Cyber Risiken im Bereich der maritimen Wirtschaft

April 22, 2016

Markus Wähler – Munich Re Global Marine Partnership

Munich RE

Munich RE

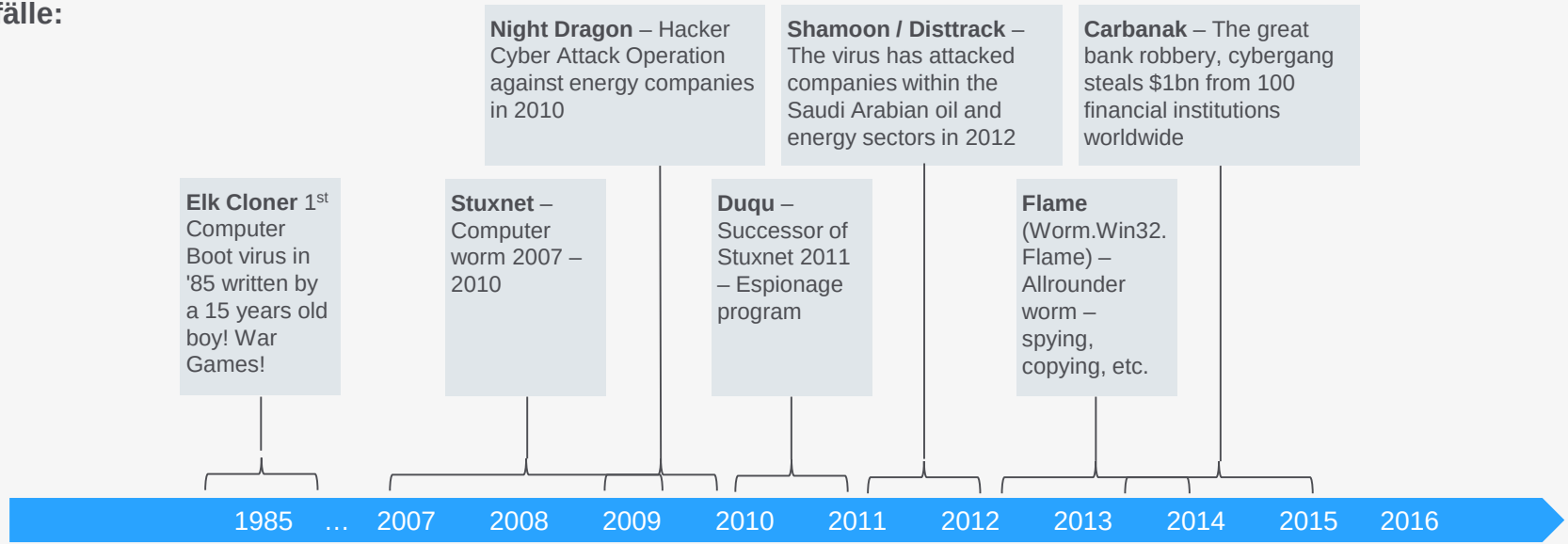
Alles ist möglich…

…aber wie wahrscheinlich ist es?

Warum jetzt?

Julian Assange / Edward Snowden

Vorfälle:



Increased regulatory attention

http://ww.spiegel.de/netzwelt/netzpolitik/cyberwar-wurm-shamoon-richtet-sich-offenbar-gegen-energiesektor-a-850734.html

