ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber

Direktion IKT&Cyber

Österreichisches Bundesheer im Cyber-Raum

Lambert SCHARWITZL
Leiter Militärisches Cyber-Zentrum

EINSATZBEREIT FÜR ÖSTERREICH
BUNDESHEER.AT

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Militärisch & Hybrid

RUS – UA (2023)

- **Cyberattack knocks out satellite communications for Russian military**
  - A satellite communications system serving the Russian military was knocked offline by a cyberattack late Wednesday and remained mostly down on Thursday, in an incident reminiscent of an attack on a similar system used by Ukraine

A view of the Kremlin in Moscow. (Sergei Ilnitsky/EPA-EFE/Shutterstock)

Quelle: https://www.washingtonpost.com/technology/2023/06/30/satellite-hacked-russian-military/

2

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Militärisch & Hybrid

RUS – UA (2023)

- **First surface vessel attack on Crimea failed as Musk turned off connection**
  - Ukraine tried for the first time to use uncrewed surface vessels against Russian vessels in Sevastopol Bay in September 2022, but 70 kilometres from the target, the connection with billionaire Elon Musk's Starlinks was lost. It was not possible to persuade Musk to turn back on the connection, so Ukraine modified the drones.

A view of the Kremlin in Moscow. (Sergei Ilnitsky/EPA-EFE/Shutterstock)

Quelle: https://www.pravda.com.ua/eng/news/2024/01/1/7435389/

3

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Militärisch & Hybrid

Israel - Gaza Conflict (Zeitraum 6. bis 17. Okt 23)

- 6. Oct 2023:
  - Cyber Av3ngers, a hacktivist group, claims responsibility for hacking the Noga Independent Systems Operator in Israel (electricity sector)
- 7. Oct 2023:
  - Within an hour of the 5000+ missile attack on Israel by Hamas, hacktivist group Anonymous Sudan launched DDOS attacks on all the alert applications used for notifying citizens about incoming rockets
- **8. Oct 2023:**
  - The Israeli government's official website becomes unreachable worldwide, and the Russian hackergroup 'Killnet' claims responsibility for the attack.
  - ThreateSecc laimed to have breached and shutdown Alfanet, Palestine's largest ISP provider.

Quelle: Cyfirma

4

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Militärisch & Hybrid

Israel - Gaza Conflict (Zeitraum 6. bis 17. Okt 23)

- October15,2023:
  - Hacktivist group „Anon Ghost Indonesia“ claims to leak the database of a dating and consolidation project for the Israeli LGBTQ-community “TheGaydar”on Pastebin.
- October16,2023:
  - Amidst other attacks Israeli news websites “AllIsraelNews”
  - “YourAnonT13x” attacks „Abu Ali Express“
- October17,2023:
  - Hacktivist group „Anon Ghost“ dumped a list of Israeli targets vulnerable to CVE-2023-29489 along with the exploit. → Global Attacs started

Quelle: Cyfirma

5

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Die Bedrohungslandschaft von heute

In jedem beliebigen 60-Sekunden-Fenster jeder Stunde eines Tages sind Hacker*innen aktiv

Angriffe auf Passwörter	34.740 pro Minute [1]
IoT-basierte Attacken	1.902 pro Minute [2]
DDoS-Attacken	1.095 pro Minute [3]
Phishing-Angriffe	7 pro Minute [4]
SQL-Injection-Attacken	1 alle 2 Minuten [5]
Entdecken neuer Infrastruk-turen, die IT-Systeme bedrohen	1 alle 35 Minuten [6]
Angriffe auf Lieferketten	1 alle 44 Minuten [7]
Ransomware-Attacken	1 alle 195 Minuten [8]

Quelle: RiskIQ (Microsoft CyberThreat Report)

6

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Die Bedrohungslandschaft von heute

Neue Hosts	79.861 pro Minute [26]
Neue IoT-Geräte	7.620 pro Minute [27]
Neue Domains	150 pro Minute [28]
Neue aktive Lets-Encrypt SSL-Zertifikate	53 pro Minute [29]
Neue mobile Apps	23 pro Minute [30]

