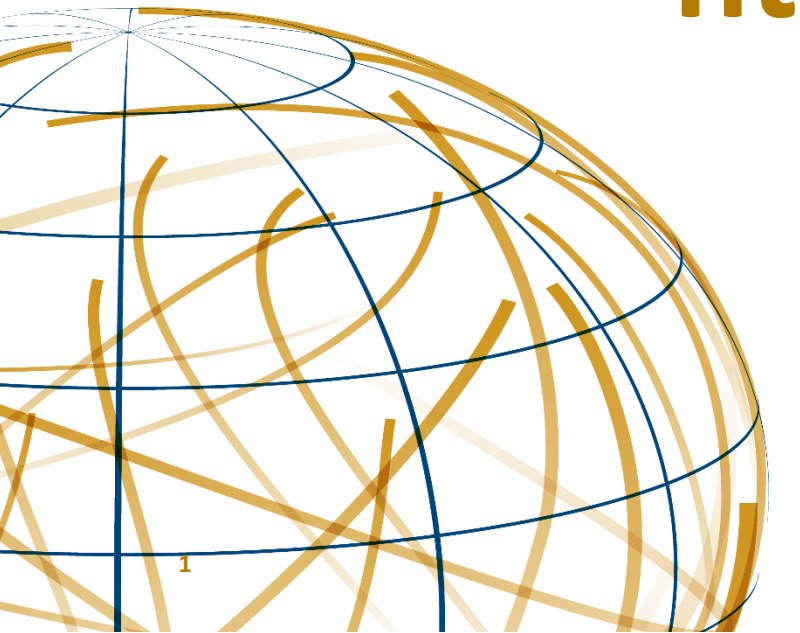
"Europäische digitale Sicherheit“ https://eurepoc.eu



Dr. Annegret Bendiek

Stiftung Wissenschaft und Politik
Deutsches Institut für
Internationale Politik und Sicherheit

16.11.23

I-
Das Problem eurepoc.eu

https://www.youtube.com/watch?v=l224bHeg9Qw

SWP

EuRepoC

Cyberangriffe: Anstieg qualitativ und quantitativ

Unknown hackers attack German IT service provider Südwestfalen-IT via ransomware *Unknown hackers attack German IT service provider Südwestfalen-IT via ransomware on 30 October. The attackers encrypted data on servers of the IT service provider. To avoid further damage, Südwestfalen-IT shut down its data centre. Südwestfahlen-IT provides IT services for German german municipal administrations. The exact number of affected municipalities is not known yet, but it is suggested to be in the range of 70.*

Pro-Hamas hacktivist group attacks Israeli entities with new BiBi-Linux wiper malware *A pro-Hamas hacktivist group targets Linux systems belonging to Israeli companies with the new BiBi-Linux wiper malware. The malware conducts file corruption by overwriting files with useless data, damaging both the data and the operating system.*

Unknown hackers disrupted services at Toronto Public Library beginning at least on 28 October 2023. *Unknown hackers disrupted services at Toronto Public Library beginning at least on 28 October 2023. The disruption affects the services of tpl.ca, "your account", tpl:map passes and digital collections as well as Public computers and printing services at their sites. the incident was reported by the Toronto Public Library on their website.*

.

Konfliktstruktur: „Cyber- und Informationsraum“

Ziel	Akteur	Konfliktstruktur
	Primär staatliche Akteure	Private Proxy-Akteure
Territoriale Kontrolle	Zwischenstaatliche militärische Bedrohung	Asymmetrische Konflikte/Kriege
Öffentliche Ordnung	Staatliche Interferenz	Hybride Bedrohungen

Fragen

- Warum ist die EU-Attributions- und Sanktionspolitik im Cyber- und Informationsraum ineffektiv, obwohl die digitale Sicherheit in Europa erst einen funktionierenden Binnenmarkt gewährleistet?
- Welche Rolle spielen öffentlich-private Partnerschaften in der digitalen Sicherheit und bei der Attribution von Cyberangriffen?
- Bietet die nationale Politik eine effektivere Lösung an?

Definitorische Annäherung

- **CIA-Triade**: Informationssicherheit ist ein Zustand von technischen oder nicht-technischen Systemen zur Informationsverarbeitung, -speicherung und -lagerung, der die Schutzziele **Vertraulichkeit, Verfügbarkeit und Integrität** sicherstellen soll. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.
- **EU**: Unter Cybersicherheit fallen alle Tätigkeiten, die notwendig sind, um Netz- und Informationssysteme, die Nutzer solcher Systeme und andere von Cyberbedrohungen betroffene Personen zu schützen. (Cyber Security Act, Art. 2.1)
- **BMI** Cybersicherheitsagenda, Juli 2022: Cybersicherheit ist essentiell für einen modernen, hochtechnologisierten und digitalisierten Industriestaat wie Deutschland. Sie umfasst Infrastrukturresilienz, Abwehr und Aufklärung von (auch staatlich gelenktem) Cybercrime sowie Sensibilisierung für Desinformationskampagnen. Zur Gewährleistung der Cybersicherheit müssen Cybersicherheitsarchitektur modernisiert, Entwicklungsfähigkeiten ausgebaut und die Cyberfähigkeiten der Sicherheitsbehörden gestärkt werden.

Definitorische Abgrenzung

- **Cybersicherheit:** Schutz von Computersystemen, Netzwerken und Daten vor Angriffen, unbefugtem Zugriff oder Schäden aus dem Cyberraum. Cybersicherheit bezieht sich auf den Schutz digitaler Informationen in Verbindung mit dem Internet, Netzwerken und Computersystemen, umfasst den Schutz vor Bedrohungen wie Hacking, Malware, Phishing, Denial-of-Service-Angriffen usw.
- **Digitale Sicherheit:** Digitale Sicherheit ist nicht ausschließlich auf den Cyberraum beschränkt, umfasst den Schutz von Daten und Informationen, unabhängig davon, ob sie online oder offline gespeichert sind. Digitale Sicherheit kann auch physische Geräte, Datenübertragungen, Speichermedien und andere digitale Elemente umfassen.

Quelle: openai.eu, Zugriff 31.10.2023

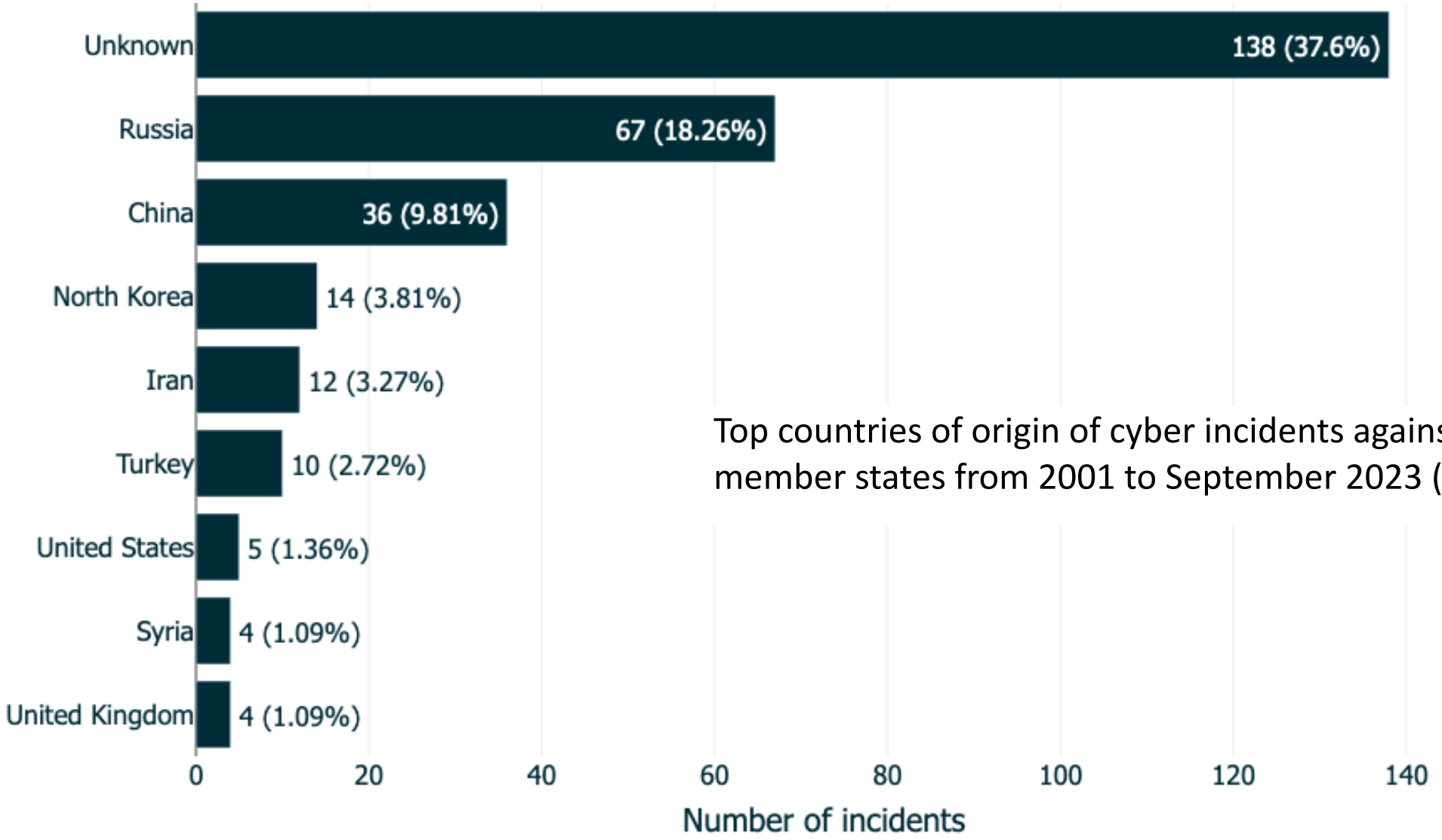
Diplomatischer Reaktionsrahmen der EU (EU Cyber DiplomacyToolbox)

