
BEDROHUNGEN
VERÄNDERN SICH.
WIR UNS AUCH.
ZUSAMMEN STÄRKER.
In den falschen Händen kann selbst ein Computer zur Waffe werden. Das Bundesheer
investiert in modernste Technologien und ist auf Cyber-Bedrohungen vorbereitet.
bundesheer.at
UNSER HEER

Der Cyber-Raum ist überall
Direktion IKT&Cyber - MilCyZ

KI im militärischen CyberRaum

Dion IKT&Cyber / MilCyZ

05 09 2023

Dipl-HTL-Ing. Lambert SCHARWITZL, MSc,MA
Leiter Militärisches Cyber-Zentrum
Tel: +43 664 622 1892
lambert.scharwitzl@bmlv.gv.at
www.bundesheer.at

Nationale Bedrohungen

CHRONIK ÖSTERREICH 17.06.2022

Nach Hackerangriff in Kärnten wurden erneut Daten veröffentlicht

Diesmal allerdings im Darknet. Daten lassen sich nun wohl nicht mehr so leicht löschen wie vor zwei Wochen.

CHRONIK

Hackerangriff legt Feldbacher EDV lahm

Am Wochenende ist die Stadt Feldbach Opfer eines Hackerangriffs geworden: Das EDV-System wurde übernommen; sollte die Stadt ihre Daten wiederhaben wollen, müsse Lösegeld bezahlt werden.

6. September 2022, 12:35 Uhr

Cyberangriff auf Innsbrucker Med-Uni: Daten im Darknet veröffentlicht

Analysen und Ermittlungen zum Ausmaß und der Art der Daten seien im Gange. Ein Großteil der zentralen Daten wurde bereits wiederhergestellt.

Letztes Update am Dienstag, 28.06.2022, 19:38

Digital Life

Salzburger Großmolkerei durch Cyberangriff lahmgelegt

23.06.2021

Die Salzburger Großmolkerei "Salzburgmilch" ist in der Nacht auf Mittwoch einem Cyberangriff zum Opfer gefallen.

Cyberangriff auf Außenministerium: Spekulationen, Gerüchte, aber kaum Fakten

Medienberichte überbieten sich in Theorien zur Urheberschaft. In Wirklichkeit ist bisher aber praktisch nichts bekannt

Analyse / Andreas Proschofsky

8. Jänner 2020, 16:00, 78 Postings

Quellen:
https://www.derstandard.at/story/2000113051137/cyberangriff-auf-aussenministerium-spekulationen-geruechte-aber-kaum-fakten
FutureZone
orf.at

Internationale Bedrohungen

Israel behind cyberattack that caused 'total disarray' at Iran port – report

Israel mum as Washington Post cites officials saying Jerusalem carried out 'highly accurate' hack, apparently in retaliation for Iran attempt to target Israeli water infrastructure

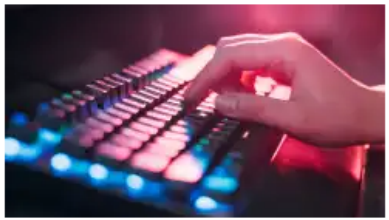
By TOI STAFF
19 May 2020, 4:38 am | 2

The Shahid Rajaee port facility in the Iranian coastal city of Bandar Abbas (Iran Ports and Maritime Organization)

Europa macht sich seine Falschinformationen längst selbst

EU sieht bei Europawahl keine groß angelegte Fake-News-Kampagne Russlands – Großteil der Falschnachrichten stammt aus EU-Ländern selbst

23. Mai 2019, 15:50, 9 Postings



> ‚sonstige Kriminalität im Internet' verzeichnete im ersten Halbjahr 2019 eine Steigerung von etwa 140 %

Hackerangriff auf Trinkwasser: Immer gleiches Passwort, Windows 7 und Teamviewer

Nach dem vereitelten Hackerangriff auf die Trinkwasserversorgung einer Stadt in Florida wird deutlich, wie schlecht die IT-Sicherheit vor Ort war.

