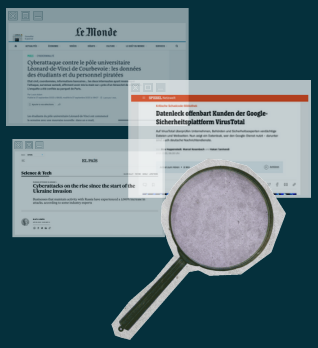
European Repository of Cyber Incidents



EU Media Reporting Tracker

September 2023

EuRepoC's EU media tracker covers 30 leading news outlets in 9 EU member states (non-paywalled articles). It analyses the extent to which these media outlets report on cyber incidents with a political dimension, compared to other sources, including reports from IT companies, governments, and social media. Cyber incidents with a political dimension, include incidents that (1) targeted political or state actors/institutions, (2) were initiated by state actors or actors associated with states, or (3) incidents that have been politicised regardless of their targets or origin.

The data provides insights into the disparities/similarities between the cyber security expert community and the mainstream media, which continues to play a crucial role in shaping public perception in European societies. By critically analysing EU media discourse on cyber incidents, this tracker contributes to EuRepoC's broader objectives of raising awareness, strengthening transparency, and building trust to support EU cyber diplomacy. For more information on the EuRepoC project and data collection methodology, see here.

This is a static version of the online interactive report updated monthly:
https://eurepoc.eu/eu-media-reporting-tracker/

September 2023
By Camille Borrett, Data Analyst for the German Institute for International and Security Affairs (SWP)

Key insight 1:

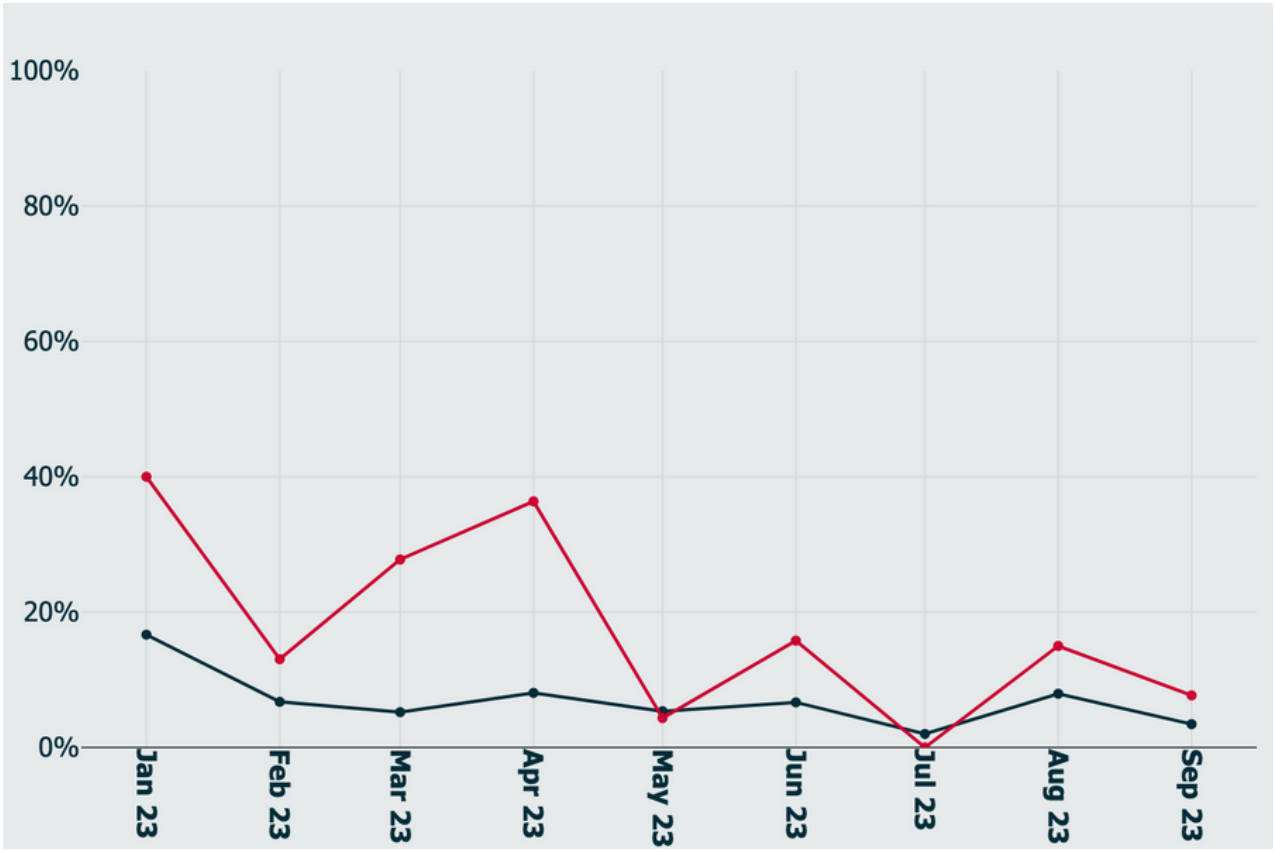
Cyber incidents receive limited attention in the mainstream EU media