Ratsschlussfolgerungen vom Juni 2017, Leitlinien zur Umsetzung vom Oktober 2017

Präventive Maßnahmen	Kooperative Maßnahmen	Stabilisierende Maßnahmen	Restriktive Maßnahmen	Völkerrechts-konforme Reaktion
-Vertrauens- und sicherheitsbildende Dialoge -Kapazitätsaufbau in Drittstaaten -Awareness raising	-EU-Demarchen (ggf. in Kooperation mit Drittstaaten) -diplomatische Protestnoten	-Gemeinsamer Standpunkt des Europäischen Rates -GASP-Beschluss -Erklärungen des HR im Namen des Rates -Erklärung des HR	-Restriktive Maßnahmen, (Art. 215 AEUV/GASP-Beschluss Title V Kapitel 2 EUV) -Kontensperrung -Reisebeschränkung	-Solidaritätsklausel (Art. 222 AEUV) -Beistandsklausel (Art. 42 (7) EUV) in Einklang mit UN Charta (Art. 51/ Recht auf Selbstverteidigung)
Resilienz (Resilience) >		**< Abwehr (Denial) >**		**< Vergeltung > (Retaliation)**

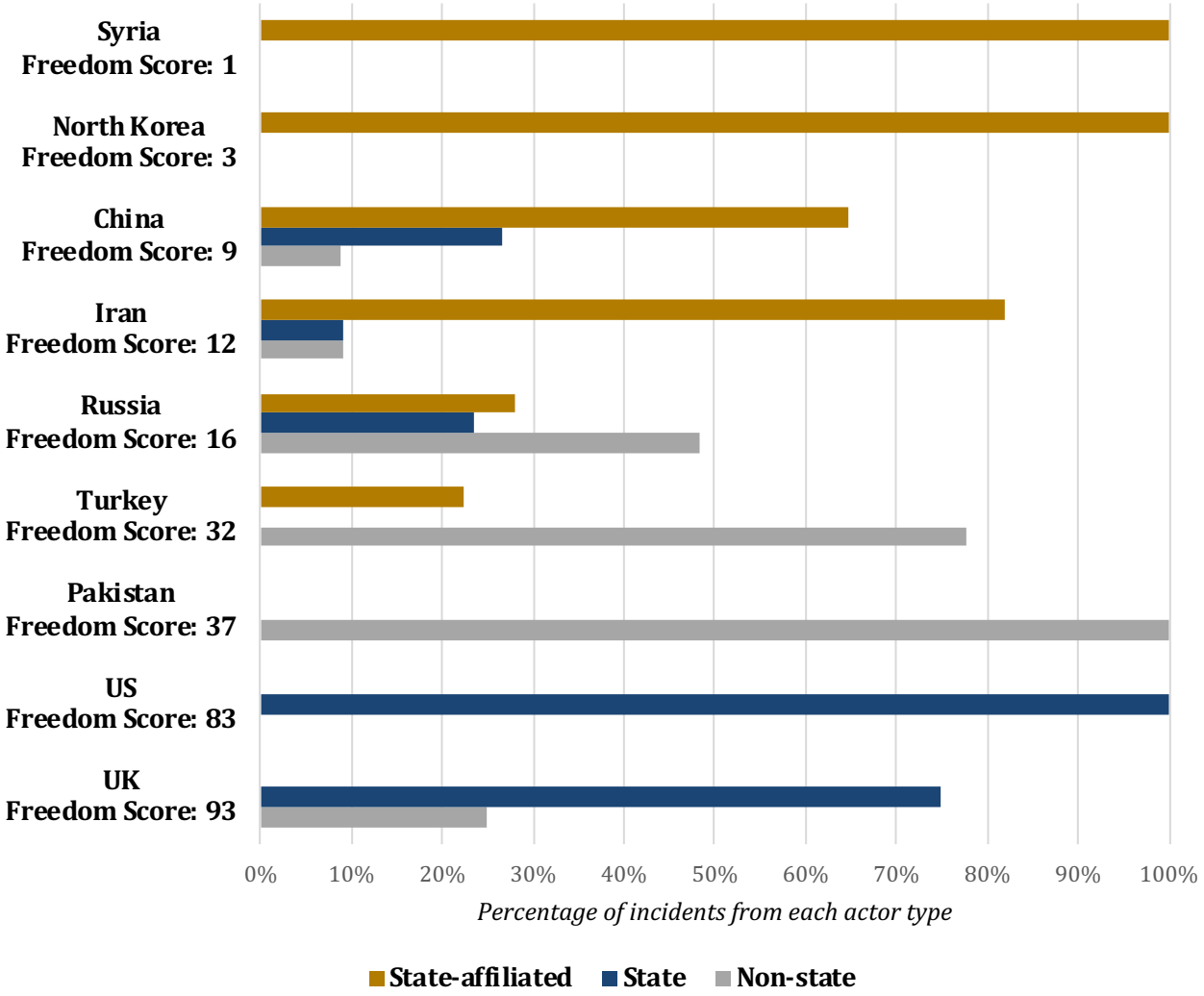
I-
Cyber incidents eurepoc.eu

Most cyber incidents against EU member states are from **unknown countries** of origin, **Russia**, **China** and **North Korea**



Top countries of origin of cyber incidents against EU member states from 2001 to September 2023 (N=367)

Among the EU's top attackers, **more authoritarian regimes**, have more incidents from **state-affiliated actors**



Most incidents originating from **China**, **Iran, North Korea** and **Syria** are from **state-affiliated actors**

However, the majority of incidents against the EU from the **US** and the **UK** are from **state actors** directly.

In the case of **Turkey**, 78% of incidents are from **non-state groups**.

