TLP:CLEAR



Treadstone 71 LLC
Cyber and Strategic Intelligence

Counting the Adversary's Press Releases

A Treadstone 71 peer review of the ENISA Threat Landscape 2026 under the ASA Evidence Standard and the Treadstone 71 Advanced SATs

SEPTEMBER 2026

About Treadstone 71

Treadstone 71 is a veteran-owned cyber and strategic intelligence training and consulting firm, operating since 2002. The firm delivers adversary intelligence, cyber counterintelligence, cognitive warfare analysis, and structured analytic training to government and corporate clients. Its published methods include the ASA Evidence Standard and the Treadstone 71 Adversary Index. More information about Treadstone 71 and its work is available at treadstone71.com.

CONTACT

To contact Treadstone 71, use the contact channels published at treadstone71.com.

AUTHORS

Treadstone 71

SUBJECT PUBLICATION

ENISA Threat Landscape 2026, European Union Agency for Cybersecurity, September 2026. ISBN 978-92-9204-807-5, DOI 10.2824/0806036. Reporting period 1 January to 31 December 2025.

LEGAL NOTICE

The present publication represents the views and assessments of Treadstone 71 LLC. Treadstone 71 is an independent firm with no affiliation to, endorsement from, or mandate from the European Union Agency for Cybersecurity (ENISA) or any other EU body. Treadstone 71 has the right to alter, update, or remove the publication or any of its contents. It is intended for information purposes only.

Third-party sources are cited as appropriate. Treadstone 71 is not responsible or liable for the content of external sources, including external websites referenced in the publication.

COPYRIGHT NOTICE

© Treadstone 71 LLC, 2026. All rights reserved. Quotation of short excerpts with attribution to Treadstone 71 is permitted.

Figures drawn from the ENISA Threat Landscape 2026 are reused under the Creative Commons Attribution 4.0 International licence (CC BY 4.0) that ENISA applies to that publication. Treadstone 71 recomputed and re-presented those figures; every change is Treadstone 71's. Cover imagery and charts © Treadstone 71.

DISCLAIMER

All references and external resources cited here were accessible on 23 September 2026. Treadstone 71 bears no responsibility for later changes to, relocation of, or removal of content hosted by third parties. References to adversary channels and leak sites appear for evidentiary purposes only; such resources are volatile and disappear through operator deletion, infrastructure suspension, or law-enforcement action.

Estimative judgments follow the Sherman Kent spectrum with half-open intervals. Evidence grades follow STANAG 2511, expanded by the ASA Evidence Standard, with source reliability and information credibility graded on separate axes. Each judgment carries its probability band and its evidence grade.

Table of Contents

Executive Summary 6
TL;DR 6
BLUF 6
Who 6
What 6
So What 7
Why Now 7
Impacts So Far 7
Outlook and Strategic Foresight 7

Methodology 9
Source Reliability (STANAG 2511) 9
Information Credibility (STANAG 2511) 9
Probability Language 10
Treadstone 71 Advanced SATs Applied 10

1. Findings 12
Finding 1. The dataset certifies adversary claims 12
Finding 2. Percentages built on slivers 12
Finding 3. The estimative scale is broken 13
Finding 4. Errors and self-contradiction 13
Finding 5. Source dependence 15
Finding 6. Political punches pulled 15

2. Advanced SATs Analysis 17
2.1 Technique Selection 17
2.2 Decompositional Uncertainty Mapping (DUM) 17
2.3 Minimal Viable Hypothesis Testing (MVHT) 18
2.4 Dynamic Bayesian Narrative Analysis (DBNA) 19
2.5 Hypothesis Evolution Tracking (HET) 20
2.6 Narrative Convergence Analysis (NCA) 21
2.7 Perception Discrepancy Analysis (PDA) 21
2.8 Perspective Distortion Analysis (PDA-2) 22
2.9 Cognitive Dissonance Mapping (CDM) 22
2.10 Causal Density Mapping (CDM-2) 23
2.11 Counterintelligence Deception Diagnostics (CIDD) 23
2.12 Cyber Adversary Reflex Mapping (CARM) 24
2.13 Adaptive Threat Calibration and Risk Indexing (ATCRI) 25
2.14 Domain Screening 25

3. Gaps and Remedies 27
3.1 Method gaps 27
3.2 Analytic gaps 27
3.3 Coverage gaps 29
3.4 Delivery gaps 30

4. So What: Who Cares 31
4.1 Crosswalk: Failure to Remedy 31

5. Where Treadstone 71 Does Not Solve the Problem 31

6. Evidence Grading 33
6.1 The report's core claims 33
6.2 External evidence used in the review 33
6.3 Treadstone 71 estimative judgments 34
6.4 Sources Consulted 34

7. Outlook and Conclusion 36
7.1 Fix Order for ETL 2027 36
7.2 Conclusion 36

Executive Summary

TL;DR

ENISA counted the adversary's press releases, then ranked Europe's threats by them. Its headline numbers rest on unverified hacktivist claims. Vector statistics rest on slivers of the data, and the probability scale fuses confidence with likelihood. Narrative reporting on state actors holds up. The quantitative spine fails peer review.