Overall, only 6% of cyber incidents recorded by EuRepoC since January 2023 were also reported in the tracked EU media.

This figure increases when looking only at cyber incidents that targeted EU member states, but still remains low at 15.5%.

In September 2023, only 3 out of 87 incidents added to our database were reported in the tracked EU media (3%). 2 targeted EU member states out of 26 in total (8%).

Percentage of cyber incidents reported by EU media out of all incidents recorded by EuRepoC



- Incidents targeting EU member states
- All incidents

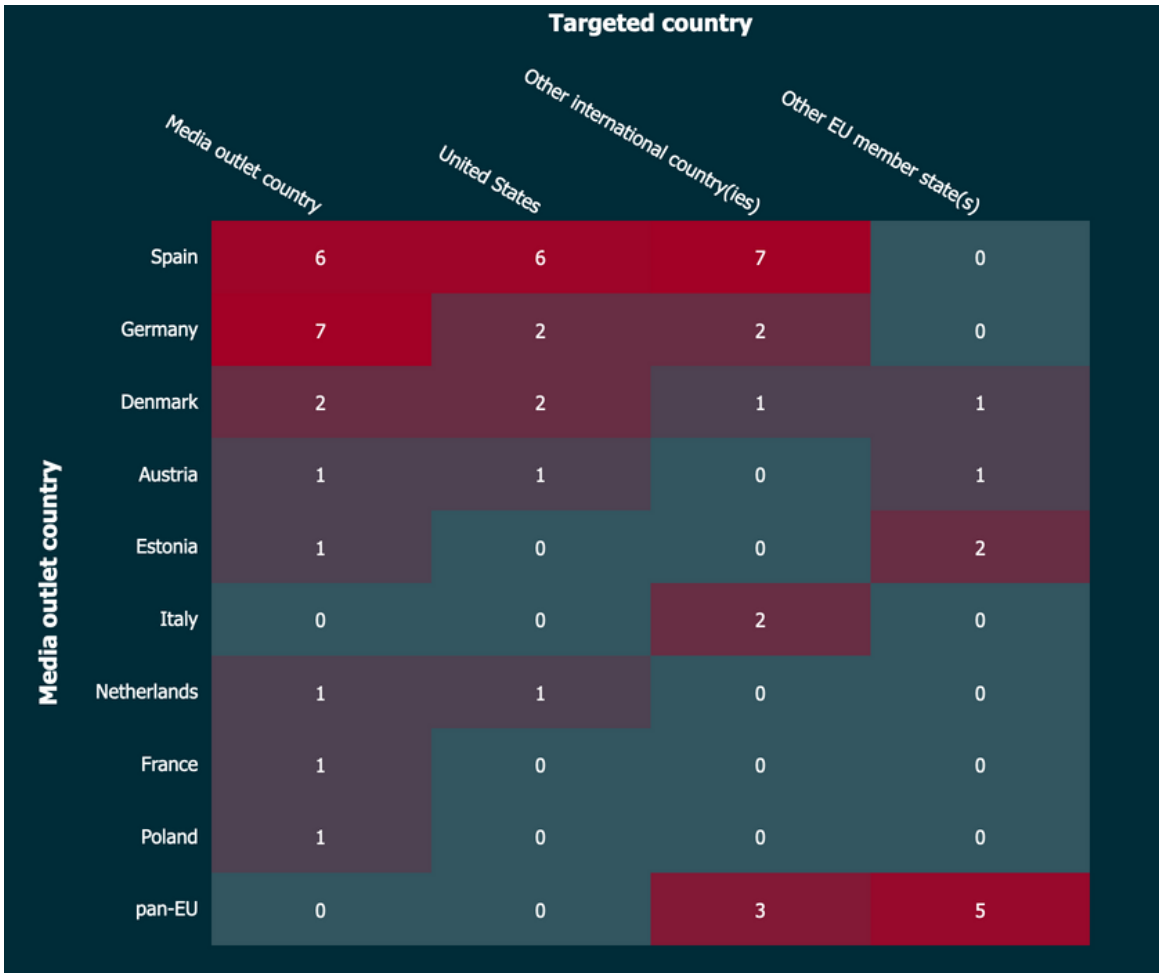
Key insight 2:

We see a lack of Europeanised reporting on cyber incidents

The EU media tend to report cyber incidents where their own country was targeted or cyber incidents targeting non-EU member states - particularly the United States. Very few outlets report cyber incidents targeting other EU member states. This is partly due to the comparatively high vulnerability of US targets to cyberattacks, but also to a particularly high number of US actors first reporting on cyber incidents, whose reports are then picked up by EU media.

The heatmap below shows the number of incidents reported by outlets in the 9 EU member states covered by this analysis by targeted country.

Number of cyber incidents reported by media country and targeted country



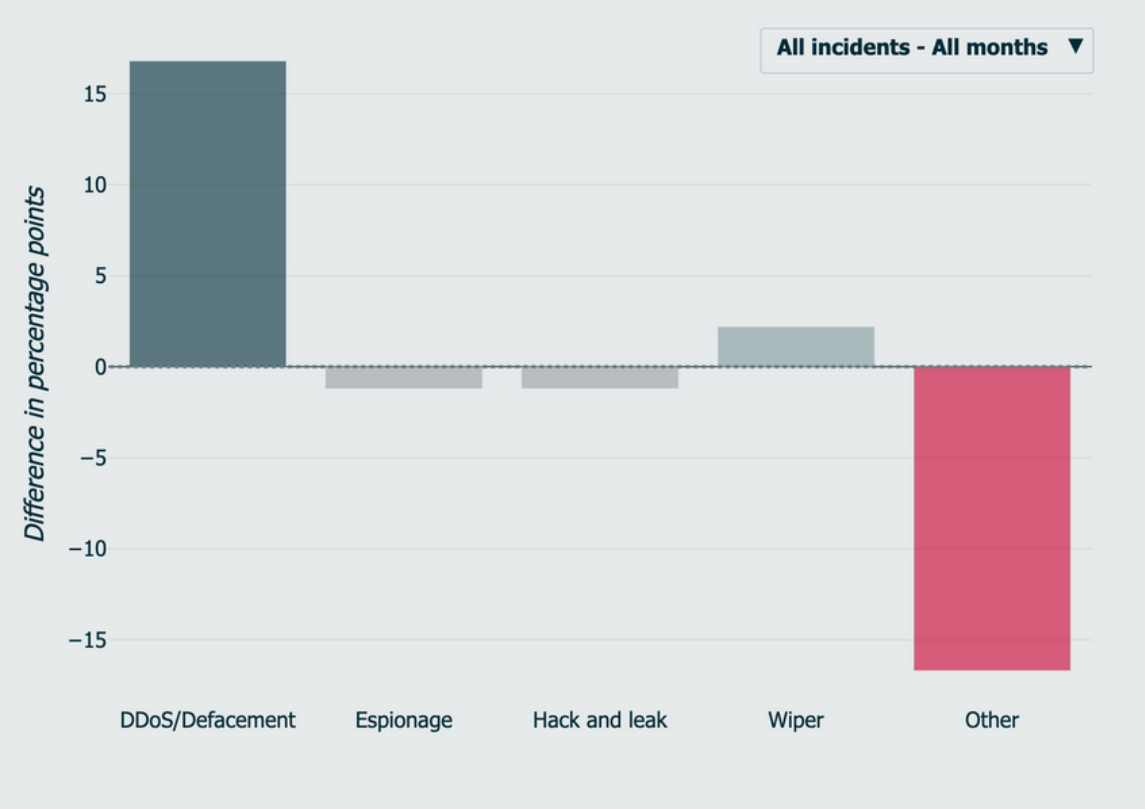
Key insight 3:

DDoS/Defacement operations are over reported

Since January 2023, 33% of incidents reported by the media were DDoS operations, whereas these operations only represent 16.5% of all operations added to the database over the same period (green bar).

Other less visible incidents (e.g. hijackings or data theft), are underreported (red bar), despite often having more severe socio-economic consequences than DDoS/defacement attacks. This is significant as the increased attention given to DDoS attacks can play in the hand of the attackers. It can lead to a distorted threat perception of European citizens as well as a misallocation of public cybersecurity resources.

Difference between EU media coverage of different operation types vs. their actual share of the EuRepoC database



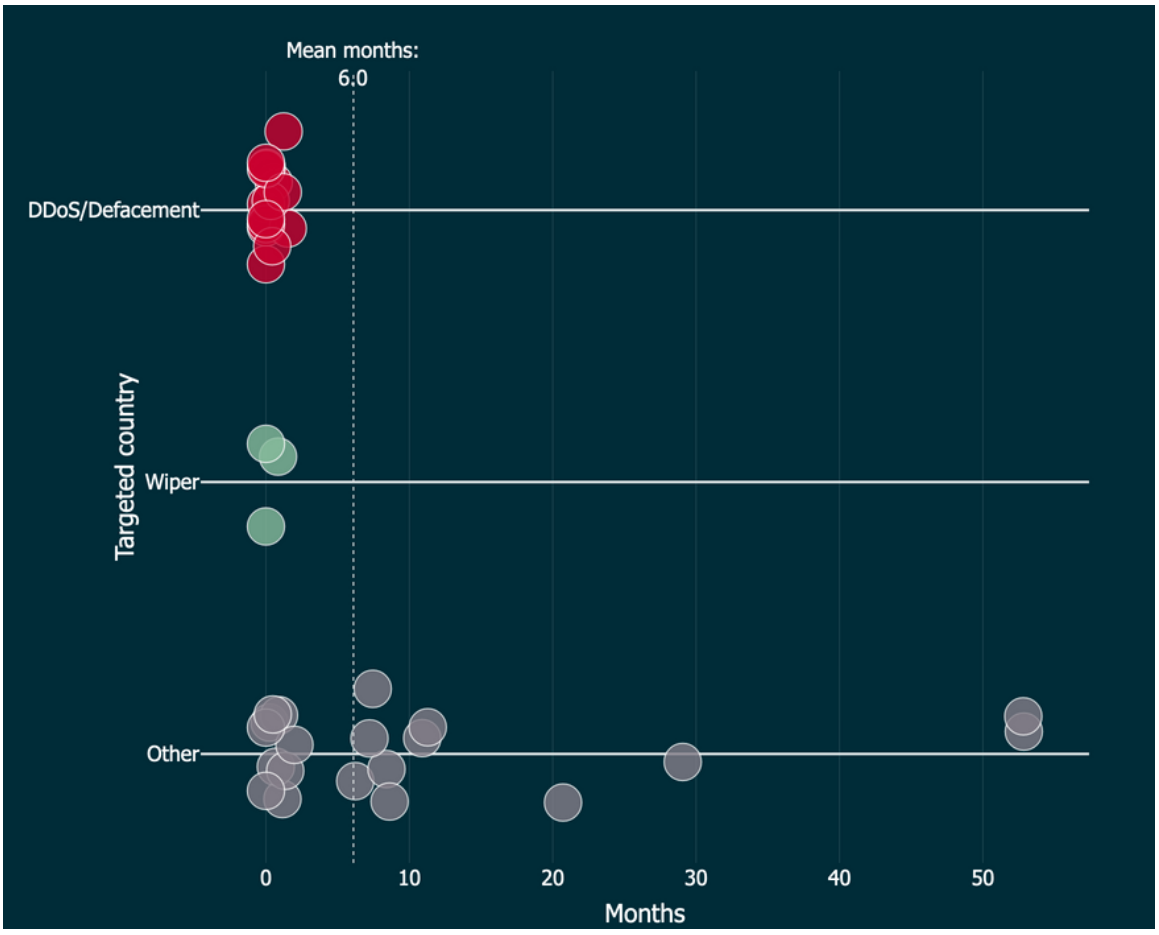
Key insight 4

There's a significant delay between the start of a cyber incident and its media coverage.

On average, incidents are reported 6 months after they initially take place. The delay ranges from a few months to as long as 53 months—approximately 4 years—in some cases. This time lag is indicative of the time often required for a cyber incident to be detected and/or disclosed by the affected parties.

DDoS/defacement and wiper operations are reported much quicker than other types of operations, as due to their disruptive effects, they are necessarily designed for timely detection, also by third parties outside of the target organisation.

