Under attack

Eine Use Case basierte Darstellung von Angriffen aus dem Cyber-Informationsraum auf deutsche Marineschiffe

Rheinmetall Electronics, André Reichow-Prehn, Head of Programme Cyber, Wilhelmshaven, 28.06.2018

Agenda

1. Ausgangsbasis
2. Angriffe sind…
3. Informationskrieg
4. OSINT
5. SIGINT/COMINT
6. Supply-Chain Attacks
7. Compromised modules and components
8. Side channel attackes
9. Rheinmetall Cyber Solutions

Ausgangsbasis (Standard Operational Procedures SOP)

- **Bedrohungsanalyse** immer nur ein Schnappschuss, Erfassung eines Momentes und eines begrenzten Anwendungsraum
- Bedrohungen können nicht erschöpfend erfasst werden → mögliches Mittel FMEA-analoge Prozedur / Attack Tree Graphs
- **Informations-/IT-Sicherheitskonzepte** immer abhängig von der Bedrohungsanalyse
- Technische Sicherheit ist in militärischen Systemen abhängig von **BSI-Zertifizierung und Zulassung** für behördliche oder eingestufte Speicherung und Übertragung
- nicht vorhandene Lösungen werden idR durch **Risikoanalyse** abgegolten

Angriffe sind

- aktiv
- Ausnutzung von jeglichen Schwachstellen
- kreativ
- dynamisch
- Exponentiell
- oft nicht vorhersehbar
- abhängig von investierten Ressourcen
- asymmetrisch

Informationskrieg

Definition:

Die Erzeugung, das Vorenthalten Veränderung oder gesteuerte Verbreitung von falschen oder echten Information wird als Informationskrieg bezeichnet.

Dies wird auch als Psychological Warfare (PsyOps), Propaganda, Opinion Management oder Public Relations bezeichnet.

Eine Besonderheiten im Cyber-Informationsraum ist die Nutzung von sozialen Medien u. a. mit dem Feature des Micro-Targeting.

Referenzfälle (Lisa, Baltikum)

Berliner Zeitung

HOME BERLIN FREIZEIT POLITIK SPORT WM 2018 KULTUR PANORAMA FAMILIE VIDEO

Themen Fußball-WM 2018 | Restaurants in Berlin | Berlin Story

Berliner Zeitung › Berlin › Polizei und Justiz › Russlanddeutsches Mädchen in Berlin: Der Fall Lisa kommt vor Gericht

Russlanddeutsches Mädchen Der Fall Lisa kommt vor Gericht

Von Katrin Bischoff 28.02.17, 20:20 Uhr

EMAIL FACEBOOK TWITTER MESSENGER

Protestdemonstration vor dem Kanzleramt nach angeblicher Vergewaltigung einer 13-Jährigen aus Marzahn.

SPIEGEL ONLINE SPIEGEL+ Anmelden

Menü | Politik Meinung Wirtschaft Panorama Sport Kultur Netzwelt Wissenschaft mehr

POLITIK Schlagzeilen | Wetter | DAX 12.297,01 | TV-Programm | Abo

Nachrichten > Politik > Ausland > Bundeswehr > Bundeswehr: Fake-News-Attacke gegen deutsche Soldaten in Litauen

Einsatz in Litauen

Nato vermutet Russland hinter Fake-News-Kampagne gegen Bundeswehr

Die Bundeswehr ist bei ihrer Baltikum-Mission Ziel einer perfiden Kampagne geworden. Nach SPIEGEL-Informationen wurden offenbar aus Russland Gerüchte über eine angebliche Vergewaltigung durch deutsche Soldaten gestreut.

Von Matthias Gebauer

Referenzfälle mit Todesfolge

TIME

U.S. POLITICS WORLD TECH ENTERTAINMENT SUBSCRIBE

WORLD • INDONESIA

Where Memes Could Kill: Indonesia's Worsening Problem of Fake News

Stories From Ideal Media

Read More

WORLD
Indonesia May Have Found Wreckage of Ferry That Sank...

WORLD
The Radical Cleric Behind Indonesia Starbucks Bombing...

WORLD
'Please Find My Son, Return Him to Me.' Families Beg for...

