CANCOM

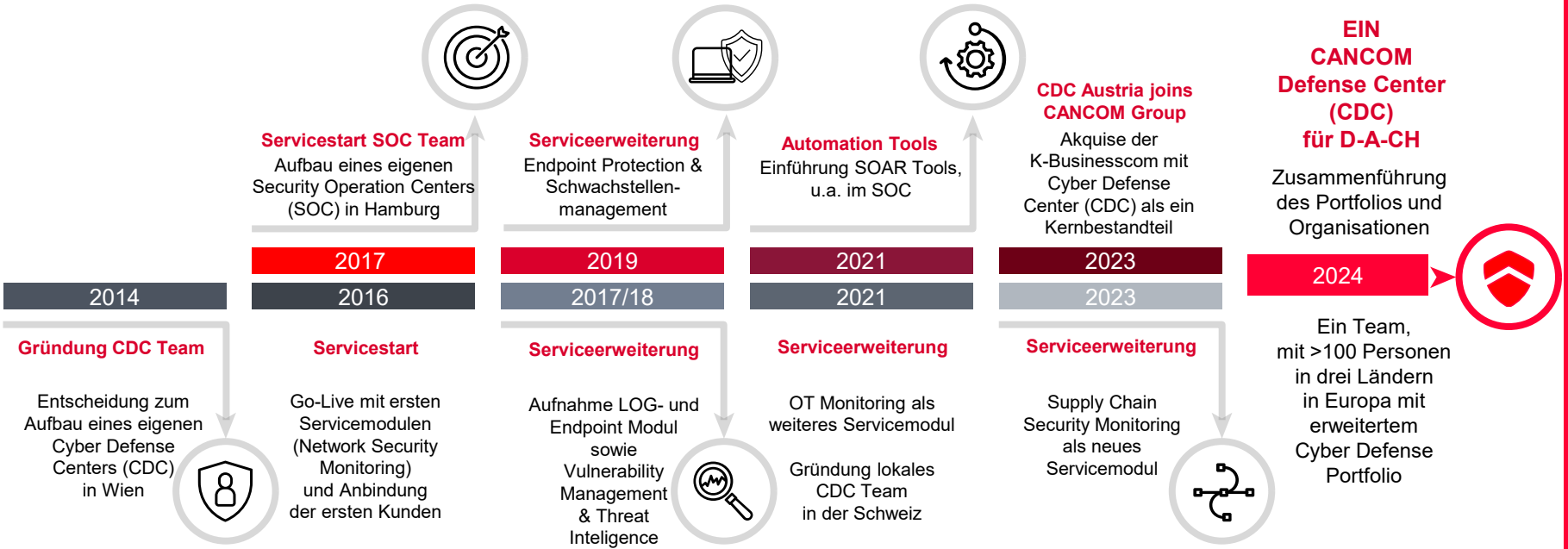
Cyber Threat Intelligence als Ausgangspunkt zur Stärkung der europäischen Cyberresilienz

Lukas Seidl (CANCOM | Principal SOC Manager)

Jan-Uwe Pettke (Crowdstrike | Practice Lead „Counter Adversary Operations“ – Zentral- und Osteuropa)

ADV CyberXChange Conference 2025 - 2.10.2025

Cyber Defense made in Europe bei CANCOM



CANCOM SOC Servicemodule

Threat Detection & Response (TDR)

LOG-based TDR aaS (SIEM)

Powered by: splunk> a CISCO company, Microsoft

Network TDR aaS (NIDS)

Powered by: corelight

Operation Technology TDR aaS

Powered by: CLAROTY

Endpoint Detection & Response (EDR)

Endpoint Protection as-a-Service

Powered by: CROWDSTRIKE, Microsoft

Threat Intelligence (TI) & Research

Vulnerability Management aaS

Powered by: Qualys., tenable

Threat Intelligence aaS

Powered by: Recorded Future®

Supply Chain Security Monitoring aaS

Powered by: Recorded Future®

CROWDSTRIKE

THREAT INTELLIGENCE

WHAT USE CASES ARE RELEVANT TO YOU?

