

Cybercrime in the News, 2019-2026: Growth, Geography and Tone of Global Coverage of Cybercrime and Online Fraud, and How It Compares with Research and Invention

Fliar BI · Prism Research Layer · Working paper, October 2026 · Dataset and code: github.com/fliarbi/prism-news-api · Licence CC BY-NC 4.0

Abstract

We measure how cybercrime and online fraud were covered in a global news index from January 2019 to July 2026, using 97,895 de-duplicated cybercrime articles, and set that coverage beside 5,195 research papers (2015-2025) and 47 patent families (2015-2024) on the topic. Six results stand out:

1. **Growth.** Cybercrime took 3.95 of every 10,000 news articles in 2019 and 8.5 in 2025, a 2.15-fold rise. The share rose in every year. The peak month was December 2024, at 12.14 articles per 10,000.
2. **Geography.** India holds 47.99% of located cybercrime news, 3.64 times its share of all news. The United States holds 16.5%, only 0.34 times its share. Cambodia (39.95), North Korea (19.54), Myanmar (14.85) and Thailand (6.1) are the most over-represented countries.
3. **Within India.** Telangana (2.38), Chandigarh (1.86), Haryana (1.8) and Jharkhand (1.56) lead by lift; Jammu and Kashmir (0.27) is lowest. US state tags remain too noisy to rank.
4. **Shifting attention.** Between 2023 and 2025, cybercrime's share of India's news rose from 19.81 to 33.3 per 10,000, and Pakistan's rose 4.3 times, the largest rise among countries with at least 100 cybercrime articles in 2025.
5. **Tone and urgency.** 81.4% of cybercrime articles are negative in tone (all news: 33.6%), and 86.2% are rated critical priority (all news: 42.6%).
6. **Research and invention.** Cybercrime papers grew from 0.36 to 1.46 per 10,000 papers between 2015 and 2025, a 4.06-fold rise in share. Patent titles rarely use the word: only 47 families in ten years.

Findings stated for citation

- **F1.** Cybercrime's share of news rose 2.15-fold, from 3.95 to 8.5 articles per 10,000, between 2019 and 2025.
- **F2.** India's share of located cybercrime news (47.99%) was 3.64 times its share of all news. The United States' (16.5%) was 0.34 times.
- **F3.** Cambodia (39.95), North Korea (19.54), Myanmar (14.85) and Thailand (6.1) were the most over-represented countries.
- **F4.** 81.4% of cybercrime articles were negative in tone, 2.42 times the all-news share.
- **F5.** 86.2% of cybercrime articles were rated critical priority by a machine rating, 2.02 times the all-news share.

- **F6.** Human trafficking appeared in 4.24% of themed cybercrime articles, 26.86 times its frequency in all news.
- **F7.** 53.19% of themed cybercrime articles carried the theme of cybercrime law and digital forensics.
- **F8.** Cybercrime papers rose 4.06-fold as a share of all papers between 2015 and 2025.
- **F9.** Only 47 patent families (2015–2024) named cybercrime or online fraud in the title; the US office held 35.9% of office filings.
- **F10.** Within India, Telangana (2.38), Chandigarh (1.86), Haryana (1.8) and Jharkhand (1.56) had the most over-represented coverage.
- **F11.** Cybercrime's share of India's news rose 1.68 times from 2023 to 2025; 3,684 articles named the "digital arrest" scam.
- **F12.** Pakistan's attention to cybercrime rose 4.3 times from 2023 to 2025, the largest rise among countries with at least 100 cybercrime articles in 2025.
- **F13.** Relative to each country's own news, cybercrime coverage departed most from the baseline in China (89.8% negative against 27.2%), Canada and the United Arab Emirates.

1. Introduction

Cybercrime covers offences committed through computers, networks and online payment systems: fraud and scams, extortion, theft of data and money, and the abuse of online identities. Official statistics on it are patchy. Many victims do not report, police recording rules differ between countries, and the same offence can be filed as fraud, theft or a computer offence. News coverage is one of the few records that spans countries on a common footing. It also shapes what the public and policy-makers treat as urgent.

This paper and its dataset measure that coverage as data. They combine three records for one topic: a global news index, research papers and patents. Each comparison uses a denominator, so that growth in the index or in publishing is not mistaken for growth in interest. The companion dataset publishes an article-level sample (24,600 rows) and full coverage tables, so every figure here can be re-derived. The [Prism News API](#) serves the full history.

2. Data and methods

News. The Prism news index holds articles from outlets worldwide; non-English articles are indexed in English translation. Each article carries its opening text (the first few sentences), a primary location, a graded tone label, an editorial priority rating (1–9), themes, keywords and named organisations. We count unique article identifiers; repeated rows for the same article are removed. When this release was built, 92.88% of the index was readable, so all counts are lower bounds.

Matching. An article is about cybercrime when its opening text contains one of 21 terms as whole words. The general terms are *cybercrime(s)*, *cyber crime(s)*, *cybercriminal(s)* and *cyber criminal(s)*. The fraud terms are *cyber fraud(s)*, *cyber fraudsters*, *cyber scam(s)*, *cyber thugs*, *online fraud*, *online scam(s)*, *UPI fraud* and *digital arrest*. Hyphenated spellings are included. Broader words that also name defensive security or state conflict (*cyberattack*, *hacking*, *ransomware*) are not used, so the topic is crime as the press names it. Two kinds of match are excluded:

- press-release wire copy from security vendors, which uses the vocabulary as marketing;
- film and series reviews that mention online fraud as a plot.