WORLD

BBC Sign in News Sport Weather Shop Earth Travel Mo

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

Zuckerberg addresses 'Facebook killing'

18 April 2017 Share

Anforderung an Lösung Sicherung im Informationskrieg

- erfordert Fähigkeiten im Bereich
  - OSINT,
  - Fremdsprachen,
  - Dialekte
  - Kultureller Kompetenz
  - Informationsmanagement Public Management

OSINT

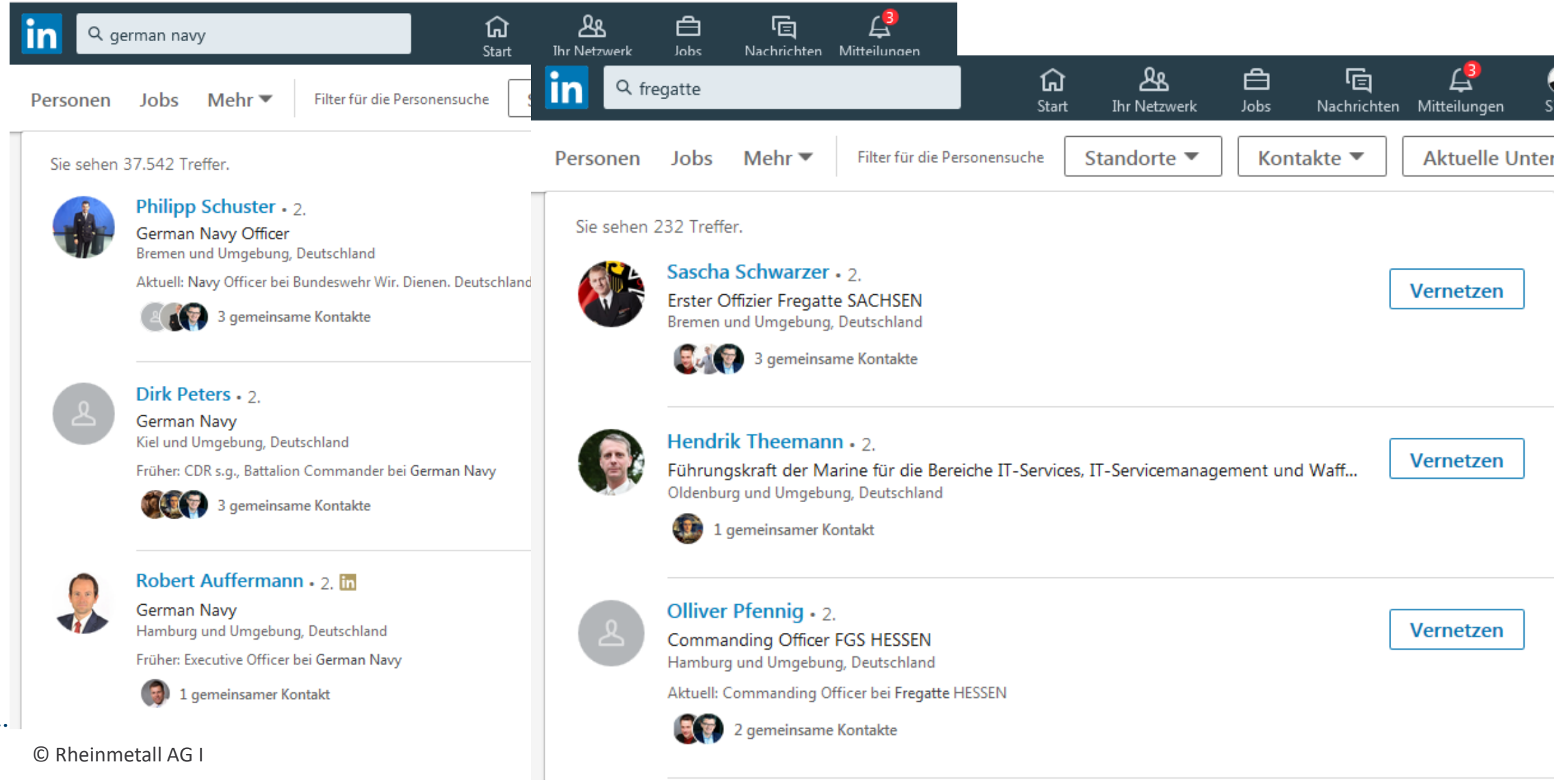
Definition:

Open Source Intelligence (OSINT) ist das Nutzen von öffentlich verfügbaren Informationen zur Aufklärung im Vorfeld von Angriffen.