AGENDA

Munich RE

Definition und Hintergrund

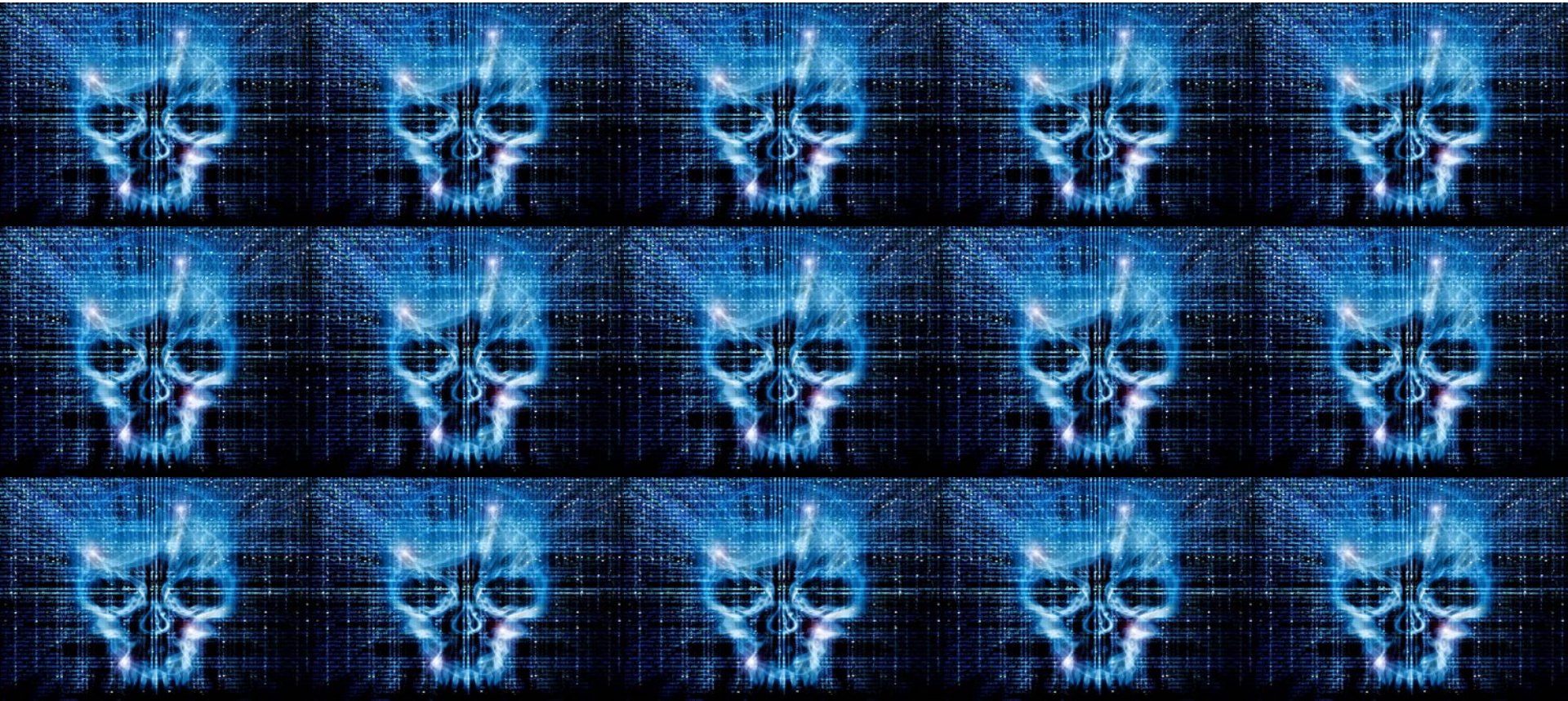
Zahlen – Daten – Fakten

Versicherungsaspekte

Was wir unseren “Underwritern” empfehlen

Definition & Hintergrund

Munich RE



Cyber Angriff definiert

A cyber attack is the deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cyber crimes, such as information and identity theft.

Cyber attack is also known as a computer network attack (CNA).

http://www.techopedia.com/definition/24748/cyberattack

Definition von Kriminalität und Terrorismus

Munich RE

Crime

An act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction.

Unlawful activity.

A serious offense, especially one in violation of morality.

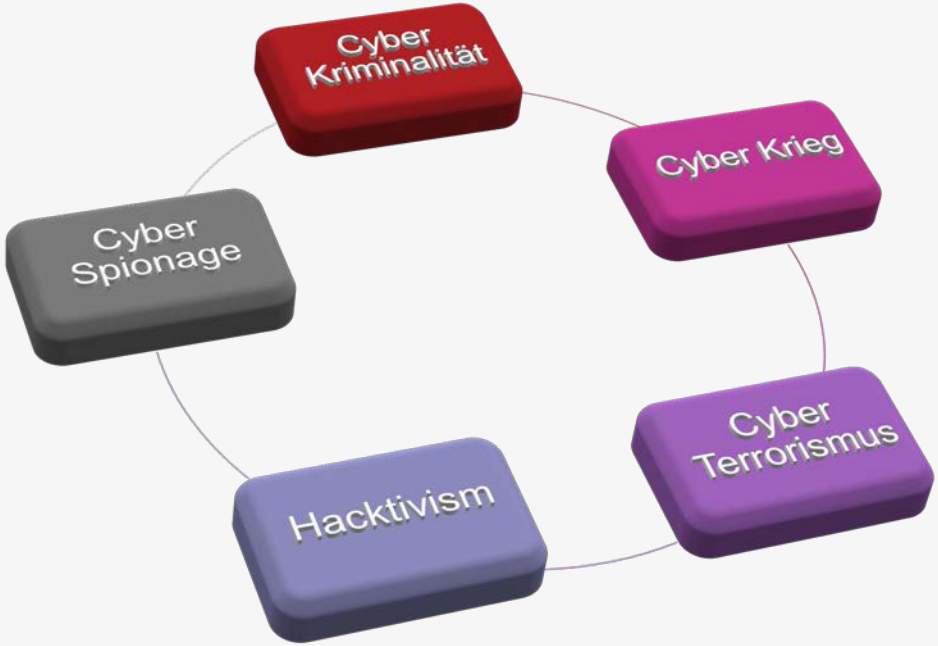
An unjust, senseless, or disgraceful act or condition.