Together these removed 670 of 98,565 raw matches (0.68%). One reviewer read 40 randomly drawn matched openings. 36 were about crime committed through computers, networks or online payments (precision 90%), and in 29 (72.5%) cybercrime was the main subject. The four false positives were two vendor product announcements, a terrorism case handled by a cyber crime police unit, and a film review.

Measures. Coverage over time is expressed per 10,000 articles in the index that month or year, because the index grew from 11,807,177 articles in 2019 to 26,990,006 in 2025 (2.29 times). Seasonality uses each year's within-year month shares, averaged over the complete years 2019–2025. Geography, tone, priority and themes use January 2023 – July 2026. Geography is expressed as lift: a country's share of cybercrime articles divided by its share of all located articles. In that window 29,318 of 66,594 articles (44.02%) carried a primary country. Place tags derived from ordinary words ("Congress", "Earth", "Winter", "Cloud") were treated as unlocated in every location field, which removed 15.3% of city-tagged articles.

Research and patents. Research papers are de-duplicated articles and reviews (2000–2025) with a cybercrime, cybercriminal, cyber fraud, online fraud, online scam, UPI fraud or digital arrest term in the title, repository deposits excluded. Patent families (2005–2024) use the cybercrime and fraud terms in the title and are counted once per filing office.

3. Results

3.1 How much and when

The index holds 97,895 cybercrime articles from January 2019 to July 2026. Raw counts rose 4.92 times, from 4,662 in 2019 to 22,939 in 2025. Because the index also grew, the fair measure is the share: 3.95 per 10,000 in 2019 and 8.5 in 2025, a 2.15-fold rise (Table 1). The share rose in every year, including 2020. The highest monthly share was December 2024, at 12.14 per 10,000. The months from October 2025 to December 2025 were the next highest (Figure 1). The first seven months of 2026 average 8.8 per 10,000, but 2026 (January–July) is partial.

Year	Cybercrime articles	All articles in index	Per 10,000
2019	4,662	11,807,177	3.95
2020	7,017	16,230,014	4.32
2021	8,956	17,281,220	5.18
2022	10,666	19,115,515	5.58
2023	13,362	20,484,506	6.52
2024	18,741	23,311,896	8.04
2025	22,939	26,990,006	8.5

Table 1. Cybercrime articles per year and as a share of the index. 2026 (January–July) is partial and omitted.

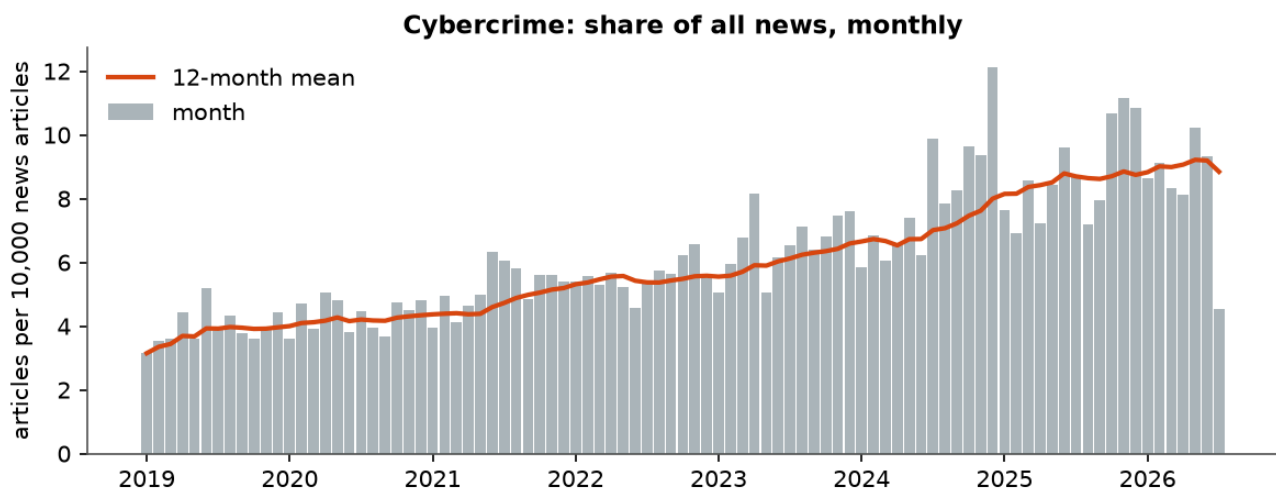


Figure 1. Cybercrime coverage as articles per 10,000 news articles, monthly, January 2019 – July 2026. Bars are months; the line is the 12-month mean.

Coverage has little seasonality (Figure 2). October to December hold 27.59% of a typical year's cybercrime articles and January to March 22.67%, against 25% for an even spread. December is the busiest month (9.37%) and February the quietest (7.37%).

