

# HOSTIS ANTE NAVES

*the enemy at the ships*  
*ο εχθρός προ των πλοίων*



# HOSTIS ANTE NAVES

*Dimitris Moutzouris-Lygeros*

*Chemical Engineer, IT Engineer*

*ICS Security Analyst and Advisor*





# HOSTIS INTRA NAVES

*the enemy onboard*  
*ο εχθρός επί των πλοίων*





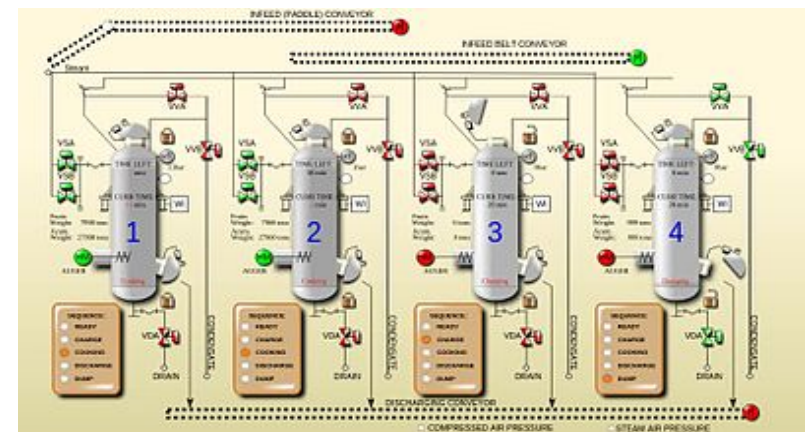
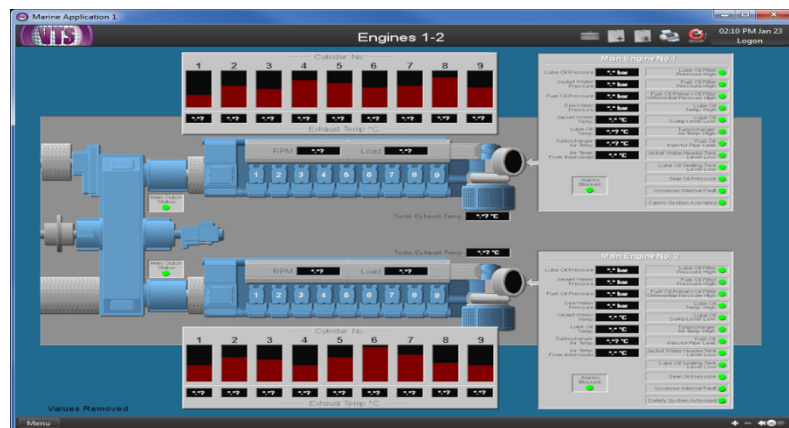