Mit der wachsenden Verbreitung des Internets mehren sich auch hier die Angriffsmöglichkeiten für Hacker*innen

Quelle: RiskIQ (Microsoft CyberThreat Report)

7

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

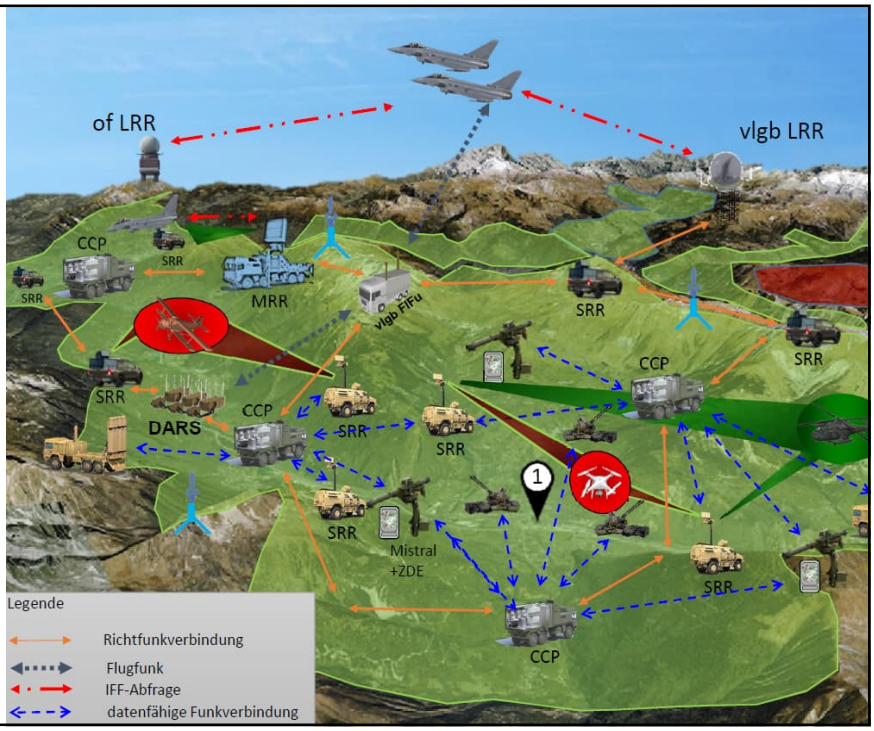
ENISA Threat Landscape – prime Threats

Quelle: www.ccdcoe.org: Escalation Roadmap

8

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

- Vollvermaschung
- IT / OT
- RealTime
- Undefinierter Raum
- Mensch / Maschine
- ...

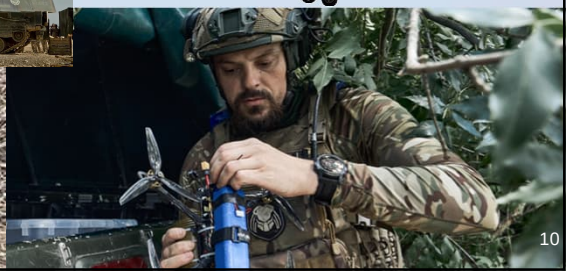


ÖSTERREICHISCHES BUNDESHEER
Direktion 6 – IKT & Cyber
Militärisches Cyber Zentrum

Militärischer Einsatz
Mil IoT







10

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Serviceverfügbarkeit Aktuelle Herausforderungen

- Angriffe kaum vorhersagbar (Zeit und Distanz außer Kraft)
- Systeme sind vernetzt (IT / OT)
- KI ist in den Systemen integriert
- Großflächige, zeitgleiche Angriffe möglich
- Einsatzzielraum nicht konkret spezifizierbar (Feuerbereich)
- Unternehmen ohne IKT nicht überlebensfähig
- Zusammenwirken von „Mensch und Maschine“ ist gefordert
- Technologische Neuentwicklungen erleichtern Angriffe

11

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Resilienz

- lateinischen „resilire” → „zurückspringen“ bzw. „abprallen“
- Resilienz ist die Fähigkeit von Systemen, bei Teil-Ausfällen oder Störungen nicht vollständig zu versagen, sondern wesentliche Systemdienstleistungen weiter aufrechtzuerhalten.