BLUF

Of 8,257 entries in the ENISA dataset, 4,709 are hacktivist claims, and about 89 percent of those are DDoS claims. ENISA's own validation work found only 23.8 percent of NoName057(16) claims confirmed by independent availability checks. Public administration tops the sector table at 31.8 percent because 81.8 percent of its entries are those same DDoS claims. The ranking measures mostly propaganda volume. Treadstone 71 assesses as **highly likely (85 to <95 percent)** that the sector and objective rankings reflect claim visibility more than compromise risk. Municipalities still carry a real ransomware load the headline hides.

The report also contradicts ENISA's own September 2025 statement on the Collins Aerospace incident, prints one of two competing attributions of the December 2025 Polish energy attack as settled, and omits the USD 1.5 billion Bybit theft attributed to DPRK.[1] Treadstone 71 practice closes most of the gaps identified here. Three limits sit outside any private firm's reach, and Section 5 states them plainly.

The Treadstone 71 Advanced SATs confirm the findings and discipline them. Minimal Viable Hypothesis Testing explains 94 percent of observations about the sector ranking only after adding a real municipal ransomware load to claim volume. Dynamic Bayesian Narrative Analysis holds the core judgment at highly likely, one band below where Treadstone 71 first set it. Hypothesis Evolution Tracking shows ENISA froze the Polish attribution at a near-even point. Adaptive Threat Calibration and Risk Indexing ranks hacktivist DDoS last of eight EU threat categories; ENISA's volume table ranks it first.

Who

Authors. The European Union Agency for Cybersecurity (ENISA), with acknowledged contributions from EEAS STRATCOM, Europol, Auto-ISAC, Aviation ISAC, and the European TLD ISAC. Its FIMI chapter reproduces the EEAS 4th report on Foreign Information Manipulation and Interference (March 2026).

Consumers. NIS2 competent authorities and national CSIRTs; boards, CISOs, and risk officers of essential and important entities; European Commission policy teams working the Cybersecurity Act revision; cyber insurers and underwriters; security vendors who cite ETL figures in sales material; journalists who repeat the headline percentages.

What

ENISA Threat Landscape 2026: 101 pages, 656 footnotes, published September 2026 (document creation date 22 September 2026), covering incidents from 1 January to 31 December 2025. The dataset holds 8,257 entries drawn mainly from open sources, with anonymised input from member states and the ENISA Cyber Partnership Programme. Chapters run from overview and sector analysis through cybercrime, state-nexus activity, FIMI, hacktivism, vulnerabilities, and an outlook.

[1] FBI Internet Crime Complaint Center, Alert I-022625-PSA, North Korea Responsible for $1.5 Billion Bybit Hack, 26 February 2025: https://www.ic3.gov/PSA/2025/PSA250226

So What

The ETL sets the reference baseline for EU cyber risk through 2027. NIS2 supervisors cite it. Boards read the sector table and set budgets from it. Policy teams anchor legislation on it. A baseline built on attacker claims pushes money toward DDoS scrubbing for public administration while ransomware, identity abuse, and supplier compromise carry the actual losses. Worse, the report hands NoName057(16) and its allies what their campaigns seek most: official certification of impact they failed to achieve on their own.

Why Now

Q4 is budget season for 2027. The Cybersecurity Act revision is in motion. NIS2 supervision cycles are maturing across member states. The ETL will be cited for twelve months, and errors in the first week of circulation harden into accepted fact by the first quarter.

Impacts So Far

One day after publication, impacts remain prospective. The headline percentages are the portable part of the report, and portable numbers travel first. Treadstone 71 assesses as **likely (55 to <85 percent)** that the sector ranking and the 60.4 percent exploitation figure appear in vendor marketing and national briefings within 30 days, stripped of the denominators that qualify them.

Outlook and Strategic Foresight

Three trajectories for ETL 2027, with signposts:

Scenario	Probability	Signposts
Status quo: claims counted as incidents, n values unpublished	Likely (55 to <85)	Unchanged CTL methodology text on claim handling; identical table structure in interim ENISA products
Partial reform: verified incidents separated from claims in main tables	Unlikely (15 to <45)	Methodology revision naming a claim-verification rule; publication of sample sizes beside percentages
Full reform: NIS2 mandatory reporting moves to the analytic center	Highly unlikely (5 to <15)	Root-cause "unknown" share in NIS2 events falls well below half; complete transposition across all 27 member states

Adversary side: pro-Russia hacktivist fronts cite EU agency figures to validate their campaigns. Treadstone 71 assesses a **roughly even chance (45 to <55 percent)** that NoName057(16) or an allied channel quotes ETL 2026 statistics in its own messaging within twelve months. Watch the group's Telegram output for ENISA or ETL references.