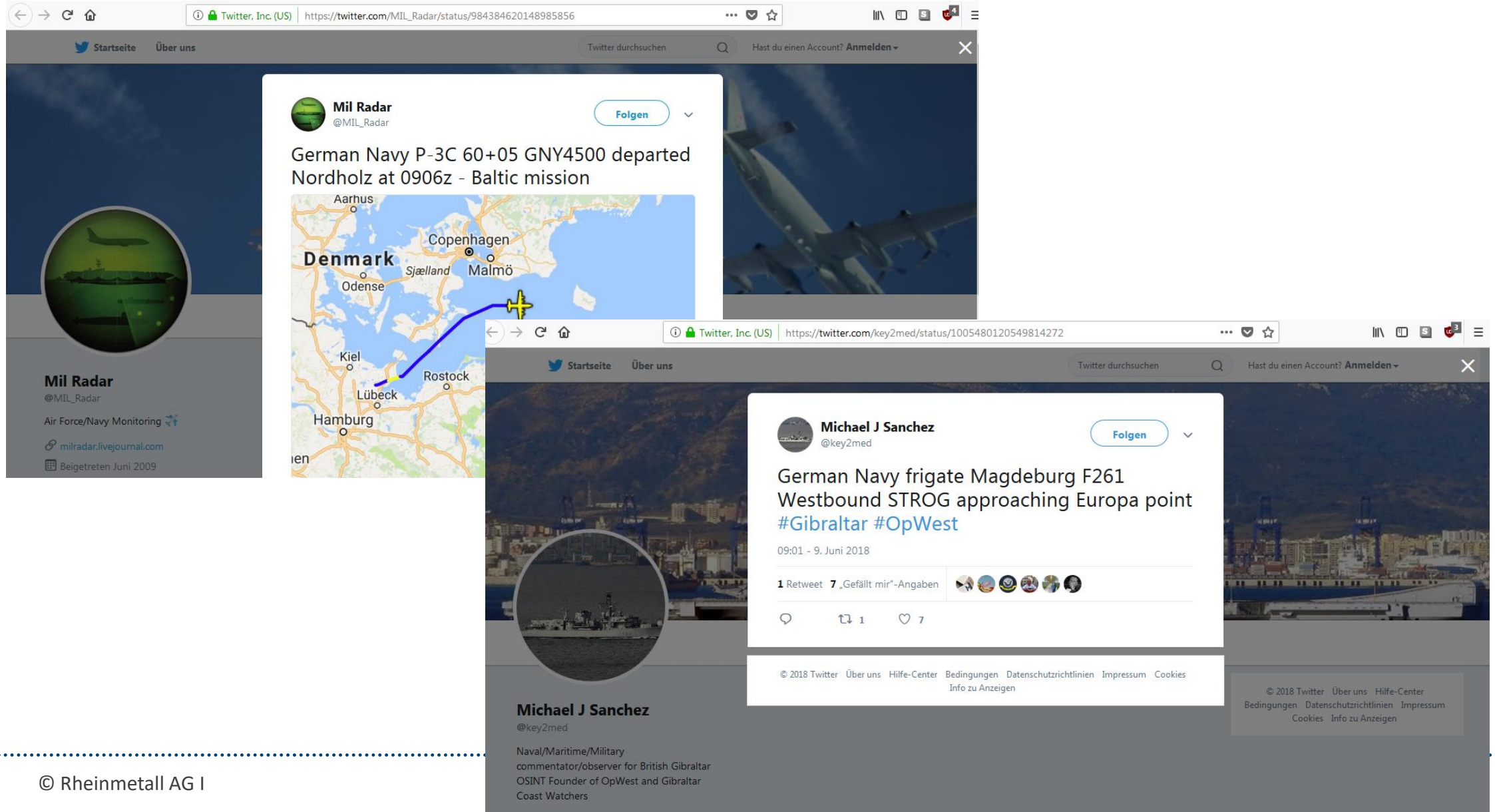
Dazu gehört die Nutzung von öffentlichen Datenbanken, Suchmaschinen, Messsystemen und soziale Medien.

OSINT ermöglicht es, passiv Informationen über ein Ziel zu erheben, um Angriffsziele zu finden und zu untersuchen.