Terrorism

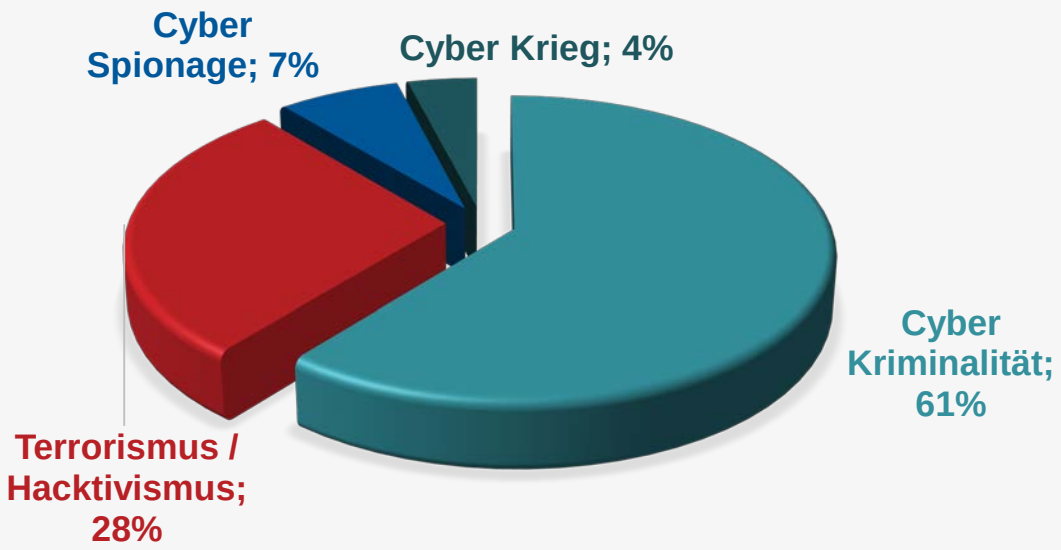
The unlawful use or threatened use of force or violence by a person or an organized group against people or property with the intention of intimidating or coercing societies or governments, often for [religious], ideological, or political reasons.

http://www.thefreedictionary.com/terrorism

Cyber Bedrohungen



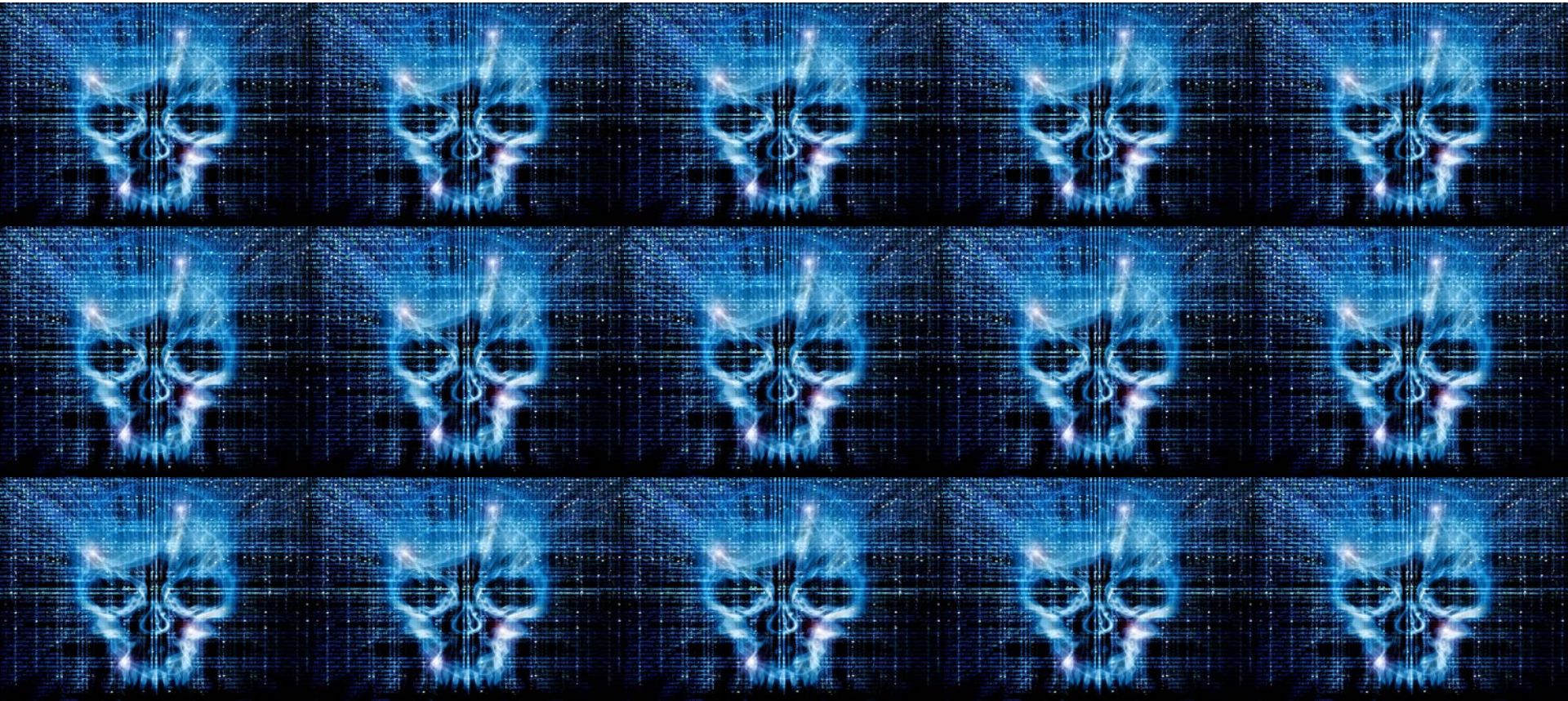
Quantifizierung von Cyber Bedrohungen
April 2016