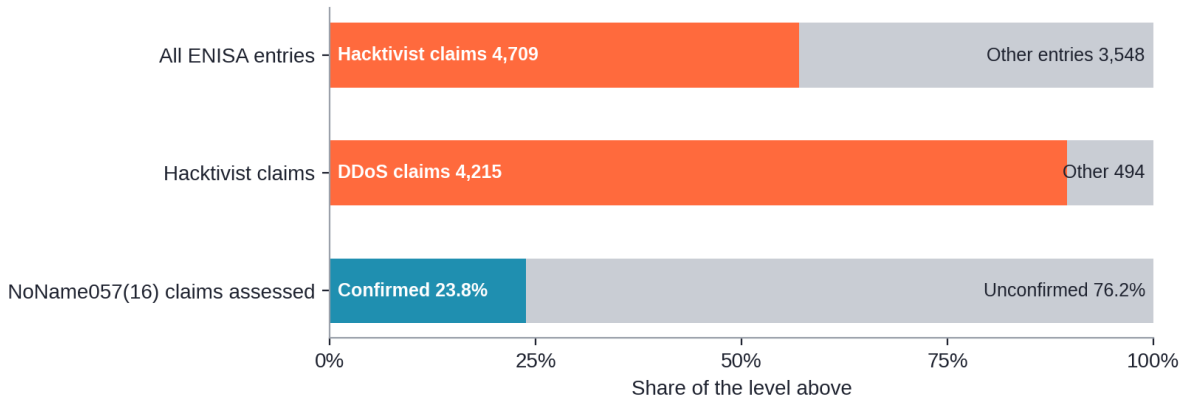

Figure 1 - What the 8,257 ENISA entries are: attacker claims, and the share ENISA itself confirmed

Methodology

Treadstone 71 reviewed the full text of the report,[2] recomputed its percentages against the stated totals, tallied its citation base by domain, and tested selected factual claims against primary sources. Evidence grading follows the ASA Evidence Standard (Public Edition 1.0, DOI 10.5281/zenodo.22662242).[3] The ASA Standard expands the classic Admiralty grid into 30 factors across 9 clusters and a T/D/F tri-score. Its classic grid serves as the entry anchor, and the grades here sit at that anchor.

Two rules govern every grade. Source reliability and information credibility are judged on separate axes and never averaged. A reliable source sometimes carries doubtful information, and an unknown source sometimes carries confirmed information. Verified facts and adversary claims never share a sentence without a marker that separates them.

Source Reliability (STANAG 2511)

Grade	Rating	Definition
A	Completely reliable	No doubt of authenticity, trustworthiness, or competency; has a history of complete reliability.
B	Usually reliable	Minor doubt about authenticity, trustworthiness, or competency; has a history of valid information most of the time.
C	Fairly reliable	Doubt of authenticity, trustworthiness, or competency, but has provided valid information in the past.
D	Not usually reliable	Significant doubt about authenticity, trustworthiness, or competency, but has provided valid information in the past.
E	Unreliable	Lacking in authenticity, trustworthiness, and competency; history of invalid information.
F	Reliability cannot be judged	No basis exists for evaluating the reliability of the source.

Information Credibility (STANAG 2511)

Grade	Rating	Definition
1	Confirmed by other sources	Confirmed by other independent sources; logical in itself; consistent with other information on the subject.
2	Probably true	Not confirmed; logical in itself; consistent with other information on the subject.
3	Possibly true	Not confirmed; reasonably logical in itself; agrees with some other information on the subject.
4	Doubtful	Not confirmed; possible but not logical; no other information on the subject.
5	Improbable	Not confirmed; not logical in itself; contradicted by other information on the subject.
6	Truth cannot be judged	No basis exists for evaluating the validity of the information.

Probability Language

Estimative language follows the Sherman Kent spectrum with half-open intervals. Bands do not overlap, and every forecast here carries a time bound or states the absence of one.

[2] ENISA, ENISA Threat Landscape 2026, September 2026, ISBN 978-92-9204-807-5, https://doi.org/10.2824/0806036
[3] Treadstone 71, ASA Evidence Standard, Public Edition 1.0, https://doi.org/10.5281/zenodo.22662242

Band	Probability range (percent)
Almost certain	95 to 99
Highly likely	85 to <95
Likely	55 to <85
Roughly even chance	45 to <55
Unlikely	15 to <45
Highly unlikely	5 to <15
Almost no chance	1 to <5

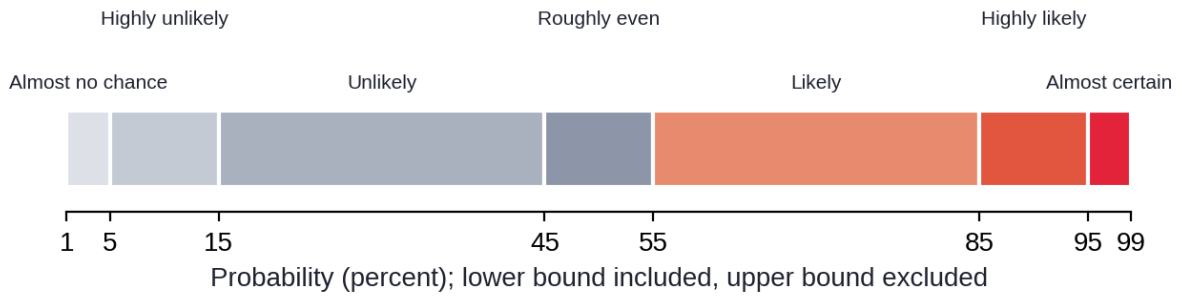

Figure 2 - The Sherman Kent spectrum with half-open intervals, as applied throughout the review

Treadstone 71 Advanced SATs Applied

The review rests on the Treadstone 71 Advanced SATs corpus. Twelve techniques ran in full; Chapter 2 carries each matrix and its result.

