Maritime Systems Security

Port Security Seminar & Exhibition

20 - 22 July 2011, New Orleans, LA

Charles McCarthy

John A. Volpe National Transportation Systems Center

U.S. Department of Transportation

Research and Innovative Technology Administration

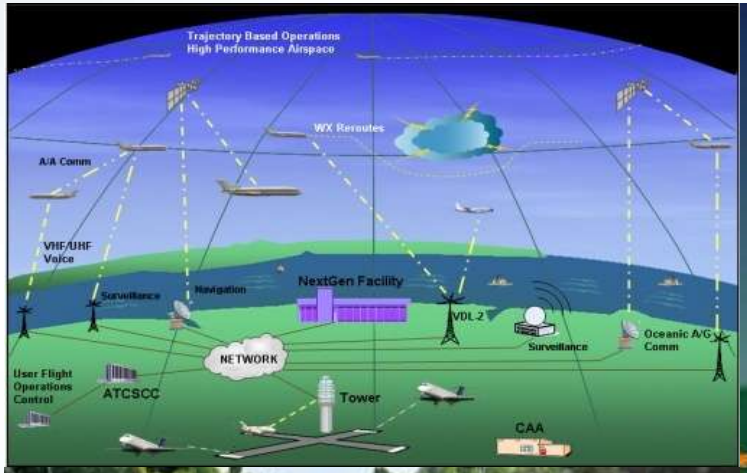
An Introduction to the

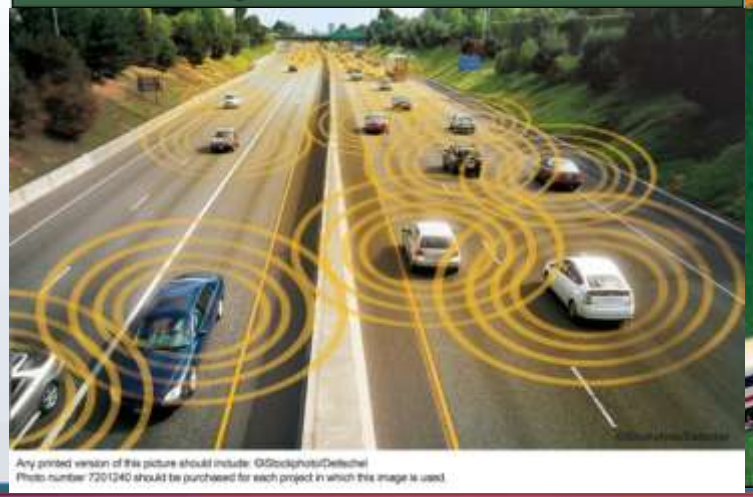
John A. Volpe National Transportation Systems Center

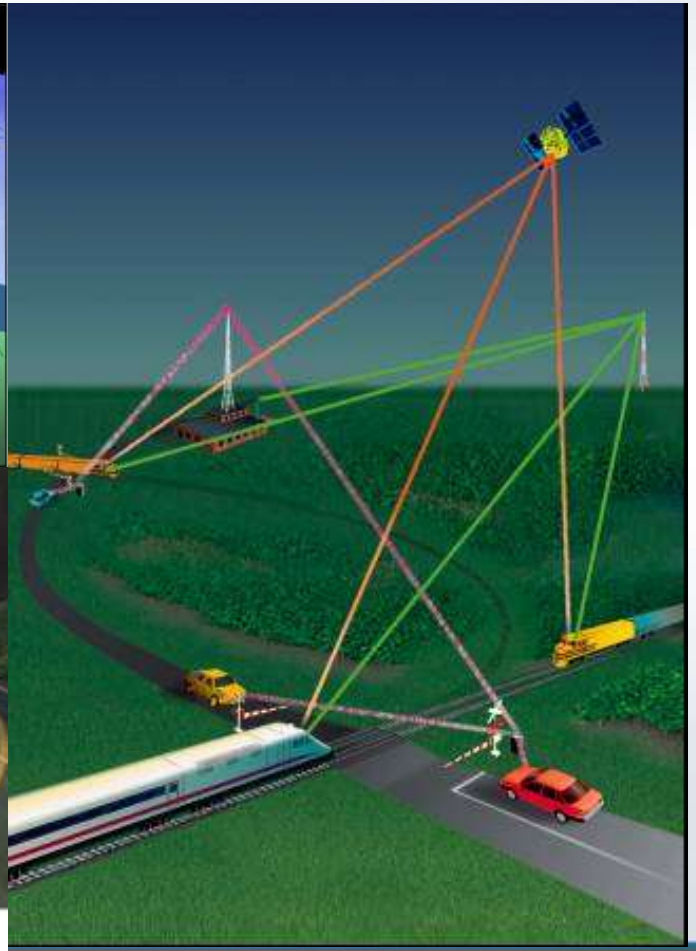
Serving the Nation as a leader in global transportation innovation since 1970