Source: http://hackmageddon.com/category/security/cyber-attacks-statistics/

Zahlen – Daten – Fakten

Munich RE



Annual econ. loss $ 300bn - $ 1tn

McAfee

Annual econ. loss: $ 350bn

EC3 EUROPOL

sueddeutsche.de

Annual econ. Loss $ 400bn

Econ. Cost: $ 114bn

THE Fiscal TIMES

1 Trillion = 1.000.000.000.000

Ausmaß der Angriffe

Munich RE

Opfer durch Cyber Kriminalität

Opfer pro Jahr
556 Millionen

Opfer pro Tag
Über 1.5 Millionen

Opfer pro Sekunde
18

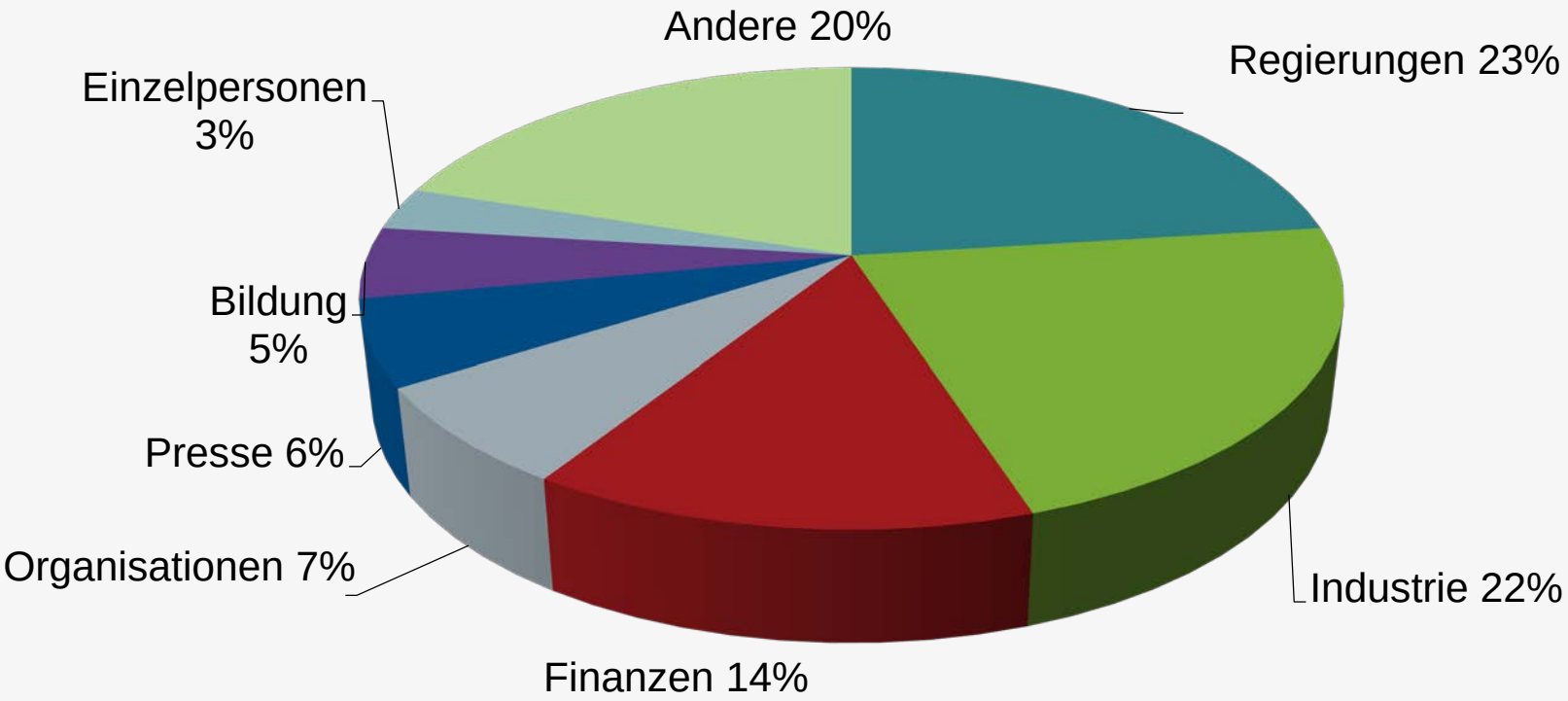
Identitäten betroffen
Mehr als 232.4 Millionen