Number of months between the start of an incident and the media report



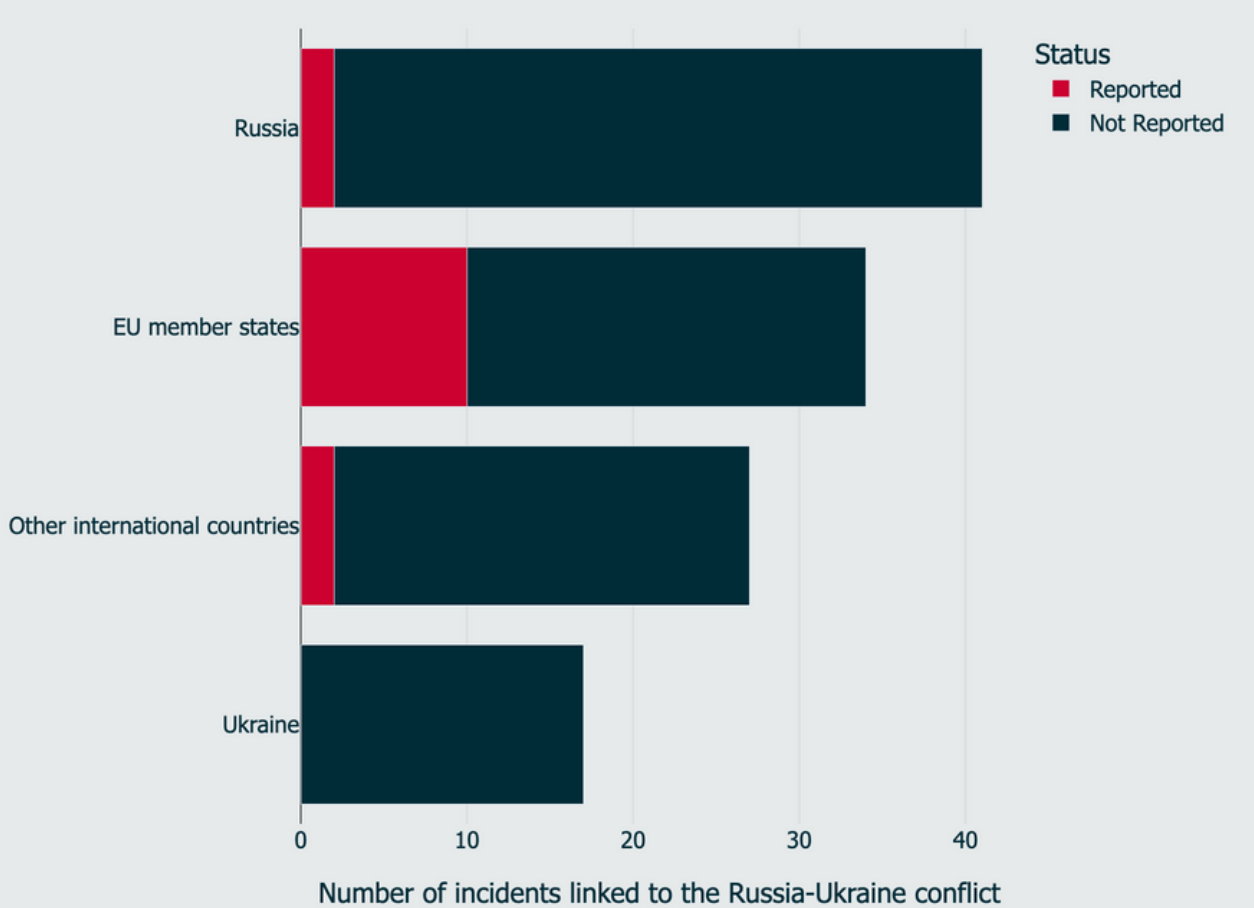
Key insight 5

Media reporting on cyber incidents linked to the Russia-Ukraine conflict has a strong national focus.

Since January 2023, we recorded 112 cyber incidents linked to the Russia-Ukraine conflict, of which only 12% (13) were reported in the EU media covered under this analysis.

The EU media mainly reported incidents linked to the conflict when EU member states were affected - particularly their own member state. Specifically, 10 of the 13 reported incidents targeted EU member states, 8 of which the country of the reporting media outlet. On the other hand, none of the incidents targeting Ukraine were reported and only 2 of those targeting Russia.

Number of cyber incidents linked to the Russia-Ukraine conflict by targeted country



Incidents reported in tracked media in September 2023

Unknown threat actors targeted telecommunications provider IFX Networks, causing the paralysis of over 30 government websites in Colombia and numerous other Latin American countries on 12 August 2023

Start date: Sep 2023
Targeted country(ies): Chile
Country of origin of initiator(s): Not available
Incident type(s): Disruption; Hijacking with Misuse; Data theft; Ransomware
Reporting media: El Pais - Spain

Ransomware group 'Lockbit' disrupted Seville City Council's computer systems beginning on 5 September 2023

Start date: Sep 2023
Targeted country(ies): Spain