RITA John A. Volpe National Transportation Systems Center
U.S. Department of Transportation

We're Increasingly Dependent on Net-centric Operations and Wireless Communications

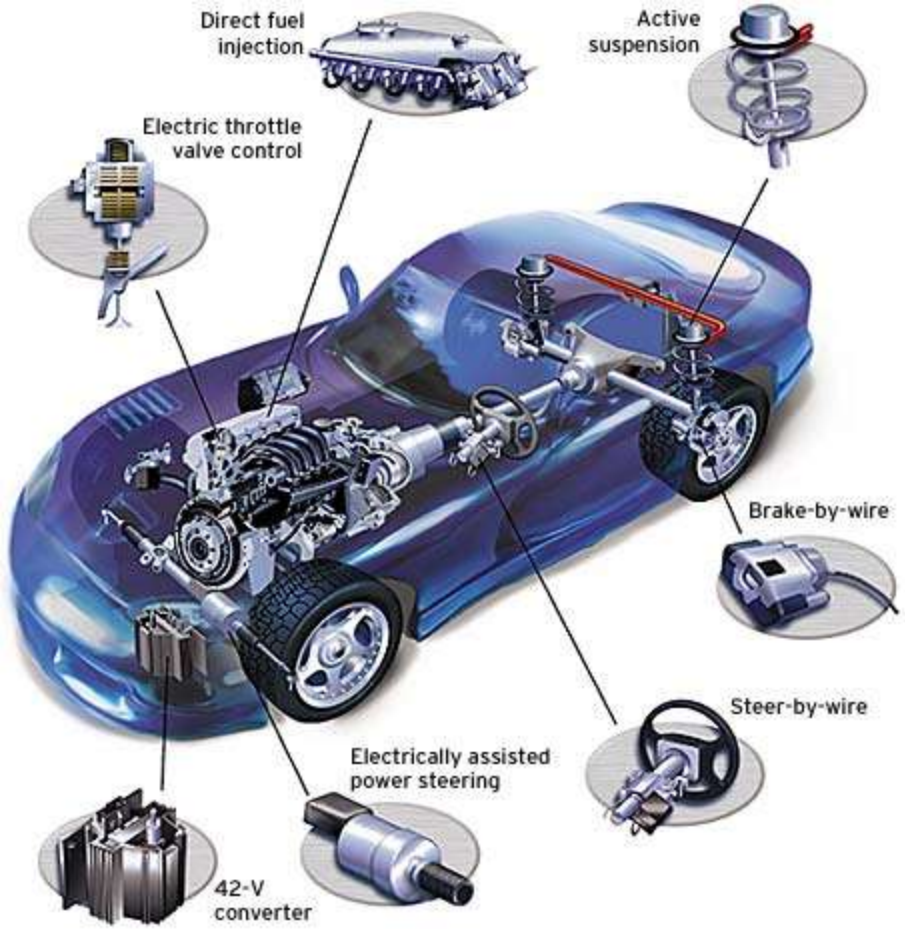






E-enabled vehicles are now the norm…

…for all of us!