- **Decompositional Uncertainty Mapping (DUM).** The verified material in the ETL is counts; its headline judgments rest on partly known or unknown ground (Section 2.2).
- **Minimal Viable Hypothesis Testing (MVHT).** Claim volume alone fails the 80 percent test at 75; adding the municipal ransomware load lifts the fit to 94 (Section 2.3).
- **Dynamic Bayesian Narrative Analysis (DBNA).** Claim visibility, not compromise risk, drives the ranking at a posterior near 0.92 (Section 2.4).
- **Hypothesis Evolution Tracking (HET).** The Polish attribution was a live contest when ENISA printed it as settled (Section 2.5).
- **Narrative Convergence Analysis (NCA).** The Collins table converged on the Everest narrative and diverged from ENISA's own 2025 statement (Section 2.6).
- **Perception Discrepancy Analysis (PDA) and Perspective Distortion Analysis (PDA-2).** Four of six perception gaps favor an adversary; the institutions distort without coordination (Sections 2.7 and 2.8).
- **Cognitive Dissonance Mapping (CDM).** Seven contradictions between ENISA's stated method and its practice (Section 2.9).
- **Causal Density Mapping (CDM-2).** Victim refusal to pay and leak-site collection gate the ransomware country ranking (Section 2.10).
- **Counterintelligence Deception Diagnostics (CIDD) and Cyber Adversary Reflex Mapping (CARM).** Per-claimant exclusion rules and a reflex forecast for NoName057(16) (Sections 2.11 and 2.12).
- **Adaptive Threat Calibration and Risk Indexing (ATCRI).** Hacktivist DDoS finishes eighth of eight by consequence (Section 2.13).

- **STEMPLES Plus driver sweep** to surface the money, law, and technology drivers the report omits (Gap 8).

1. Findings

Finding 1. The dataset certifies adversary claims

The arithmetic tells the story.

DDoS equals 51.3 percent of 8,257 entries, roughly 4,236. Hacktivist DDoS claims equal roughly 4,215 (89.5 percent of 4,709). About 99 percent of the report's largest category is self-reported by the attacker. ENISA states in Chapter 6 that the gap between claims and verified disruption suggests some claims served an influence objective.

The Executive Summary, the sector chapter, and the Outlook then build on those claims anyway.

That is circular reporting under a government seal.

NoName057(16) needs an audience to convert DDoS traffic into perceived instability. ENISA supplied the audience. The pattern repeats with operational technology: 124 Q4 OT claims entered the count, and in most cases the claims named no victim and no TTP.

Fallacies present. Availability heuristic: visible equals significant. Equivocation: incident, event, and claim used interchangeably across chapters. McNamara fallacy: count what is countable, then treat the count as the threat.

MVHT sets the limit of the charge. Claim volume explains 75 percent of what the report shows about the sector; a real ransomware and supplier load on municipalities, including the attack on a Swedish IT supplier serving about 200 municipalities, explains most of the rest.[4]

> **Treadstone 71 remedy.** The ASA Evidence Standard enters every self-published adversary claim as an adversary claim, never as a verified event, and caps its credibility grade until independent confirmation arrives. Counterintelligence Deception Diagnostics grades each claimant before its output touches a count, and ENISA's own 23.8 percent validation rate is exactly the discrepancy history CIDD consumes. The Cognitive Warfare Monitor treats hacktivist claims as influence activity to be measured for effect, not as intrusions to be tallied.

Finding 2. Percentages built on slivers

The Executive Summary states that 60.4 percent of unauthorised access used vulnerability exploitation, with no caveat. Chapter 1 reveals that ENISA identified an intrusion vector in only 5.2 percent of unauthorised-access cases. Unauthorised access totals about 3,262 entries; 5.2 percent is about 170; 60.4 percent of 170 is about 103. The state-nexus figure follows the same pattern: vector known in 20 percent of roughly 500 cases, so the 70 percent exploitation share rests on about 70 incidents. Decimal precision on small, self-selected samples is false precision. Base-rate neglect follows when readers generalize 103 cases to 3,262.

[4] Swedish Authority for Privacy Protection (IMY) decision on Miljödata, 2.2 million people affected, as reported by BleepingComputer: https://www.bleepingcomputer.com/news/security/sweden-fines-milj-data-183-000-over-breach-affecting-22-million/

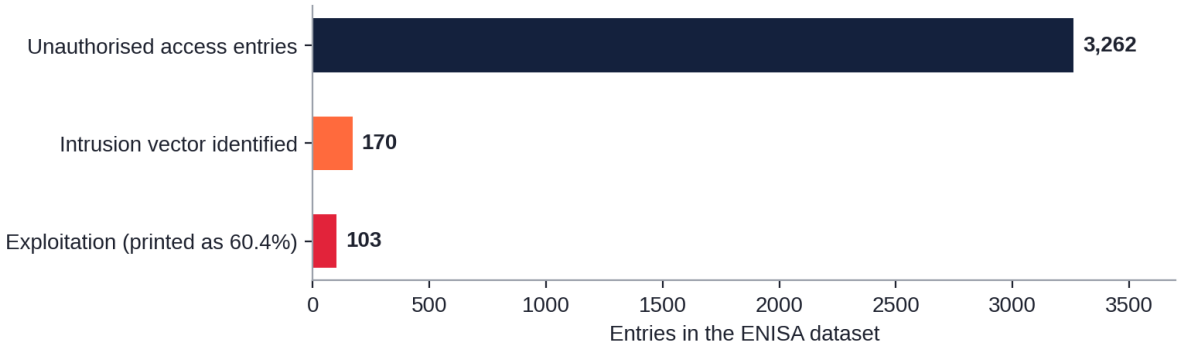

Figure 3 - The denominator behind the 60.4 percent exploitation share

The MITRE technique count carries the same flaw. Exfiltration over C2 (T1041) at 73.3 percent against encryption for impact (T1486) at 13.7 percent, in ENISA's words, is likely to confirm a shift to extortion. Vendor write-ups describe novel behavior and skip routine encryption. Frequency in reporting differs from frequency in operations. T1486 also appears twice in the TTP table.

