DCSO

WebCast

It’s the Geopolitics, Stupid

Die Rolle geopolitischer Faktoren im Bereich der Cyber Threat Intelligence

Thomas Hemker, CISSP, CISM, CISA, CDPSE

Dr. Kerstin Zettl-Schabath

15.01.2026

TLP:CLEAR

Thomas Hemker, CISSP, CISM, CISA, CDPSE

Senior Director Cyber Defense

Bei der DCSO zuständig für den Threat Intelligence Service und den DCSO Fachbeirat.

- 30 Jahre Cybersecurity
- BSI Expertenkreis (prev. ENISA ETL, ISF Council)
- ISACA, (ISC)2 / TeleTrust, VDMA
- Sprecher, Autor, Lehrbeauftragter
- NAI, PGP, SYMC
- Hamburg, Musik, Rad, Berge

researchgate.net/profile/Thomas_Hemker3

linkedin.com/in/themker

xingcom/profile/Thomas_Hemker/cv

Dr. Kerstin Zettl-Schabath

Senior Cyber Threat Intelligence Analyst

Bei der DCSO im Threat Intelligence Research and Intelligence Team als Analystin tätig.

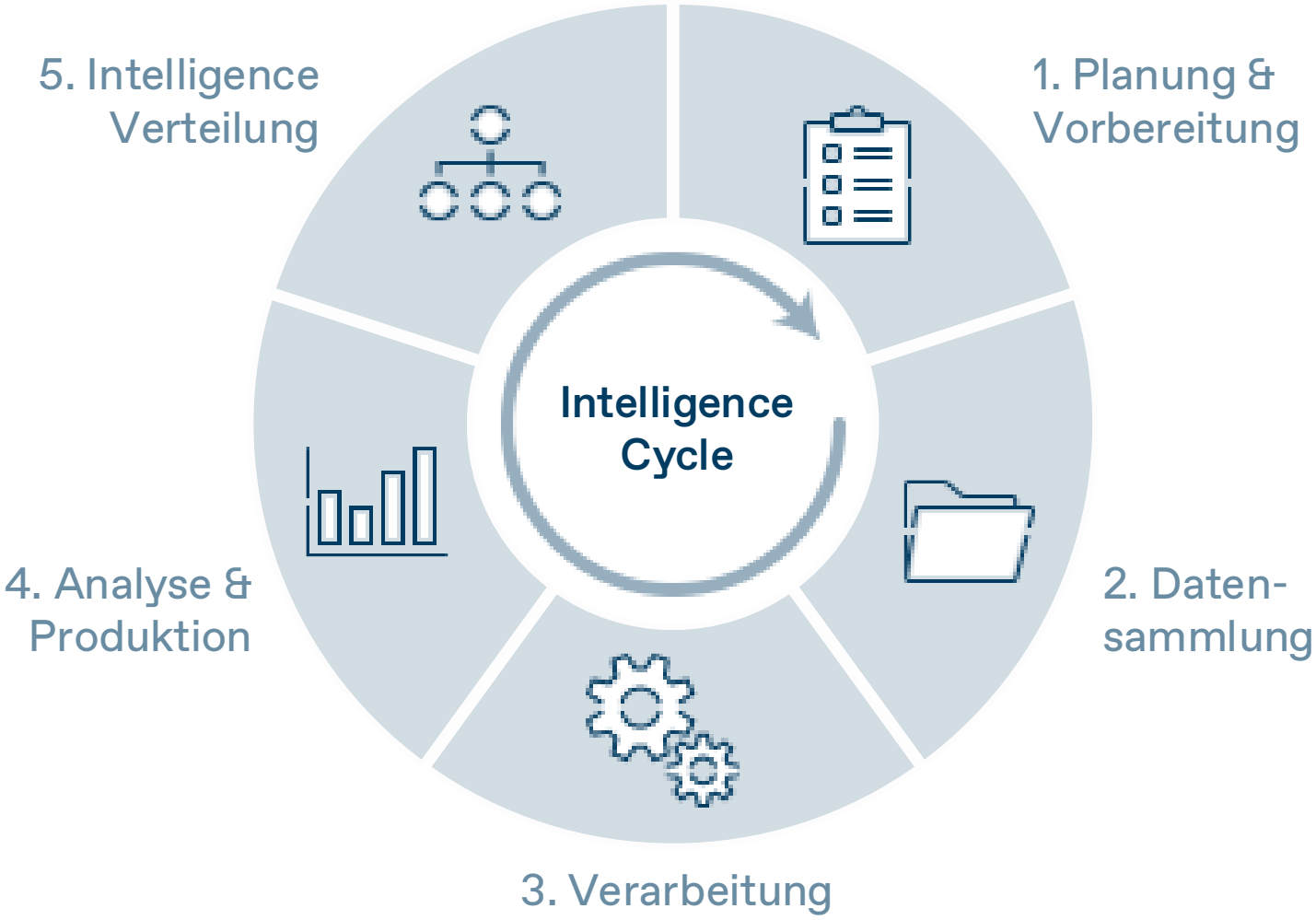
- Von Haus aus Politikwissenschaftlerin
- Zuvor tätig in diversen Cyberkonfliktforschungsprojekten (z.B. EuRepoC an der Uni Heidelberg)
- Regelmäßig Sprecherin bei Konferenzen; öffentlichen Veranstaltungen; Podcasts
- Beheimatet in BW