**Based on Freedom House Scores for 2023*

Different trends emerge when comparing incidents from Russia, China and Turkey against EU member states

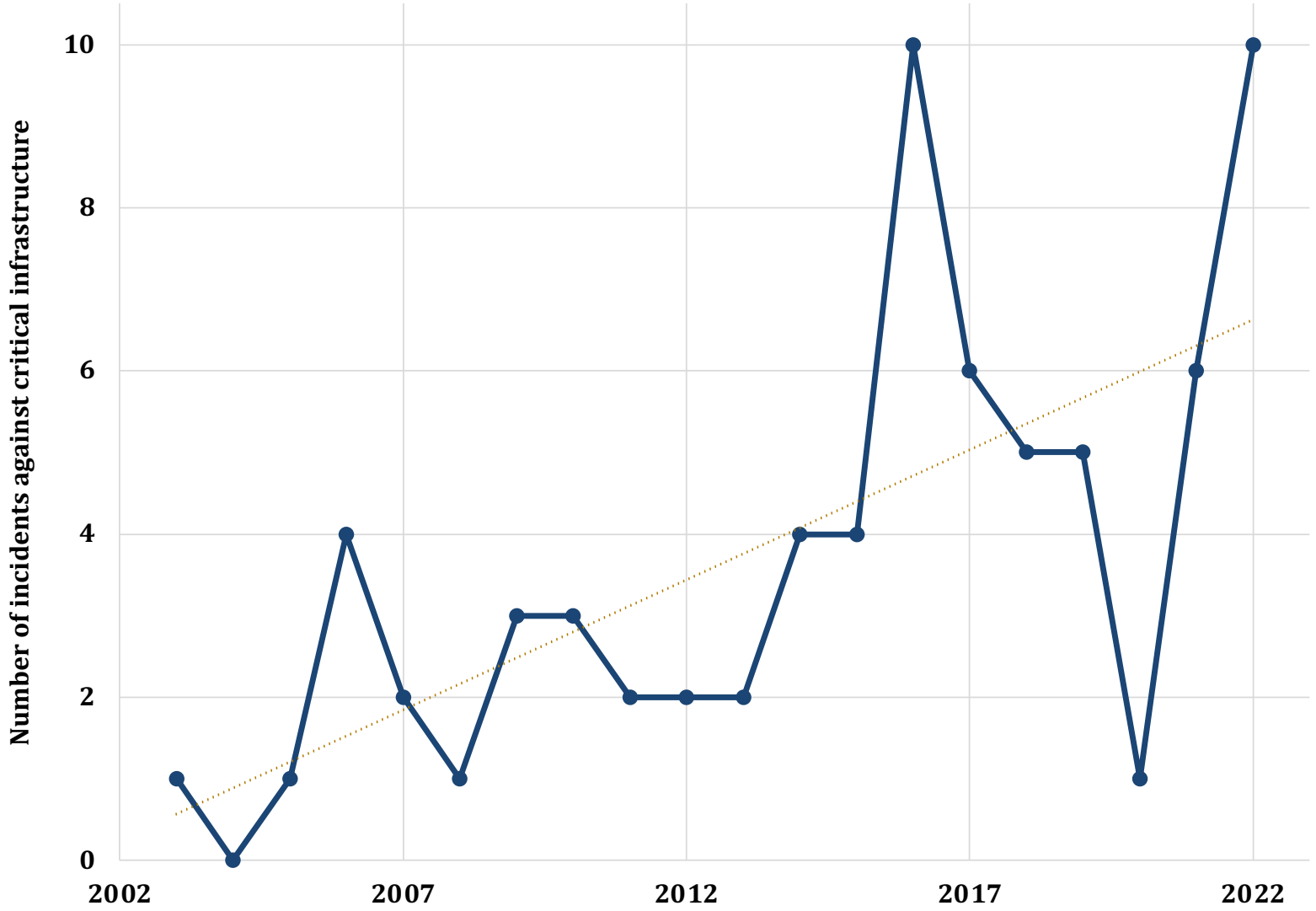
	CHINA	RUSSIA	TURKEY
Main type of incident	Espionage (81%)	-DDoS/Defacement (48%) -Espionnage (9%) -Other (36%)	DDoS/Defacement (90%)
Main type of actor	State-affiliated actors (65%)	-State-affiliated actors (28%) -State actors (23%) -Non-state actors (48%)	Non-state actors (78%)
Main type of target	Corporate targets (50%) State/political targets (50%)	State/political targets (72%)	-State/political targets (50%) -Corporate targets (40%)
Nb incidents against EU in EuRepoC database	36	67	10
	↓	↓	↓
	CONSISTENT TREND IN INCIDENT TYPES, ACTORS AND TARGETS	**MORE VARIATION IN INCIDENT TYPES AND ACTORS**	**MAINLY NON-STATE ACTORS**

II-
Protecting critical targets
eurepoc.eu

SWP

EuRepoC

Incidents against critical infrastructure are **increasing** in the EU

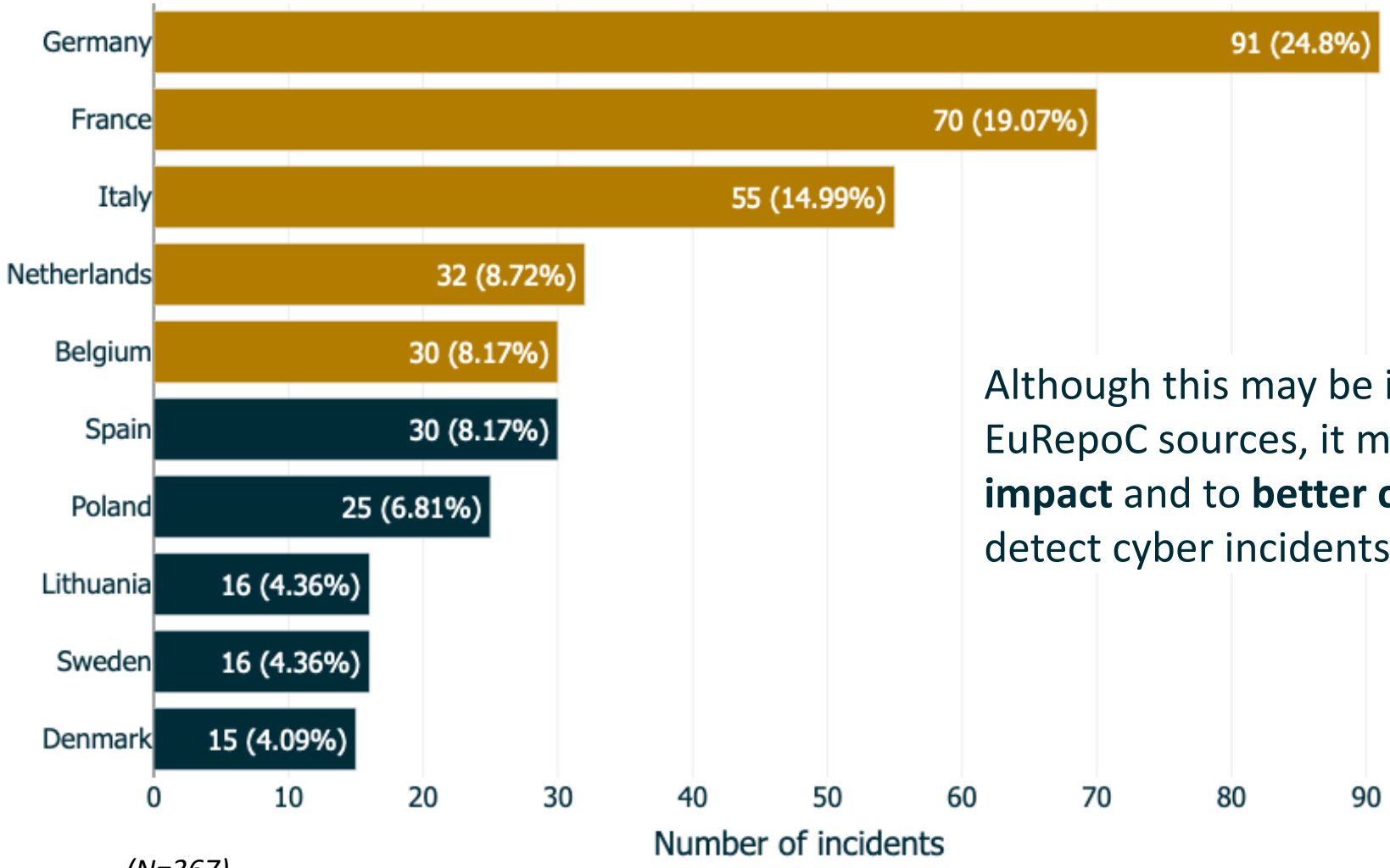


Compound Annual Growth Rate between 2003-2022: 21.4%

Cyber incidents against critical infrastructure in EU member states over time (N=76)

Founding member states are targeted by cyber incidents more than other member states