Country of origin of initiator(s): Netherlands
Incident type(s): Disruption; Hijacking with Misuse; Ransomware
Reporting media: El Mundo - Spain ; Kleine Zeitung - Austria

FBI disrupted Qakbot control infrastructure and removed Qakbot malware from infected computers

Start date: Aug 2023
Targeted country(ies): Not available
Country of origin of initiator(s): United States
Incident type(s): Disruption; Hijacking with Misuse
Reporting media: El Pais - Spain

Note on methodology

This analysis only covers media articles that are not behind a paywall.

Each source is scanned daily and automatically as part of the general EuRepoC data collection methodology. We cover media sections on national and international politics and columns on cybersecurity/technology.

Please note that EuRepoC only considers cyber incidents that have a political dimension. It is possible that the EU media outlets covered by this analysis reported on additional cyber incidents outside the scope of the EuRepoC project.

Media outlets covered

Country	Newspaper
AT	Der Standard
	Die Presse
	Kleine Zeitung
DE	Die Welt
	Frankfurter Allgemeine Zeitung
	SPIEGEL Online
	Süddeutsche Zeitung
DK	Berlingske
	Jylands Posten
	Politiken
EE	Eesti Päevaleht
	Postimees
ES	ABC
	El Mundo
	El Pais
	La Vanguardia
EU	Euractiv
	Euro News
	Euro Topics
	Politico EU
FR	Le Figaro
	Le Monde
	Les Echos
IT	Corriere della Sera
	Il Sole 24 Ore
	La Stampa
NL	De Telegraaf
	De Volkskrant
	NRC
PL	Gazeta Wyborcza
	Rzeczpospolita