&

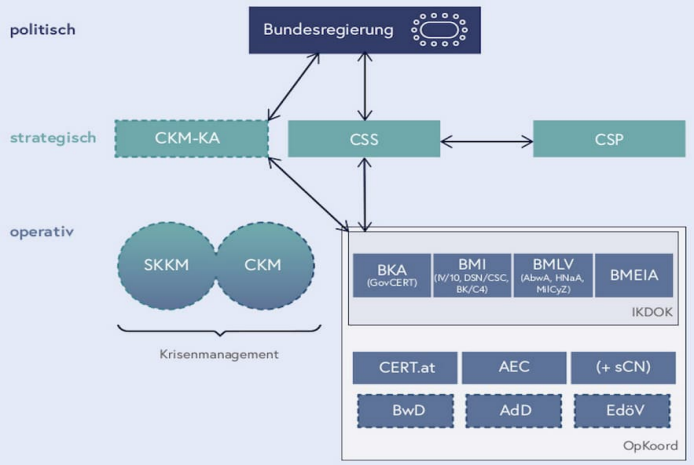
Incident-Mngt

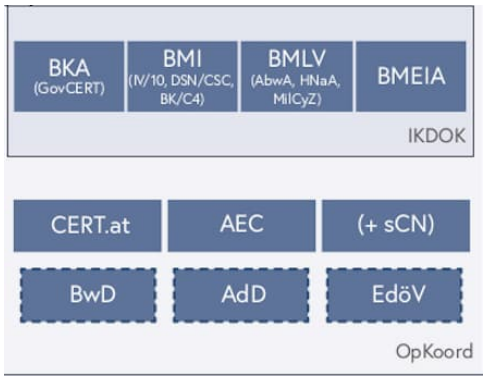
- Incident eine kurzfristige Störung oder unerwarteter Vorfall, der den normalen Betriebsablauf eines Unternehmens beeinträchtigt und rasch behoben wird.
- Ein Incident ist ein für sich stehendes und somit isoliertes Ereignis
- Security Incident Mngt ist die schnelle Reaktion auf sicherheitsrelevante Vorfälle.

12

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Nationale Cyber-Sicherheitsstrukturen