Linkedin.com/in/dr-kerstin-zettl-schabath-62a232259

DCSO TI Service

Kurze Übersicht

- Wir betreiben relevante Sharing Communities für die TI-Teams unserer Kunden.
- Wir bieten Berichte über unser Portal und technische Information über unsere MISP-Instanzen und eigene technische Plattform („TIE“).
- Wir sind einer der größten Managed Service Provider in Deutschland für die MISP-Instanzen unserer Kunden, welche diese für das Indicator Management und den Austausch benutzen.



Agenda

1. CTI Grundlagen
2. Geopolitik
3. Staatlich „vs.“ Cybercrime
4. Cyber goes physical
5. TI-Forecast
6. Fragen und Antworten

1 Grundlagen

Warum ist Cybersicherheit und damit auch TI eben KEIN rein technisches Thema?

Einordnung von Threat Intelligence

Zielgruppengerechte Kommunikation

Strategisch

Ziel: Geschäftsleitung bei Entscheidungen zu unterstützen

C-Level Exec, Group Security, Business Stakeholders, Risiko Manager

Wirtschaft & Politik

(Industrie) Spionage
Sabotage

Reports | Presse

Dossiers

Operational

Ziel: Angreifer und ihre Vorgehensweise verstehen

Fähigkeiten, Motivation, Ziel
TTPs

Incident Responder, Threat Hunter, Netzwerk Architekten, System Administratoren, Schwachstellenmanagement, Red Teams, IT-Manager