Mehr als 600.000 Facebook Accounts werden jeden Tag kompromittiert

1 von 10 Social Network Nutzern haben schon einmal berichtet Opfer einer Cyber Attacke in einem Sozialem Netzwerk gewesen zu sein

http://www.go-gulf.com/wp-content/uploads/2013/06/cyber-crime.jpg

Top Ziele



Source: http://hackmageddon.com/category/security/cyber-attacks-statistics/

Beispiele von Attacken 2014 – 2016

36	Apr 7	OpIsrael	Special M the 7 o launched consiste addition operation
37	Apr 13		As a rea "doxes" Anonymo
32	Jun 30	Dragonfly	
26	Aug 14	?	
24	Jan 7		
33	May 28	?	

ID	Date	Author	Target	Description	Attack	Target Class	Attack Class	Country
2	16/01/2016	Russia?	Kiev Airport	Ukrainian authorities announce to review the defences of government computer systems, after detecting a cyber attack on Kiev's main airport launched from a server in Russia.	Targeted Attack	Airport	CW	UA
1	02/01/2016	New World Hacktivists (NWH)	donaldjtrump.com	The hacking group New World Hacktivists (NWH) takes down the official Election Campaign website of American Presidential candidate Donald Trump (donaldjtrump.com). The same attackers claim responsibility for the DDoS attack that crippled the BBC website during the New Year's Eve.	DDoS	Single Individual	H	US

compromised by hackers in a recent targeted attack.

Source: http://hackmageddon.com/

Counter Attack

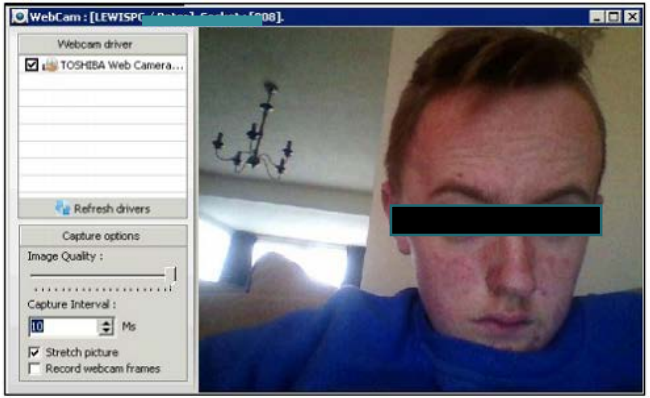
Munich RE

10. Peter Lewis

IP: [redacted]

Location: [redacted]

https://twitter.com/AnonLw6



12. [redacted]

Location: Malaysia

http://www.algemeiner.com/2014/04/10/israeli-hackers-strike-back-at-anonymous-opisrael-expose-participants-with-their-own-webcams-photos/