Top 10 targeted EU member states by cyber incidents from 2001 to September 2023

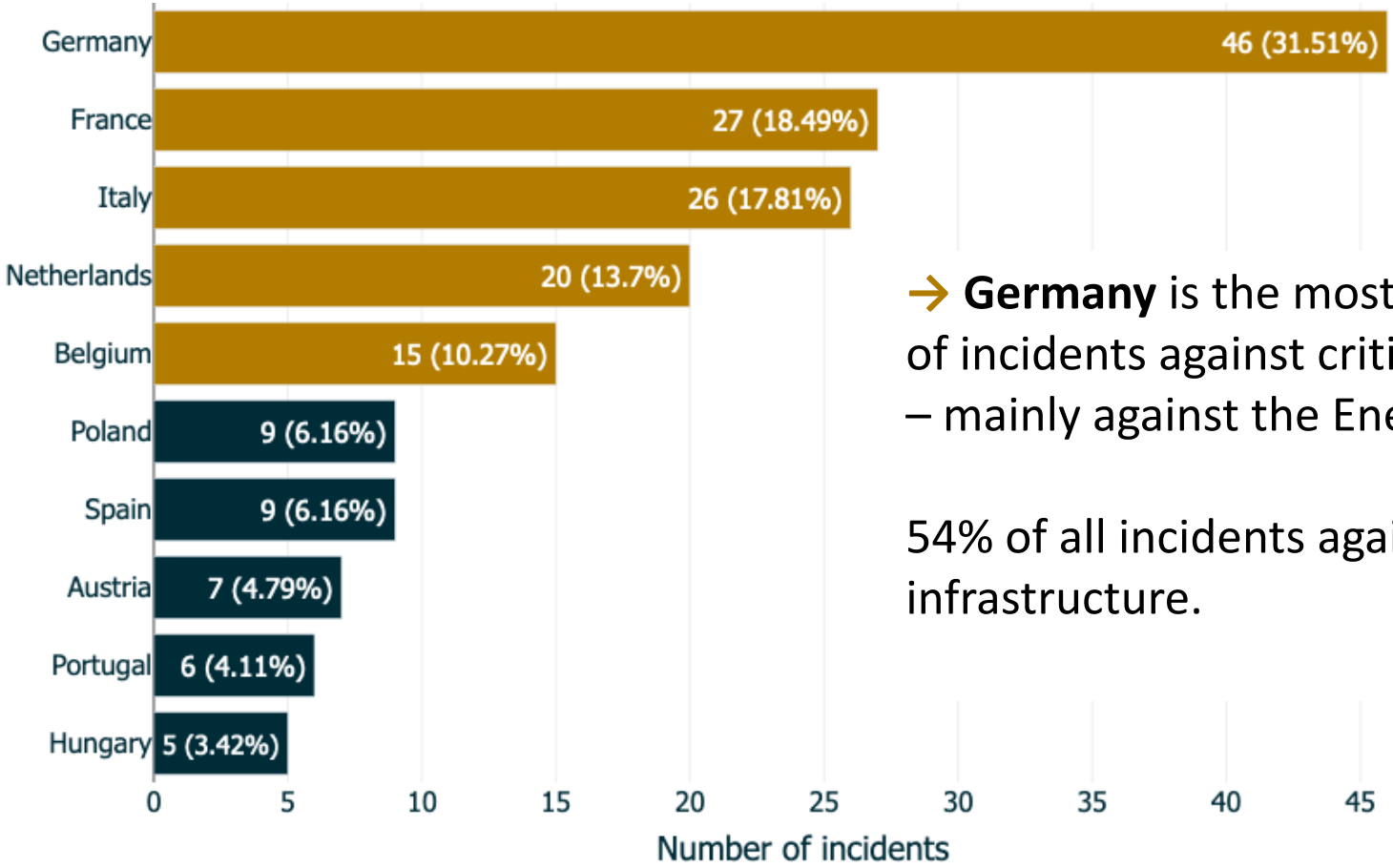


(N=367)

Although this may be influenced by a media bias in EuRepoC sources, it might also be linked to a **greater impact** and to **better capacities** in these countries to detect cyber incidents.

This also applies to incidents **against critical infrastructure**

Top targeted EU member states by cyber incidents against critical infrastructure from 2001 to April 2023



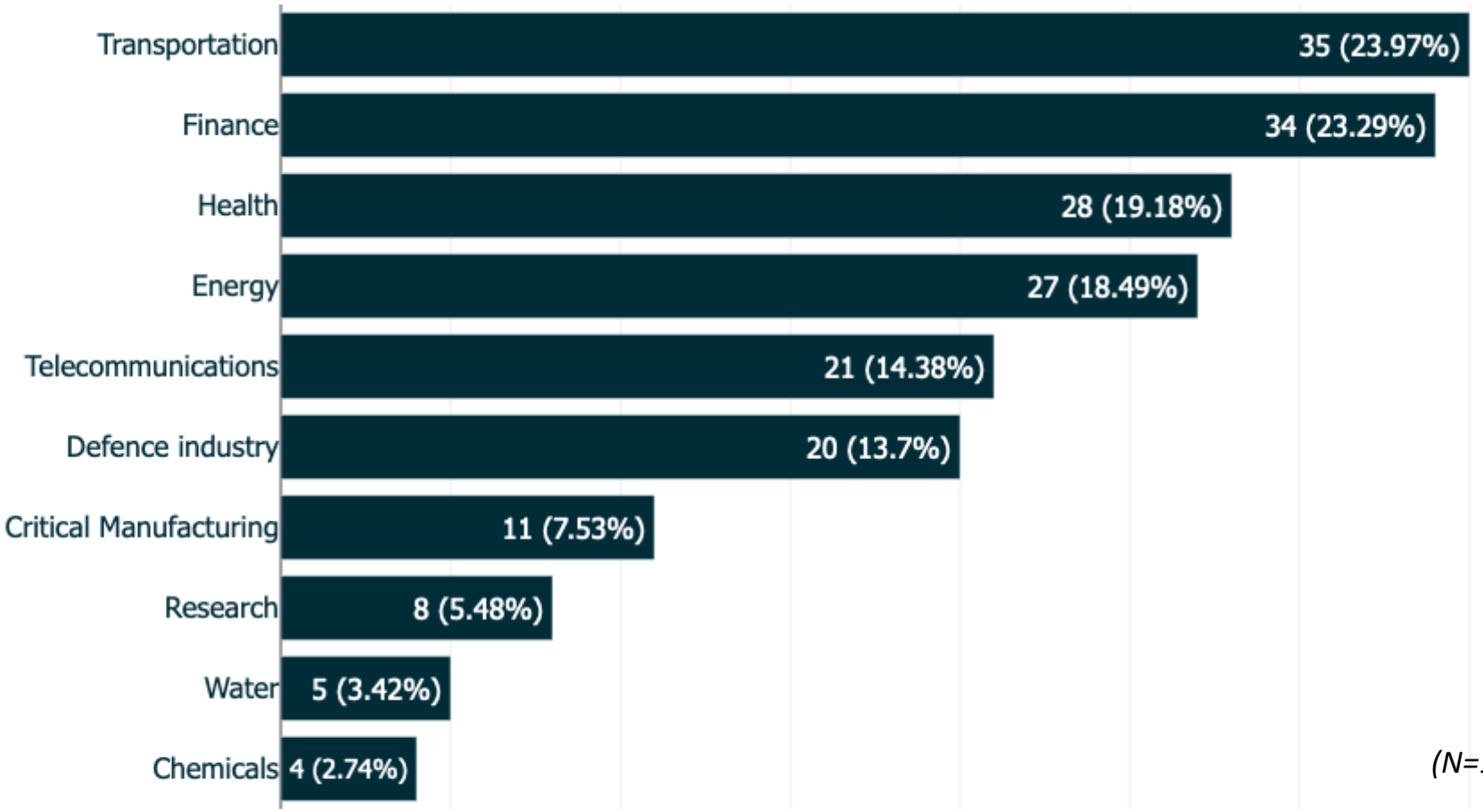
(N=146)

→ **Germany** is the most targeted EU member state, with 32% of incidents against critical infrastructure targeting Germany – mainly against the Energy and Transportation sectors.

54% of all incidents against Germany were against critical infrastructure.