TTPs | Fähigkeiten

Diamond Model

Taktisch

Ziel: Wissen anwenden, um Angriffe aufzuspüren

Informationen direkt in Detektions, Korrelations und Abwehrsysteme einspeisen

SOC-Team, SIEM, Sicherheitstechnologie

File Hashes | URLs, IPs

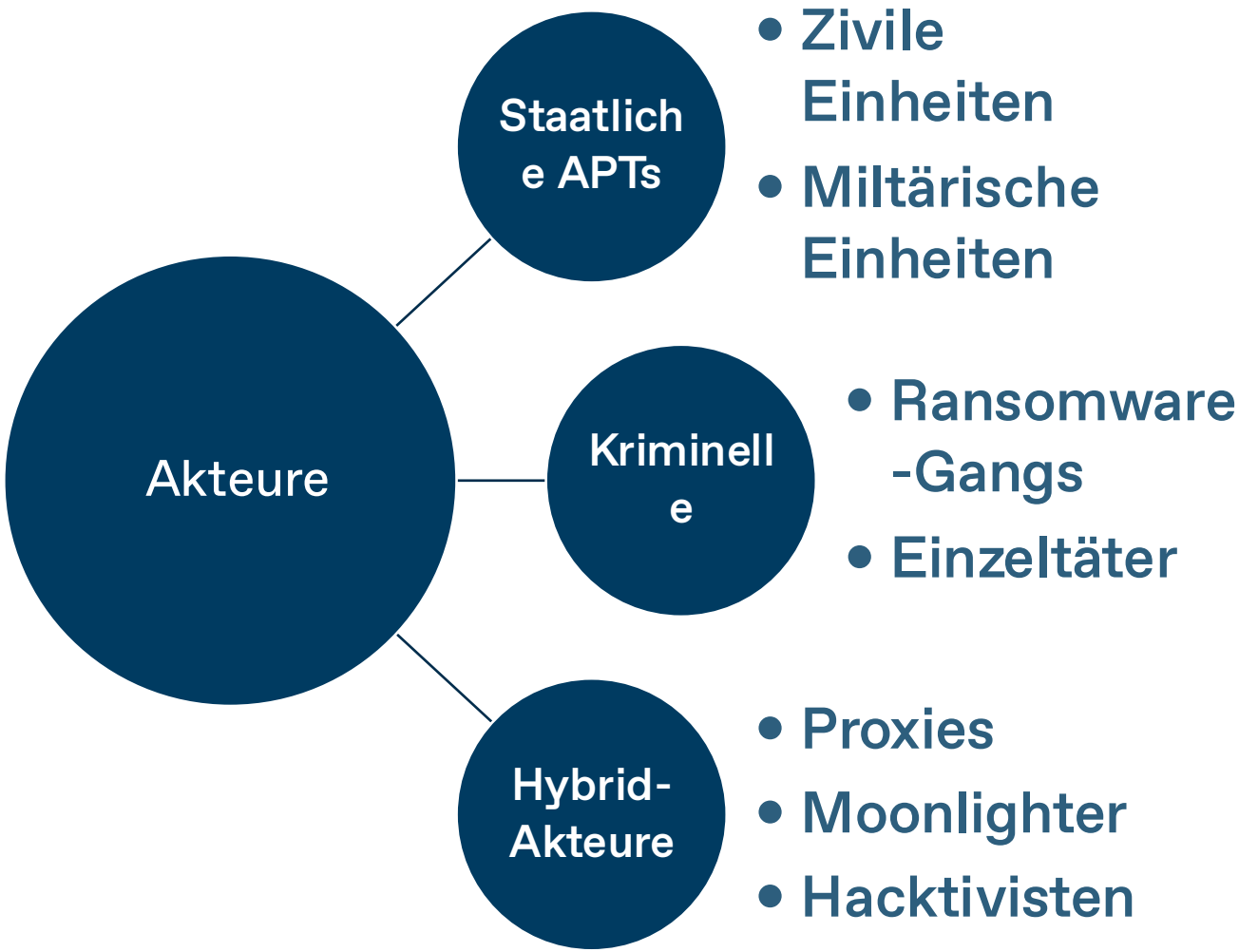
Domains, pDNS | Signatures

2 Geopolitik

Welche Rolle spielen geopolitische Faktoren für den offensiven Cyberkonfliktaustrag?