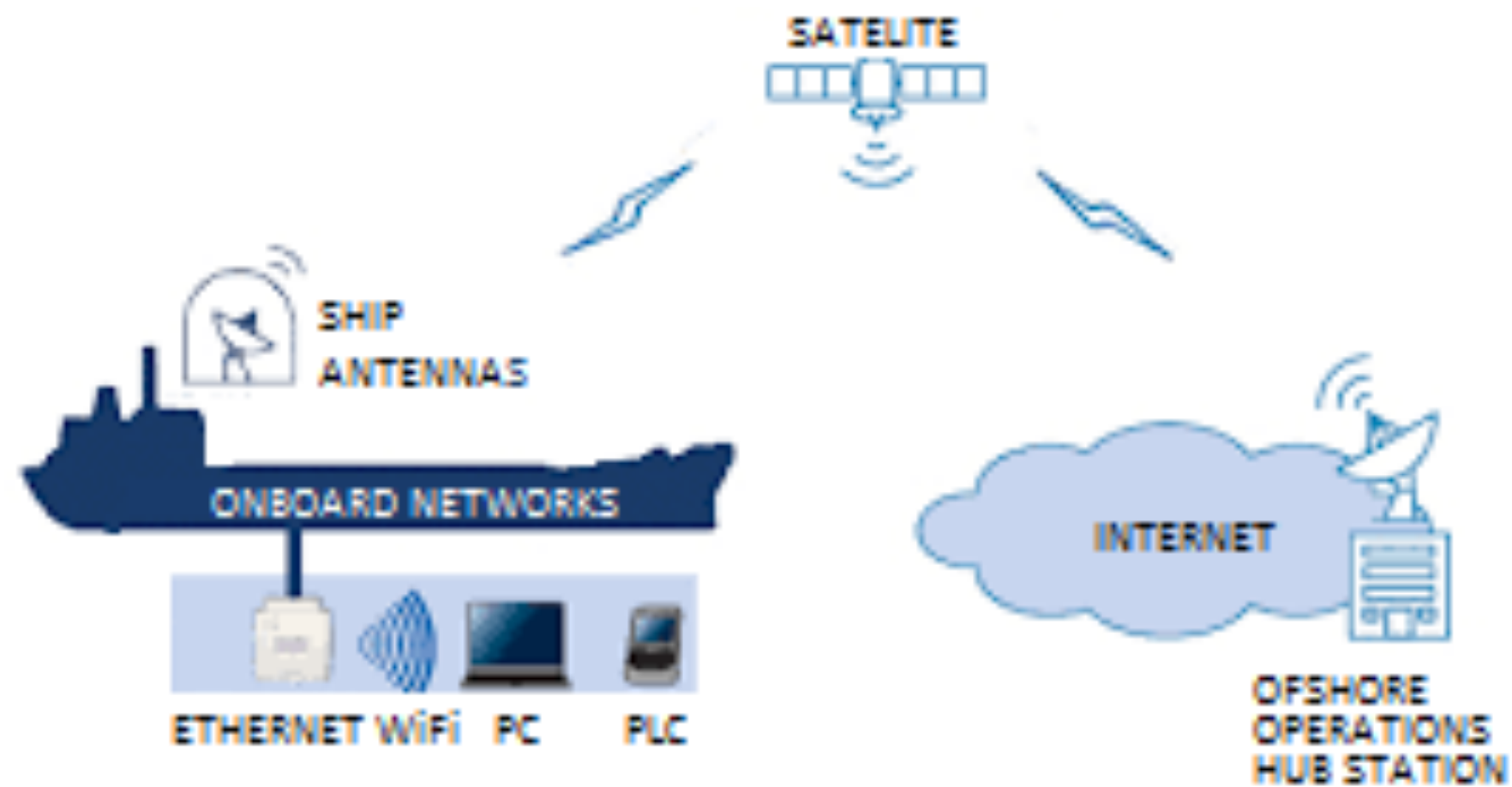
























ACCESS GRANTED

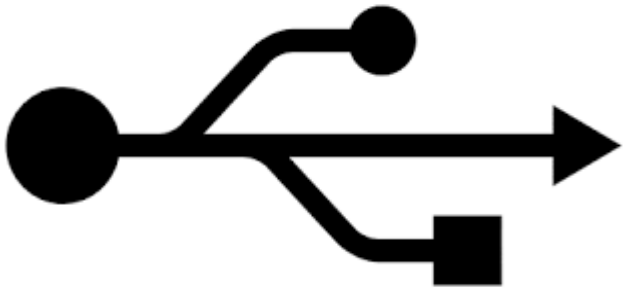






**Stealing, theft and security violation do not have to do so much with technology or required programming knowledge; but with the **inspiration** of the hackers who are willing to steal.**





**Stealing, theft and security violation do not have to do so much with **technology** or required **programming knowledge**; but with the **inspiration** of the hackers who are willing to steal.**





# CASE ONE

# STUXNET



# 2010



# STUXNET

- Is a malware
  - Is a worm
  - Belongs to the payloads category
  - Contains 5 vulnerabilities
  - 4 of them was “zero day attacks”
  - The code was written in various programming languages
  - The code was very big for a virus (~1,5 MB)
  - Affect Windows XP, Vista, 7, Server 2007, Server 2008
  - Avaya, Nortel, 3DM systems
- 
- The first variant appears in June 2009
  - The second, in March 2010
  - The third, in April 2010
  - Was discovered in June 2010
- 
- Using 4 known but un-patched “zero day attack” vulnerabilities, plus another one (known but unsolved0,
  - Using driver certificates original but stolen,
  - Using various servers worldwide,
  - Contain server and client parts in his code,
  - The client part contains two rootkits

# STUXNET



AFFECT THE IRANIAN URANIUM ENRICHMENT FACILITIES IN  
NATANZ FACTORY





# STUXNET



AFFECT THE IRANIAN URANIUM ENRICHMENT FACILITIES IN  
NATANZ FACTORY



# STUXNET

stuxnet

[All](#)

[News](#)

[Videos](#)

[Images](#)

[Books](#)

[More](#)

About 1,280,000 results (0.41 seconds)