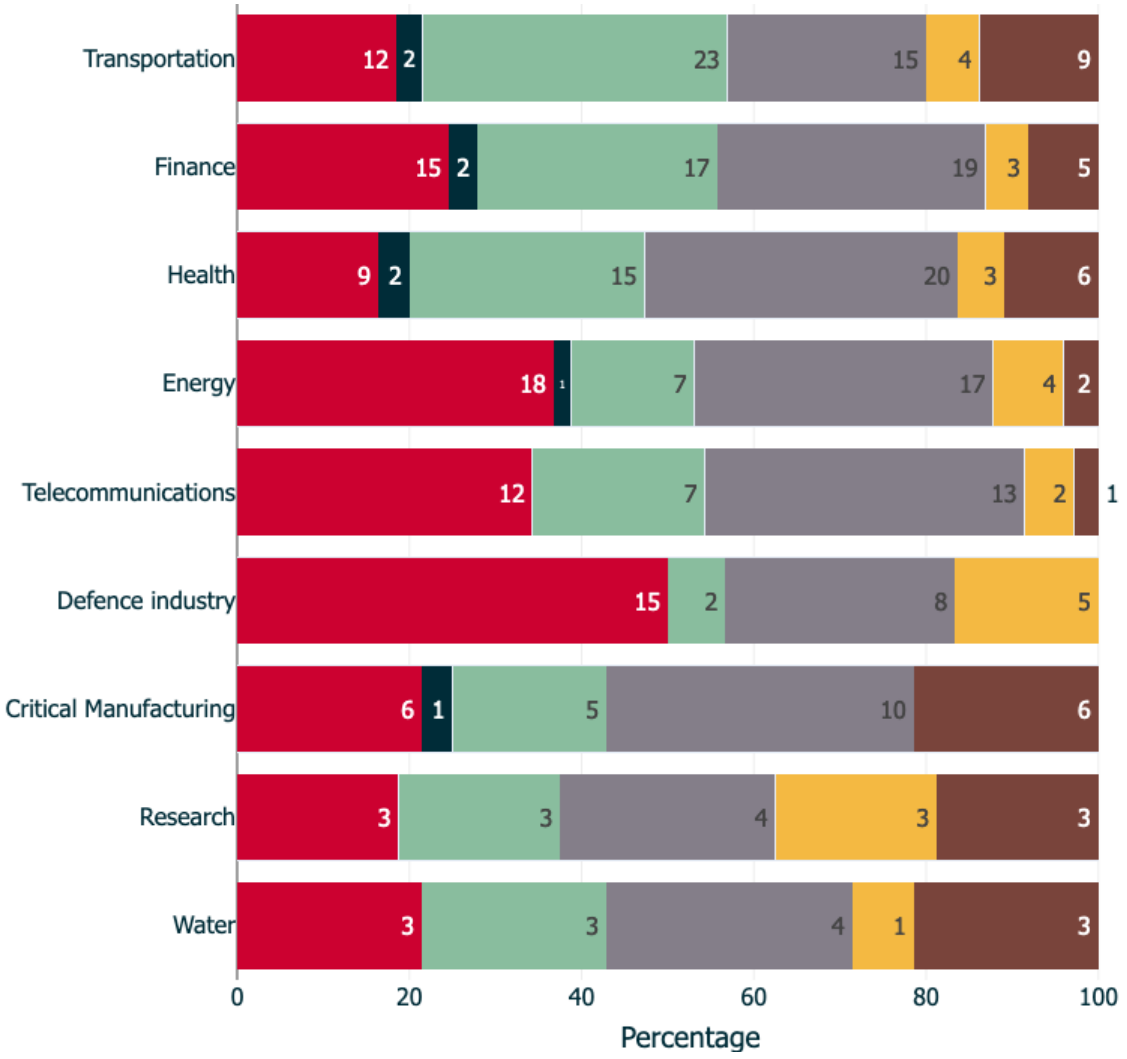
The **transportation** and **finance** critical infrastructure sectors are the most targeted by cyber incidents in EU member states

Critical infrastructure sectors targeted by cyber incidents in EU member states from 2001 to September 2023



(N=146)

Top targeted critical infrastructure sectors by type of cyber incident in EU member states from 2001 to September 2023



Cyber incidents against critical infrastructure vary in nature depending on the specific sector.

The transportation sector predominantly faces disruption incidents, whereas the defence and energy sectors are often victims of data theft incidents. The finance and health sectors are primarily targeted by incidents involving hijacking with misuse.

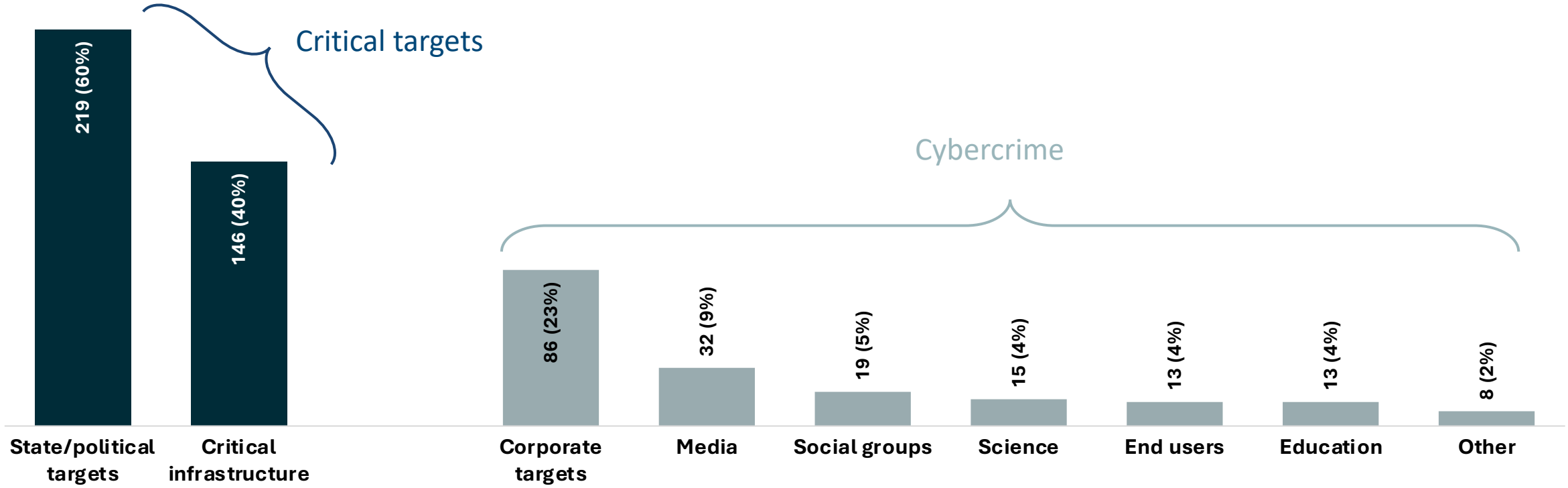
Among attributed incidents, **Russia** and **China** are the main countries of origin of incidents against critical infrastructure in the EU

- **33%** (48) of incidents targeting critical infrastructure are **not attributed**
- 18% (26) of incidents were initiated by **Russian** actors
- 10% (15) of incidents initiated by **Chinese** actors

A **one-size-fits-all** approach thus **does not work** for regulating EU sanctions

- The EU faces different types of threats and cyber incidents depending on the country of origin
- More nuance in a European response to cyber incidents would be more effective