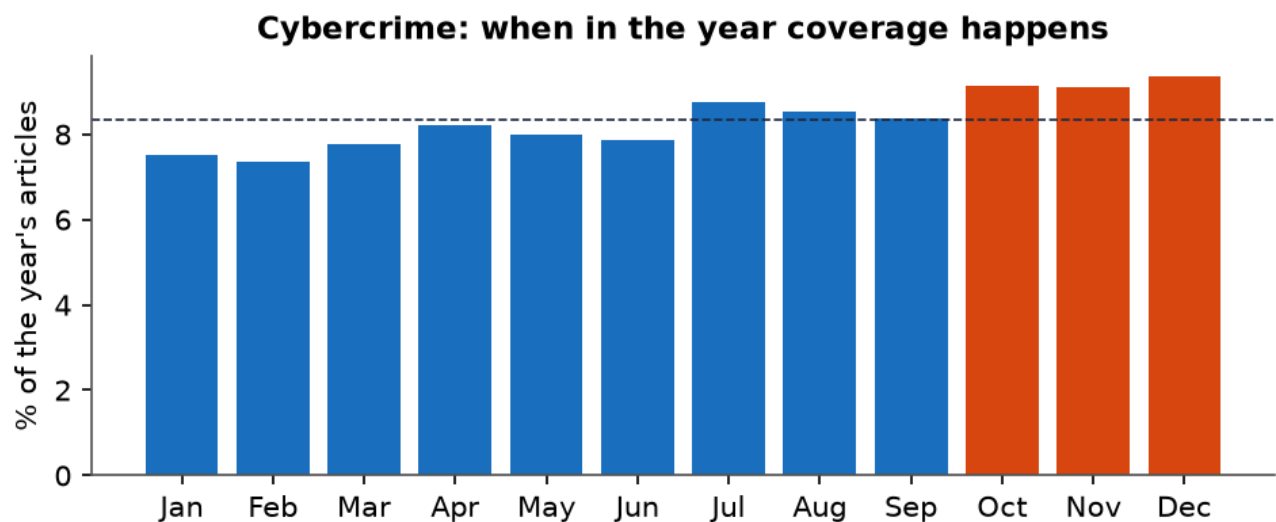


Figure 2. Share of each year's cybercrime articles published in each month, averaged over 2019-2025. Dashed line = an even spread (8.3% per month).

3.2 Where

Between January 2023 and July 2026, 29,318 cybercrime articles carried a primary location. India holds the largest share (47.99%), with a lift of 3.64. The United States holds 16.5%, but its lift is only 0.34: cybercrime takes a much smaller share of American news than of news overall. The most over-represented countries are in mainland Southeast Asia, where large scam compounds have been reported, and North Korea, whose state-linked hacking groups are often named in coverage of thefts (Table 2, Figure 3).

Country	Located cybercrime articles	Share %	Lift vs all news
India	14,069	47.99	3.64
United States	4,837	16.5	0.34
United Kingdom	1,377	4.7	0.8
Nigeria	911	3.11	2.27
China	680	2.32	0.88
Australia	544	1.86	0.87
Singapore	509	1.74	1.95
United Arab Emirates	358	1.22	1.87
Thailand	339	1.16	6.1
France	267	0.91	0.46
Russia	261	0.89	1.18
Philippines	255	0.87	2.76
Pakistan	241	0.82	1.81
Ghana	232	0.79	1.64
Canada	215	0.73	0.34
North Korea	210	0.72	19.54
Cambodia	210	0.72	39.95
Myanmar	141	0.48	14.85

Table 2. The 17 countries with the most located cybercrime articles (North Korea and Cambodia tie at 210), plus Myanmar for its lift, January 2023 – July 2026, with lift against all located news.

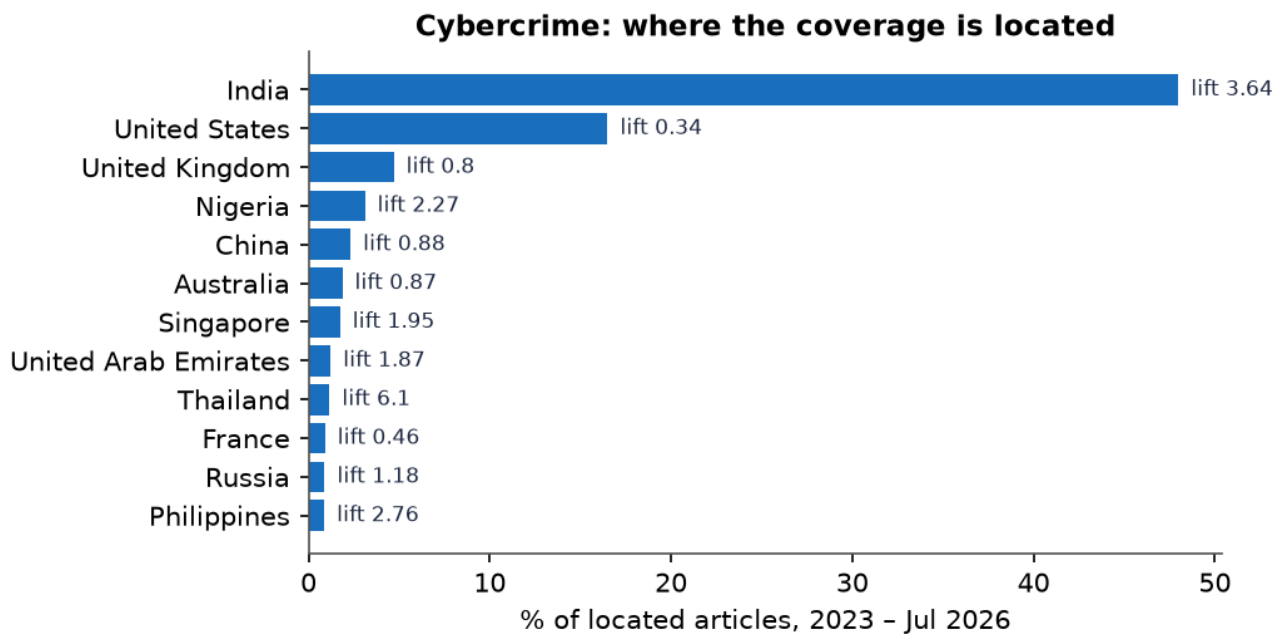


Figure 3. Leading countries by share of located cybercrime articles, 2023 – Jul 2026, labelled with lift against all located news.