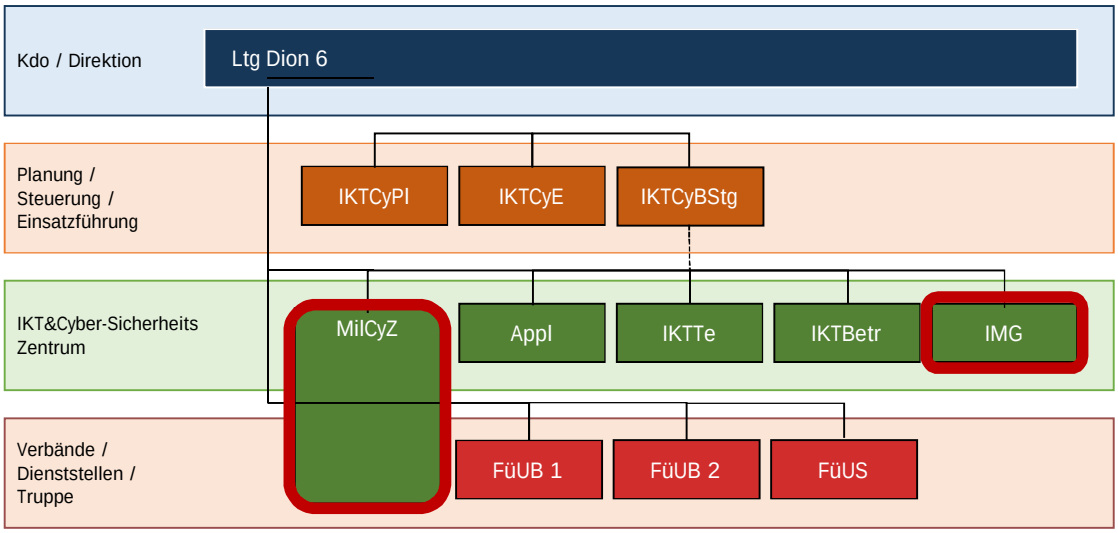




13

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Struktur Dirketion 6 IKT&Cyber

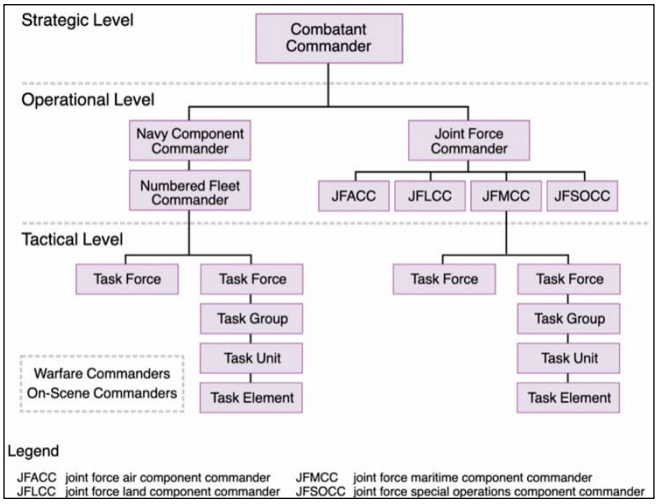


14

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Klassische mil. Einsatzstrukturen auch im Normbetrieb

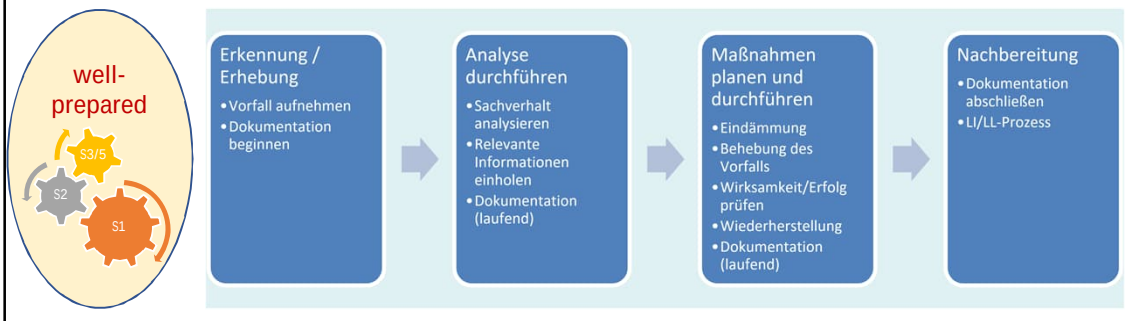
- Definierte Kompetenzen
- Festgelegte Prozesse
- Festgelegte Eskalationsstufen
- Festgelegte Meldeformate
- Incident Mngt auf allen Ebenen