# CASE TWO

# GPS SPOOFING



2013



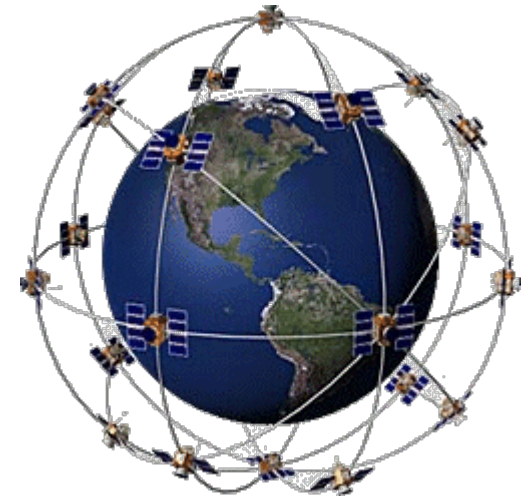
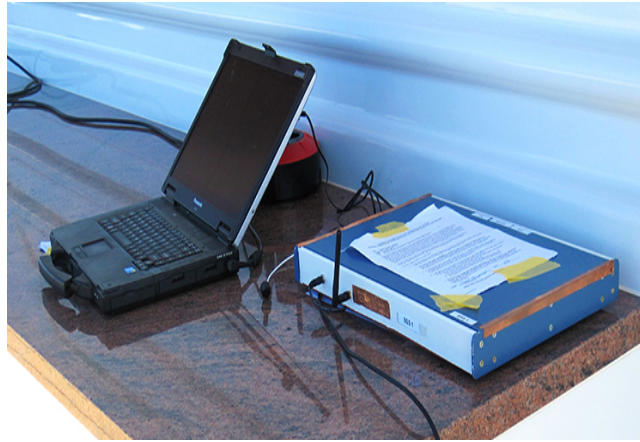
# GPS SPOOFING

- Summer 2013
- “White Rose” depart from Monaco to Creta
- 30 miles after Italian coast they proceed with the attack

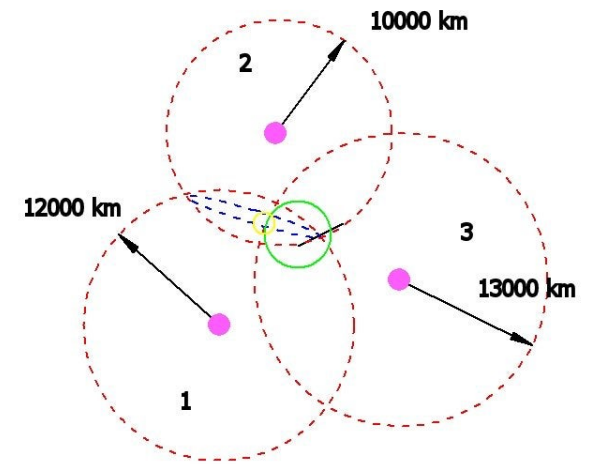
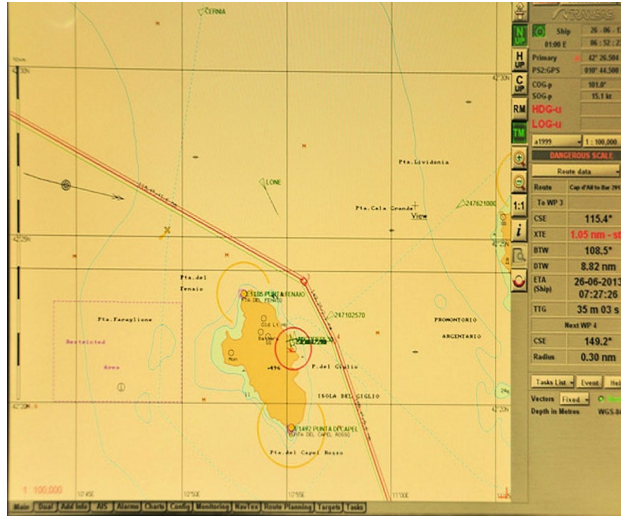
<b>David</b>	<b>vs</b>	<b>Goliath</b>
Professor's team		White Rose yacht
Equipment 2 kg		DWT 270 tn
Value 3000 \$		Value 80m \$

**Stealing, theft and security violation do not have to do so much with technology or required programming knowledge; but with the **inspiration** of the hackers who are willing to steal.**