12. Februar 2021, 10:01 Uhr 305 UPDATE heise online

Quellen:
https://www.it-daily.net/it-sicherheit/cybercrime/24120-cyberangriff-auf-die-kritische-infrastruktur-der-israelischen-wasserversorgung
https://www.timesofisrael.com/israel-said-behind-cyberattack-that-caused-total-disarray-at-iran-port-report/
https://www.reuters.com/article/us-australia-cyber/australia-sees-china-as-main-suspect-in-state-based-cyberattacks-sources-say-idUKKBN23P3T5
https://www.derstandard.at/story/2000103697721/europa-macht-sich-seine-falschinformationen-laengst-selbst
BKA Cybersicherheitsbericht 2020

Internationale Bedrohungen

- **BSI Deutschland:**

  Sicherheitslücken in Insulinpumpen/Herzschrittmachern

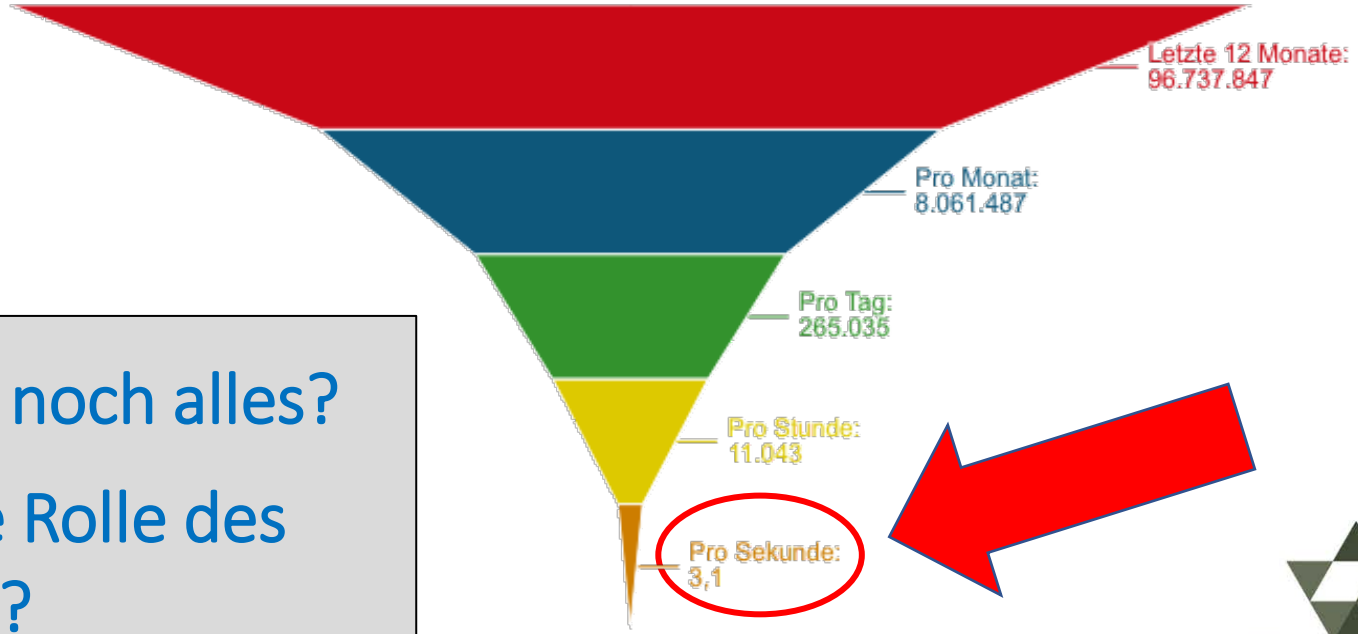
  - In zehn Medizinprodukten insgesamt 150 Sicherheitslücken gefunden
  - Beispiel: Mögliche Manipulation einer Insulinpumpe, eine tödliche Dosis zu verabreichen

Quelle: https://www.rnd.de/politik/cyber-studie-sicherheitslucken-bei-insulinpumpen-und-herzschrittmachern-DWNNSJ2S5ZCEDGJPJG6SJXUIMM.html

