VIth AIDA Europe 2016

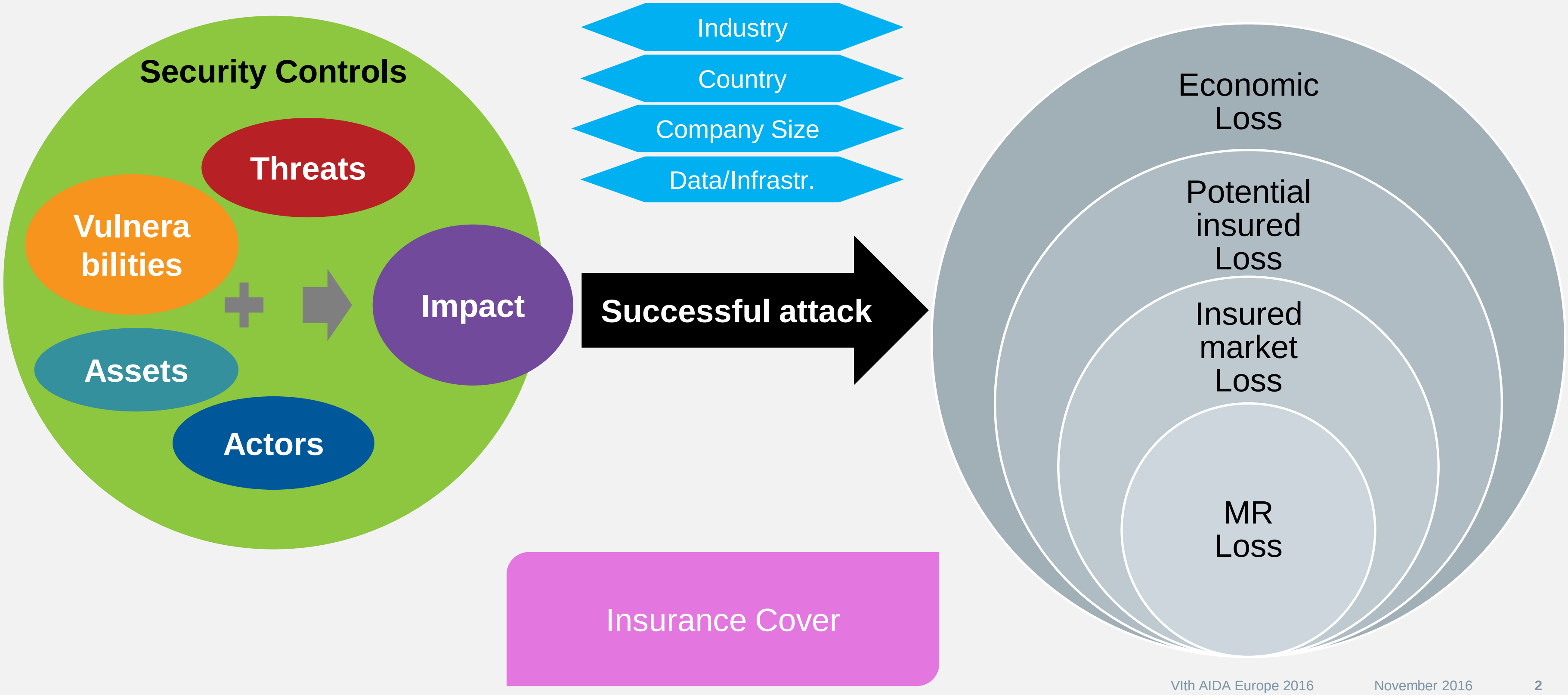
Cyber Risks in Marine & Offshore Energy

03.11.2016
Martin Kreuzer

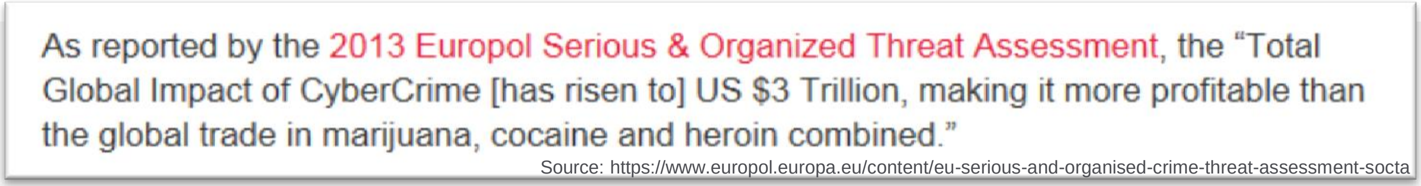
Munich RE

Cyber Insurance – Central Aspects

Munich RE

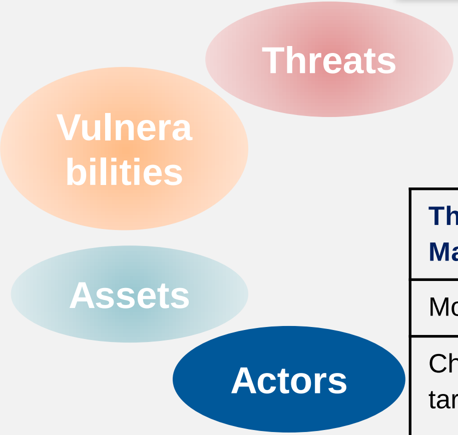


Cyber Threat Actors



As reported by the 2013 Europol Serious & Organized Threat Assessment, the "Total Global Impact of CyberCrime [has risen to] US $3 Trillion, making it more profitable than the global trade in marijuana, cocaine and heroin combined."

Source: https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta



Threat-Matrix	Cybercrime	Cyberkid	Cyberwar and Cyberspionage	Cyber-Terrorist	Hacktivist
Motivation	Money	Fun, curiosity	Strategic	Ideologie/Religion	Politics, Ethic
Choice of targets	Individual, by chance or directly aimed	By chance, political reasons	Individual, collateral	ideological, anti-western, collateral, media-effected	Ideological and political targets
Organisation	Strongly pronounced	Partially	Perfect	Regional	Structured
Competence	High	Low-high	Very high	Low-high (external help)	Middle-high

Cyber Threat Actors:

From a Skript Kiddie to a Cyber Jihadist

Junaid Hussain

2012 vs 2014

Cyber Threat Actors & Critical Infrastructure

Munich RE

ICIT-Institute for Critical Infrastructure:

"*The anatomy of cyber jihad*" – June 2016

"…Russian BlackEnergy malware can be used to compromise critical systems such as electrical grids. Variants, which are less sophisticated, are available for purchase on dark web forums…Today's Cyber-Jihadists are unskilled outsiders, able to accomplish little remotely