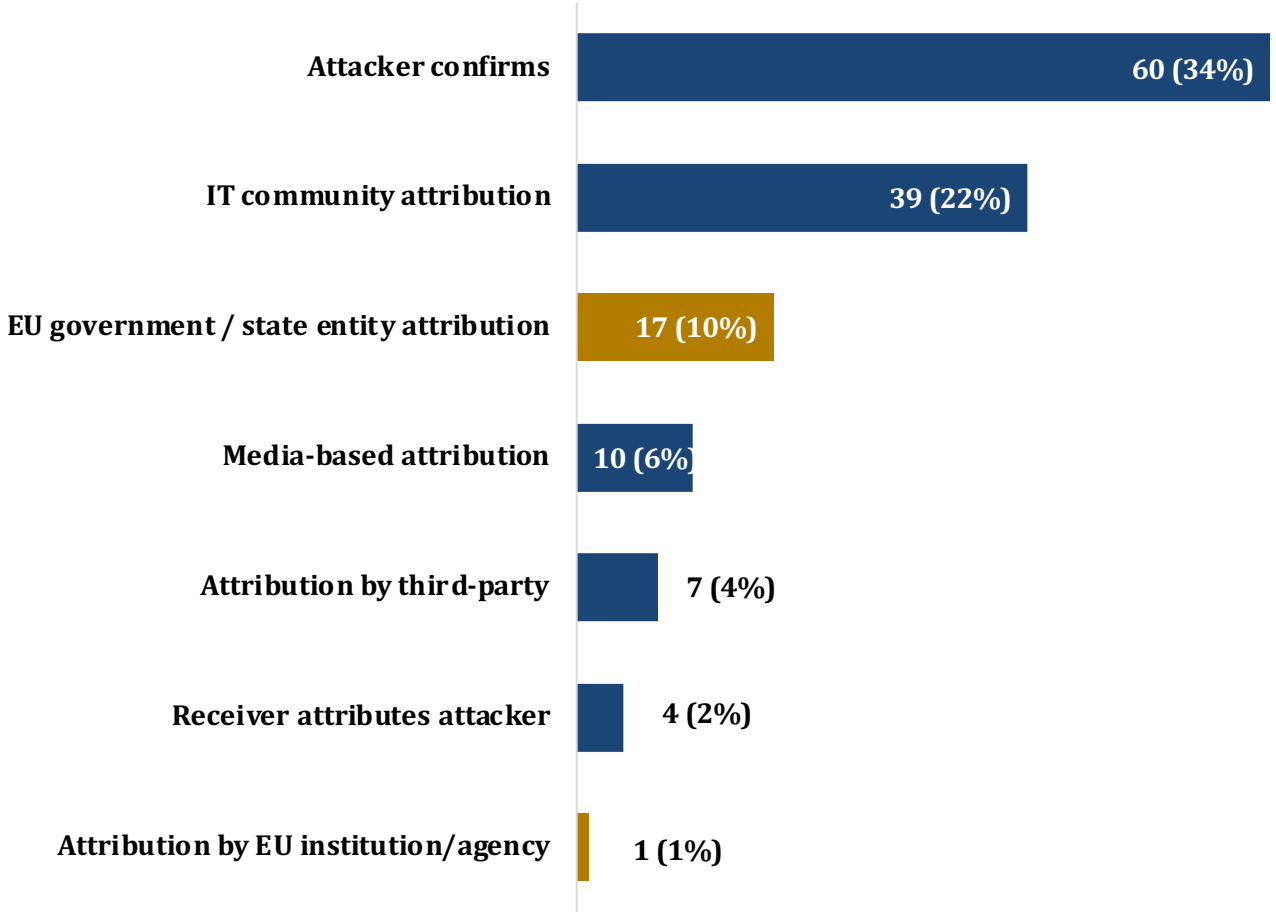
Policy solutions are lacking to address incidents targeting state institutions, political systems and critical infrastructure - although **86% of EuRepoC incidents** in the EU target these sectors.



Cyber incidents against EU member states from 2001 to September 2023 by targeted sector (N=367)

III-
Attributing cyber incidents eurepoc.eu

Attribution capabilities are within the hands of the **private sector**



Number of attributions by attribution basis for cyber incidents targeting EU member states (N=174 – sample of incidents coded since September 2022)

The most common attribution basis for incidents targeting EU member states is **confirmation by the attacker**, followed by **IT community** attributions.

→ Government attributions are behind, with **only 10%** of incidents having an **attribution by an EU government** and only **1 by EU institutions**.

On average, it took the **IT community 8.7 months** to attribute incidents targeting EU members from the start date of incidents. *[sample of 39 incidents coded since Sep 2022]*

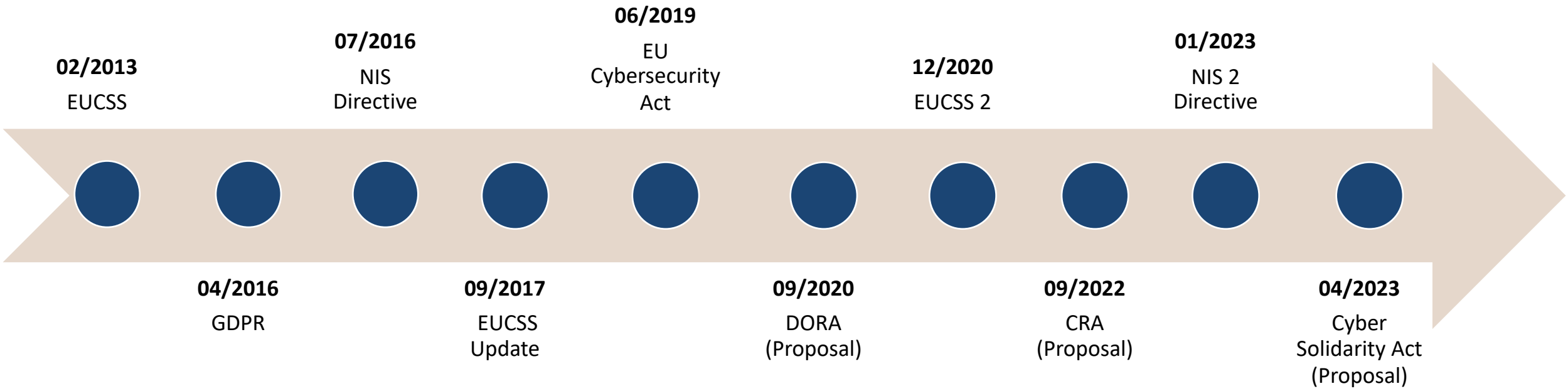
It took **EU governments 9.1 months** on average to attribute incidents in which they were targeted. *[sample of 16 incidents coded since Sep 2022]*

Private-Public-Partnerships are needed to improve attribution

- Private-Public-Partnerships: The more information is shared between private companies and public institutions, the better attribution can become.

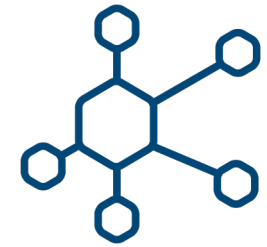
- Current problem: Companies are usually unwilling to share data about the attacks they suffer.

EU Cybersecurity Regulation - timeline

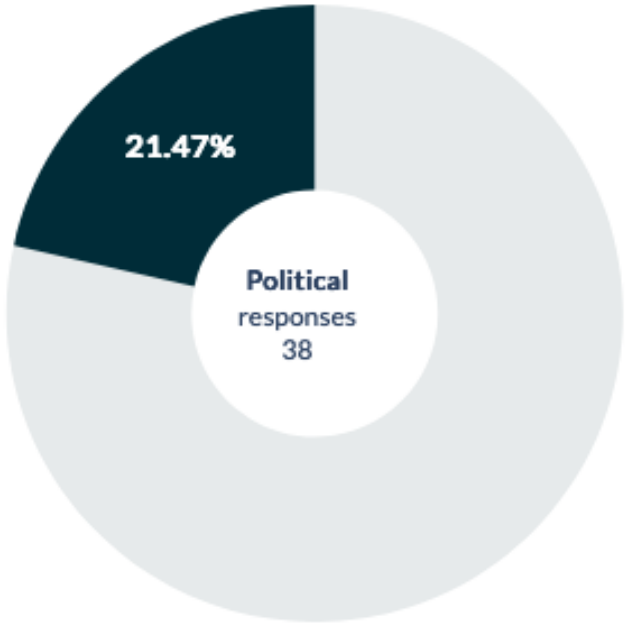


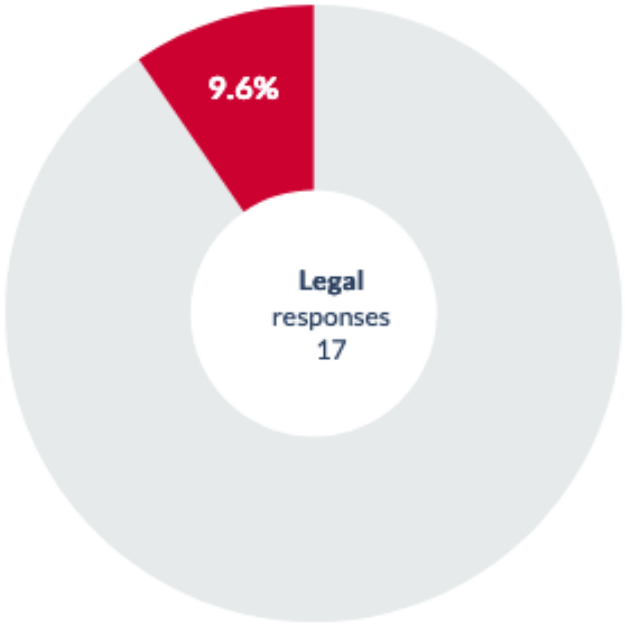
IV-
Responses to cyber incidents
eurepoc.eu