Source: aa1car.com

We're Demanding & Exploiting Connectivity

4G Technology at 2011 Consumer Electronics Show

GM OnStar MyLink
www.engadget.com

Hyundai Blue Link
www.latestcar.us

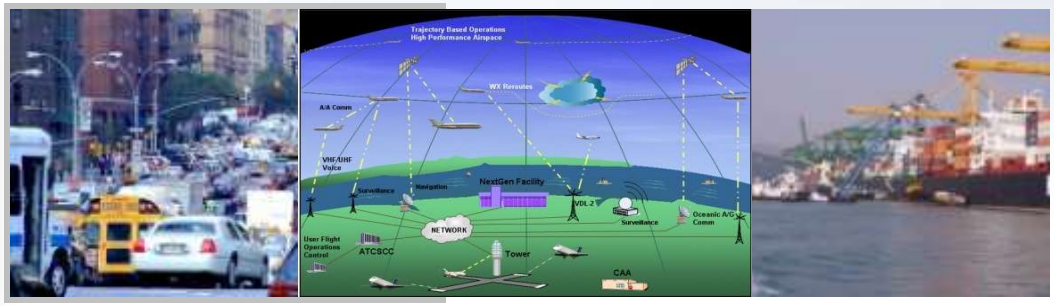
Ford MyKey
thetorquereport.com

Access vehicle diagnostics
Unlock doors
Slow cars down with geofencing
Limit driving speed of teens

"We're redefining what it means to be a really fast computer"
Audi Chairman Rupert Stadler

Research Systems & Their Strategic Importance in Transportation

Cyber-physical Control Systems



Traffic Control, Logistics & Operations Management Systems

Safety Management Systems

Traveler & Operator Services: “511”, E-commerce, E-payment

Intelligent Transportation System Vulnerabilities: Variable Message Signs on Highways Hacked

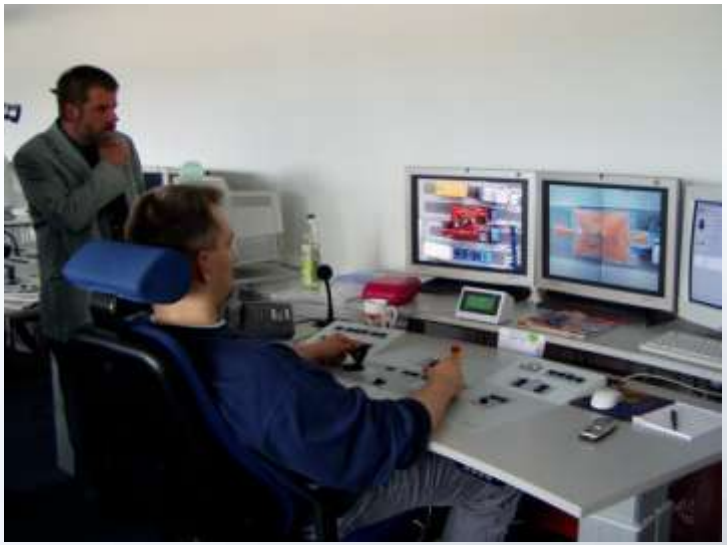
Hacking instructions were available on i-hacked.com.

14 Year Old Boy Derails Polish Trams with Modified TV Remote

Source: Telegraph.co.uk, 11 January 2008

Automated Maritime Systems

- Today's maritime environment includes automation throughout our nation's ports
  - Automated entry systems
  - Wireless cargo tracking
  - Driverless cranes and other vehicles



Terminal Automation

- **Information Technology**
  - Terminal Operation System (TOS)
  - Container Terminal Management System (CTMS)
  - Payroll, other back office systems

- **Communications**
  - E-mail, cargo messages
  - Website, cargo tracking
  - Wireless, cargo apps

- **Access Control**
  - Security / ID Card system
  - CCTV
  - Truck gates
  - Personnel gates

Terminal Automation

- **Scheduling Software**
  - Vessels
  - Yard equipment
  - Maintenance

- **Control Systems**
  - Seaside cranes
  - Yard Cranes
  - Other Yard Equipment
  - Remote monitoring
  - Buildings
  - Gates

Vessel Automation

- **Navigation**
  - Radar
  - Automatic Identification System (AIS)
  - Electronic Charts (ECDIS)
  - GPS
- **Communications**
  - Radio
  - Satellite
  - Broadband
    - Internet
    - E-mail
- **Integrated bridge**
  - All systems interconnected

Vessel Automation

- **Control Systems**
  - Main engine
  - Ballast tanks
  - Generators
  - Life support
  - Fuel & lube oil
  - Cargo hold fans
  - Water tight doors
  - Fire alarm & control

Automated Container Terminal Entrance

- Optical Character Recognition (OCR):
- Reads Vehicle & Container ID
  - License Plate
  - Container Number
- Imaging can also detect container damage