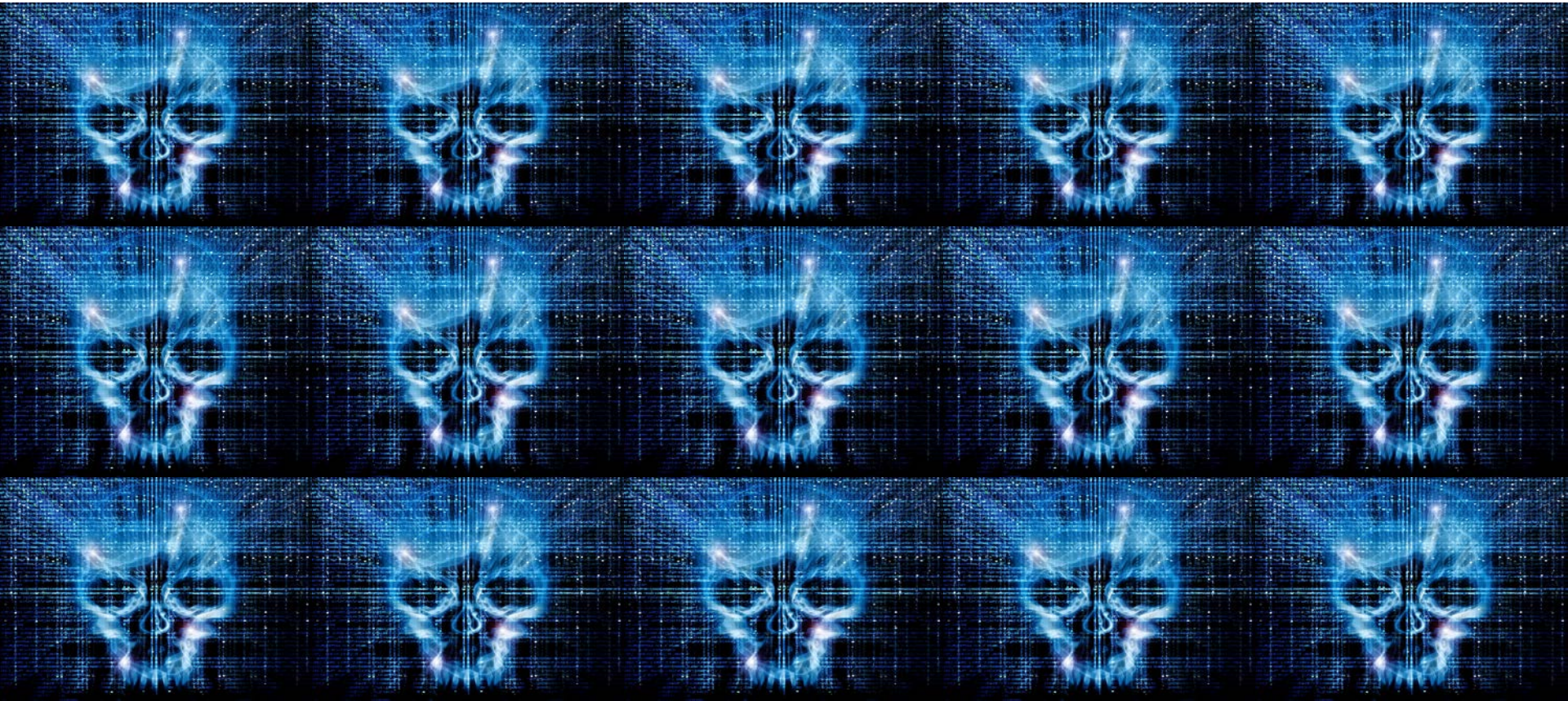
STUXNET

Munich RE

- https://www.youtube.com/watch?v=7g0pi4J8auQ

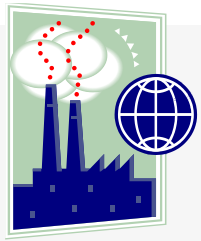
Versicherungsaspekte

Munich RE



Modellszenarien

Munich RE



attacks **on industrial systems** like production plants in general, power plants, power grids, telecommunication, healthcare and public supply systems (water, heating etc.)**, financial sector.**

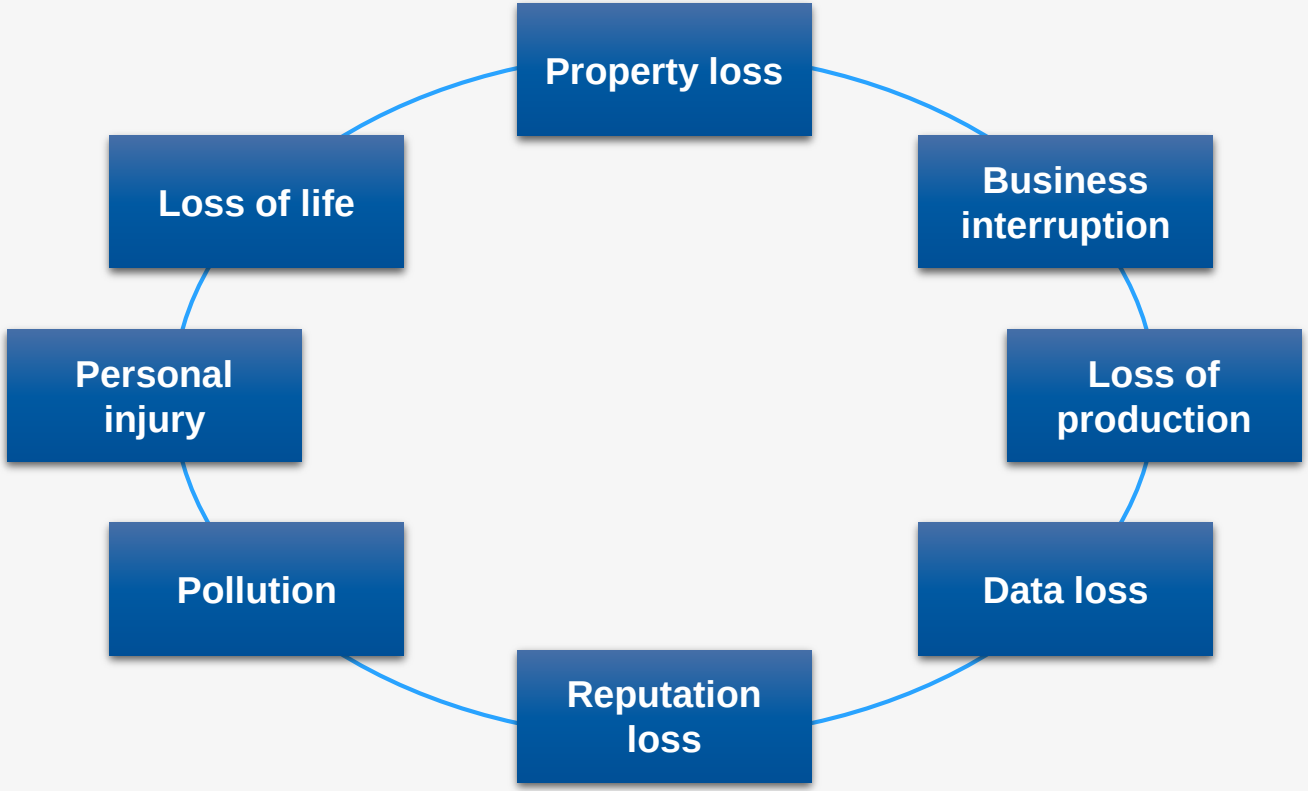
attacks on critical IT infrastructure, which could paralyze data for marine, as well as for the oil / gas producers for example, as many huge corporations don't know how much they depend on IT infrastructure until an attack has occurred