Akteursebene

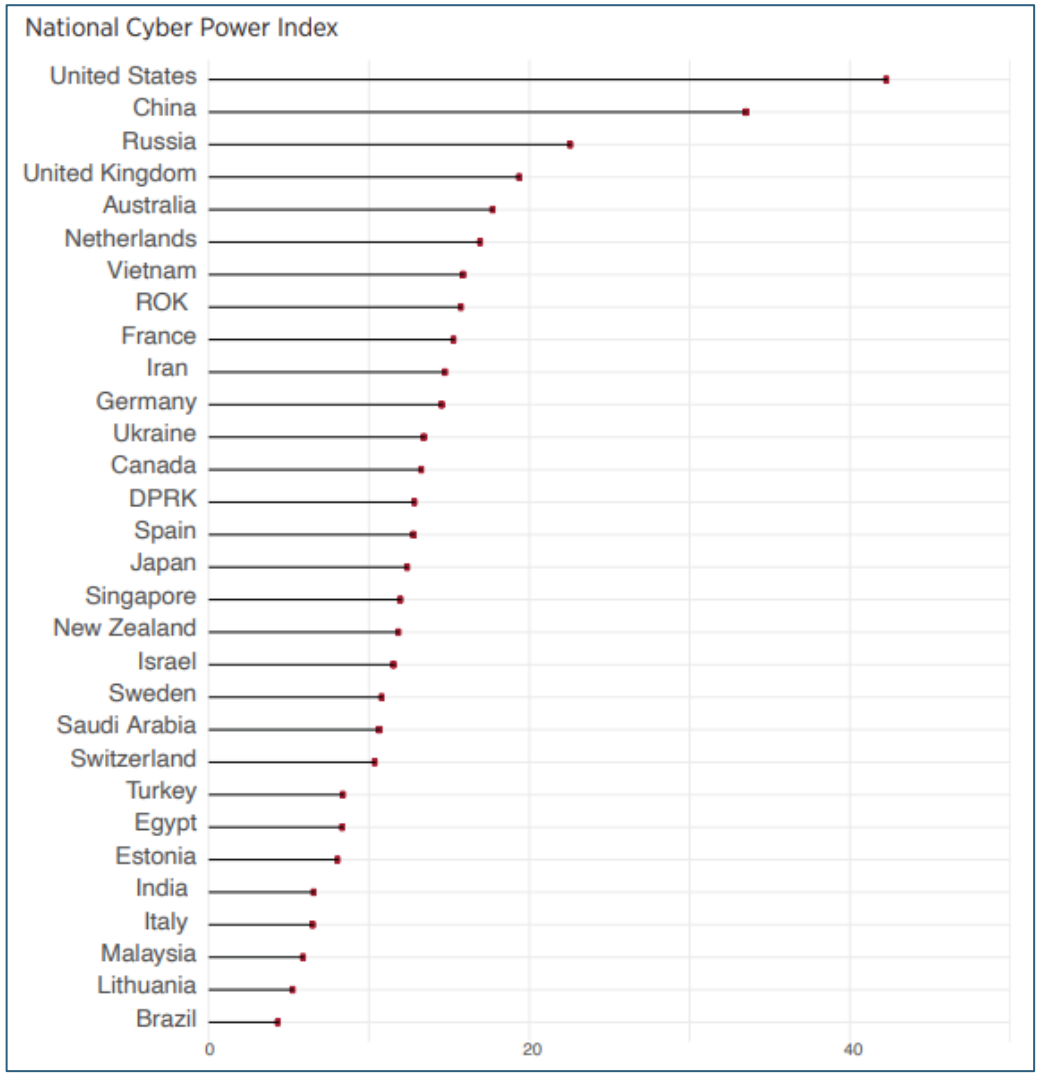
Wer ist beteiligt?



Systemebene

Wie wirkt der Regime-Typus?

- Es werden immer mehr Staaten im Cyberraum "aktiv"
- Spionage als kleinster gemeinsamer Nenner
- Autoritäre Systeme nutzen Cyberraum strategisch zum Zweck des Machterhalts
- Jeweiliger Legitimationsansatz leitet sich aus Regimetyp ab --> bestimmt Außen- und Innenpolitik und die Rolle von "Cyber"
- CHN, RUS, IRN, PRK als prägende Akteure; Spektrum erweitert sich aber ständig (Indien, Vietnam, Türkei, Pakistan etc.)



Quelle: Harvard Kennedy School, 2022

Zielebene

Wofür werden Cyberoperationen von wem eingesetzt?