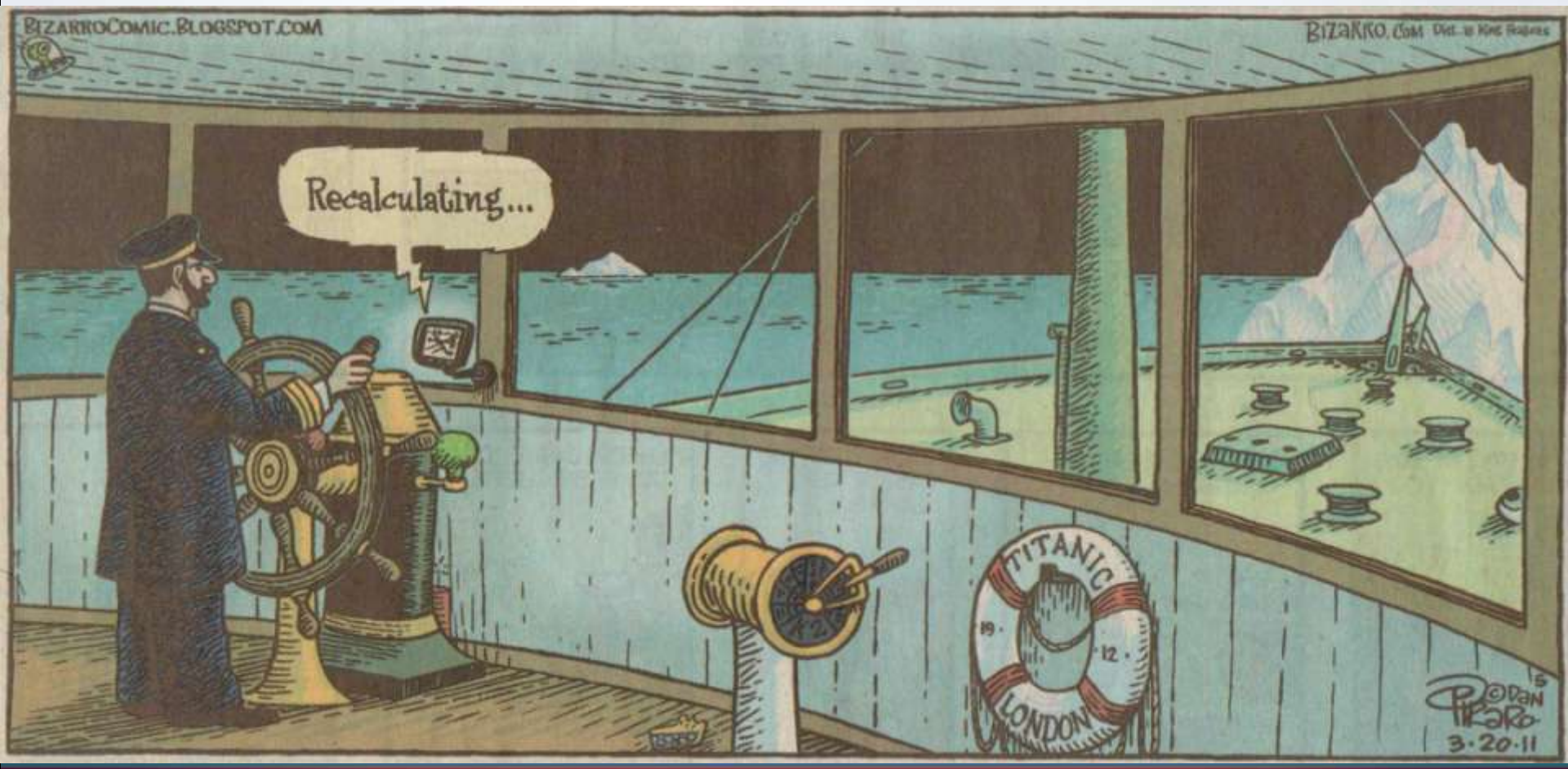
OCR & Image Capture

Driverless Vehicle

Hamburg Germany. Driverless vehicle moving 40’ container to automated storage crane.

Volpe Center Image

Automated Maritime Systems



Crane Accident

- Oakland, CA. Dropped cargo container.
- Is this a result of a Control System failure?

Dry-dock Malfunction

- Dubai. Opened sea gate while workers were under vessel resulting in 27 deaths and the loss of 2 vessels.

Navigation Malfunction

- Human error or equipment malfunction?