SWP



Very few cyber incidents against EU member states are met with a political or legal response

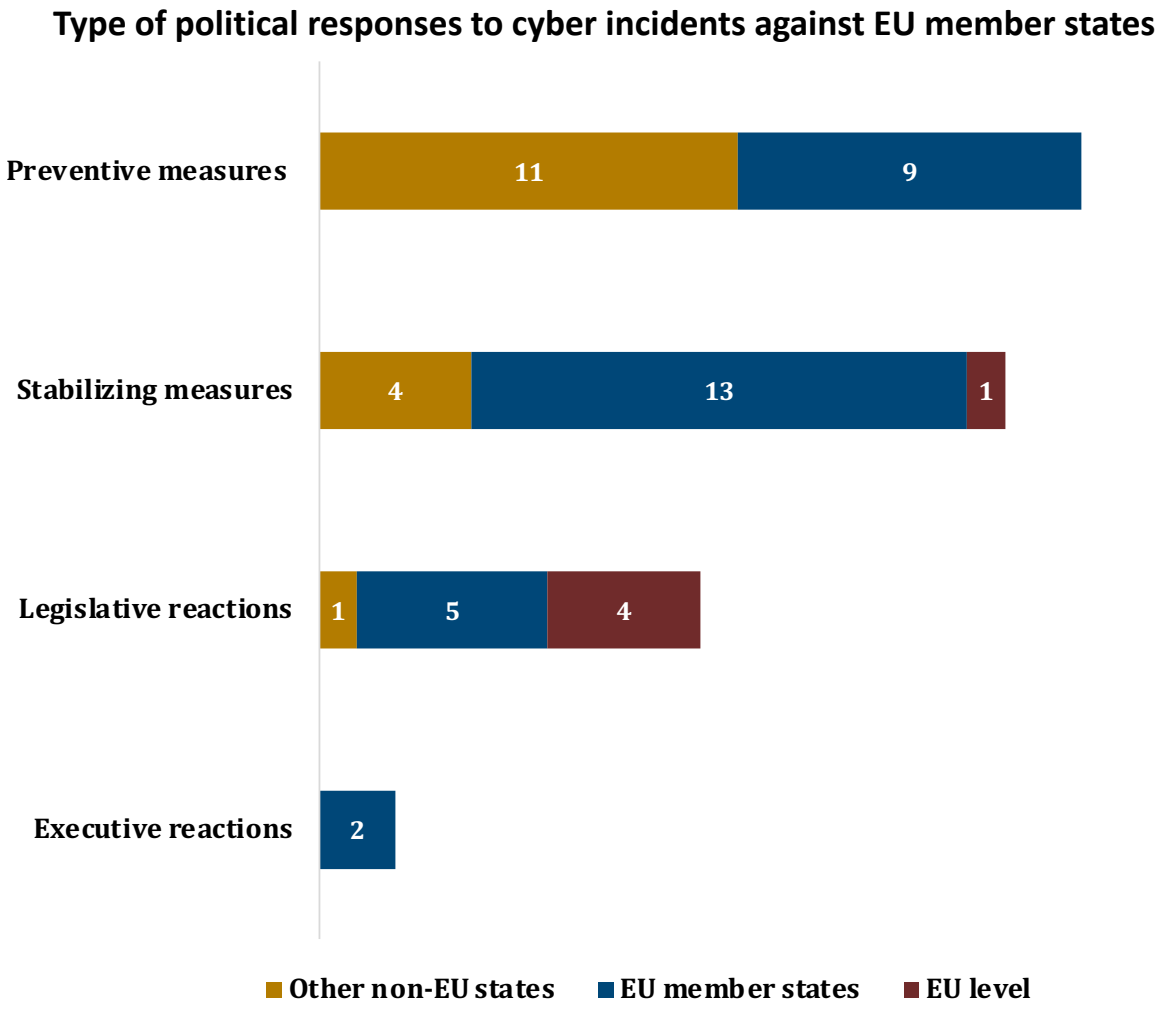




N=177 – only incidents coded since Sep 2022

Cyber incidents against EU member states with a political or legal response

EU member states responded to cyber incidents on a political level mainly with stabilising and/or preventative measures.



N=38 – only incidents coded since Sep 2022

- Stabilising measures by EU member states include **statements** by ministers/members of parliament (8); by subnational executive officials (2); heads of state (1); foreign ministers (1)

- Preventative measures by EU member states include only **awareness-raising**

Only one cyber incident coded since Sep 2022 against the EU led to economic sanctions.

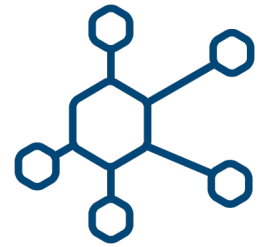
Out of the 17 legal responses:

- Other legal measures on national level (e.g. law enforcement investigations, arrests): 16