Russland	VR China
• Politische Spionage • Cyberoperationen im Kontext militärischer Konflikte • Cyberoperationen als Teil hybrider Kriegsführung • "Management" von Ransomware-Gruppen	• Wirtschaftsspionage, Technologietransfer • Nationale Interessen, Taiwan, Südchinesisches Meer • Pre-Positioning in kritischen Infrastrukturen
Iran	**Nordkorea**
• Politische Spionage • Überwachung von Dissdenten, Journalisten, Aktivisten im In- und Ausland • Sabotage-Versuche (sog. Faketivists) • Ideologisch motivierte Ransomware	• Politische Spionage • DPRK IT Worker Scams • Finanzierung des Nuklearprogramms durch staatliches Cybercrime

•Welche Rolle spielen geopolitische Faktoren für den offensiven Cyberkonfliktaustrag?

3 State-Crime Nexus

Inwiefern verschwimmen die Grenzen zwischen staatlich affiliierten und kriminell motivierten Operationen?

Cyberwarfare und Cybercrime

...nähern sich immer weiter an

Akteursebene	Wer arbeitet mit wem?
Infrastrukturebene	Was wird gemeinsam genutzt?
Werkzeugebene	Womit wird gearbeitet?
Taktikebene	Wie wird vorgegangen?
Motivebene	Warum passiert das?

•Welche Rolle spielen geopolitische Faktoren für den offensiven Cyberkonfliktaustrag?

4 Cyber-Physical Nexus

Inwiefern besteht ein Nexus zwischen Cyberoperationen und physischen/kinetischen Operationen/Gewaltakten?

Cyber goes physical...

Staatlich-affiliierte Akteure

Kashoggi-Mord: Pegasus-Spyware auf Handy von Ehefrau gefunden

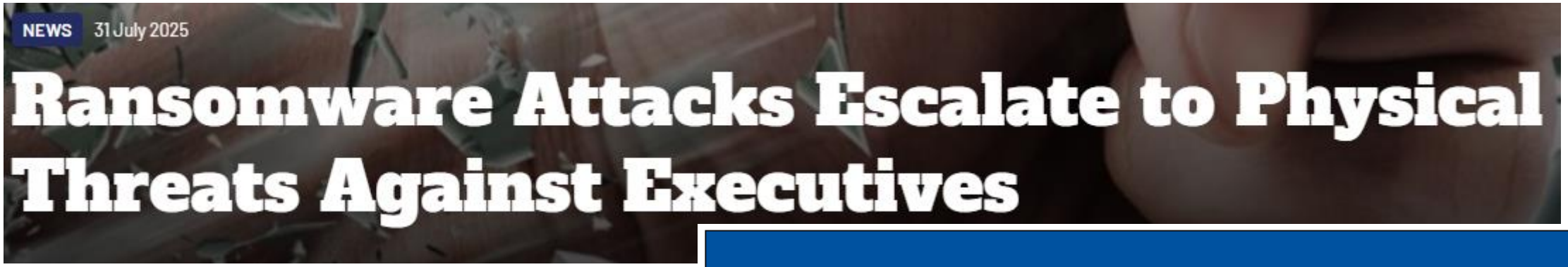
Mithilfe der Pegasus-Spyware sollen saudi-arabische Sicherheitsbehörden Mobilgeräte der Ehefrau des Journalisten Jamal Kashoggi ausgespäht haben – und zwar schon Monate vor dessen Ermordung.

Von Claudia Wieschollek

22.12.2021, 13:45 Uhr • 2 Min.

Cyber goes physical...

Kriminelle Akteure



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Alert Number: I-072325-3-PSA
July 23, 2025

The Com: Theft, Extortion, and Violence are a Rising Threat to Youth Online

---

The Federal Bureau of Investigation is warning the public about a growing and evolving online threat group known as The Com, short for The Community. The Com is a primarily English speaking, international, online ecosystem comprised of multiple interconnected networks whose members, many of whom are minors, engage in a variety of criminal violations. The FBI estimates thousands of individuals identify as current or recent

•Welche Rolle spielen geopolitische Faktoren für den offensiven Cyberkonfliktaustrag?

