attack on Saudi Aramco which took over 30,000 computers

What About Ports and Maritime?

- Ports and maritime are susceptible to attacks. This susceptibility was outlined in a recent Brookings report by Commander Joseph Kramek
- The report points out that U.S. port facilities rely as much upon networked computer and control systems as they do upon stevedores to ensure the flow of maritime commerce that the economy depends upon

The Brookings Report May Have Understated the Problem

- The report looked at ports as an independent industrial entity and not as a system
- A port is a system of systems that work together that includes vessel traffic, rail, bridges, roads, trucking and terminal operations
- An attack on any of these systems could cause significant economic damage



Have Attacks Happened in Ports?

- A Netherlands based drug ring recently hacked into the operating systems of two terminals to change the location and delivery times of drug laden containers
- This was not the first and wont be the last such attack
- What if the hackers took down the systems, or changed the location of every container
- How long would it take to fix the problem, and at what cost?

Who is Involved in Cyber Terrorism?

- Cyber terrorism is scary because it is sponsored by Countries, Non-State Actors, Splinter Groups, or Individuals
- The attack can be perpetrated from long distances
- It is sometimes done by individuals with no motivation other than they see it as a challenge
- As technologies evolve more vulnerabilities are created