# GPS SPOOFING



# GPS SPOOFING

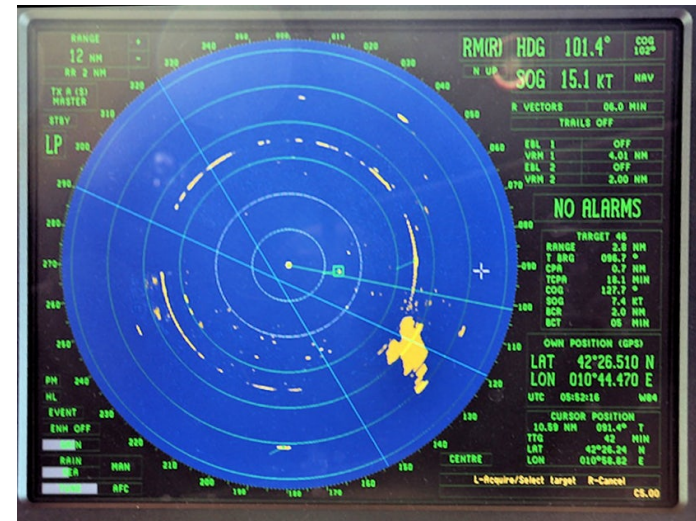




# Remember?

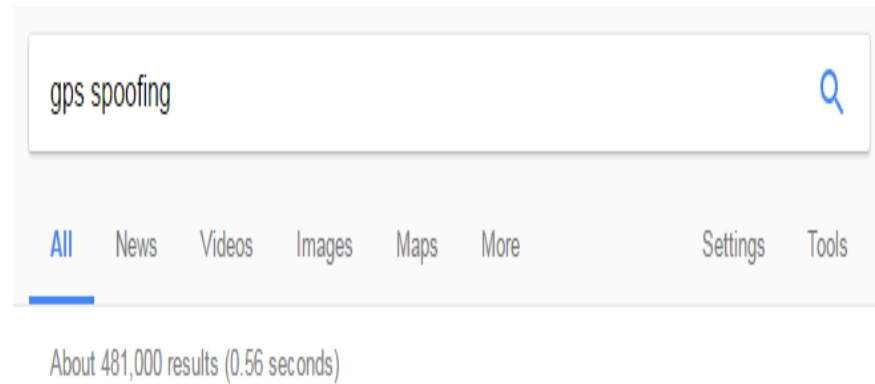


- started changing the rpm from 2-2500 (normal rpm was 1200-1500)
- deactivated the FSC/ESD systems
- and then hide the real values of rpm of the PLC giving false values on the computer displays
- from the CCR cameras and from the noise, the personnel from the control room understood that something had happened.



- the indicated course of the yacht was altered by a few degrees, although the ship had not actually turned
- the ship radar system change the route according the fail indicators
- the crew felt the moving when the systems continue to indicate the scheduled route

# GPS SPOOFING



A screenshot of a Google search interface. The search bar contains the text "gps spoofing" and a blue magnifying glass icon. Below the search bar, there are tabs for "All", "News", "Videos", "Images", "Maps", and "More". The "All" tab is selected and highlighted with a blue underline. To the right of these tabs are links for "Settings" and "Tools". Below the tabs, the text "About 481,000 results (0.56 seconds)" is displayed.

gps spoofing

[All](#) [News](#) [Videos](#) [Images](#) [Maps](#) [More](#) [Settings](#) [Tools](#)

About 481,000 results (0.56 seconds)





# CASE THREE

# MARITIME COMPANIES



# MARITIME COMPANIES









## The cybercrime yesterday, today and tomorrow

Till 2020 it is almost certain that in the cyberspace they will exist two major categories of cybercrime.

The first one, will specialize in business attacks some times on order.

Industrial espionage, data theft and destruction of business reputation will be much wanted in black market.

The second category of cybercrime will aim to our everyday-like activities.

The money transfer systems for instance, or other relevant activities will become the centre of attention for the new hackers generation.

# The cybercrime yesterday, today and tomorrow

Till 2020 it is almost certain that in the cyberspace they will exist two major categories of cybercrime.

The first one, will specialize in business attacks some times on order.

Industrial espionage, data theft and destruction of business reputation will be much wanted in black market.

The second category of cybercrime will aim to our everyday-like activities.

The money transfer systems for instance, or other relevant activities will become the centre of attention for the new hackers generation.

Hackerville



# Proposals

1. Accept the reality of cyber crime in your field
2. Don't go to trap "who cares about me"
3. Organize your networks security in Head Offices, make strict rules of computers using in the ships
4. Train, train, train, train your people.
5. Fire everyone violate these rules.
6. Have always in mind that your ships are alone somewhere in the ocean but also are linked through internet with your offices.
7. Don't believe that antivirus programs are the panacea.

# Proposals

1. Accept the reality of cyber crime in your field
  2. Don't go to trap "who cares about me"
  3. Organize your networks security in Head Offices, make strict rules of computers using in the ships
  4. Train, train, train, train your people.
  5. Fire everyone violate these rules.
  6. Have always in mind that your ships are alone somewhere in the ocean but also are linked through internet with your offices.
  7. Don't believe that antivirus programs are the panacea.
  8. Policy not implemented effectively, is no better than policy not made.
- DEFCON 2011



**THE ENEMY  
IS ALREADY  
ONBOARD**

*If it is to become sunk  
let be in the ocean,  
not in the trough!*

Εάν βυθισθώμεν  
ας βυθισθώμεν εις τον ωκεανόν,  
ουχί εις την σκάφην!

Μενέλαος Λουντέμης





THANK YOU