5 TI Forecast 2026

Was erwartet uns (mutmaßlich) in 2026?

Grundlage

Podiumsdiskussion auf dem DCSO Insight Day 2025

- Normalisierung offensiver Cyberoperationen im Namen der Cyberdefensive
- Verschmelzung staatlichen Cyberkonfliktaustrags und Cybercrime
- Weniger "attacker-controlled infrastructure"
- Schäden durch Cybercrime als Black Box --> Risikobewertung erschwert
- Schwächung diplomatischer Bemühungen

TI-Forecast 2026

1

Weitere Verschmelzung staatl. und kriminell. Handlungen

Attribution weiter erschwert; Gleiches gilt für Risikobewertung durch erschwerte Motivationsbewertung --> Um was für eine Bedrohung handelt es sich?

2

Ausnutzen ökonomischer Schieflagen/Herausforderungen

Gezieltes Anvisieren des Themenbereichs Recruiting; Job-Interviews etc. durch staatliche und kriminelle Akteure

3

Insider-Threats sind gekommen, um zu bleiben

Wird vermutlich in unterschiedlichsten Operationsszenarien weiterhin von steigender Relevanz sein. Auch in Verbindung mit Punkt 2.

4

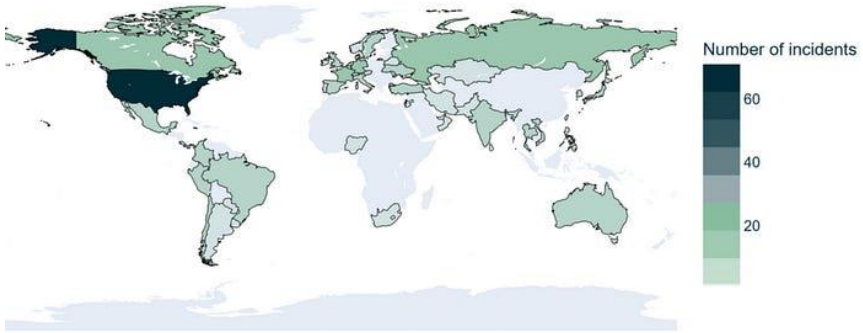
Noch mehr Krisen, Konflikte... und Kriege?

Konflikte als Nährboden politisch motivierter oder im selben Fahrwasser agierender Cyberangriffe.