THREAT INTEL CAPABILITY

Tactical | Operational | Strategic

TACTICAL

Focused on performing malware analysis & enrichment, as well as ingesting atomic, static, and behavioral threat indicators into defensive cybersecurity systems.

STAKEHOLDERS:
- SOC Analyst
- SIEM
- Firewall
- Endpoints
- IDS/IPS

"Mechanic"

OPERATIONAL

Focused on understanding adversarial capabilities, infrastructure, & TTPs, and then leveraging that understanding to conduct more targeted and prioritized cybersecurity operations.

STAKEHOLDERS:
- Threat Hunter
- SOC Analyst
- Vulnerability Mgmt.
- Incident Response
- Insider Threat

"Race Car Driver"

STRATEGIC

Focused on understanding high level trends and adversarial motives, and then leveraging that understanding to engage in strategic security and business decision-making.

STAKEHOLDERS:
- CISO
- CIO
- CTO
- Executive Board
- Strategic Intel

"The Owner"

CTI ermöglicht die **proaktive Identifikation von Bedrohungen**, bevor sie Schaden anrichten.

Die EU plant mit dem Cyber Solidarity Act ein **europaweites Warnsystem**, das auf CTI basiert und nationale sowie grenzüberschreitende Cyber-Knotenpunkte nutzen soll.

Frühzeitige Erkennung und Warnung

Verbesserte Reaktionsfähigkeit

CTI liefert die nötigen Informationen, um **schnell und gezielt auf Vorfälle zu reagieren**

CTI fördert die **Kooperation zwischen Mitgliedsstaaten**, Behörden und Unternehmen.

Die EU-Strategie setzt auf sektorübergreifende Sicherheitsstandards und zentrale Meldesysteme, die durch CTI gespeist werden.

Informationsaustausch und Zusammenarbeit

Risikobasierte Sicherheitsmaßnahmen

CTI unterstützt die Umsetzung des CRA, indem es **Risiken identifiziert**, die bei der Produktentwicklung berücksichtigt werden müssen

CTI ist nicht nur ein technisches Werkzeug, sondern ein strategischer Hebel zur **Erhöhung der Cyberresilienz** in Europa.

CROWDSTRIKE

Cyber Threat Intelligence als Ausgangspunkt zur Stärkung der europäischen Cyberresilienz

Jan-Uwe Pettke – Practice Lead „Counter Adversary Operations“ – Zentral- und Osteuropa

CROWDSTRIKE

01	Some necessary definitions
02	The threat landscape
03	Hybrid threats and cybe threat intelligence
04	Stakeholder analysis

CROWDSTRIKE

A definition of cyber resilience

> “Cyber resilience is an organization’s ability to minimize the impact of significant cyber incidents on its primary goals and objectives.”

Source:
World Economic Forum
Unpacking Cyber Resilience

CROWDSTRIKE

A definition of intelligence

Threat intelligence enables stakeholders to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors or security-related risk.*

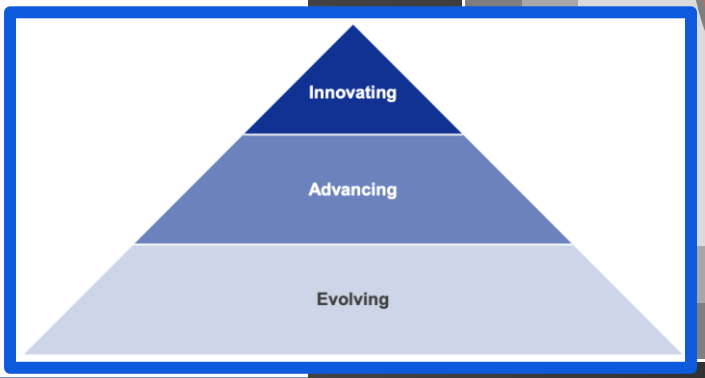
→ Therefore, benefits of an intelligence-led approach can only be realized when we first take the time to listen and understand stakeholders!