3.3 Geo intelligence: continents, states and shifting attention

The world map (Figure 4) shows the pattern at a glance. Cybercrime is over-represented in the news of South and Southeast Asia and West Africa, and under-represented in North America, most of Europe, Japan and South America. By continent, Asia (2.58) and Africa

(1.62) are over-represented. Oceania (0.8), Europe (0.64), South America (0.63) and North America (0.31) are not (Figure 7, left).

Cybercrime: which countries over- and under-cover the topic

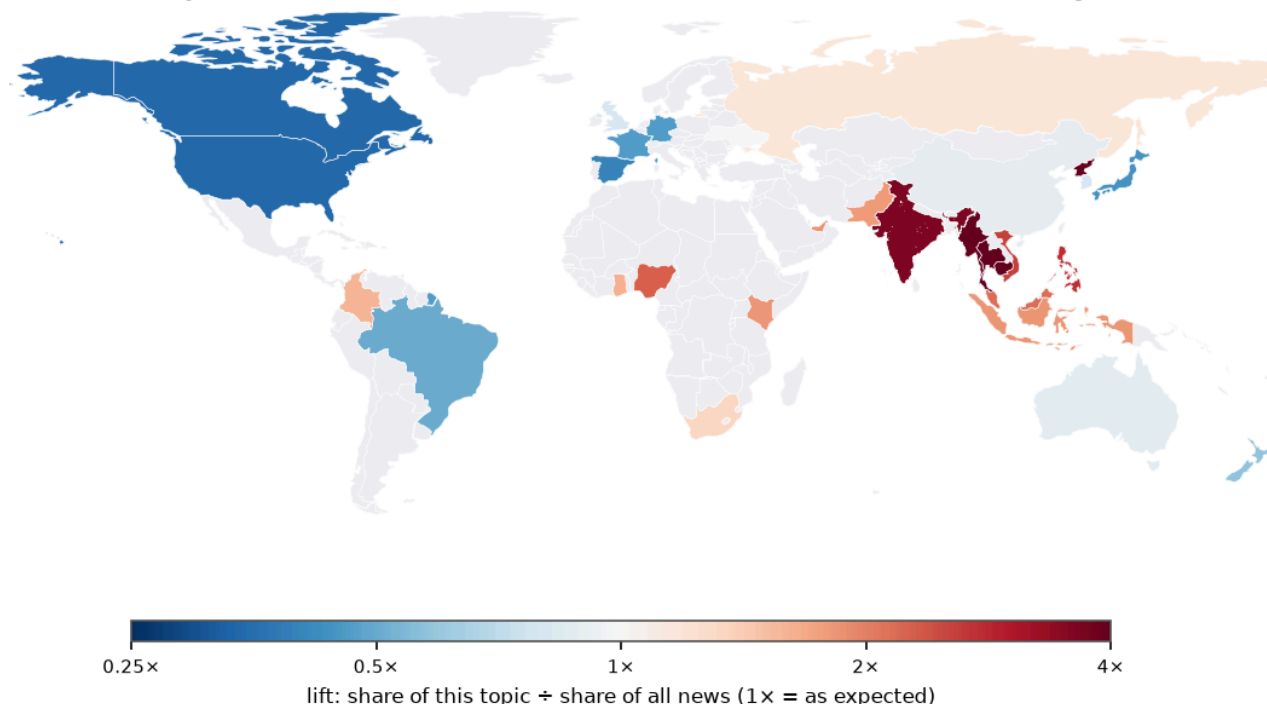


Figure 4. Lift of each country's share of located cybercrime articles, January 2023 – July 2026 (red = over-represented, blue = under-represented, grey = fewer than 100 articles). India is drawn with its official outline.

Within India the spread is narrow (Table 3). Of 12,336 located Indian cybercrime articles, every large state reports some, and lifts range from 0.27 to 2.38. Measured against each state's share of Indian news, Telangana (2.38), Chandigarh (1.86), Haryana (1.8), Jharkhand (1.56) and Rajasthan (1.36) are the most over-represented. Jammu and Kashmir (0.27), Himachal Pradesh (0.49), West Bengal (0.5) and Chhattisgarh (0.62) are the most under-represented (Figure 5). Maharashtra has the most articles (2,145) with a lift close to one (1.09). In the sample, Telangana rows are mostly tagged to Hyderabad and Jharkhand rows often to Jamtara, so these leads rest on real places.