attacks on the government, public safety & security and administration systems

attacks on people, targeted and collateral loss of life

Attacks on transportation infrastructure

Auswirkungen auf Versicherungen



Mögliche Szenarinen in Marine

Munich RE

Jedes Schiff hat eine Hintertür, die Kommunikationseinrichtungen

Geringe Wahrscheinlichkeit eines erfolgreichen Angriff

eNavigation!

Höhere Wahrscheinlichkeit eines erfolgreichen Angriffs mit eNavigation

Image "radio man": Bundesarchiv Bild 101I-695-0410-04A, Warschauer Aufstand, Funker" by Bundesarchiv, Bild 101I-695-0410-04A / Falke / CC-BY-SA. Licensed under CC BY-SA 3.0 de via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Bundesarchiv_Bild_101I-695-041004A,_Warschauer_Aufstand,_Funker.jpg#/media/File:Bundesarchiv_Bild_101I-695-041004A,_Warschauer_Aufstand,_Funker.jpg

Picture 1-3 © MEYER WERFT PAPENBURG

Was ist eNavigation?

- **eNavigation** is a Strategy developed by the International Maritime Organization **(IMO)** to bring about increased safety of navigation in commercial shipping through better organization of data on ships and on shore, and better data exchange and communication between ships and the ship and shore
- **eNavigation will improve the safety at sea!**
- **But a global overview about the international flow of goods is possible!**

Mögliche Szenarien in Offshore Energy

Munich RE

Eindringen in Kommunikationsnetzwerke


Image: Florian Kopp/ imageBROKER/ Corbis

Höhere Wahrscheinlich-keit einer erfolgreichen Attacke


Image: Omer Torres/ Getty Images

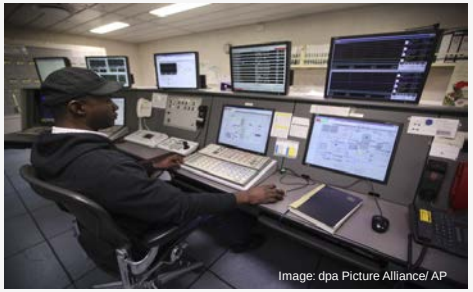


Image: dpa Picture Alliance/ AP

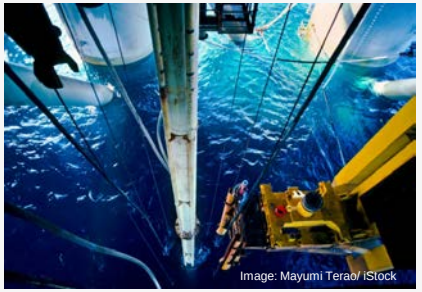


Image: Mayumi Terao/ iStock

Night Dragon & Shamoon

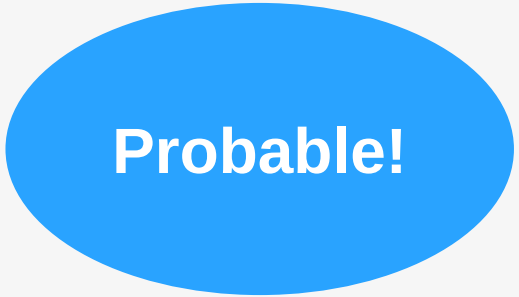
Munich RE

Night Dragon – since 2009 (possibly 2005), hackers from SE Asia (?) have successfully infiltrated networks of at least a dozen multinational oil, gas, and petrochemical companies as well as individuals and executives in Kazakhstan, Taiwan, Greece, and the US. Five firms confirmed the attacks.