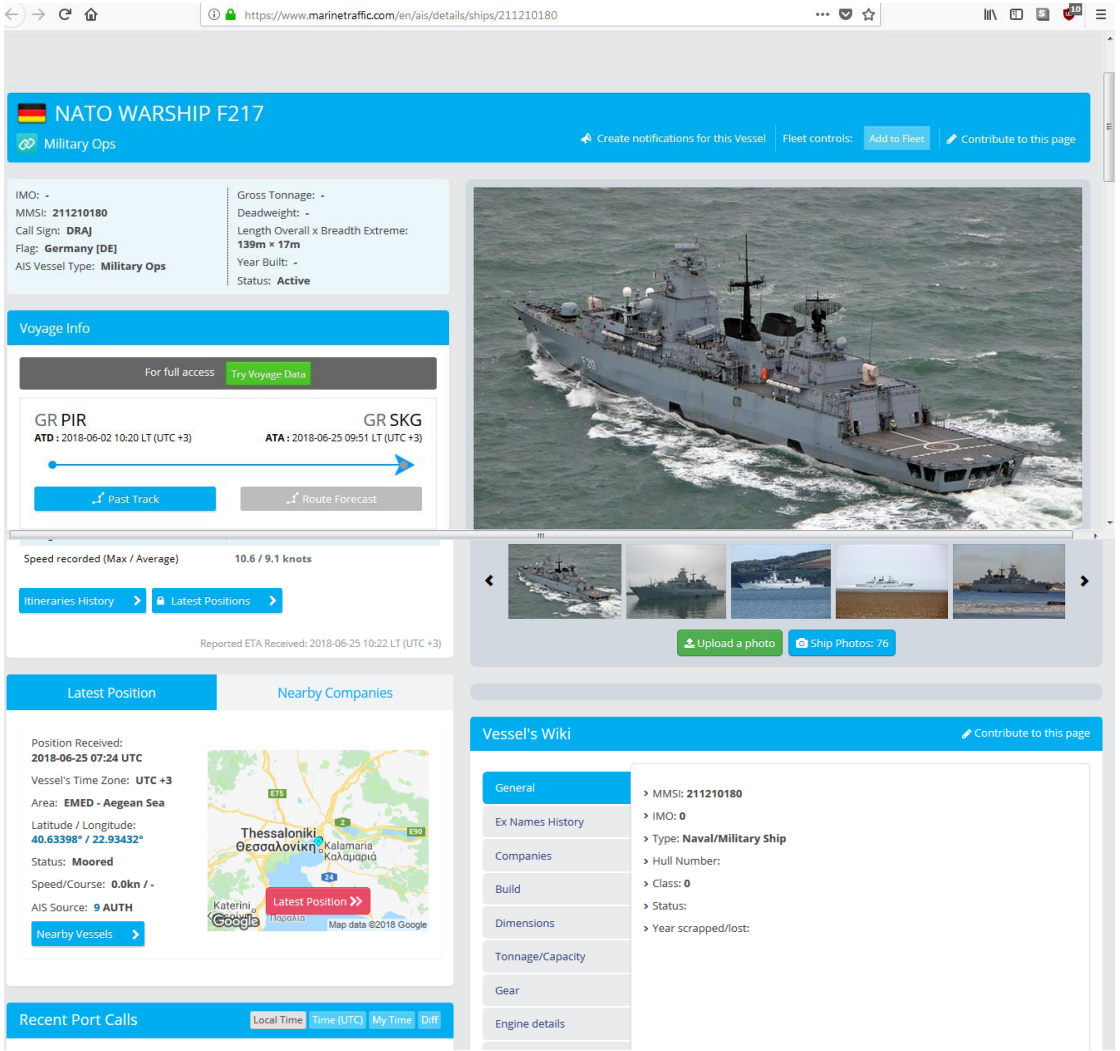
Soziale Medien (Bsp. LinkedIn)

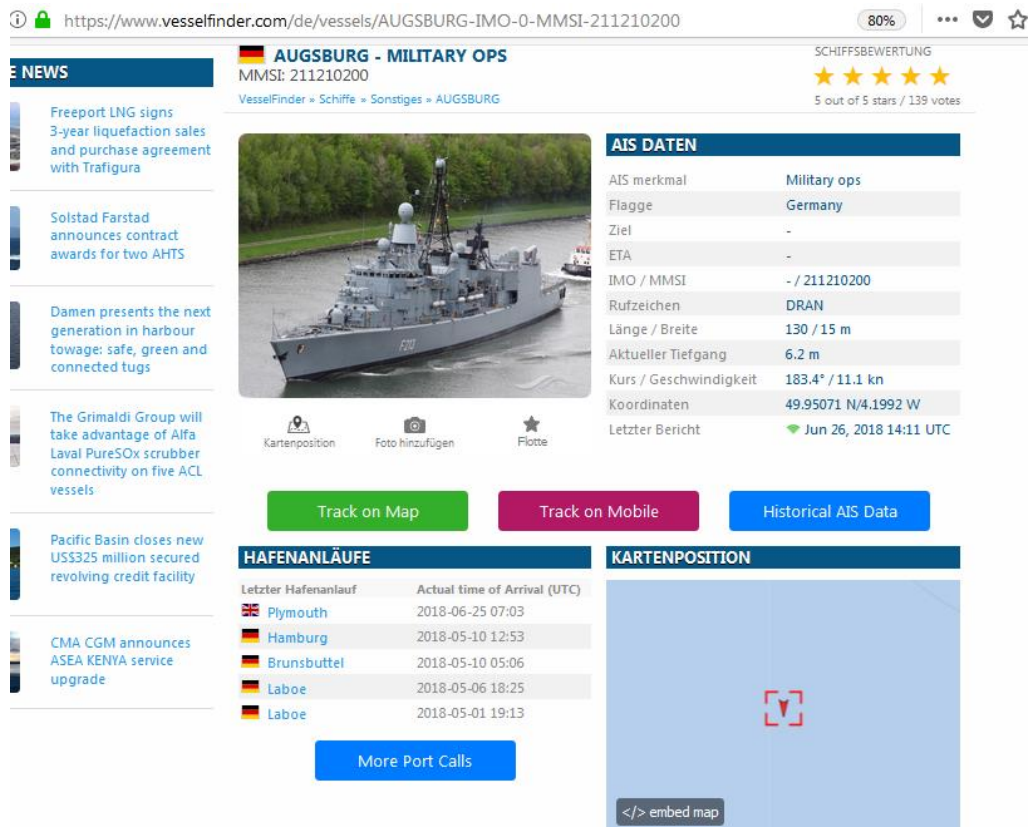


Soziale Medien (Bsp. Twitter)



Open Source AIS-Tracking (Marinetraffic / Vesselfinder)





SIGINT/COMINT

Definition:

Signalaufklärung (SIGINT) oder Kommunikationsaufklärung (COMINT oder KOMINT) beschreiben das Abfangen und Verarbeiten von technisch-physikalischen, d. h. optischen oder elektromagnetischen Signalen oder der Kommunikation mit Medien der Informations- und Kommunikationstechnik.