The US picture is not reliable enough to rank (Figure 6). Of 2,527 located US articles, New York has the most (357, lift 1.21). The states with the highest lift on the map do not rest on real places when their sample rows are read: Massachusetts on "Norton", the security brand, tagged as the town of Norton; Alabama on surnames and ordinary words tagged as small towns ("Dora", "Opp", "Foley"); Nevada on rows whose city is "California" or that repeat one templated list of places. "Washington" and "Georgia" can also mean the US capital and the country. The US map is shown for completeness only, no US state is ranked in Table 3, and no US state result is stated as a finding. Iowa and Arkansas, which led before the place-word rule, now fall below 50 articles. States with fewer than 50 articles are left out of the text.

India: state	Articles	Share %	Lift
Telangana	1,020	8.27	2.38
Chandigarh	71	0.58	1.86
Haryana	567	4.6	1.8
Jharkhand	467	3.79	1.56
Rajasthan	583	4.73	1.36
<i>lowest:</i> Chhattisgarh	104	0.84	0.62
West Bengal	213	1.73	0.5
Himachal Pradesh	82	0.66	0.49
Jammu and Kashmir	79	0.64	0.27

Table 3. Indian states with the highest and lowest lift in cybercrime coverage, January 2023 – July 2026 (states with at least 50 articles). US states are not ranked because their leads rest on mis-tagged words (see text). Lift = the state's share of the country's located cybercrime articles ÷ its share of all located news from that country.

Cybercrime: states of India by lift

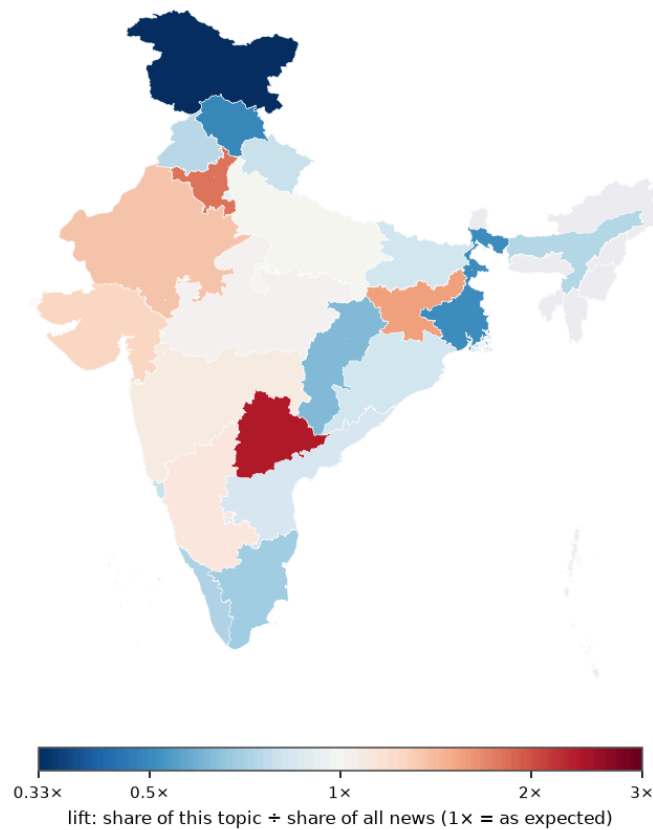


Figure 5. Lift of each Indian state's share of located cybercrime articles against its share of all located Indian news, January 2023 – July 2026. Official outline; Ladakh is drawn within Jammu and Kashmir in the boundary file used.