Navigation Error

- Rotterdam. Human error or equipment malfunction?

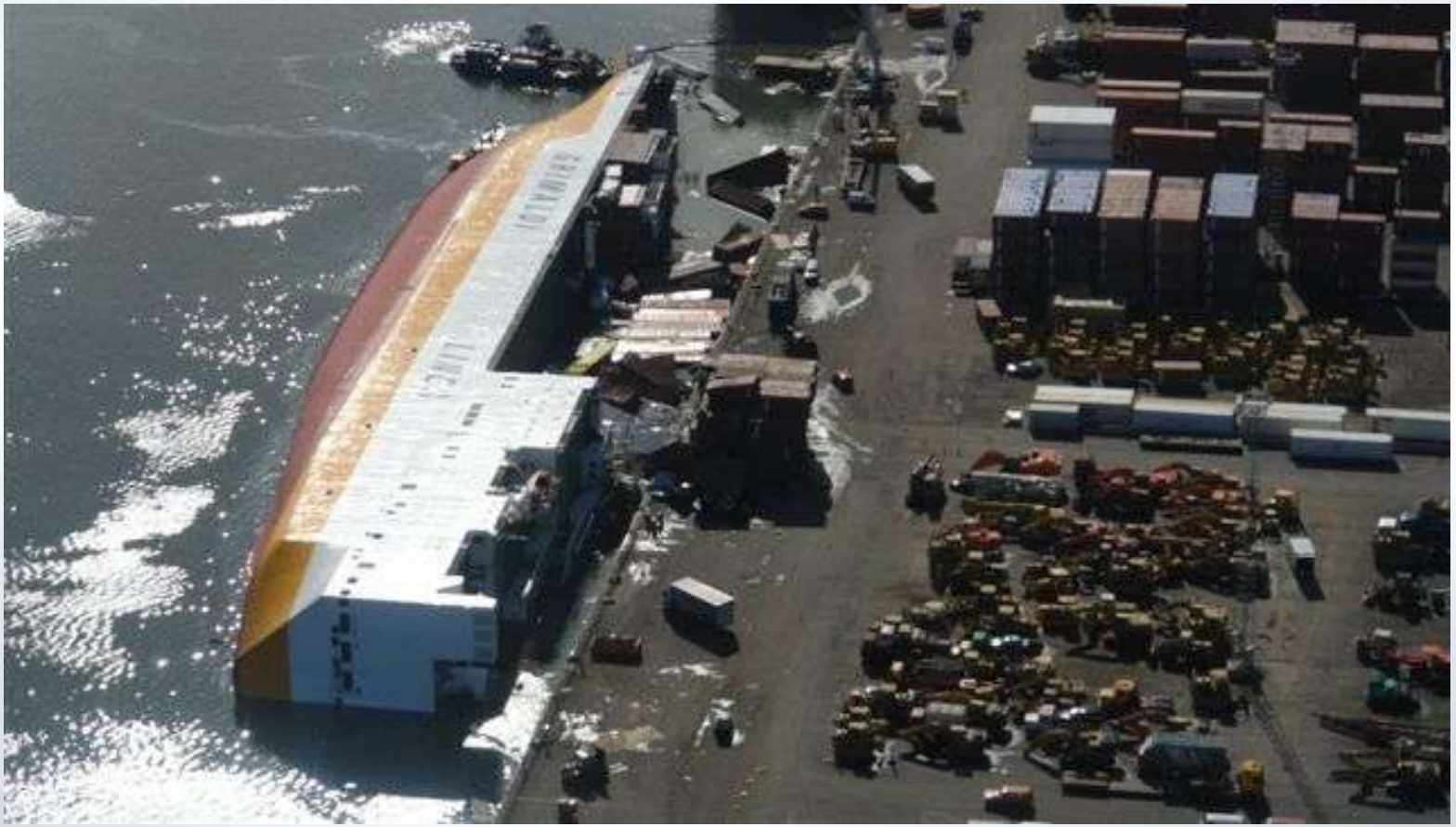
Vessel Balance Accident

Liberia. Vessel storage usually planned with bay planning software.

Countryman & McDaniel

Rollover Accident

- Antwerp 2007. Vessel unbalanced due to ballast tanks?
- Software or human error?



Fire Onboard

- Could bad planning software have made it worse?
- Hazmat too close together?