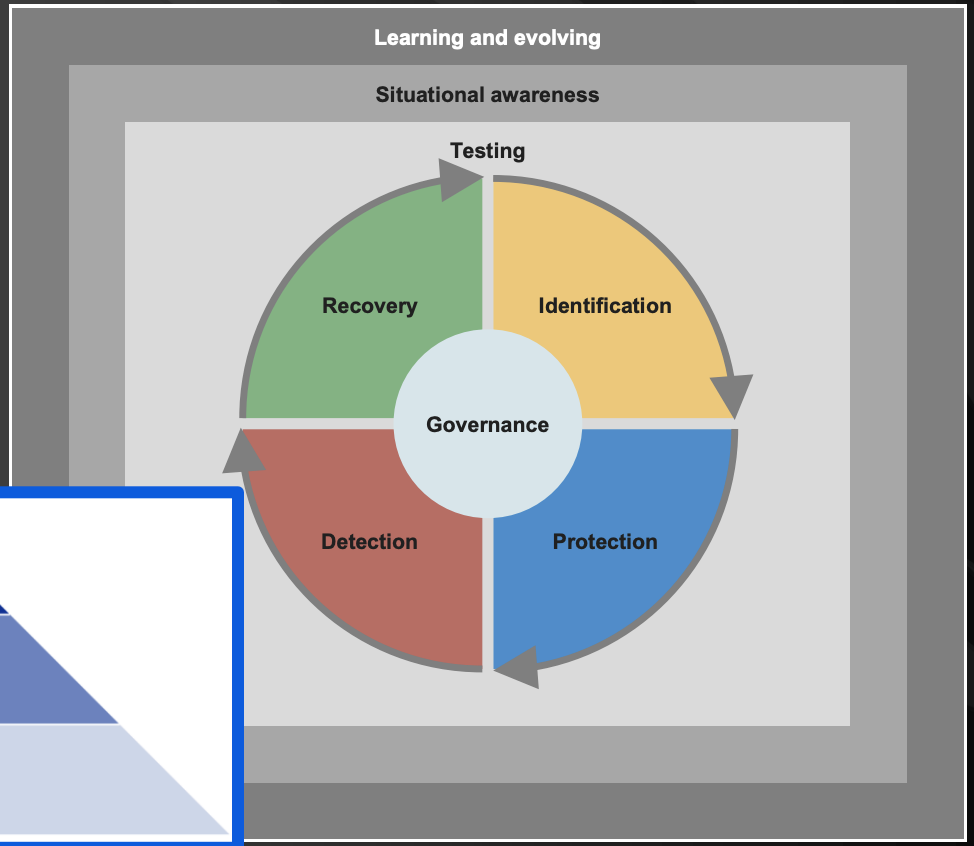
→ Therefore, an intelligence-led approach is a stakeholder/client-led approach!