Cybercrime: states of United States by lift

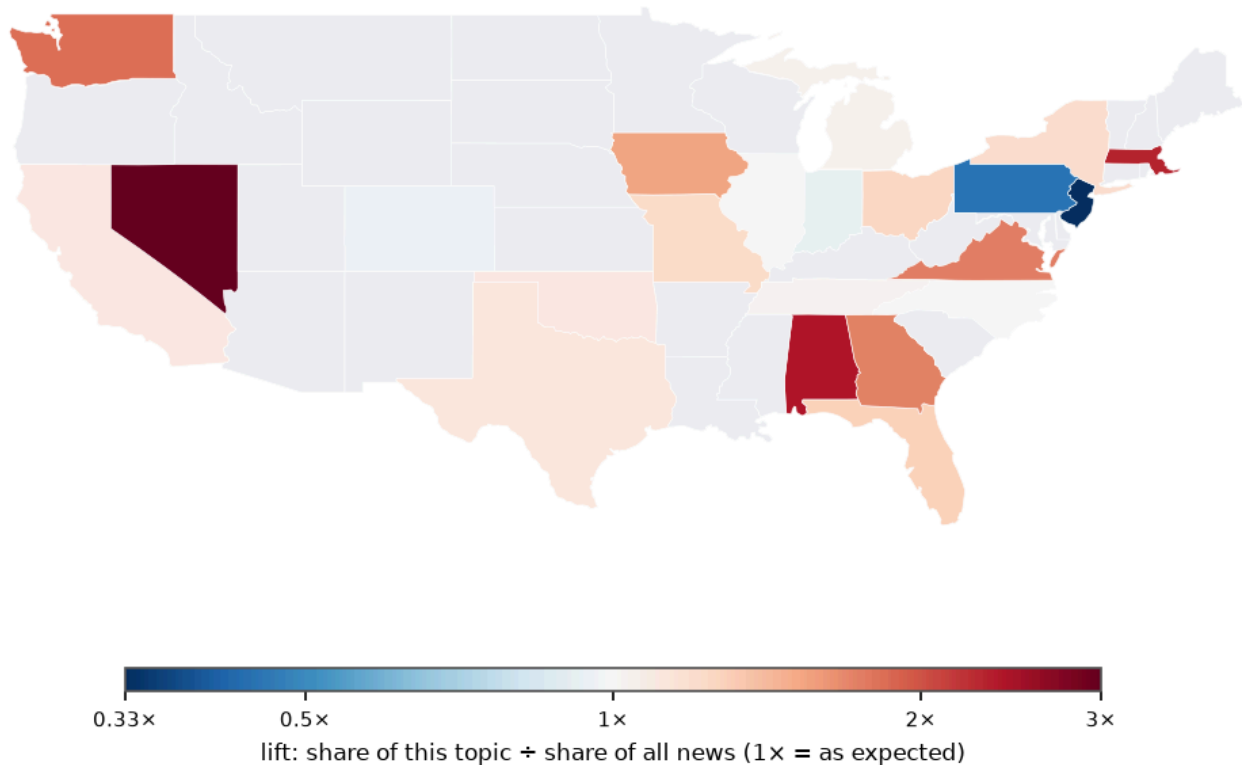


Figure 6. Lift of each US state's share of located cybercrime articles against its share of all located US news, January 2023 – July 2026.

Attention also moves between countries from year to year (Figure 7, right). Measured as cybercrime articles per 10,000 of each country's located news, India rose from 6.8 in 2019 to 19.81 in 2023 and 33.3 in 2025. Among countries with at least 100 cybercrime articles in 2025, the largest rises from 2023 to 2025 were in Pakistan (5.97 to 25.68, 4.3 times), Ghana (2.51 times), Thailand (2.28 times) and Singapore (2.08 times). Cambodia, below that threshold, rose from 65.54 in 2023 to 311.97 in 2025 on a small national news base. China (0.77) and Australia (0.91) fell over the same years, and the United Kingdom (1.0) and the United States (1.12) changed little.

Cybercrime coverage is negative in tone everywhere, but the gap with each country's own news differs. It is widest in China (89.8% negative against 27.2% for Chinese news overall, a gap of 62.6 percentage points), Canada (89.6% against 27.1%, 62.5 points), the United Arab Emirates (82.4% against 24.6%, 57.8 points) and Thailand (92.6% against 35.8%, 56.8 points). It is narrowest in Russia (92.3% against 72.1%, 20.2 points) and North Korea (97.1% against 76.1%, 21 points), where news overall is already mostly negative. Singapore has the least negative cybercrime coverage (66.2%), and Ghana the next least (70.3%).

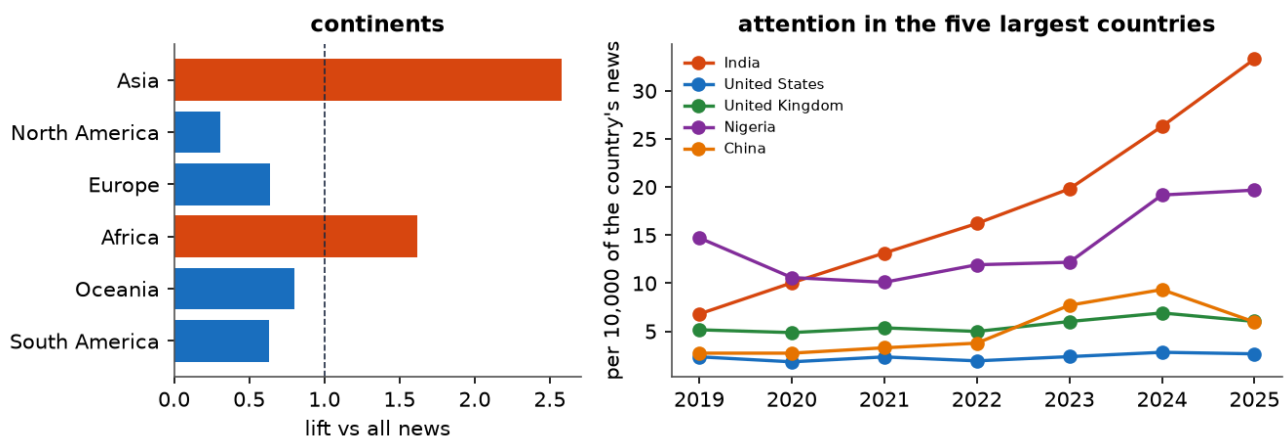


Figure 7. Left: lift by continent, January 2023 – July 2026. Right: cybercrime articles per 10,000 of each country's located news, 2019–2025, for the five countries with the most articles.

3.4 Tone, urgency and themes

Cybercrime coverage is more negative and more urgent than news in general (Figure 8). Among articles with a tone label, 81.4% are negative, against 33.6% across the index (2.42 times). The machine-assigned editorial priority rating puts 86.2% of cybercrime articles at critical level (7 or higher), against 42.6% of all news (2.02 times).