> **Treadstone 71 remedy.** Every Treadstone 71 percentage carries its n. The ASA Standard requires disclosure of the sample behind any rate, and Decompositional Uncertainty Mapping, taught in the Treadstone 71 Advanced SATs curriculum, tiers every figure as known, partly known, or unknown before it reaches the BLUF.

Finding 3. The estimative scale is broken

Appendix B fuses two separate axes into one table: "High confidence, >90%, HIGHLY LIKELY." Confidence describes the quality of the evidence behind a judgment. Likelihood describes the event. Fusing them makes a well-sourced 60 percent judgment and a thin 60 percent judgment read identically. Bands overlap at 60 and at 90. The top band stops at highly likely with no almost certain. PLAUSIBLE covers 10 to 40 percent, a word most readers take as closer to even odds.

Across 101 pages, the word confidence appears in analytic use twice. Each instance is borrowed from third-party vendors. ENISA never states its own confidence in any of its own judgments. Forecasts carry no time bounds, as in the statement that AI will highly likely increasingly support malicious operations. Several forecasts are unfalsifiable: hacktivist DDoS will persist as a nuisance.

Under the ASA Standard, an assessment without a confidence marker is a draft.

> **Treadstone 71 remedy.** Every product from the firm uses the Kent spectrum with half-open intervals, grade source reliability and information credibility on separate axes, and attach a time bound to every forecast. The full method sits in a public white paper with a DOI, so any reader audits the scale instead of taking it on trust.

Finding 4. Errors and self-contradiction

Collins Aerospace

The cybercrime table attributes the September 2025 Collins Aerospace disruption to the Everest group through FTP access to vMUSE. Yet the report's own transport chapter calls it a ransomware incident. ENISA publicly confirmed ransomware on 22 September 2025, consistent with the ransomware disclosure in the RTX filing with the US Securities and Exchange Commission.[5] Hudson Rock's analysis (graded B2) separates two events in the same week: a ransomware attack that forced the MUSE shutdown, and a distinct Everest data-theft claim built on credentials harvested by an infostealer in 2022.[6] The table merges them, then reports airport shutdowns across Europe. Heathrow, Brussels, Berlin, and Dublin moved to

[5] BlackFog, Collins Aerospace ransomware timeline, including ENISA confirmation of ransomware on 22 September 2025: https://www.blackfog.com/ransomware-on-collins-aerospace/
[6] Hudson Rock, Collins Aerospace Hit Twice: 2022 Infostealer Infection Enabled a Separate Breach, 23 October 2025: https://www.infostealers.com/article/collins-aerospace-hit-twice-2022-infostealer-infection-enabled-a-separate-breach/

manual check-in and boarding; none closed. The ransomware family itself remains contested: HardBit rests on one researcher's post, and other reporting points to Loki.[7] Treadstone 71 assesses as **highly likely (85 to <95 percent)** that the table conflated two incidents.

The Polish energy attack

The coordinated destructive attack of 29 December 2025 is the most consequential state operation against EU infrastructure in the reporting period.

ENISA gives it one sentence and omits Poland's name. Its DragonFly label is accurate as far as it goes: CERT Polska linked the attack infrastructure to the cluster tracked as Static Tundra, Berserk Bear, Ghost Blizzard, and Dragonfly.[8] The failure is omission. ESET attributed the operation to Sandworm with medium confidence, and Dragos assessed a moderate-confidence overlap with Sandworm through its ELECTRUM designation.[9][10] Neither assessment appears. CERT Polska itself described the code overlap with Sandworm as general and stated it was unable to determine conclusively whether the Sandworm cluster took part. Vendor reporting, not CERT Polska, ties the Static Tundra cluster to FSB Center 16; Sandworm belongs to the GRU. The omitted view changes which Russian service answers for the attack, and FSB versus GRU decides deterrence signaling and sanctions targeting.

The scale vanished as well: more than 30 wind and photovoltaic sites, a manufacturing firm, and a combined heat and power plant serving close to half a million customers, with RTUs damaged and HMI data destroyed. CERT Polska's August 2026 follow-up, published before the ETL went to print, added a second heat and power plant serving 50,000 residents. There the attacker entered through a private APN and shut down a steam turbine and the water-treatment system.[11] CERT Polska called the campaign the first attack on Poland's energy sector with a purely destructive objective. Customers lost neither heat nor power.

Treadstone 71 Hypothesis Evolution Tracking result: Russian state responsibility, **almost certain (95 to 99 percent)**. Specific unit on public evidence, **roughly even chance (45 to <55 percent)** between the FSB-linked and GRU-linked hypotheses, with a shared-access or handoff hypothesis not yet excluded. The matrix shows ENISA printed one side of a contest that shifted with each technical release of early 2026 as if the contest had closed.