15

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

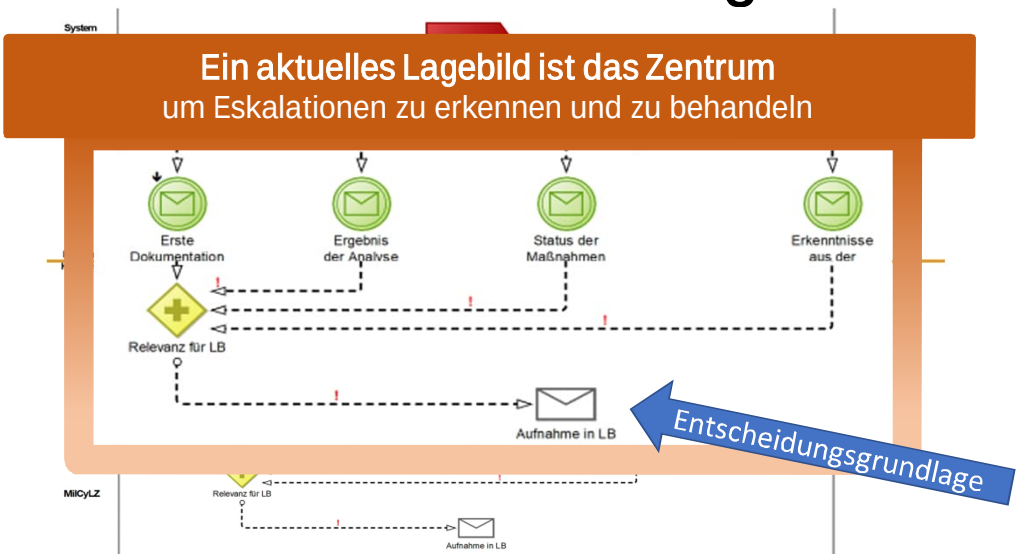
Incident Mngt beginnt im Normbetrieb



16

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Prozess des Incident Managements



17

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Focus Area für Defence in Depth Strategy

Incident-Mngt ist mehr als Technik

Defence in Depth Strategy

People | **Technology** | **Operations**

Defence in Depth Focus Areas

- Defend the Network
- Defend the Enclave Boundary
- Defend the Computing Environment
- Defend the Supporting Infrastructures

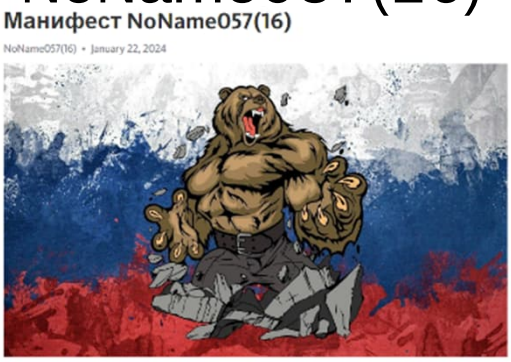
18

Quelle: www.ccdcoe.org: Cyber Red Teaming

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

DDoS bei Hacktivisten – NoName057(16)

- Aktiv seit 03/2022 (Beginn der Hacktivisten bei Krieg in UA)
- Motivation:
  - Für „russische Werte“ und gegen „russophobische“ Nationen/Organisationen
- Modus Operandi:
  - DDoS Angriffe mit Hilfe eines „volunteer“ Botnetzes gegen Webseiten
  - Ziele werden täglich geändert



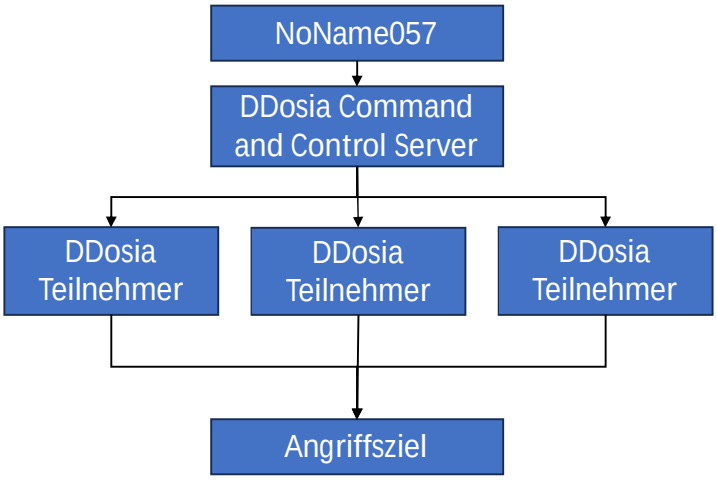
Мы не первый год отстаиваем интересы России на информационном фронте. Мы видим, как растут недовольства адекватных граждан иностранных государств, власти которых наплевали на проблемы своих соотечественников и тратят огромные средства на спонсирование украинских террористов. Видим мы и тотальную цензуру, которая не дает говорить правду жителям этих стран. Там стало недопустимо позитивно высказываться в адрес России. От свободы слова на Западе не осталось абсолютно ничего.