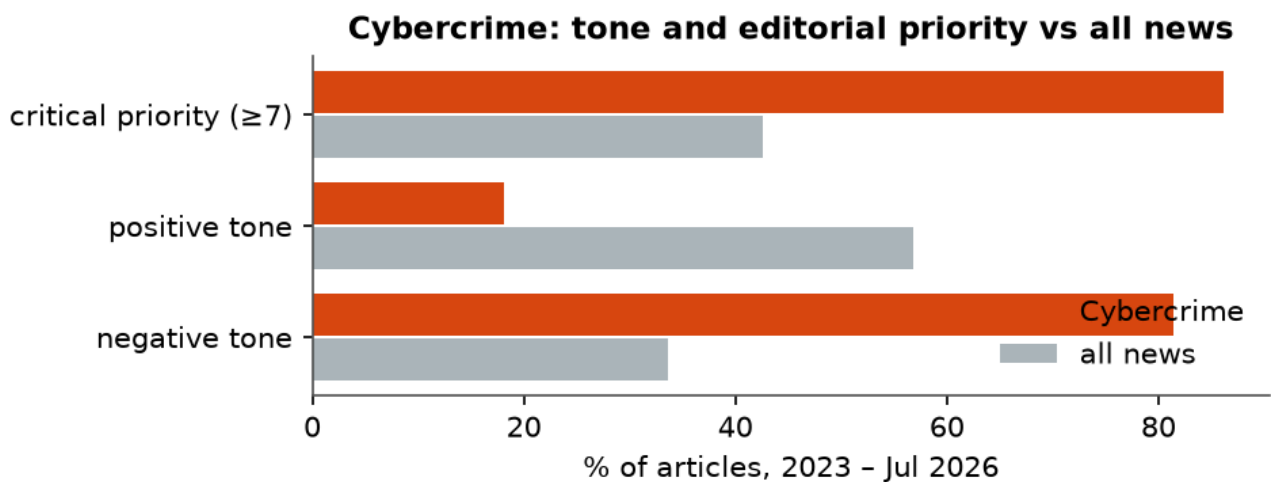


Figure 8. Tone and the share rated critical priority, cybercrime articles vs all news, 2023 – Jul 2026.

Themes show how the stories are framed (Table 4). Cybercrime law and digital forensics is the most common theme (53.19% of themed articles). Theme labels are machine-assigned, so this indicates framing around law and investigation rather than measuring it. Guides to phishing, fake websites and phone scams are smaller but highly specific to the topic. Human trafficking appears in 4.24% of themed articles, 26.86 times its rate in all news. This is consistent with reporting on scam compounds that hold trafficked workers, though the labels do not show why.

Theme	Articles	Share %	Lift
public safety technology and surveillance	8,682	21.54	379.88
social engineering tactics	1,009	2.5	345.22
phishing attack techniques	1,435	3.56	317.56
education on recognizing fake websites and apps	537	1.33	248.34
cybercrime laws and digital forensics	21,438	53.19	246.14
email and phone scam detection guides	1,301	3.23	234.19
phishing scam prevention guides	2,014	5.0	223.93
ransomware attack vectors	1,050	2.61	154.1
human trafficking prevention and prosecution	1,709	4.24	26.86

Table 4. Themes most specific to cybercrime coverage (lift against all themed news), January 2023 – July 2026, with human trafficking added.

The most frequent "organisation" label is SIM (2,675 articles), which is the SIM card used to open mule accounts and make scam calls, not an organisation. Technology platforms follow: Google (1,882), Microsoft (1,749) and Instagram (1,009). The leading enforcement body named is Europol (561), and the leading security vendor is Kaspersky Lab (642). The list reflects how stories are sourced more than who acts.

3.5 Research attention and invention

Research on cybercrime grew much faster than the scientific literature. Papers with a cybercrime or online-fraud term in the title rose from 0.36 per 10,000 papers in 2015 to 1.46 in 2025, a 4.06-fold rise in share, while the total literature in the corpus grew by a factor of 1.0 over the same years. Between 2015 and 2025, 5,195 such papers were published, and 6,438 since 2000. The most-cited work applies criminological theory to cybercrime [1, 3], studies its victims [4, 5] and tracks the rise of fraud during the COVID-19 pandemic [7, 8].

News and research attention rose together (Figure 9). From 2019 to 2025, the research share rose 2.7 times and the news share 2.15 times. Both rose in every year.