Vessel Accident – Bayplan Software

- **MV Annabella**
- Load plan/bayplan software did not recognize 30’ containers and assumed all were 40’.
- 7 stacked 30’ containers weighed 225 tons – no alarm
- Bayplan would alarm if 40’ container stack weighed 240 tons.
- Stack collapsed during voyage.
- 26 Feb ‘07

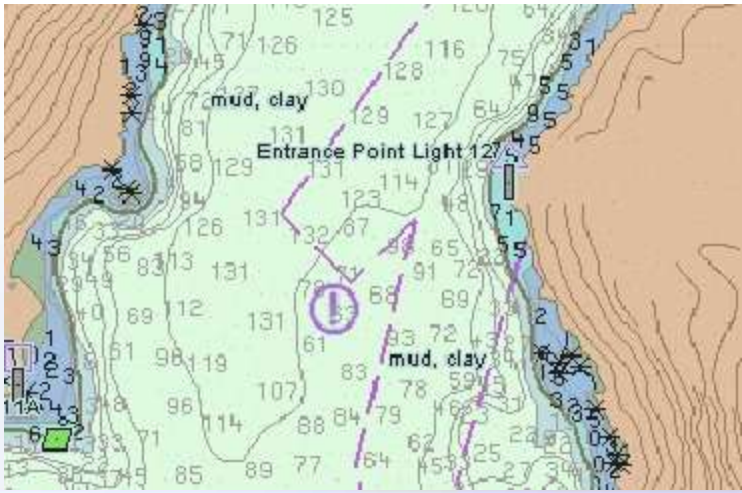
- Many terminals do load plan for vessels.

Vessel Accident

- **MV Royal Majesty – Bermuda to Boston**
- Integrated bridge, 2 GPS & electronic charts (ECDIS)
- Antenna line broke and GPS registered Dead Reckoning for 30 hours.
- DR is guess based on speed and heading.
- Crew didn't notice DR indicator light or 2nd GPS
- Crew thought radar signal of Nantucket Island was rain until they ran aground.
- Crew navigating solely with broken GPS.
- 10 June '95

Vessel Vulnerability

- **<u>Resolution of Electronic Charts</u>**
- Electronic chart display system (ECDIS)
- 2 different systems may show different underwater hazards even though settings are the same:
- Wrecks, rocks, & other underwater obstructions.
- Depends of settings of safety contour (depth)
- Crew must be familiar with system in use.



Botnet Threat

- Collection of remotely controlled robot agents
- On zombie (compromised) computers
- Sophisticated, advanced, persistent malware
- Run software autonomously and automatically

- Botnet controller then attempts:
- Denial-of-service attacks against online web servers, or
- Theft of data:
  - including bank account details,
  - credit card numbers,
  - user names,
  - passwords, etc.

Botnet Threat

- Botnet kits sold on the black market, or
- Illegal Warez sites
- Allows almost anyone to set up a botnet

- The Volpe Center discovered an illegal warez site on a ferry call-in and ticket purchase center.
- Site was so big, the ferry operator was about to expand their system thinking it was overloaded.

Botnet Threat

Top 10 Biggest Botnets*

1. TDLBotnetA
2. RogueAVBotnet
3. ZeusBotnetB
4. Monkif
5. Koobface.A
6. Confiker.C
7. Hamweq
8. AdwareTrojanBotnet
9. Sality
10. SpyEyeBotnetA

* from Damballa Inc.