* Source: https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/

EUROPEAN CENTRAL BANK
EUROSYSTEM

Cyber resilience oversight expectations for financial market infrastructures

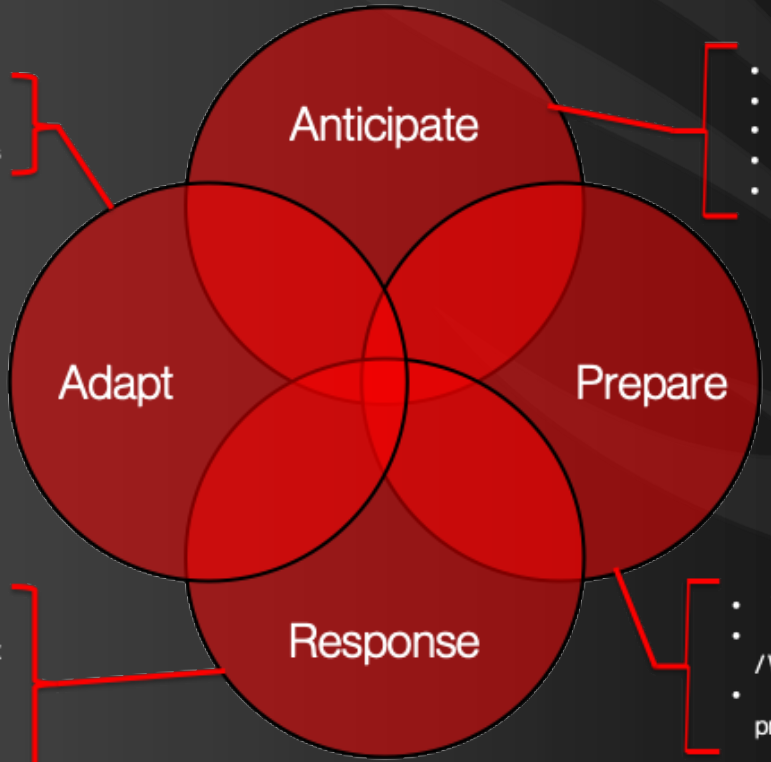




December 2018

Intelligence-led Cyberresilience

- After action reviews
- Lessons learned
- Root cause analysis



- Threat intelligence
- Risk management
- Strategic foresight
- Threat modelling
- Red teaming

- Threat hunting
- Crisis management
- Incident response
- Early stage remediation