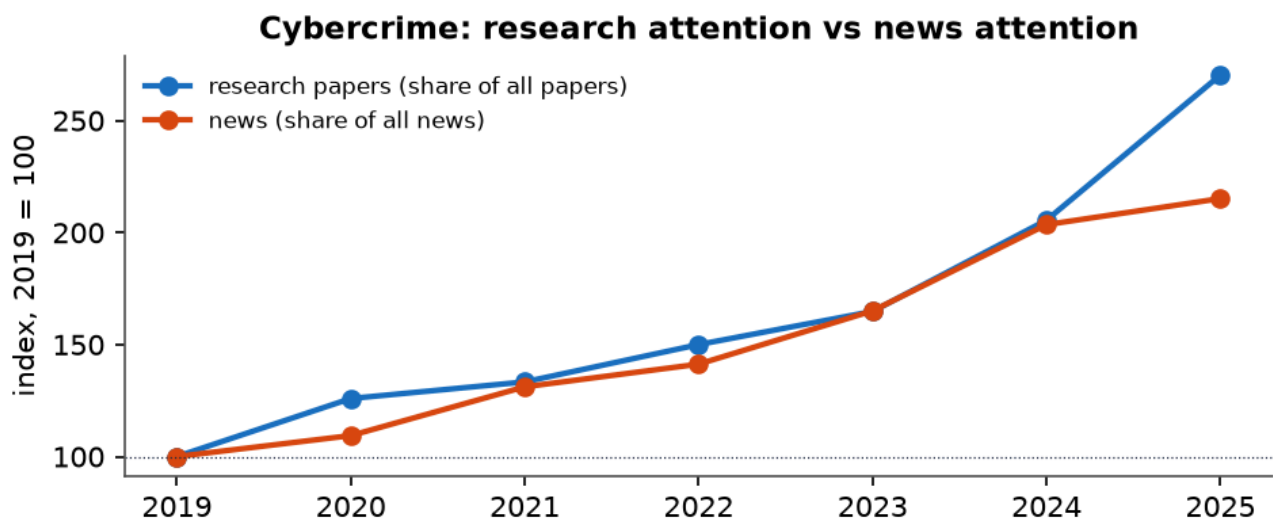


Figure 9. Research papers with cybercrime terms in the title (share of all papers) and cybercrime news (share of all news), each indexed to 2019 = 100.

Patent titles rarely name the crime. Only 47 patent families published from 2015 to 2024 used cybercrime, cyber fraud, online fraud or online scam in the title, too few for a figure. The United States office holds 35.9% of office filings, China 15.4% and the European office 10.3%. The leading technology class is data processing for commerce and finance (G06Q, 11

families). Inventions against fraud are usually titled by technique, such as authentication or anomaly detection, so this count is a floor.

4. Discussion

Three points matter for anyone who uses news as a record of cybercrime. First, coverage measures attention. The steady rise from 2019 to 2025 shows a topic that gained a larger share of the news each year, with no fall in 2020. It does not show how many offences took place. Second, raw shares mislead in both directions. India dominates located coverage. Part of this may be vocabulary: Indian reports often name the "cyber crime" police unit in the opening, which this match counts. The United States is under-represented relative to its weight in the index. Third, geography is changing. Cambodia, North Korea, Myanmar and Thailand are the most over-represented countries, and among countries with at least 100 cybercrime articles in 2025, attention in Pakistan, Ghana and Thailand rose fastest from 2023 to 2025. Within India, the leading states (Telangana, Haryana, Jharkhand) rest on real places; US state tags still carry word artefacts and are not ranked.

Research and news moved together over the period. Patents do not follow, because inventors describe technique rather than crime. The dataset lets researchers link news to other records, for example to compare state-level coverage in India with registered case counts, or to test whether coverage of a scam type is followed by research on it.

5. Limitations

- **Index availability.** 92.88% of the index was readable at build time, so counts are lower bounds. Shares and lifts are less affected if the missing part is spread evenly across topics.
- **Coverage after May 2026.** The index thins after May 2026, so 2026 (January-July) is partial and is excluded from year comparisons.
- **Matching.** Matching uses the article opening and the press's own words. Articles on ransomware, hacking or phishing that never use a cybercrime term are missed, and 10% of matches are not about cybercrime.
- **Vocabulary differs by country.** Indian reporting may use "cyber crime" and "cyber fraud" more than other varieties of English, which would raise India's share and lift.
- **Machine labels.** Location, tone, priority and themes are machine-labelled. Place tags derived from ordinary words were treated as unlocated (15.3% of city-tagged articles), so location shares rest on the remaining tags. The city field is still noisy and is not analysed, and some US state tags rest on surnames or brand names read as towns.
- **Outlet mix.** The index over-represents English-language outlets and has many Indian sources. US state counts are small.
- **Research and patent counts.** These match titles only. Patent counts are very small and measure naming practice more than invention.

Data availability

The dataset (article sample, monthly and country tables, research and patent tables, all metrics) is released under CC BY-NC 4.0 with this paper. The sample holds 24,600 of 97,889 matched articles to 31 July 2026. Full article text, headlines, publishers, later articles and other topics are served by the Prism News API: <https://github.com/fliarbi/prism-news-api>

(base URL <https://radar-api.fliarbi.com/news>). A worked query: prism-news trends "cybercrime" --since 2019-01-01 --until 2026-07-31 --granularity monthly.

References

1. Rutger Leukfeldt et al. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*. <https://doi.org/10.1080/01639625.2015.1012409>
2. Mohammed Ali Al-Garadi et al. (2016). Cybercrime detection in online communications: The experimental case of cyberbullying detection in the Twitter network. *Computers in Human Behavior*. <https://doi.org/10.1016/j.chb.2016.05.051>
3. Thomas J. Holt et al. (2013). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*. <https://doi.org/10.1080/01639625.2013.822209>
4. Monica T. Whitty et al. (2012). The Online Romance Scam: A Serious Cybercrime. *Cyberpsychology Behavior and Social Networking*. <https://doi.org/10.1089/cyber.2011.0352>
5. Mark Button et al. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian & New Zealand Journal of Criminology*. <https://doi.org/10.1177/0004865814521224>
6. Nir Kshetri (2019). Cybercrime and Cybersecurity in Africa. *Journal of Global Information Technology Management*. <https://doi.org/10.1080/1097198x.2019.1603527>
7. Rennie Naidoo (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*. <https://doi.org/10.1080/0960085x.2020.1771222>
8. Steven Kemp et al. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice*. <https://doi.org/10.1177/10439862211027986>
9. Fliar BI (2026). *Cybercrime in the News 2019-2026: article-level dataset and coverage tables*. Prism News API. <https://github.com/fliarbi/prism-news-api>