WhatsApp and Fitness Tracker

BBC Sign in News Sport Weather Shop Earth Travel

NEWS

Home Video World UK Business Tech Science Stories Entertainment & Arts

Technology

Facebook told to stop collecting German WhatsApp data

27 September 2016 Share

Support The Guardian Subscribe Find a job Sign in Search International edition

The Guardian

News Opinion Sport Culture Lifestyle More

World ▸ Europe US Americas Asia Australia Middle East Africa Inequality Cities Global development

GPS

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Latest: Strava suggests military users 'opt out' of heatmap as row deepens

Alex Hern

@alexhern

Sun 28 Jan 2018 21.51 GMT

29,816

This article is over 4 months old

▲ A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava. Photograph:

most viewed


Second Spanish church falls prey to well-intentioned restorer


Live VAR controversy and crunch time in World Cup Groups C and D - as it happened


Argentina's Jorge Sampaoli hits back amid reports of squad revolt


David Squires on ... hostility, culture and Nordic noir at the World Cup


UK democracy under threat and need for reform is urgent, says regulator

Intelligence Systems

- HF/UHF Finder
- LI-Systems (PSTN)
- IMSI-Catcher
- Satellite Interception and Monitoring Systems

Supply-Chain Attacks

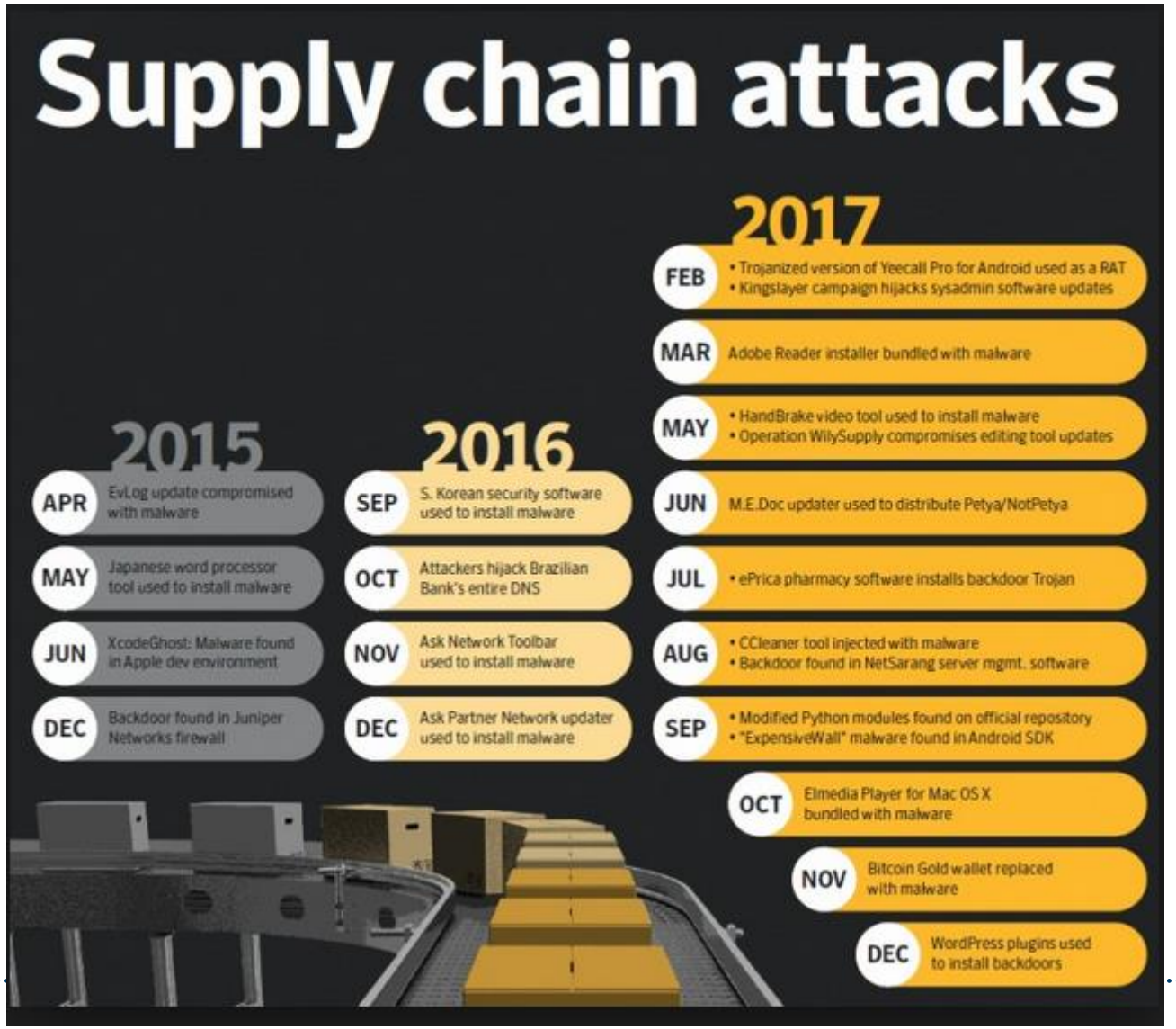
Definition:

Supply-Chain Attacks sind Angriffe, die sich gegen Unternehmen der Zulieferindustrie, Logistikdienstleistern oder deren Personal richten.

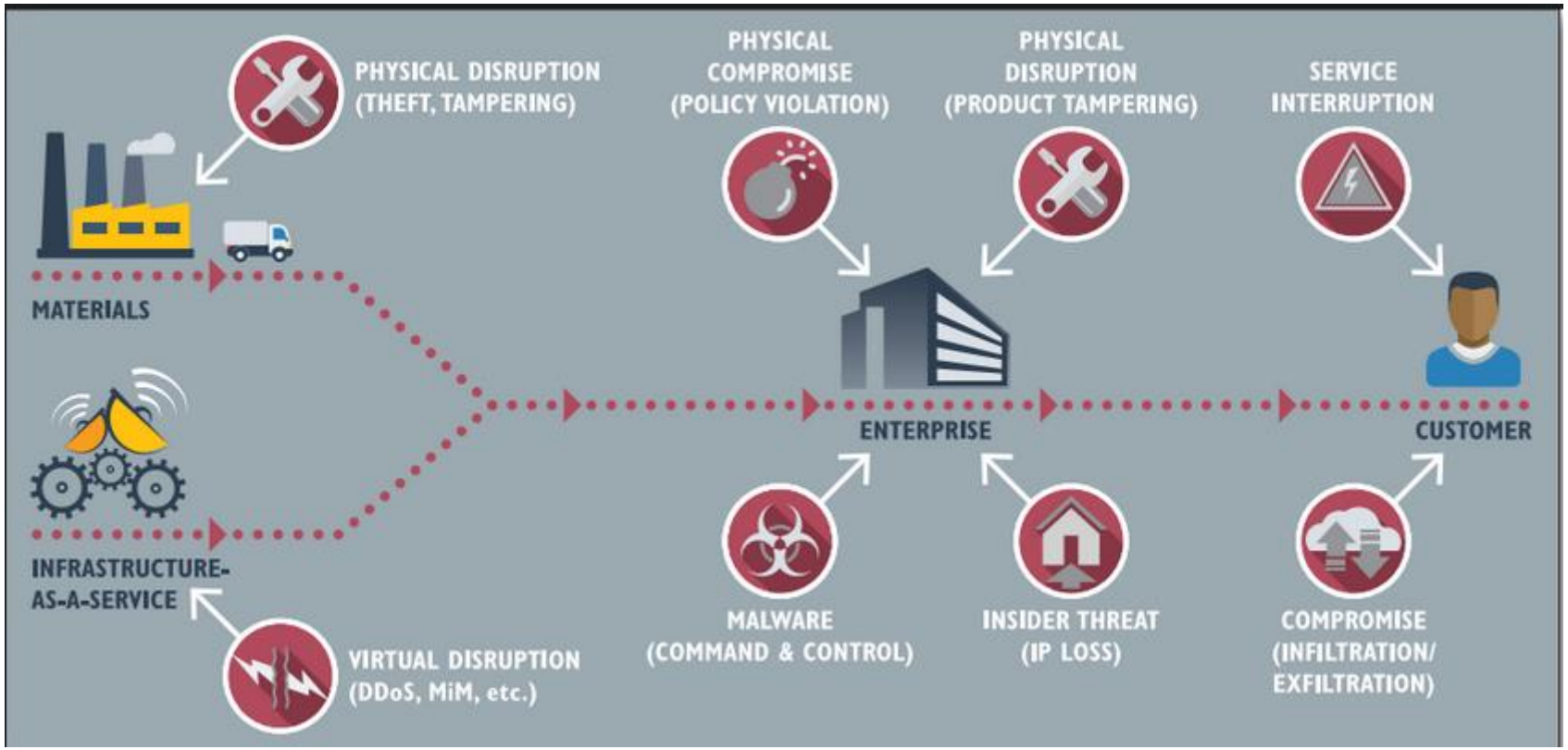
Das Ziel ist die Unterbrechung oder das Kompromittieren der Versorgungskette.