Die Gesellschaft hat sich verändert

Petersplatz
Papst Wahl

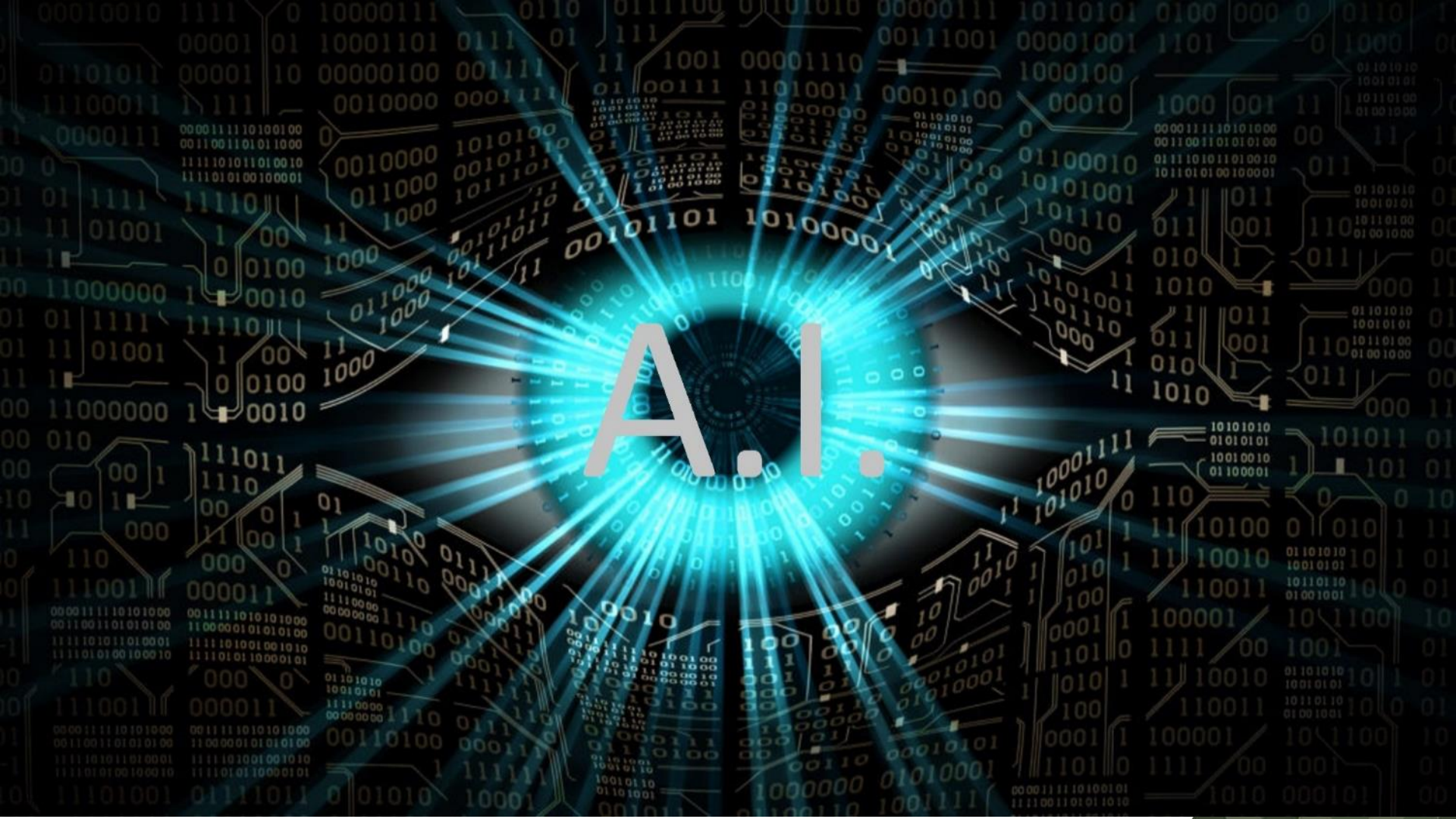
Neue Malware pro Sekunde 2023



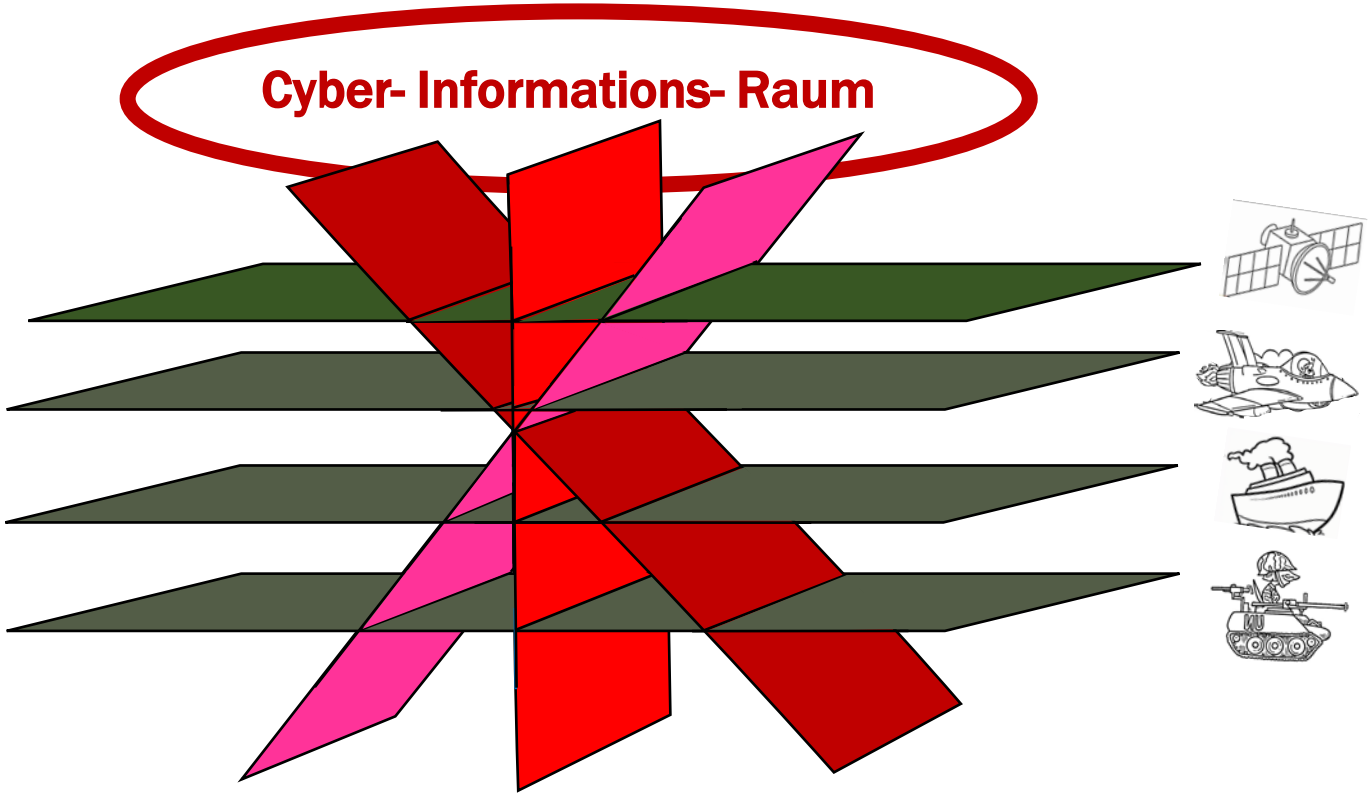
Kann IT da noch alles?

Was ist die Rolle des Menschen?

Quelle: https://portal.av-atlas.org/malware 28.08.2023


A.I.

Domänen moderner Kriegsführung



Space

Air

Maritime

Land

Militärische IT – aktuelle Cyber-Alarme

Beschreibung	Q1+Q2 2023 (01.01. bis 30.06.)	Φ KW 2023
Security-relevante Ereignisse	~86.000.000.000	~3.308.000.000
Malware & Exploit Events	601.050	23.117
Alarme („Offenses“) aus Sicherheitssystemen	800	31
Vermutlich gezielte Angriffe	26	2
Useranfragen / Usermeldungen	756	29
Denial-of-Service	78	3

Cyber-Herausforderungen im Militär

- **Angriffe kaum vorhersagbar** (Zeit und Distanz außer Kraft)
- Waffensysteme sind vernetzt
- KI ist in den mil-Systemen integriert
- Großflächige, zeitgleiche Angriffe möglich
- Einsatzraum nicht konkret spezifizierbar (Feuerbereich)
- Militär ohne IKT nicht einsatzfähig
- Zusammenwirken von „Mensch und Maschine“ ist gefordert
- Technologische Neuentwicklungen erleichtern Angriffe

Gefechtsfeld der Zukunft

- **Künstliche Intelligenz**
  maschinelles Lernen, analysieren, interpretieren, entscheiden

- **Fortgeschrittene Robotik und autonome Systeme**
  unbemannte Systeme Betrieb ohne menschliche Überwachung