from the shadows beyond temporary website defacements or service interruptions. However, if groups like ISIS could ever recruit agents working inside of critical infrastructure facilities, say power plants or water treatment facilities, our perception of the threat they pose would be catastrophically changed overnight…"

"…In October 2015, U.S. law enforcement officials revealed that hackers tied to the Islamic State were actively attempting to breach ICS and SCADA systems in the Energy sector. Caitlin Durkovich, the assistant secretary for Infrastructure Protection at the Department of Homeland Security confirmed to company executives at a conference on American energy that, ISIL is beginning to perpetrate cyberattacks…"

Cyber Vulnerabilities & Offshore Energy

Vulnera bilities

Assets

1. Lack of Awareness
2. Remote work & maintenance
3. Use of standard IT
4. Limited cyber security culture among vendors, suppliers and contractors
5. Insufficient separation of data
6. Use of mobile devices
7. Data networks between on- and offshore facilities
8. Insufficient physical security of data rooms
9. Vulnerable software
10. Outdated and ageing control systems in facilities

Cyber Vulnerabilities in Offshore Energy

Possible scenarios in Offshore Energy

Munich RE

- Business Interruption of offshore unit
- Manipulation / destruction of storage facilities and stored goods
- Interruption of the supply chain
- Manipulation of production
- Destruction of production
- Oil pollution could happen as a result of the attack
- LNG interruption of the cooling process
  (FLNG, LNG Plant, Transportation)