Die Angriffe können sich direkt gegen die Verfügbarkeit der Unternehmen richten, die Kommunikation stören oder sich gegen die Infrastruktur oder Personen richten. Angriffe reichen dabei von Denial-of-Service, Insider Threat über Wirtschaftsspionage und weitere Sabotage.

Wachstum der Angriffe auf die Versorgungskette (Quelle: Symantec)



Angriffsvektoren auf die Versorgungskette (Quelle: Zemana Blog)



Compromised Components and Modules

Definition:

Der Angriffsvektor Compromised Components and Modules ist verbunden mit dem Angriff Supply-Chain Attacks kann aber auch bereits im Vorfeld durch Einflussnahme auf Normungsgremien und Standardisierung sein.

Backdoors in Military Grade Chipsets bereits in 2012 nachgewiesen

CRN
CONNECTING THE AUSTRALIAN CHANNEL
NEWS FEATURES PHOTOS IMPACT AWARDS CRN PIPELINE MAGAZINE EVENTS RESOURCES LOG IN SUBSCRIBE

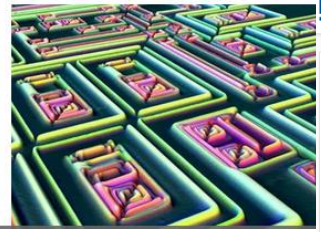
Chinese "backdoors" discovered in US military chips

By Juha Saarinen
May 30 2012
1:50PM

0 Comments

A Cambridge University research team has claimed Chinese manufacturers put "backdoors" into electronic chips used by the US military.

Using "breakthrough silicon chip scanning technology", researcher Sergei Skorobogatov said his team had found unauthorised access mechanisms inserted by the Chinese manufacturer of a chip used by the military.



Military.com BENEFITS NEWS VETERAN JOBS MILITARY LIFE VIDEOS DISCOUNTS Search Military.com Login

DEFENSETECH

News

Proof That Military Chips From China Are Infected?

30 May 2012 | By John Reed

For years, everyone has warned that counterfeit microchips made in China and installed on American military hardware could contain viruses or secret backdoors granting the Chinese military cyber access to U.S. weapons systems. These warnings/predictions recently expanded beyond counterfeit parts, now we're worried that any Chinese-made components could be infected. The problem was that until this week, these warnings were educated guesses and theories. Well, a scientist at Cambridge University in the United Kingdom claims to have developed a software program proving that China -- and anyone else -- can, and is, installing cyber backdoors on

MILITARY NEWS

- Military Opinion
- US Military Budget for Fiscal Year 2018
- Military Events
- Army
- Navy
- Air Force
- Marine Corps
- Coast Guard
- Procurement
- Technology
- Gear

SELECT SERVICE

ARMY MARINES NAVY AIR FORCE
NATIONAL GUARD COAST GUARD SPOUSE LOGIN

Stay informed.
TECHNOLOGY & DEFENSE FROM EVERY ANGLE

Einfluss auf Normen und Standards

golem.de IT-NEWS FÜR PROFIS

HOME TICKER VIDEO AUDIO FORUM Suchen

TOP-THEMEN: Cebit 2018 E3 2018 Smartphone Auto Computex 2018 Raumfahrt mehr...

SERVICES: PREISVERGLEICH STELLENMARKT TOP-ANGEBOTE IT-KÖPFE GEHALTSCHECK NEWSLETTER ABO

BSAFE

NSA bezahlte RSA Security, um Krypto-Backdoor einzusetzen

10 Millionen US-Dollar zahlte die NSA an das Sicherheitsunternehmen RSA Security, um Dual_EC_DRBG in seiner BSafe-Bibliothek als Standard einzusetzen. Bereits im September 2013 hatte RSA davor gewarnt, die Bibliothek zu nutzen.