- Economic sanctions: 1

IV-
Zoom on Germany
eurepoc.eu

SWP



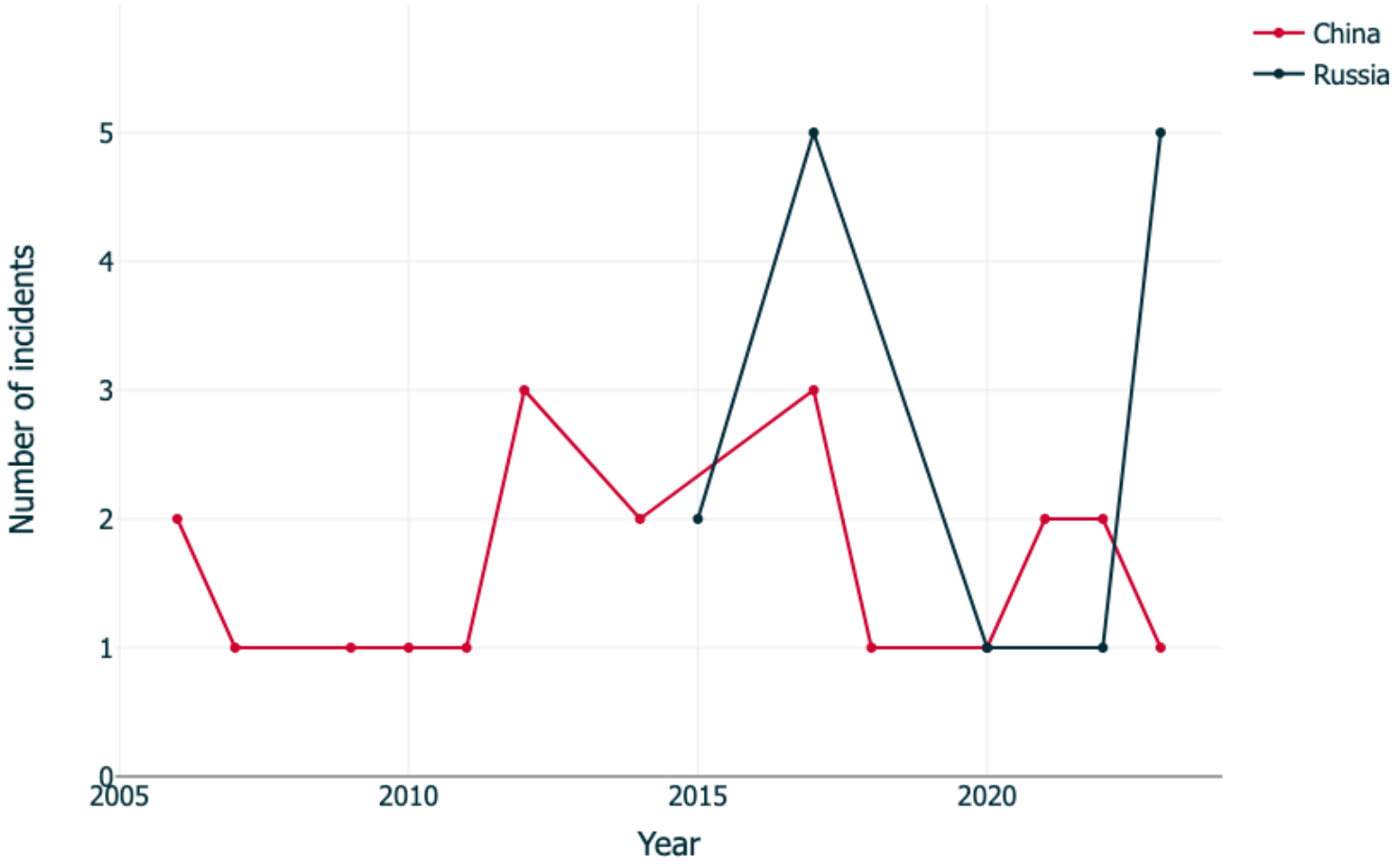
EuRepoC

Overview

- Germany is the **most frequently targeted EU member state** – with 91 cyber incidents recorded by EuRepoC since 2001 (this represents 25% of all incidents against EU member states).
- The main sectors targeted in Germany are **critical infrastructure**, **state institutions** and **corporate targets**.
- **54% of all incidents against Germany targeted critical infrastructure**, 16% of which against the **energy** sector, 15% against **transportation** and 13% against the **health** sector.

Origin of attacks

- 25% (23) of cyber incidents against Germany are from **unknown origin** – remain unattributed.
- 22% (20) originated from **China** and 15% from **Russia** (18) – for both countries, mainly from state-affiliated groups (cyber proxies).
- Since 2006, China has been the primary country of origin of attributed cyber incidents against Germany. This trend has been changing since 2015 with **increasing numbers of incidents of Russian origin.**
- So far, in 2023, we have coded 5 incidents against Germany attributed to Russia and only 1 involving Chinese actors.

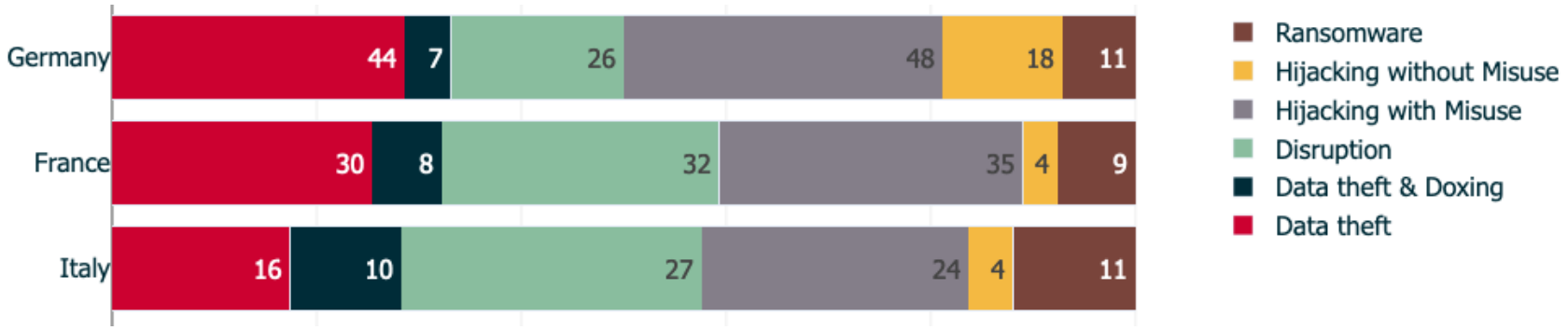


Main types of incidents against Germany

- In Germany, 53% of incidents were **hijacking with misuse** incidents, followed by **data theft** incidents (48%). This differs from the overall EU trend, where disruption incidents were the most frequent across all member states.

- Disruption incidents in Germany represented only 29% of incidents, while in France and Italy, these represented 46% and 49%, respectively.

Types of cyber incidents by member states between 2001 and September 2023



Attribution

Based on 46 incidents against Germany ***coded since September 2022***

- **The IT community has been the main source of attributions for incidents against Germany** (28% (13) had attributions by the IT community)

Incidents against Germany attributed by German actors:

- **Only 7 cyber incidents (15%) against Germany coded since Sep 2022 had an attribution by a German actor, of which only 2 were by the German government.**
- Although this is low, it is above the EU average of 9%
- Germany fares better than its EU counterparts (Italy and France), who face similar numbers of cyber incidents. In Italy, only 9% of incidents targeting the country were attributed by national actors, whereas we recorded no attributions from French actors. *[for incidents coded since Sep 2022]*

Member State	Incidents attributed by national actors	Total incidents against the country	Percentage of nationally attributed incidents
Bulgaria	2	3	67%
Germany	**7**	**46**	**15%**
Spain	4	16	25%
Netherlands	4	19	21%
Czech Republic	2	6	33%
Poland	3	15	20%
Romania	1	3	33%
Italy	**3**	**33**	**9%**
Sweden	1	5	20%
Austria	0	3	0%
Slovakia	0	4	0%
Luxembourg	0	2	0%
Latvia	0	3	0%
Greece	0	3	0%
Ireland	0	2	0%
Cyprus	0	3	0%
Croatia	0	1	0%
Finland	0	2	0%
EU (region)	0	2	0%
Denmark	0	8	0%
Lithuania	0	7	0%
Hungary	0	5	0%
Portugal	0	7	0%
Estonia	0	7	0%
Belgium	0	11	0%
France	**0**	**32**	**0%**

Responses und Fazit:

- 9 of the 46 incidents against Germany coded since Sep 2022 received a political response from Germany (19.5%)
- Only 2 received a legal response from Germany (6.5%),

✓Nationale Politik ist ebenfalls wenig effektiv und bietet keine Lösung.

✓Technische, rechtstaatliche und politische Attribution (Verantwortungszuschreibung) von schwerwiegenden Cyberangriffen ist auf EU und nationaler Ebene gleichermaßen unzureichend.

✓Sanktionen haben keine abschreckende Wirkung auf Angreifer.

✓Kumulative Angriffe auf EU-Staaten bleiben nahezu unbeantwortet.

EU Cyber Posture Mai 2022

Computer Network Defense (CND)	Computer Network Exploitation (CNE)	Computer Network Attack (CNA)	Cyber Threat
Industry Policy	Trojans	Intrude, disrupt or destruct network (i.e. DOS Denial of Service ..)	Force majeure
Certification	Backdoors	Data manipulation, espionage, sabotage	Blackout scenario, Distroyed Data Clouds
IT-security	Threat Hunting	Counter Attacks on infrastructure	Counter Attacks on critical infrastructure
ENISA, Joint Cyber Unit, CERT-EU, EEAS EU INTCEN	***Europol, (2020/0349(COD), ENISA***	***EEAS, EU INTCEN, EUMS INTEL, ENISA, Art. 222 TFEU (?)***	***Cyber Defense Force (Cyber-Rapid-Response Team CCRT) (42, 6 EUV; 42, 7 EUV, Art. 4 and 5 Nato)***
Defensive (resilience)	*Investigative*	*Active Defense*	*Offensive Defense (electronic combat, „hackbacks“)*
Peace (prevent)	*Peace (discourage)*	*Hybrid (deter)*	*War (respond)*

KI basierte Szenarien

What could future digital conflicts in geopolitics look like in 2035?

What role could the EU, China and non-governmental actors play in solving them?

https://vimeo.com/378332238/1ef679a7af

https://we.tl/t-3Xxqveh2cD

Caveat: Possible media bias?

- There are **significantly fewer publicly disclosed cyber incidents initiated by Western actors**.
- We find only 2% of incidents against EU member states with an American or British origin.

⇒ Is this a reflection of reality, or do Western sources disclose fewer incidents stemming from allied countries?