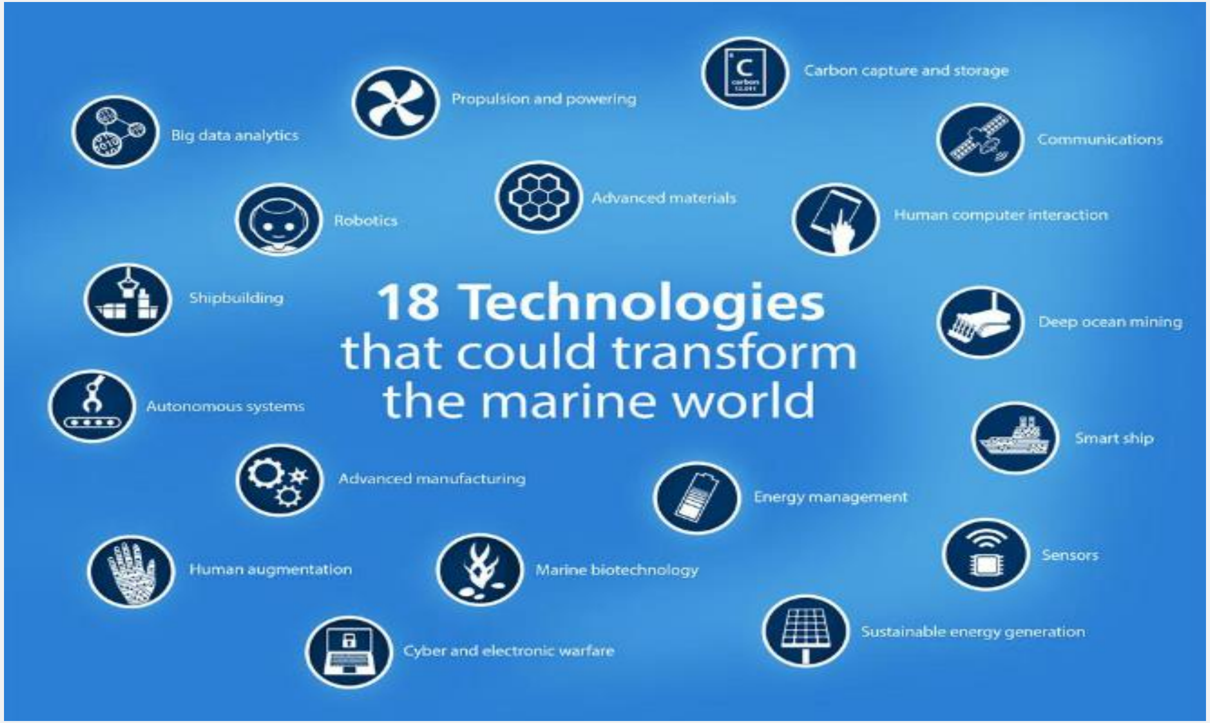
Vulnerable!