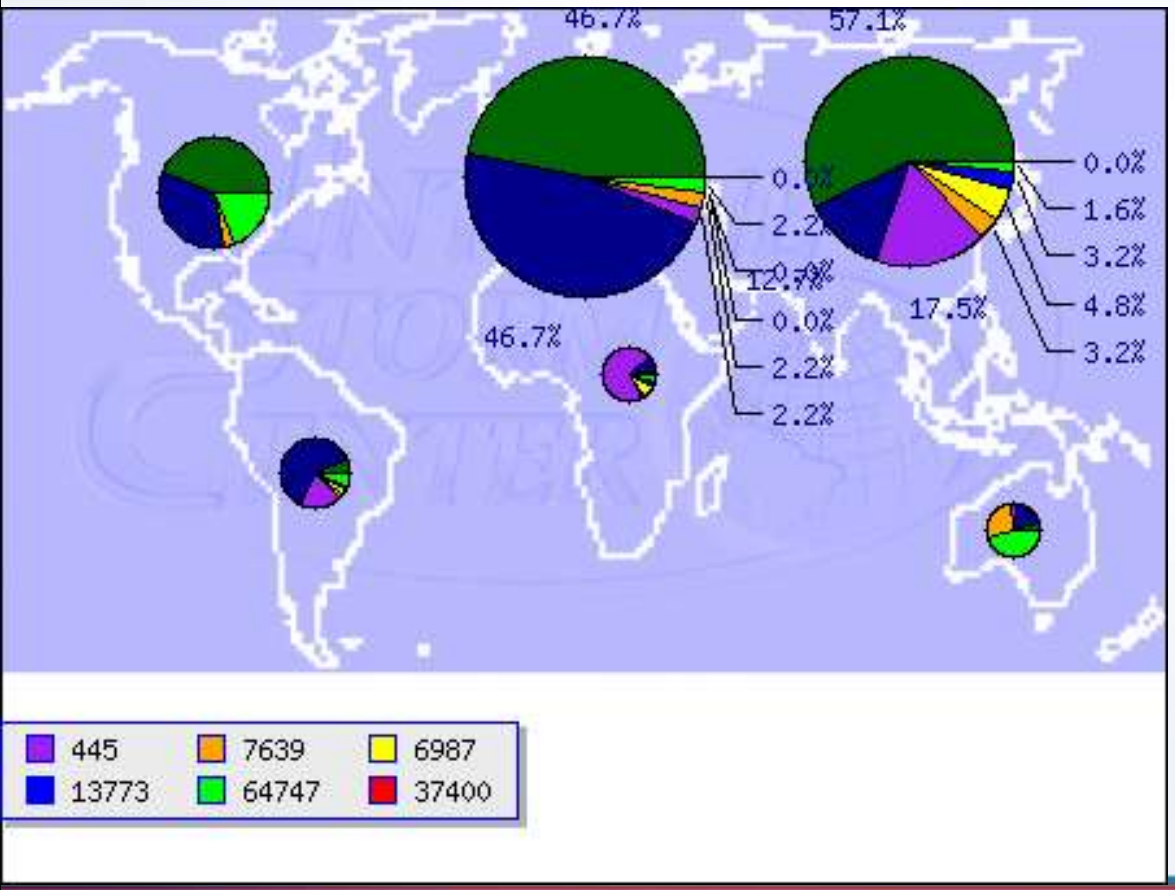
Botnet Threat

Stuxnet worm:

- Targets industrial control software and equipment
- Includes a programmable logic controller (PLC) root kit

SANS Internet Storm Center

- Publishes a world map with current computer port attacks
- **www.dshield.org**



Ports	Reports
445	306,700
1433	139,422
22	133,680
7639	128,434
5060	89,749
3306	87,129
80	86,160
37400	48,420
139	47,024
443	38,031

What To Do

- **Managing Risk**
- Threat & Vulnerability Analysis
- Free publication: NIST SP 800-53
- Guidelines for selecting security controls for IT systems
  - Includes control catalogue

- 3 categories:
  - Technical Controls
  - Management Controls
  - Administrative Controls

Where To Go For Help

- **DHS Control System Security Program (CSSP)**
- **Industrial Security Tools & Guides**
- DHS Cyber Security Evaluation Tool (CSET)
- DHS Catalogue of Security Recommendations
- Guide to Industrial Control Systems Security, NIST SP-800-82
- Recommended Security Controls, Appendix I – Industrial Control Systems, NIST SP-800-53
- http://www.us-cert.gov/control_systems/index.html

Where To Go For Help

FEDERAL

- DHS - Computer Emergency Readiness Team (CERT)
- NIST – Computer Security Resource Center
- USCG – Cyber Command, COTP
- TSA – TSS CWG
- FBI – Computer Crime Squad, SAC
- US DOT/ RITA/ Volpe Center/Infrastructure Protection

Where To Go For Help

Associations

- HTCIA [law enforcement, tech investigations, forensics]
- INFRAGARD [associated w/ FBI Computer Crime Squad]
- ISSA [computer security management]
- SANS [tech training]

Questions / Feedback

Charles J. McCarthy, JD
Maritime Project Manager
(617) 494-3469 (office)
(617) 512-4910 (cell)
Charles.mccarthy@dot.gov