- Training
- Exercises (Tabletop / Wargames)
- BCM / emergency procedures

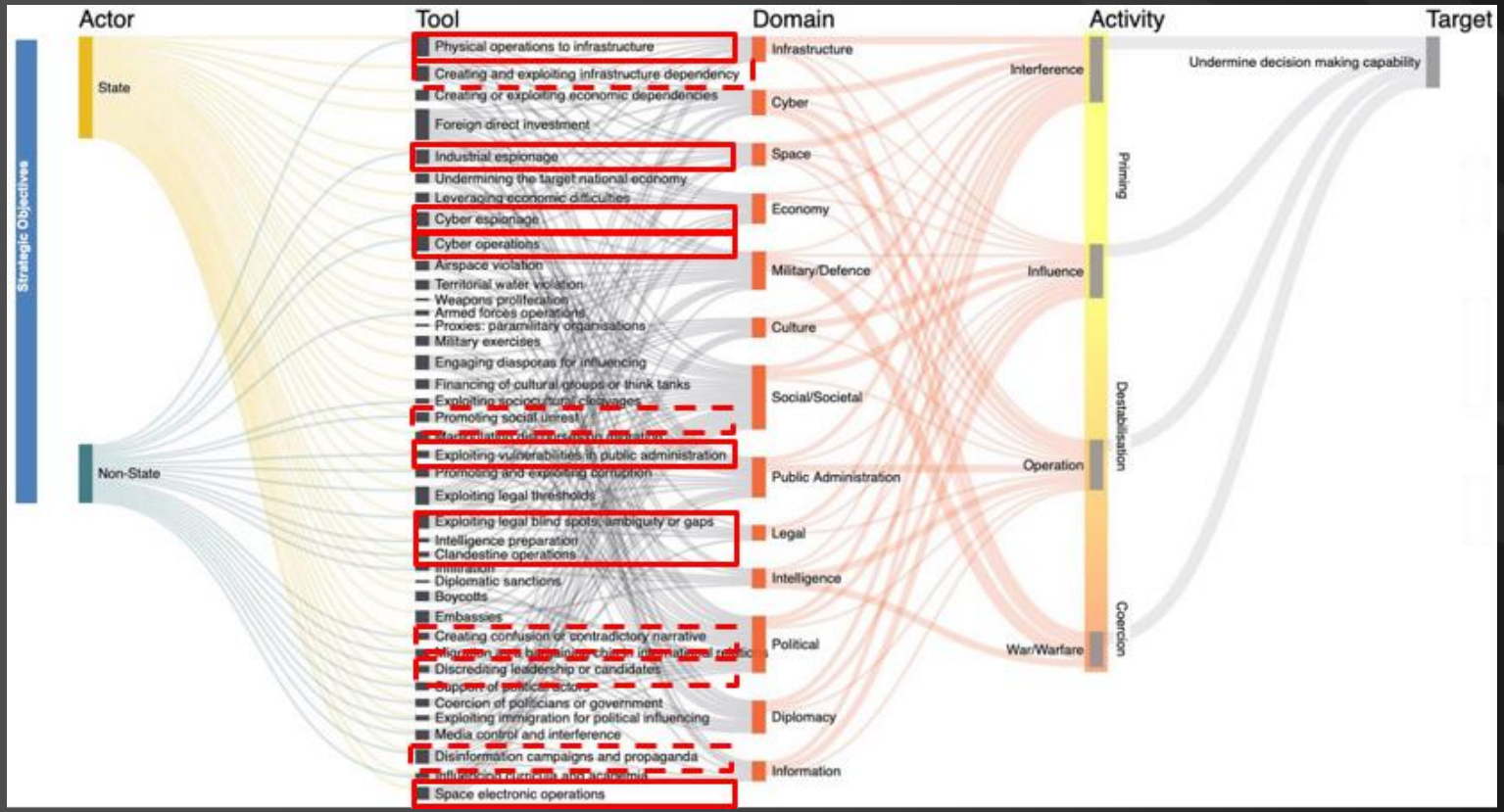
CROWDSTRIKE

Global adversaries

- 14 New Adversaries
- 265+ Total Tracked
- 150+ Malicious Activity Clusters

CROWDSTRIKE

Hybrid threats



Hybrid tools – Cyber espionage

Neue Zürcher Zeitung

China spioniert seit Monaten grosse Telefonanbieter aus. Die USA können kaum etwas dagegen tun

In einer riesigen Cyberaktion sind chinesische Hacker an vertrauliche Gespräche gelangt. So funktioniert das Spionieren der Zukunft.

Actors

- Salt Typhoon a.k.a. Ghost Emperor[1] (CSA-241137)
- Ethereall Panda (CSA-241105)
- Vanguard Panda (CSA-240476)

Sectors

- Telecoms (Verizon, AT&T, Lumen)

Measures

Collection of communication data, voice communication and text messages of key personnel in politics and administration. It is furthermore unclear whether attackers were able to gain access to email communications or other data.

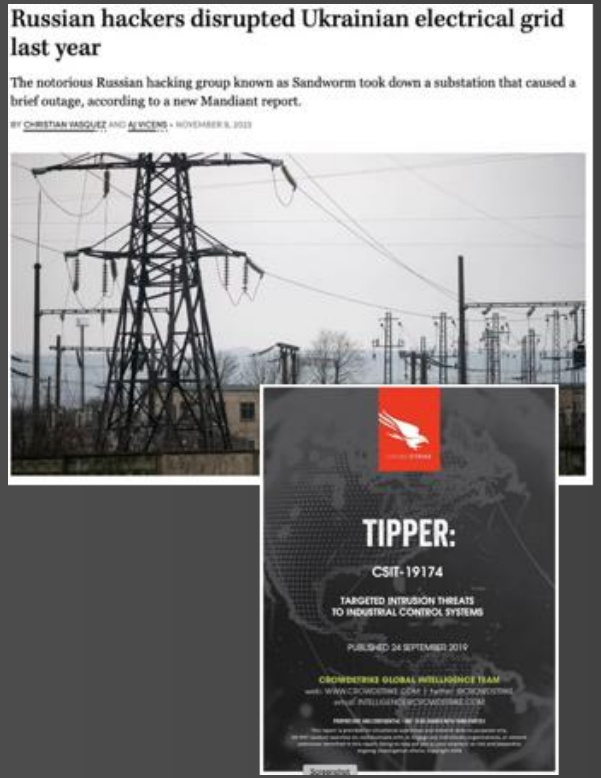
In 2024, U.S. government officials warned that China-nexus operators had allegedly pre-positioned themselves for future military conflicts, referring to intrusion activity conducted by adversaries such as VANGUARD PANDA.

Intention (hypothetical)

- Collection of data for future cyber attacks
- Collection of confidential data for further espionage campaigns or information operations / cognitive warfare
- Intelligence collection

[1] CrowdStrike Intelligence cannot currently verify these claims and does not attribute *GhostEmperor* or *Demodex* to any known adversaries.