- **Biotechnologie**
  gentechnische Modifikation, medizinische Versorgung, …

- **Sateliten und weltraumgestütze Technologien**
  Zugang zum Weltraum, Aufklärung Navigation, Kommunikation, …

DROHNENFLUG

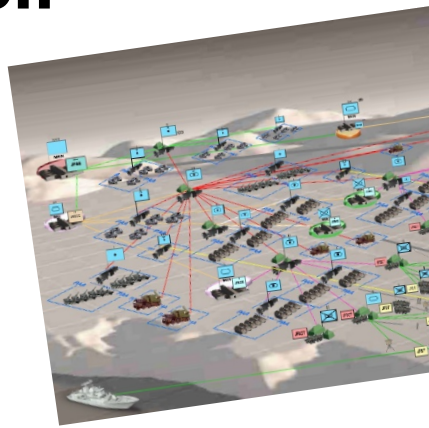
Künstliche Intelligenz schlägt Weltmeister

Eine von künstlicher Intelligenz (KI) gesteuerte Drohne hat im Wettflug gleich zwei amtierende Weltmeister geschlagen. Das von der Universität Zürich entwickelte System, das auf einer speziellen Form des maschinellen Lernens basiert, stellt laut den Studienautoren einen Meilenstein dar – sowohl für die Robotik als auch für KI.

Leonard Bauersfeld

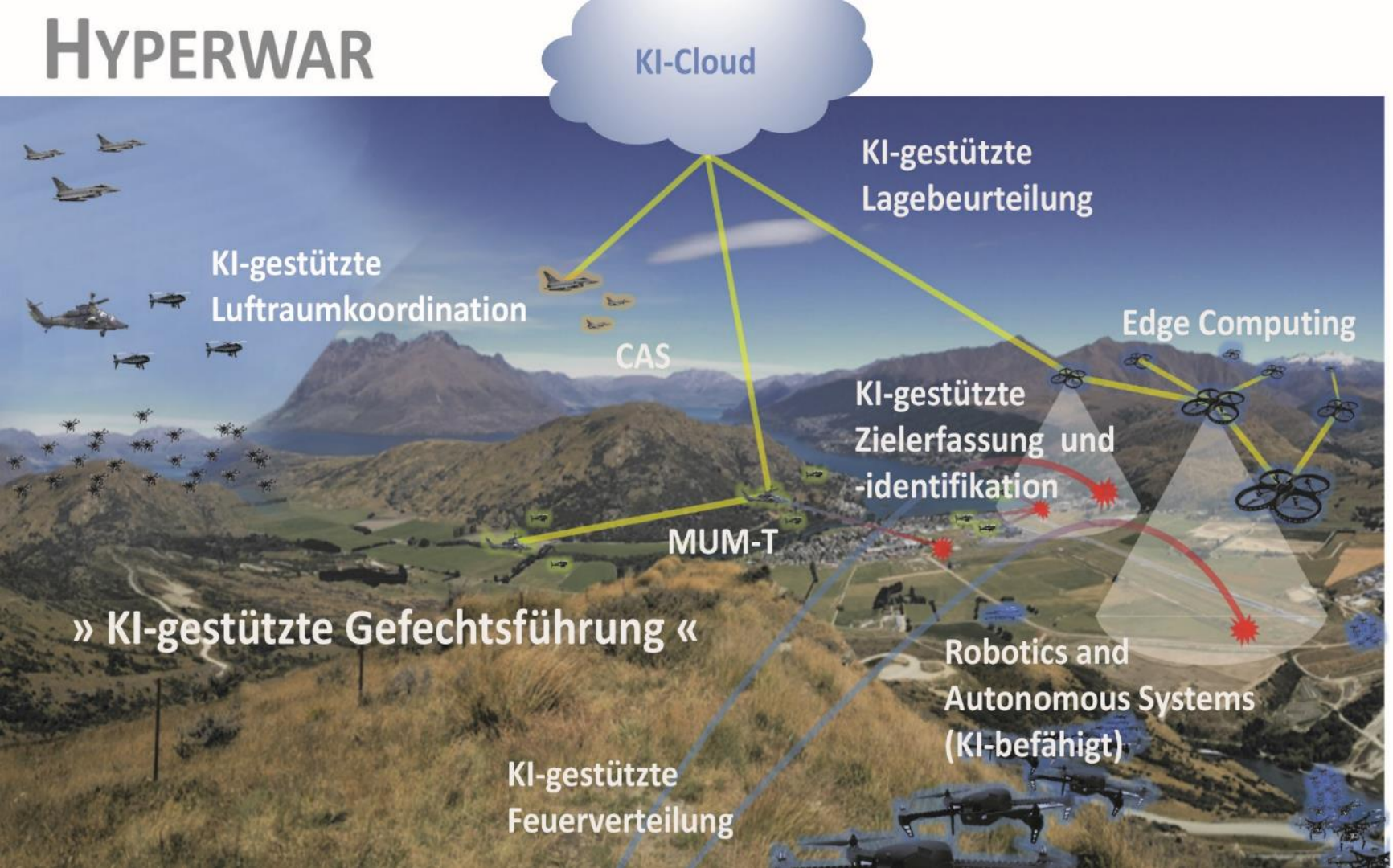
Quelle: Quelle: https://science.orf.at/stories/3220957/ 31.08.2023