Cyber Vulnerabilities in future marine world

Munich RE

Vulnera
bilities

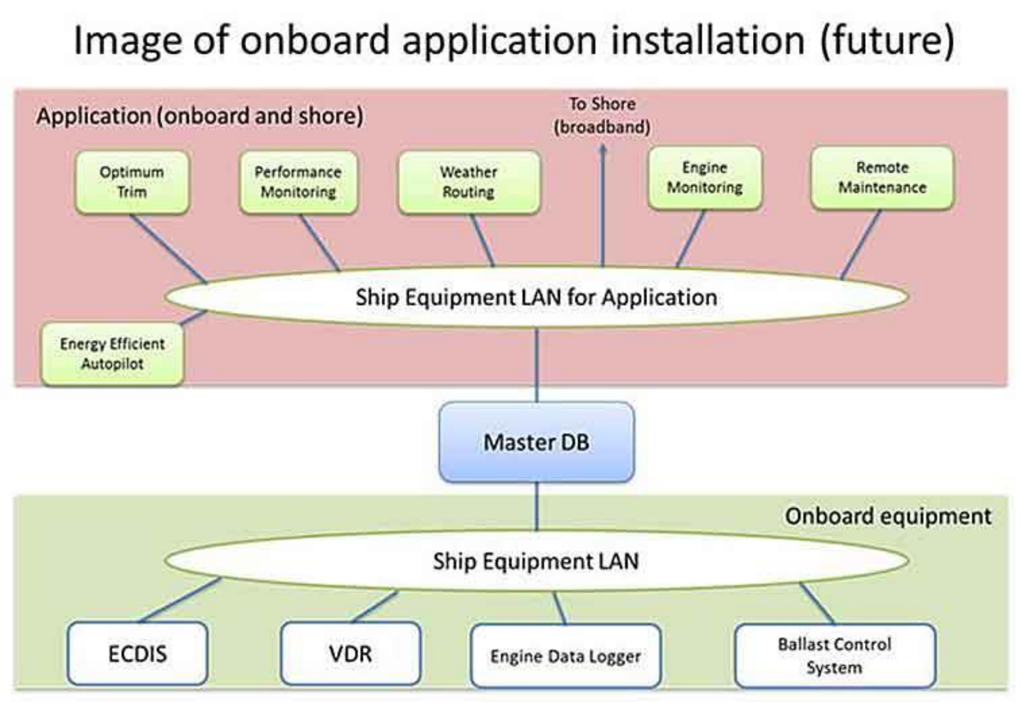
Assets



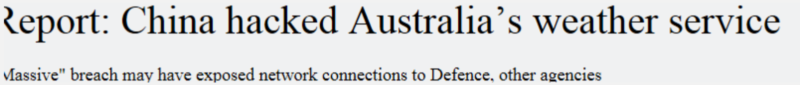
Source: www.worldmaritimenews.com

Smart Navigation of the future

Munich RE

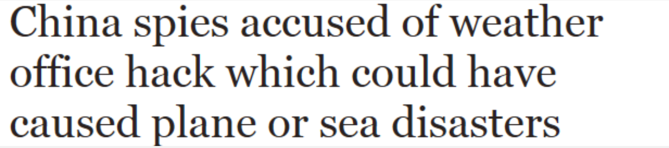


Cyber Incidents in marine world



Report: China hacked Australia's weather service

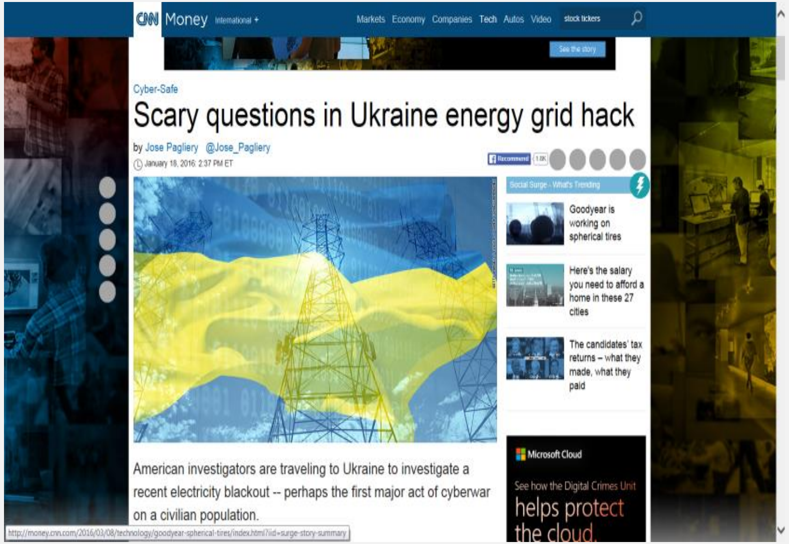
Massive" breach may have exposed network connections to Defence, other agencies



China spies accused of weather office hack which could have caused plane or sea disasters

Cyber Incidents in energy sector

Munich RE



Cyber-Safe

Scary questions in Ukraine energy grid hack

by Jose Pagliery @Jose_Pagliery

January 18, 2016: 2:37 PM ET

American investigators are traveling to Ukraine to investigate a recent electricity blackout -- perhaps the first major act of cyberwar on a civilian population.

Goodyear is working on spherical tires

Here's the salary you need to afford a home in these 27 cities

The candidates' tax returns – what they made, what they paid

http://money.cnn.com/2016/03/08/technology/goodyear-spherical-tires/index.html?iid=surge-story-summary

(Re-)Insurance projects and challenges

Munich RE

Pricing and Wording

- MARKET RATE LOOKUP DATABASE
- BENCHMARK RATE TABLES
- PRICING MODEL
- Adapt wordings to cyber-developments

Loss/Exposure Database

- Systematically store all kind of cyber related loss and risk data for critical infrastructure (including cases with no loss).
- Tap all possible data sources, i.e. UW submissions, loss/risk bordereaus, commercial sources, internet,
- Link data with data and information available elsewhere at MR
- Make data and/or derived results available

Insurance and Reinsurance solutions

- Support and underwriting of Cyber Treaties
- "White Label Product" – modular Wording for standardized coverages
- Accumulation management – participation in and contribution to group wide projects
- Service Delivery: Trainings, Knowledge Transfer, Contribution to Cyber-Market Events, Client workshops, Risk Assessments, etc.

Threat Database

- Market leading MR cyber threat platform (analogue positioning as Nathan in NatCat)
- "Early warning system" customized for different industries, regions, company sizes
- Cyber UW should be informed about new and changing cyber threats and the impact on covers.

Cyber Accumulation & Mega-Cat-Scenarios

- Targeted Attacks against Critical Infrastructures
- Wide spread virus
- Outage of Internet
- Corrupted software scenario
- Multi data breach/Cloud scenario
- Bottleneck 3rd parties for Critical Infrastructure

Thank you!

Martin Kreuzer

Munich RE