Hybrid tools – Cyber sabotage



Actors
- Voodoo Bear (CSIT-19174) a.k.a. Sandworm

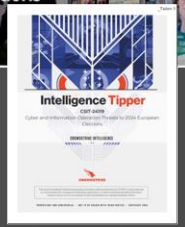
Sectors
- Enegery & financial sector

Measures

Due to their ability to affect physical processes, as well as their nexus to proprietary business information, these systems are a tempting target for a number of targeted intrusion adversaries that may seek to collect intelligence or execute a destructive attack on ICS vendors or owner/operators.
Energy, oil & gas, and chemical companies are much more likely to be targeted with a destructive attack by a state-sponsored adversary due to the potential kinetic outcomes of a successful breach.

Intention (hypothetical)
- Collection of data for future cyber attacks
- Collection of confidential data for further espionage campaigns
- Executing destructive, cyber-physical attacks to promote social unrest (TOOL)
- Executing destructive, cyber-physical attacks in the course of a military intervention / war
- Retaliation for political unfavorable behaviour

Hybrid threats – further use cases



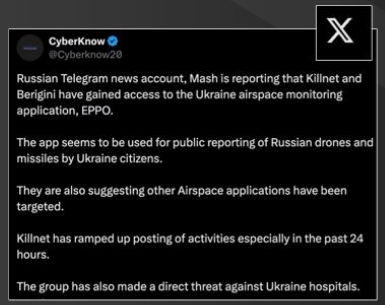
CSIT-24119 Cyber and Information Operation Threats to 2024 European Elections

Actors
- Various (Russia, China, Iran, DPRK)

Measures
Russia-nexus state and proxy actors are the most likely adversaries to conduct cyber operations as well as IO to undermine EU unity, sow discord, and cast doubt on electoral processes.

China, Iran, and the Democratic People's Republic of Korea (DPRK) are unlikely to directly interfere with or influence the 2024 EP election; however, Chinese and Iranian IO will likely seek to influence EU opinion on geopolitical issues using state messaging and political influence networks.

Intention (hypothetical)
- Sow discord
- Support extremist parties
- Cast doubt on electoral process and democratic institutions
- Shaping the information environment



CSA-250653 Killnet Claims Responsibility for Breach of Ukrainian Airspace-Monitoring Application

Actors
- Killnet (pro-Russian hacktivist)

Measures
Killnet claimed responsibility for breaching a Ukrainian airspace-monitoring application. "EPPO". The Ukrainian airspace-monitoring application is used by civilians and armed forces members to track enemy aerial targets such as drones, aircraft, and missiles. Killnet made this claim through Russian social media news outlet Mash and later reposted the Mash post to their own account, which they have used to make claims since reemerging in 2025