Shamoon – detected in 2012 by Israeli security company Seculert. Shamoon is a new Trojan found in the Middle East. It has apparently been used in targeted attacks against specific individuals or companies, including at least one firm in the energy sector – Saudi Aramco, Saudi Arabia's state-owned oil-production company.

Weitere mögliche Szenarien in Offshore Energy

- Betriebsunterbrechung der Offshore Einheit
- Manipulation / Zerstörung der Langereinrichtung
- Unterbrechung der Lieferkette
- Manipulation der Produktion
- Zerstörung der Produktion
- Ölverschmutzung als Resultat einer Cyber Attacke
- LNG Unterbrechnung des Kühlungsprozesses (FLNG, LNG Herstellung, Transport)



Auswirkungen von Cyber Angriffen auf die Marine & Offshore – Energy Industrie

- Voraussichtliche Kosten der Öl- und Gasindustrie bis 2018: US$ 1.87 Billion*
- 40% aller Cyber Angriffe in den USA auf kritische Infrastrukturen 2012, waren gegen den Energiesektor gerichtet

*Source: Willis Energy Market Review 2014 / Image middle: „Exval" von http://response.restoration.noaa.gov/photos/exxon/02.html. Lizenziert unter Gemeinfrei über Wikimedia Commons - http://commons.wikimedia.org/wiki/File:Exval.jpeg#/media/File:Exval.jpeg / Image right: "Apdx F2 - Aerial photo after explosion". Licensed under Public Domain via Wikipedia - http://en.wikipedia.org/wiki/File:Apdx_F2_-_Aerial_photo_after_explosion.jpg#/media/File:Apdx_F2_-_Aerial_photo_after_explosion.jpg

Welche Deckungen sind bereits in Nicht-Marine erhältlich?

Begrenzte Deckungen für private und kleine, kommerzielle Geschäftsbereiche

Keine Katastrophendeckungen für den industriellen Geschäftsbereich als Standardprodukt

Derzeitiger Marktansatz – Ausschluss via Cl. 380

Clause 380

INSTITUTE CYBER ATTACK EXCLUSION CLAUSE

Umfassender und gut formulierter Ausschluss

Begrenzter Wiedereinschluss für Kriegs- und Terrrorismusdeckungen!

Professionelles underwriting von Cyber Risiken

Cyber Risiken stellen ein erhebliches Risiko für den Marine und den Offshore Energy Markt dar!

Deckungen sollten nur durch spezialisierte Underwriter und IT Experten erfolgen.

Die Cl. 380 hilft um sich vor unerwarteten Risiken zu schützen!

Spezielles underwriting und maßgeschneiderte Produkte sind unverzichtbar, insbesondere bei der

- **Risikoeinschätzung**
- **dem Pricing**
- **der Kumulkontrolle**

Herzlichen Dank für Ihre Aufmerksamkeit

Munich RE

ご清聴ありがとうございました

Շնորհակալություն ուշադրության համար

Mauruuru no to outou whakarongo

Thank you for your attention

תודה רבה על אדיבותך

귀하의 관심에 감사드립니다

Спасибі за Вашу увагу

Благодаря ви за вниманието

Σας ευχαριστώ για την προσοχή σας

Cảm ơn bạn đã quan tâm của bạn

Terima kasih atas perhatiannya

Anda Salamat sa iyong pansin

Ngiyabonga ngokungiphendula

დიდი მადლობა ყურადღებისთვის

感謝您的關注

İlginiz için teşekkürler

Gracias por su atención

Dziękuję za uwagę

شكرا لاهتمامكم

Kiitos huomiota

Tack för er uppmärksamhet

Dank u voor uw aandacht

Tänan tähelepanu eest!

Paldies par jūsu uzmanību

Dėkojame už Jūsų dėmesį

Asante kwa mawazo yako

आपले लक्ष धन्यवाद

Анхаарал тавьсан та бүхэнд баярлалаа

உங்கள் கவனத்திற்கு நன்றி

Je vous remercie de votre attention

Tibi gratias ago pro studio vestro

សូមអរគុណចំពោះការយកចិត្តទុកដាក់របស់អ្នក

ຂໍຂອບໃຈສຳລັບຄວາມສົນໃຈຂອງທ່ານທີ່ທ່ານ

Tänan teid tähelepanu eest

Grazzi għall-attenzjoni tiegħek

Назар аударғаныңызға рақмет

Go raibh maith agat as do aire

Diolch i chi am eich sylw

Daalụ maka itinye uche gị

Grazie per la vostra attenzione