KI hat neue Herausforderungen geschaffen



- **Angriffe mit KI**
  KI um Angriffe zu automatisieren und zu verbessern
- **Schlacht der Algorithmen**
  Wettlauf zwischen Angreifern und Verteidigern
- **Fehlende Transarenz**
  KI-Systeme können undurchsichtig agieren und Entscheidungen nachzuvollziehen
- **Datenschutzbedenken**
  Zugriff auf große Mengen sensibler Daten, um Modelle zu trainieren
- **Ethik und Verantwortung**

HYPERWAR



UNSER HEER

EU/EDA und NATO Festlegung: Principles for Responsible Use of AI in mil. Defense

(1) **Lawfullness** (Rechtmäßigkeit)

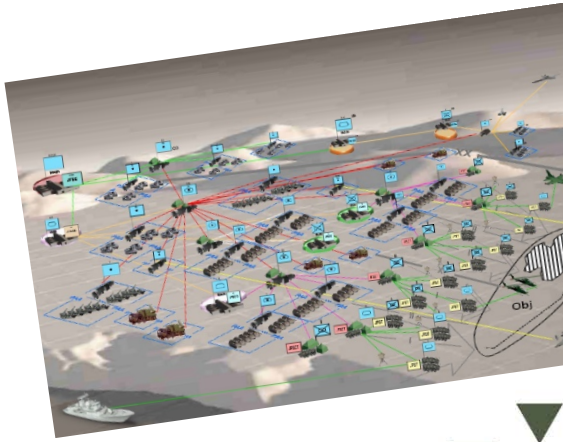
(2) **Responsibility** (Verantwortung)

(3) **Reliability** (Verlässlichkeit)

(4) **Governability** (Beherrschbarkeit)

(5) **Explainability and Traceability**
(Erklärbarkeit + Nachvollziehbarkeit)

(6) **Bias Mitigation** (Abschwächung von Vorurteilen)

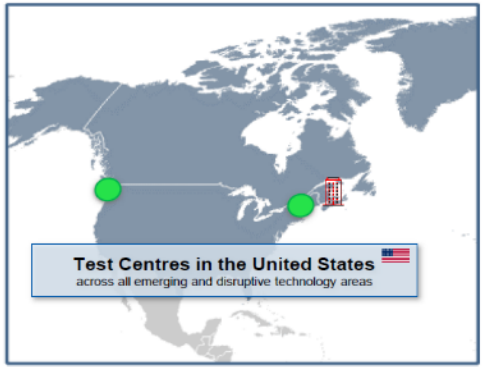


Updated DIANA footprint: Test Centres

June 2023

Key

- Regional Offices
- Regional Hub
- Test Centres
- Accelerators



GERMANY – 9 sites
AI, data, autonomy, space, quantum, hypersonics, secure communications, energy and propulsion, semiconductors

DENMARK – 4 sites
quantum, nanotechnologies, novel materials, optics, laser, metrology

NETHERLANDS – 2 sites
AI, robotics, autonomous systems, novel materials, energy, quantum

NORWAY
data, autonomy, robotics

BELGIUM – 14 sites
AI, autonomy, hypersonics, manufacturing, cyber, nanoelectronics, ICT

UNITED KINGDOM
operational testing

FRANCE – 10 sites
AI, autonomy, quantum, biotechnologies, energy and propulsion, novel materials, advanced manufacturing, hypersonics, space

SPAIN – 5 sites
AI, maritime, neurotechnology, 5G, quantum communications, energy