Manifest NoName057(16) – Telegraph

19

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

NoName057(16) – DDosia Botnet



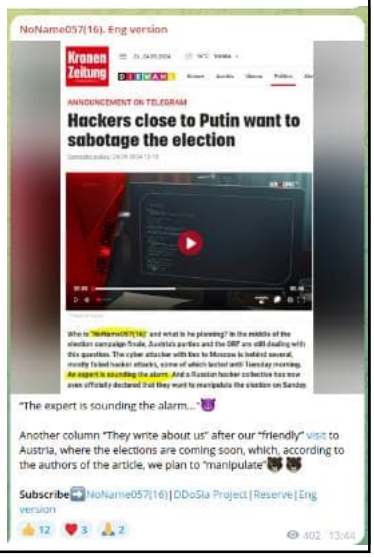
- Angekündigt am 15.09.2022
- Freiwillige melden sich via Telegram an und installieren Software
- NoName057 stellt Ziellisten auf Server
- Software holt sich regelmäßig Ziellisten und führt die Angriffe aus

20

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

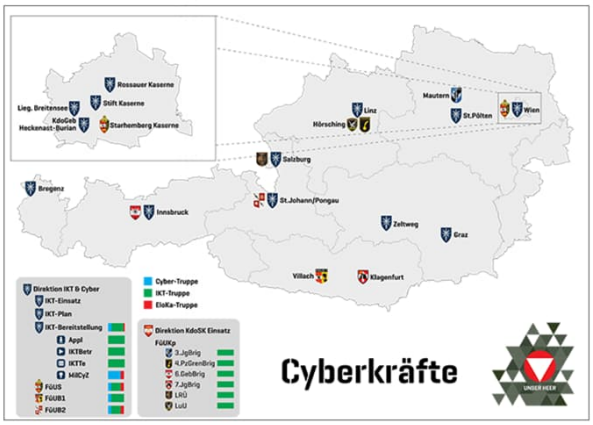
Einschätzung zu NoName057(16)

- Angriffe auf maximale mediale Sichtbarkeit ausgerichtet
  - oftmals aus tagespolitischem Geschehen (und zugehörigen russ. Medienberichten) ableitbar
- Erfolgsmeldungen auf sozialen Medien (Twitter, Telegram)
  - Berichte über Nichterreichbarkeiten
  - Rubrik „Sie schreiben über uns“:
    Verbreitung von Medienberichten über die Aktionen
- Nach Kampagne zieht Gruppierung weiter
- Funding für „volunteer“ Botnetz unklar -> Mögl. Konnex zu RU ND



ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

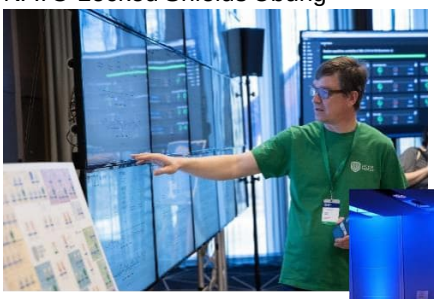
Bundesheer als Cyberausbilder



ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

Gemeinsam Fähigkeiten trainieren

NATO Locked Shields Übung



Quelle: https://ccdcoe.org/exercises/locked-shields/

KSÖ Planspiele

Quelle: Kompetenzzentrum Sicheres Österreich

Quelle: https://verbotengut.at/

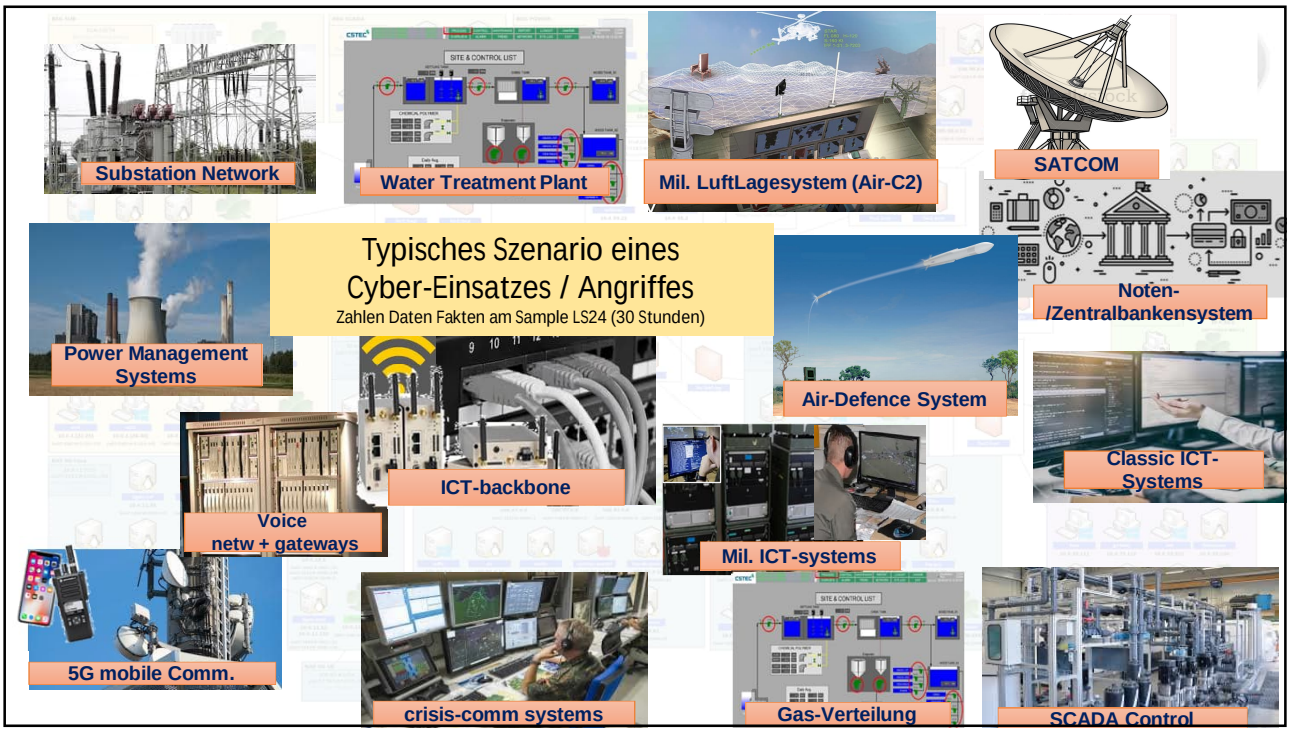
CSA Cybersecurity Challenge

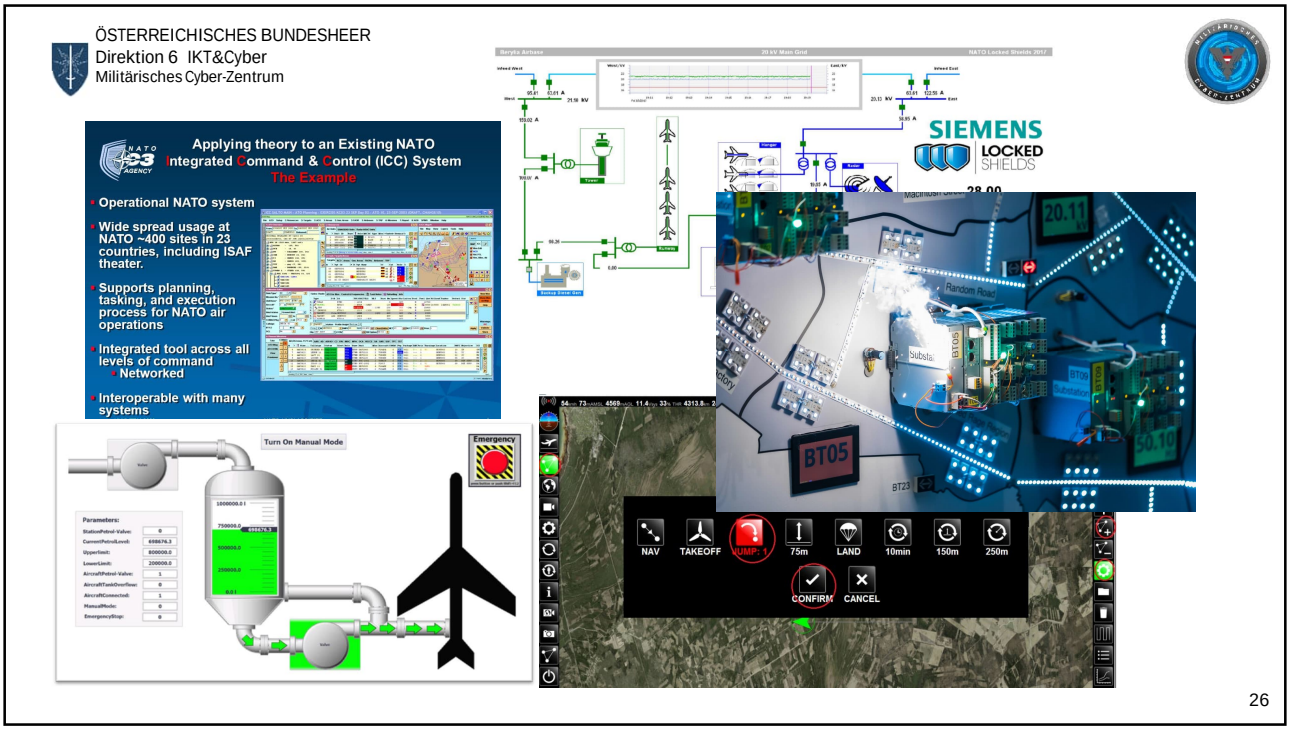
23

ÖSTERREICHISCHES BUNDESHEER
IKT & Cybersicherheitszentrum
Militärisches Cyber-Zentrum

LOCKED SHIELDS 2024

Weltweit größte Cyber-Übung


Substation Network
Water Treatment Plant
Mil. LuftLagesystem (Air-C2)
SATCOM
Typisches Szenario eines
Cyber-Einsatzes / Angriffes
Zahlen Daten Fakten am Sample LS24 (30 Stunden)
Power Management Systems
Noten-/Zentralbankensystem
Air-Defence System
ICT-backbone
Classic ICT-Systems
Voice netw + gateways
Mil. ICT-systems
5G mobile Comm.
crisis-comm systems
Gas-Verteilung
SCADA Control


ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum
Applying theory to an Existing NATO Integrated Command & Control (ICC) System
The Example
Operational NATO system
Wide spread usage at NATO ~400 sites in 23 countries, including ISAF theater.
Supports planning, tasking, and execution process for NATO air operations
Integrated tool across all levels of command
Networked
Interoperable with many systems
SIEMENS
LOCKED SHIELDS
Turn On Manual Mode
Emergency
BT05
NAV
TAKEOFF
75m
LAND
10min
150m
250m
CONFIRM
CANCEL
26


ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT & Cyber
MilCyZ


LOCKED
SHIELDS
2023

ÖSTERREICHISCHES BUNDESHEER
Direktion 6 IKT&Cyber
Militärisches Cyber-Zentrum

In einer unsicheren Welt braucht es

belastbare IT-Infrastrukturen

und

gelebte Prozesse!