Quality-control defects

- Executive Summary and body disagree: cyberespionage 5.9 versus 6.3 percent; financially motivated 29.3 versus 29.2; essential entities 72.9 percent versus essential and important entities 73 percent, two different populations; business services 8.5 versus 8.45.
- CVE-2025-30333 in the text does not match the Cisco firewall pair; Table 1 correctly lists CVE-2025-20333.
- CVE-2025-53770 maps to EUVD-2025-21981 in the text and EUVD-2025-23309 in Table 1.
- "Word Leaks" appears for World Leaks. Calisto and Callisto appear interchangeably for the same intrusion set.
- Figure numbers are corrupted throughout: 2928, 290, 3830, 4031, 322, 336, 347, 4935, 5136, 375. Two figures carry the number 7.

[7] Infosecurity Magazine, UK National Crime Agency arrest and the HardBit claim: https://www.infosecurity-magazine.com/news/nca-arrest-hardbit-ransomware/ ; SecurityWeek: https://www.securityweek.com/european-airport-cyberattack-linked-to-obscure-ransomware-suspect-arrested/ . BleepingComputer reported sources pointing to Loki.

[8] CERT Polska, Energy Sector Incident Report, 29 December 2025 (January 2026): https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/

[9] ESET Research, Sandworm behind cyberattack on Poland's power grid in late 2025, 23 January 2026: https://www.welivesecurity.com/en/eset-research/eset-research-sandworm-cyberattack-poland-power-grid-late-2025/

[10] The Hacker News, reporting the CERT Polska, ESET, and Dragos positions, January 2026: https://thehackernews.com/2026/01/poland-attributes-december-cyber.html

[11] CERT Polska, Follow-Up Report of the December 2025 Energy Sector Incident, August 2026: https://cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/

- The report states that CWE-78, CWE-22, and CWE-502 allow memory modification. Path traversal reads and writes files; it does not modify memory.
- The disclaimer says AI supported collection and processing, then says no AI-generated content was used. Model, validation method, and error rate go undisclosed in a report whose data quality is the central question.

> **Treadstone 71 remedy.** Hypothesis Evolution Tracking, Narrative Convergence Analysis, and Cognitive Dissonance Mapping run before publication. Each competing attribution carries its own probability band, and every earlier agency statement gets checked against the new text. Treadstone 71 analytic writing standards require a second-reader check of every number against its source table before release.

Finding 5. Source dependence

The report carries about 598 URL citations across 265 domains. Roughly two thirds point to vendor and other non-government sites, about one fifth to government or EU bodies, and the remainder to media and social platforms. Microsoft and Google Cloud together draw 48 citations, more than Europol and ENISA combined at 28. Vendor taxonomies flow into the report without deconfliction. ENISA admits it does not know whether Storm-2372 and UTA0307 are the same actor. Vendor commercial incentives, telemetry skewed toward each vendor's customer base, and naming competition go unexamined.

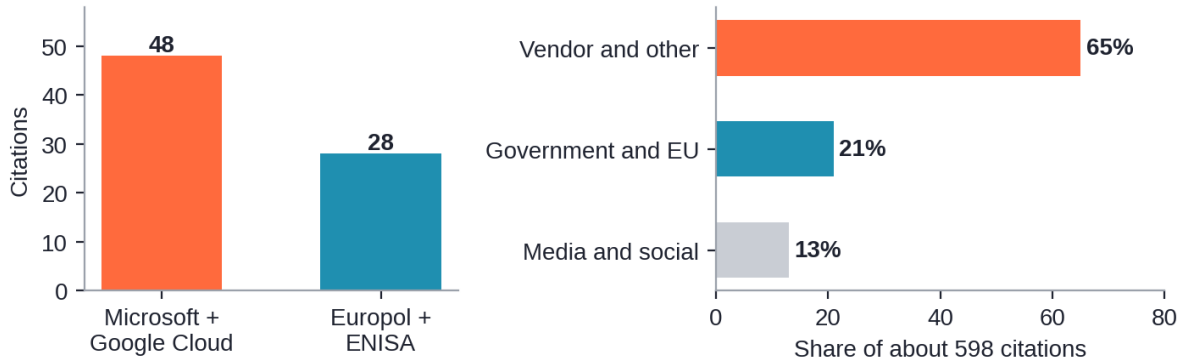

Figure 4 - Where the ETL 2026 citations point

The result is an appeal to authority at scale, and a picture of Europe drawn largely through American corporate telemetry.

> **Treadstone 71 remedy.** The ASA Standard grades every source for reliability and collection bias, including vendor sources, before its information enters a judgment. Native-language adversary-side collection supplies a second stream that does not pass through vendor telemetry (Gap 15). Treadstone 71 is also a vendor, and Section 5 addresses what that means.

Finding 6. Political punches pulled

The spyware section names vendors (Paragon, Candiru, Intellexa) and victims. Missing: the EU member-state governments documented as customers. Italy's Paragon case appears through three footnotes without naming the Italian state as operator. An EU agency declines to grade EU governments. The report should either say so or scope the chapter honestly.