21. Dezember 2013, 9:56 Uhr, Jörg Thoma

PCWorld FROM IDG

NEWS REVIEWS HOW-TO VIDEO BUSINESS LAPTOPS TABLETS PHONES HARDWARE SECURITY SOFTWARE

Home / Government

NEWS

Overreliance on the NSA led to weak crypto standard, NIST advisers find

By Lucian Constantin

Romania Correspondent, IDG News Service | JUL 15, 2014 10:20 AM PT

FCW The Business of Federal Technology

People IT Modernization Digital Government Security Acquisition Congress IT L

SECURITY

SHARE... E-MAIL THIS PAGE PRINTABLE FORMAT

What NSA's influence on NIST standards means for feds

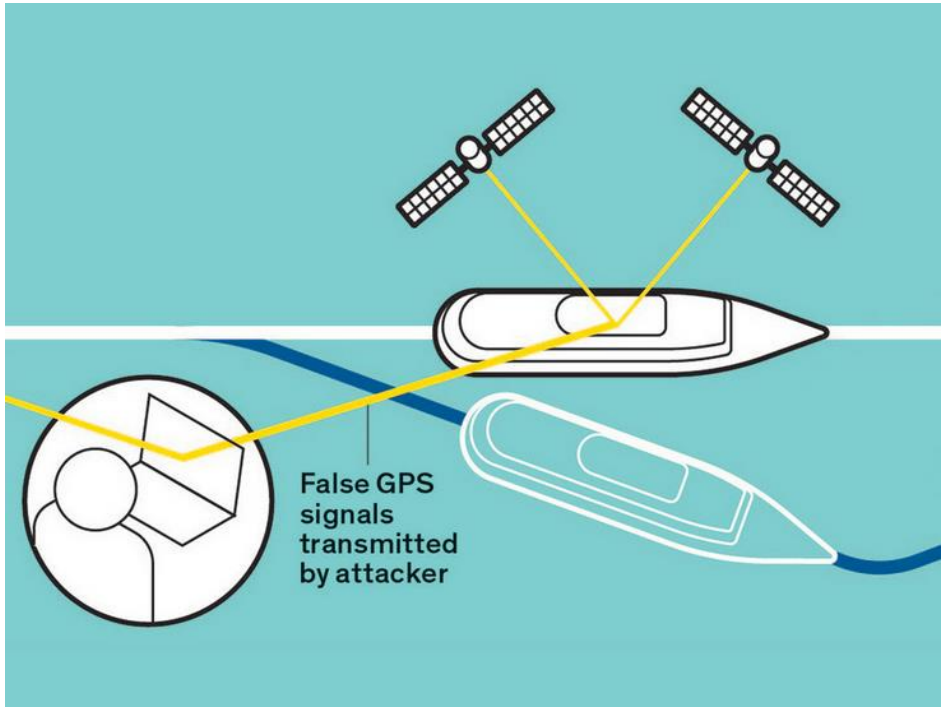
By Frank Konkel | Sep 06, 2013

Side Channel Attacks

Definition:

Side Channel Attacks oder Seitenkanalangriff beschreiben Angriffe gegen Systeme deren Funktionen im Verbund mit dem eigentlichen Zielsystem laufen und über die man auf die bestehende System wirken kann.

GPS Jamming / Spoofing



Hijacking von anderen Schiffen als Kamikaze-Drohnen?

techworld FROM IDG

Features Technology Innovation Jobs Follow:

Home 〉 Analysis 〉 Security Analysis 〉 Can you hack a ship? Global maritime industry ripe for hacking

Can you hack a ship? Global maritime industry ripe for hacking

Security researchers have for years been warning the maritime industry that it is low hanging fruit as incredibly high-value cargo is fitted to ships with legacy (at best) systems, bad awareness, poor processes, and seaports that can suffer from the same problems.

By Tamlin Magee | Apr 03, 2018

Share

The maritime shipping industry is the main conduit for global trade, with more than 80 percent by volume transported from region to region by ships, and 10.3 billion tons in total moving between seaports around the world globally in 2016. Despite this, incident after incident has demonstrated just how much the trillion dollar industry is open to cyber attack.

Security researchers have for years been warning the maritime industry that it is low hanging fruit as incredibly high-value cargo is transported on ships with legacy systems, combined with poor processes and awareness, while the seaports they dock in often suffer from the same problems.

Seitenkanalangriffe (Bsp. VSAT und Spectre/Meltdown)

Ships Are Vulnerable to Cyber Attacks Due To Maritime Platform Flaw

By Waqas on October 29, 2017 Email @hackread HACKING NEWS SECURITY

Fake News of Next Generation Eloka?

INDEPENDENT

News World Cup Politics Voices Indy/Life InFact Sport Business Video Culture IndyBest Subscribe

News › World › Europe

Russia claims to have weapon that could cripple the US Navy

State news report surfaces three years after alleged use of jammer against American destroyer

Jon Sharman | Thursday 20 April 2017 19:17 | 20 comments

Like Click to follow The Independent Online

Tuesday, June 26, 2018 Sign in / Join About VT Disclosures Resources Events Contact

VT VETERANS TODAY

GOVERNMENT INVESTIGATIONS LIFE HISTORY VT RADIO WARZONE WORLD VETERANS

Home › WarZone › AEGIS Fail in Black SEA, Ruskies Burn Down USS Donald "Duck"

WarZone

AEGIS Fail in Black SEA, Ruskies Burn Down USS Donald "Duck"

By VT Senior Editors - November 13, 2014 6115 53

Search VT

SUPPORT VT Help Us Expose Truth Contribute Now GET INVOLVED! AND DONATE

What's HOT from Senior Editors

AWAKE: A Dream from Standing Rock

Jim W. Dean, Managing Editor - June 26, 2018 2

Cyber Solutions – Fields of Activity