CrowdStrike Daily Report: 19 May 2025

Actors
- China-nexus actors

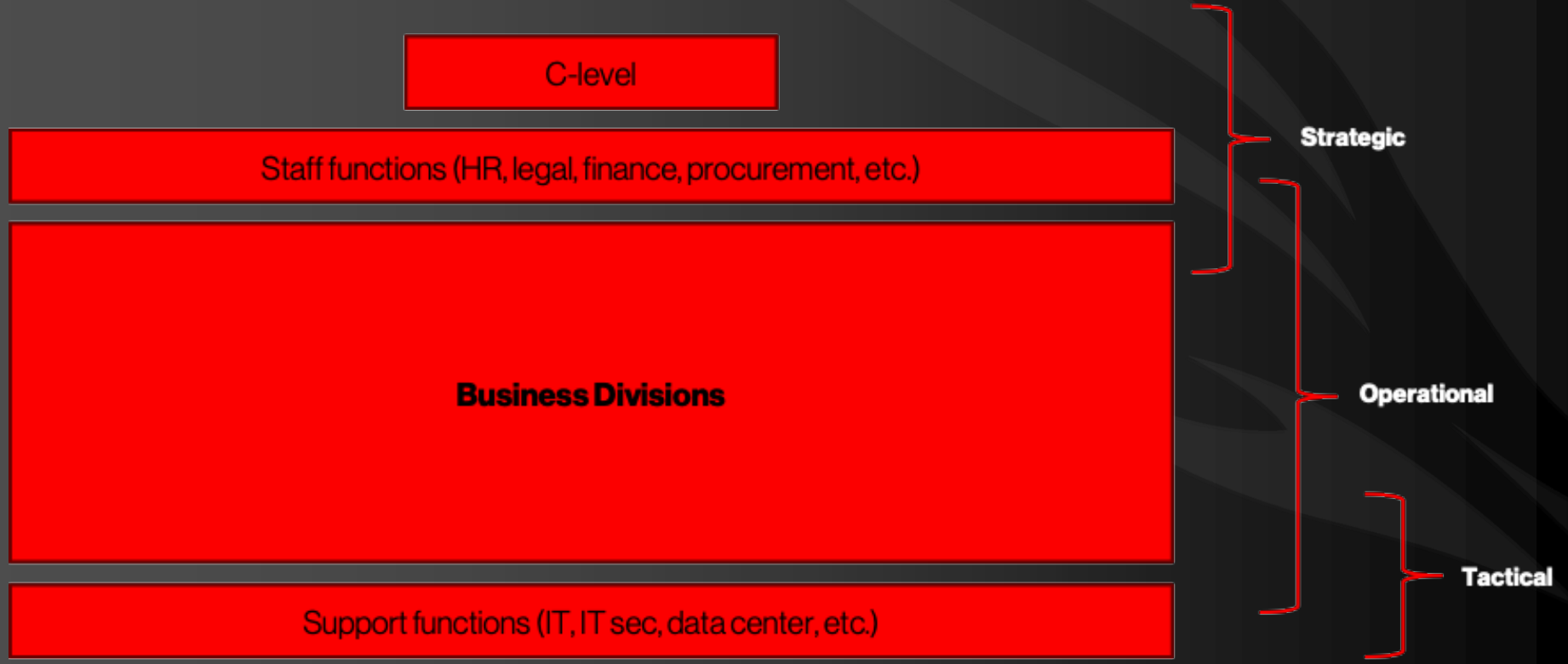
Measures
U.S. officials are reportedly assessing risks from Chinese-made power inverters used in renewable energy infrastructure after identifying undocumented communication equipment in some inverters. Some security researchers as well as an unnamed official have claimed that these undocumented communications devices could facilitate disruptions to power grids. According to public reporting, some solar power inverters located in the U.S. and other countries were disabled remotely from China in November 2024. However, press reports cannot presently confirm the extent of the November 2024 incident, and the U.S. Department of Energy declined to comment.

Intention (hypothetical)
- Wide-spread control of critical infrastructure
- Ability to cause black-outs (local and regional - Spain / Portugal May 2025)
- Political coercion
- Evicting anxiety and panic within local population

- Discrediting leadership & candidates
- Misinformation & propaganda
- Supply chain attacks