The FIMI chapter is lifted from the EEAS report of March 2026, not produced by ENISA analysts. X at 88 percent of observables reflects where EEAS holds collection access, not where manipulation lives. Telegram at 3 percent strains belief for Eastern Europe. Sixty-five percent of the 540 FIMI incidents remain unattributed. Impact is measured in views, never in changed belief or behavior.

> **Treadstone 71 remedy.** The Treadstone 71 Adversary Index grades partner states alongside adversaries: the v2.1 catalog scores the UAE at 50 next to the Tier 0 adversaries. Independence from any government customer lets Treadstone 71 name operators, not only vendors, where evidence supports the call.

2. Advanced SATs Analysis

The Treadstone 71 Advanced SATs corpus holds 33 techniques. Selection followed one test: does the technique answer a question the ENISA report raises? Twelve passed and ran in full; their matrices follow. Fourteen ran as screens for gaps. Seven had no purchase on the material: ACLS, AABDA, AARD, AGCP, CIS, CWC, and HTIM, each built for operational countermeasures or collection the ETL does not attempt.

2.1 Technique Selection

Technique	Question it answers here
Decompositional Uncertainty Mapping (DUM)	Which ETL claims are known, partly known, or unknown?
Minimal Viable Hypothesis Testing (MVHT)	What is the simplest explanation of the sector ranking?
Dynamic Bayesian Narrative Analysis (DBNA)	How probable is each reading of the ranking after the evidence?
Hypothesis Evolution Tracking (HET)	How did the Polish attribution move, and where did ENISA freeze it?
Narrative Convergence Analysis (NCA)	Whose narrative did ENISA adopt on Collins Aerospace?
Perception Discrepancy Analysis (PDA)	Where does claimed impact diverge from verified impact?
Perspective Distortion Analysis (PDA-2)	Which institutional frames bend the report?
Cognitive Dissonance Mapping (CDM)	Where does ENISA contradict its own stated method?
Causal Density Mapping (CDM-2)	What actually produces the ransomware country ranking?
Counterintelligence Deception Diagnostics (CIDD)	How reliable are the adversary claimants ENISA counted?
Cyber Adversary Reflex Mapping (CARM)	How will NoName057(16) react to the ETL itself?
Adaptive Threat Calibration and Risk Indexing (ATCRI)	What should the EU threat priority order be?

2.2 Decompositional Uncertainty Mapping (DUM)

Question. Which of the report's load-bearing claims rest on verified fact, and which do not? DUM separates the report into three tiers, then asks which gaps collection resolves.

ETL claim or data point	Tier	Confidence	Resolvable by
Dataset of 8,257 entries; 4,709 hacktivist claims	Tier 1: Known	High	Stated in report
23.8 percent of assessed NoName057(16) claims validated (July to November subset)	Tier 1: Known	High	Stated in report
1,954 NIS2 events; about half of 941 malicious events with unknown root cause	Tier 1: Known	High	Stated in report
Destructive attack on Polish energy sites, 29 December 2025	Tier 1: Known	High	CERT Polska report
Public administration as most targeted sector	Tier 2: Partly known	Low	ENISA split of verified from claimed entries
60.4 percent exploitation share (n of about 103)	Tier 2: Partly known	Low	ENISA release of vector-known subset
Shift from encryption to exfiltration (T1041 versus T1486)	Tier 2: Partly known	Low	Incident-response telemetry, not vendor write-ups
Unit behind the Polish attack (FSB or GRU cluster)	Tier 2: Partly known	Moderate	Further CERT Polska or allied technical release
True ransomware victimization by country	Tier 3: Unknown	None	Insurer claims data; negotiator data; not public

ETL claim or data point	Tier	Confidence	Resolvable by
AI tools used in ENISA collection and their error rate	Tier 3: Unknown	None	ENISA disclosure only
Behavioral effect of FIMI campaigns on EU audiences	Tier 3: Unknown	None	Baseline polling and panel studies
Accuracy of ETL 2025 forecasts	Tier 3: Unknown	None	ENISA self-grading

Finding. Uncertainty density concentrates exactly where the report places its headlines.

Every Tier 1 item is a count, while each judgment the Executive Summary sells sits in Tier 2 or Tier 3. Five of the eight Tier 2 and Tier 3 gaps are resolvable by ENISA alone, from data it already holds.

> **Collection priority.** First, the verified-versus-claimed split of the 31.8 percent public administration figure. Second, the vector-known subset behind the 60.4 percent. Third, disclosure of AI tooling in collection. Each closes a gap from data ENISA already holds.

2.3 Minimal Viable Hypothesis Testing (MVHT)

Question. Why does public administration top the ETL sector table? MVHT proposes the simplest explanation and accepts it for decision use only if it explains at least 80 percent of observations.

Minimal viable hypothesis, first form. The ranking is driven by hacktivist DDoS claim volume against public-facing government websites.