PORTUGAL
AI, data, autonomy, novel materials

ITALY – 2 sites
data, maritime, ISR, air, space, materials

SLOVENIA – 3 Sites
AI, 5G, cybersecurity, critical infrastructure

ESTONIA – 6 sites
AI, data, autonomy, cyber, robotics, space, quantum, biotechnologies, novel materials, manufacturing, unmanned vehicles, aerospace

LATVIA
AI, data, communication technology

LITHUANIA – 6 sites
AI, data, autonomy, cyber, greentech, biotechnology, space, novel materials, energy and propulsion

POLAND – 7 sites
AI, data, autonomy, CBRN, cyber, communication technology, quantum

SLOVAKIA – 6 sites
AI, data, autonomy, robotics, cyber, space, aerospace, biotechnology

HUNGARY – 2 sites
AI, autonomy, cyber

ROMANIA – 2 sites
AI, hypersonics

BULGARIA – 3 sites
AI, data, autonomy

TÜRKIYE – 2 sites
AI, data, autonomy, computing, cyber, biotechnology, space, hypersonics, quantum

GREECE – 4 sites
AI, data, autonomy, space, quantum, biotechnology, novel materials and manufacturing

Quelle:
https://www.nato.int/cps/en/natohq/news_213074.htm 31.08.2023

Kann KI bei Randsomewareangriffen helfen

eine Frage an ChatGPT

** Verhaltensanalyse **

** Mustererkennung **

** Echtzeitschutz **

** Benachrichtigung und Berichterstellung **

** Verbesserung der Sicherheitsmaßnahmen **

KI kann Ransomware-Angriffe nicht verhindern

Ein ganzheitlicher Ansatz zur Cybersicherheit ist entscheidend
Updates, Backups, User-Schulungen, RiskMngt usw.


MILITÄRISCHES
CYBER-ZENTRUM
UNSER HEER

MILITÄRISCHES CYBER-ZENTRUM

UNSER HEER

MILITÄRISCHES CYBER-ZENTRUM

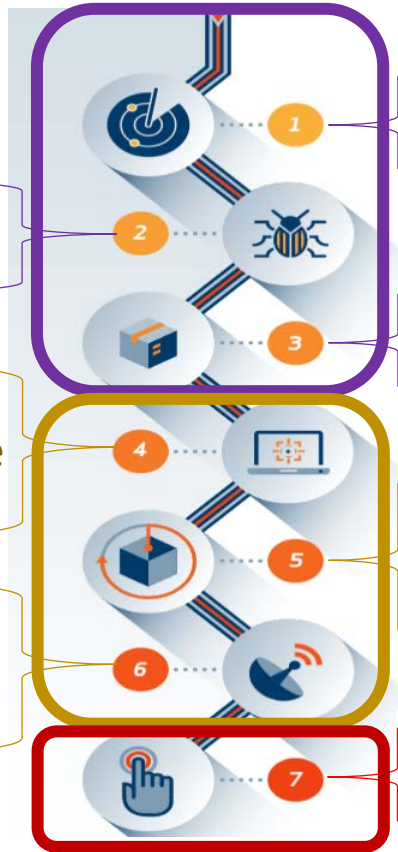
UNSER HEER

CYBER KILL CHAIN (nach LOCKHEED MARTIN)

Reconnaissance: *Aufklärung* von techn. und pers. Informationen des Ziels

Weaponization: der Bau von Angriffswerkzeugen

Delivery: Auslieferung der gebauten Angriffswerkzeuge zu dem Ziel



Exploitation : über die Ausnutzung einer Schwachstelle im Zielsystem aktiv werden

Installation: die Payload des Angriffswerkzeugs Schadsoftware installieren.

Command und Control: Aufbau eines C2-Kanals zur Steuerung des Angriffs

Actions on Objectives: vorgegebene Ziele umzusetzen

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 – IKT & Cyber
Militärisches Cyber Zentrum

Ukraine 2022

INVASION BEGINS

Political-military events

January 13
Intensive diplomatic talks between Russia, US, Ukraine, NATO, Europe fail.

February 1
President Putin says the US and NATO completely ignored Russian security demands, after reviewing written responses that the US and NATO had submitted to Russian demands.

February 17
Kremlin said it would be "forced to respond" with military-technical measures if the US continued to ignore calls for guarantees that Ukraine will never be admitted to NATO but denied plans to invade Ukraine.