CROWDSTRIKE

Stakeholder mapping



CROWDSTRIKE

Stakeholder group – C-Level

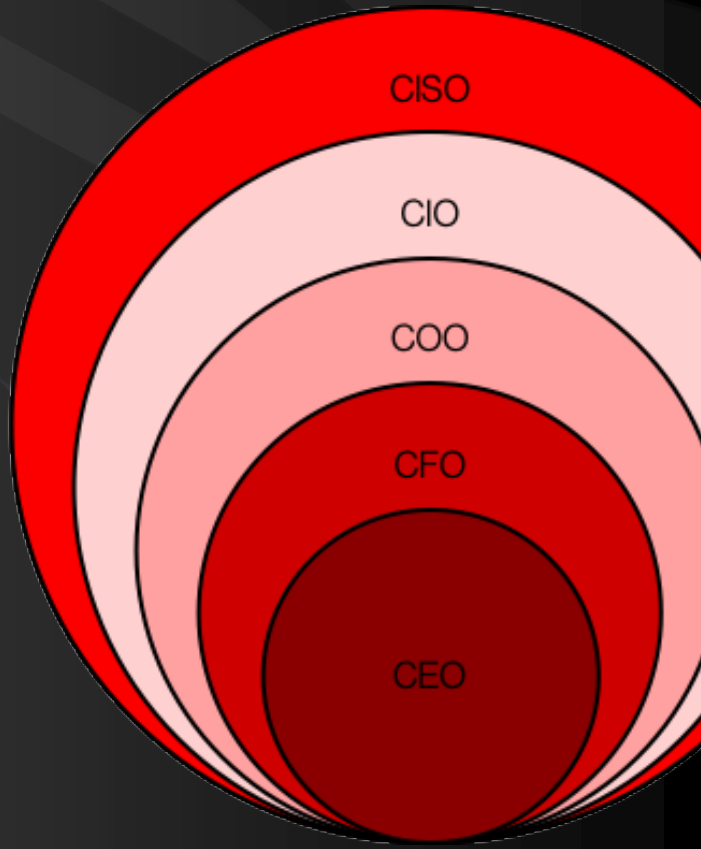
CEO – assessing the overall impact of cyber-related threats on the business strategy of the organization and protecting the trust of key external stakeholders such investors

CFO – assessing the financial risk of cyber-related threats (shareholders, investors) as well as investments into cyber security

COO – assessing the risks related to a digitized production/business and smart products as well as understanding regulatory related risks

CIO – assessing the risks related to the IT organization

CISO – assessing the capabilities of the IT sec in relations to the cyber-related threats and risks



CROWDSTRIKE

Stakeholder group – Staff functions

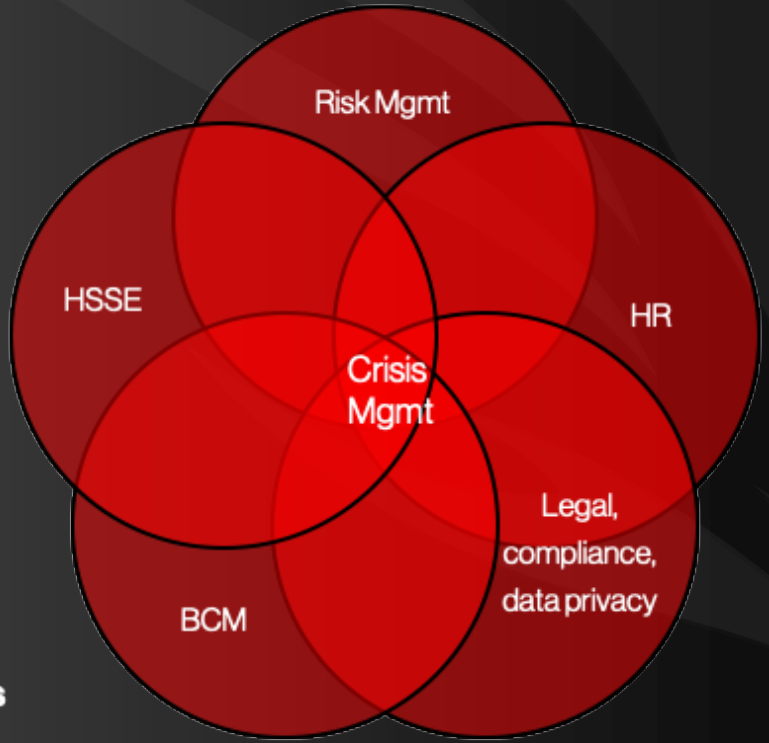
Risk Mgmt – Quantifying & observing directly & indirectly cyber-related risks and steering the implementation of risk mitigation measures

HR – Collaborating in Insider Risk Programs, Qualifications schemes of employees, supporting awareness campaigns

Legal, compliance & data privacy – Understanding legal implications of various cyber attacks and accompanying various mitigations measures

Business Continuity Management – understanding cyber-related risks to business continuity (Business Impact Assessments –BIA) and developing appropriate Business Continuity Plans

Health, Safety, Security, Environment – Understanding risks to ICS and its implications for HSSE



CROWDSTRIKE

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?