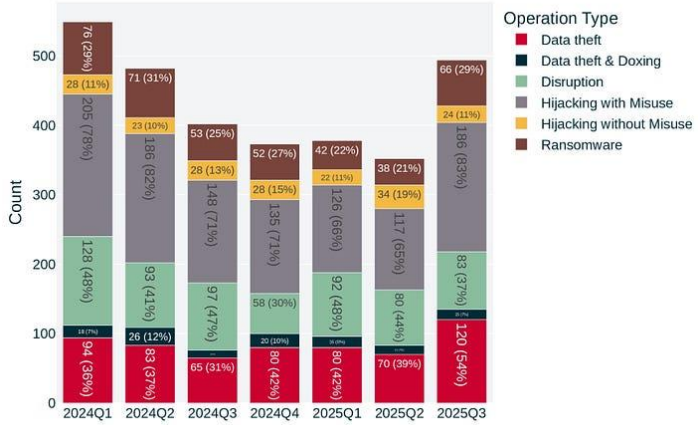
Cyber Conflict Briefing

https://medium.com/@DCSO_CyTec

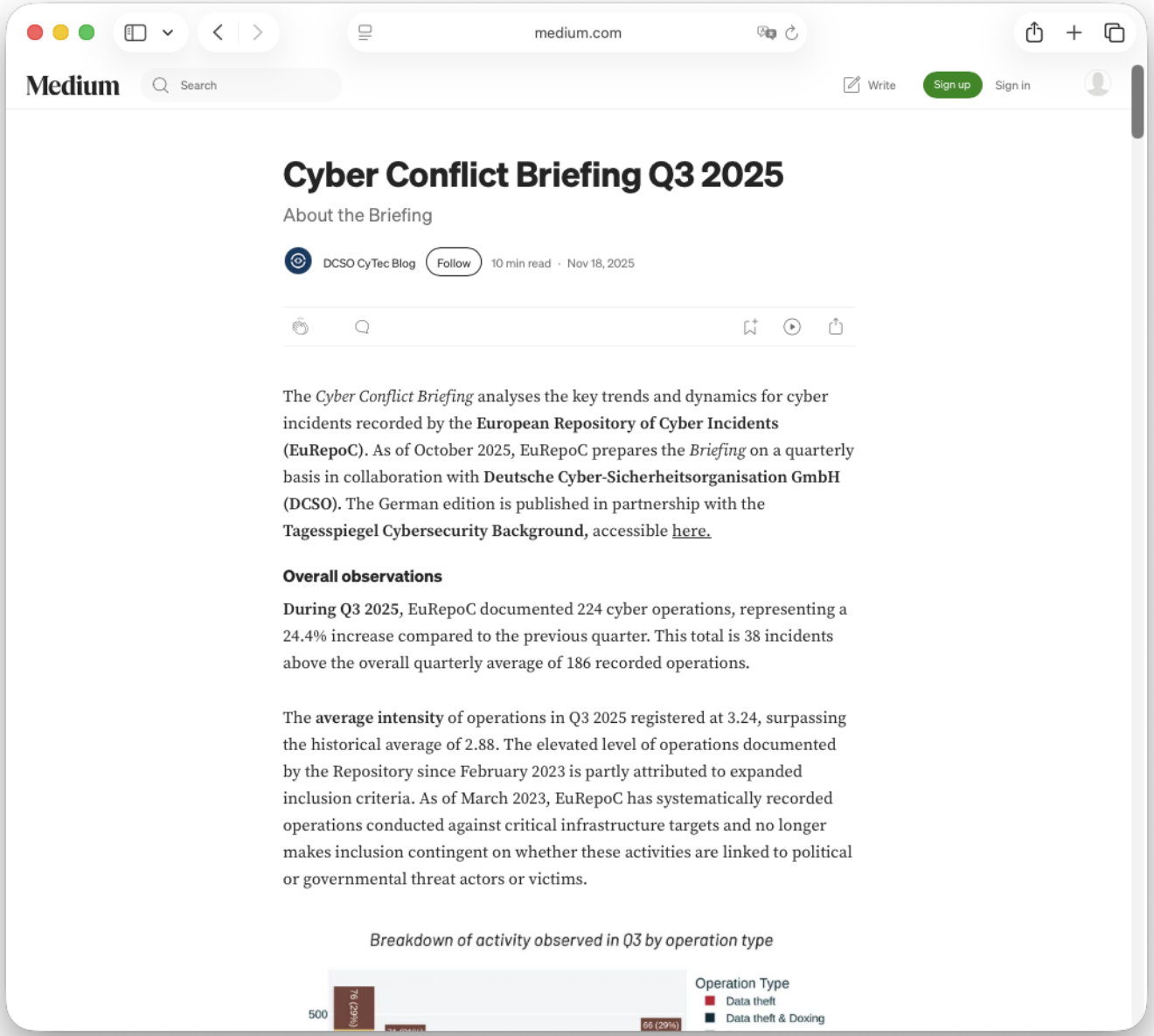
Geographic distribution of affected organizations Q3 2025



Breakdown of activity observed in Q3 by operation type



Note: Individual cyber incidents may have several operation types in combination



6 Fragen?

und Antworten!

TLP:CLEAR