February 21
President Putin recognizes independence of Ukrainian separatist regions, nullifying terms of existing Minsk peace agreements with Ukraine.

February 24
Russia invades Ukraine.

January ..... February

Cyberattacks

January 13
DEV-0586 deploys WhisperGate wiper to limited number of Ukrainian government and IT sector systems.

January 14
DEV-0586 defaces and an unknown actor starts a distributed denial of service (DDoS) attack on Ukrainian government websites.

February 15–16
Russian military intelligence (GRU) DDoS attacks against Ukrainian financial institutions.

February 23
IRIDIUM deploys FoxBlade wiper to hundreds of systems in Ukrainian government, IT, energy, and financial sectors.

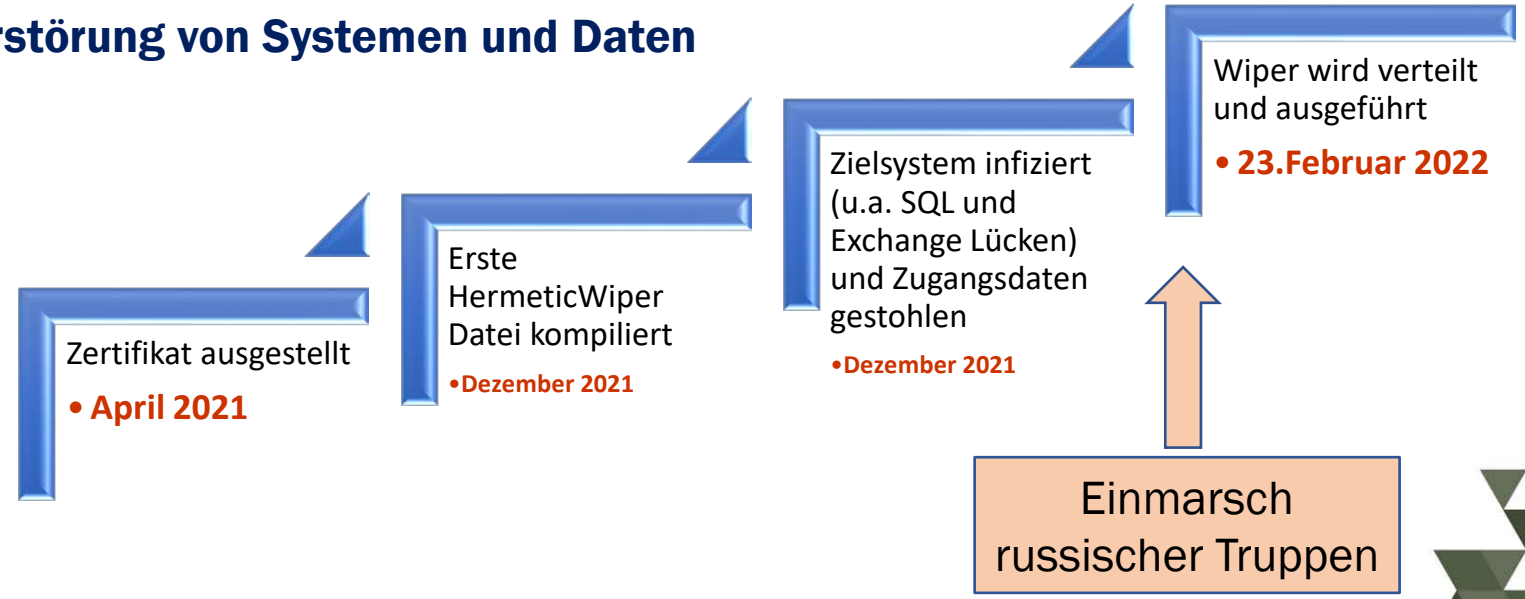
Hermetic Wiper

February 24
External reporting indicates that the GRU launches a denial of service attack against Viasat, disrupting broadband service to tens of thousands of users in Ukraine and throughout Europe.

Cyber-Aktivitäten sind geplant
Bsp. Konflikt Ukraine 2014 - 2022

Hermetic Wiper Malware

Ziel:
Zerstörung von Systemen und Daten



ÖSTERREICHISCHES BUNDESHEER
IKT & Cybersicherheitszentrum

CYBER FORCES

CONNECT and PROTECT

UNSER HEER