Observation (from the report)	First form	Amended form
O1. 81.8 percent of public administration entries are DDoS	Explained	Explained
O2. NoName057(16), Dark Storm Team, and Mr Hamza lead the sector's claims	Explained	Explained
O3. Financially motivated activity is 8 percent of the sector's entries	Explained	Explained
O4. ENISA describes impact as largely temporary website disruption	Explained	Explained
O5. 23.8 percent of assessed NoName057(16) claims validated	Explained	Explained
O6. Public administration holds 45.8 percent of all hacktivist entries	Explained	Explained
O7. Ransomware on a Swedish IT supplier hit about 200 municipalities	Not explained	Explained
O8. NIS2 member-state reporting also ranks public administration first	Not explained	Partly explained
Share of observations explained	75 percent	94 percent

The first form fails the 80 percent threshold. O7 is real operational impact, and O8 comes from a separate dataset with different thresholds that still places the sector first. **Amended hypothesis.** Hacktivist DDoS claims against government websites drive most of the ranking, layered on a smaller but real ransomware and supplier-compromise load concentrated on municipalities. NIS2 data is partly explained because NIS2 counts near misses and threats, which public bodies report more often.

> **Consequence.** MVHT supports the direction of Finding 1 and trims the absolute: propaganda volume drives most of the ranking, and municipalities carry a real ransomware exposure the headline hides. Finding 1 and the BLUF carry each point.

2.4 Dynamic Bayesian Narrative Analysis (DBNA)

Question. Three narratives compete to explain the sector ranking. DBNA assigns priors, updates them against the evidence in sequence, and reports posteriors. Evidence items are treated as conditionally independent, a simplification stated here so the reader tests it directly.

Narrative	Prior	After E1	After E2	After E3	After E4
N1. Public administration faces the highest compromise risk in the EU	0.40	0.21	0.10	0.16	0.08
N2. The ranking is an artifact of hacktivist claim volume	0.40	0.62	0.77	0.64	0.76
N3. The ranking reflects reporting and collection bias toward public bodies	0.20	0.17	0.13	0.20	0.16

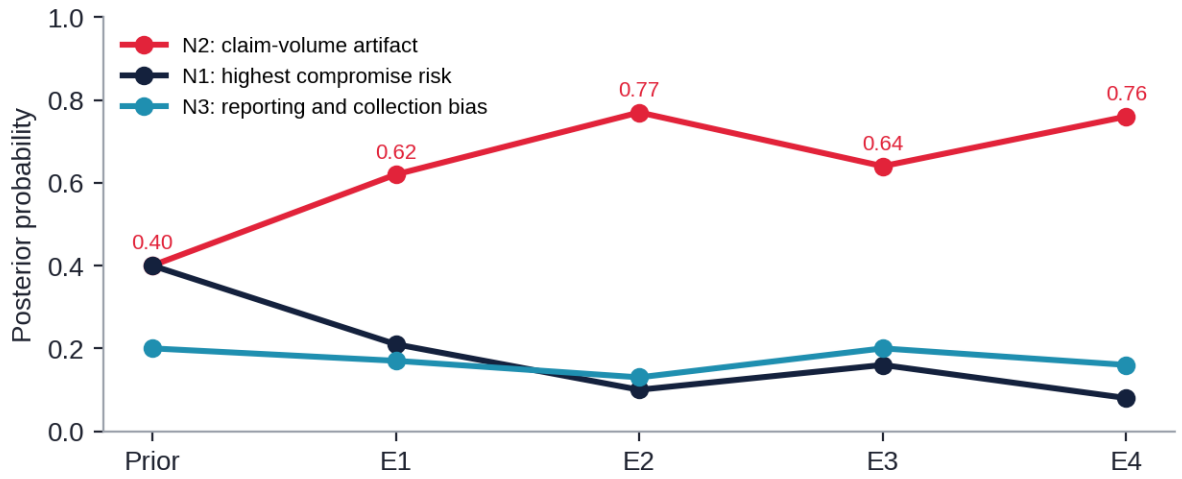

Figure 5 - Dynamic Bayesian Narrative Analysis: posterior probability of each narrative after each evidence item

Evidence and likelihood P(E given N)	N1	N2	N3
E1. 81.8 percent of sector entries are DDoS claims	0.3	0.9	0.5
E2. 23.8 percent of assessed NoName057(16) claims validated	0.3	0.8	0.5
E3. NIS2 member-state data also ranks public administration first	0.8	0.4	0.7
E4. Financially motivated entries only 8 percent of the sector	0.3	0.7	0.5

Result. N2 ends at 0.76: likely (55 to <85). N1 ends at 0.08: highly unlikely (5 to <15). Combined, N2 and N3 give about 0.92 that visibility, not compromise risk, explains the ranking. E3, the NIS2 data, was the only item that moved the analysis back toward ENISA's reading. DBNA shows it was worth the move and not enough to reverse the result.

Recalibration. Treadstone 71 first set the judgment at almost certain (95 to 99). DBNA supports highly likely (85 to <95), and the review carries that band throughout. The finding stands; the band tightens to what the evidence carries.

2.5 Hypothesis Evolution Tracking (HET)

Question. Who ran the 29 December 2025 destructive attack on Polish energy sites?

HET tracks each hypothesis through its lifecycle in a Hypothesis Evolution Matrix, so the reader sees where each judgment stood when each source spoke.

Hypothesis	Event (29 Dec 2025)	ESET (23 Jan 2026)	Dragos (early 2026)	CERT Polska (Jan 2026)	ETL (Sep 2026)
H1. Static Tundra (Dragonfly); FSB Center 16 per vendor reporting	0.30	0.25	0.22	0.42	0.42
H2. Sandworm, GRU	0.45	0.55	0.58	0.38	0.38
H3. Shared access or handoff between Russian services	0.10	0.10	0.12	0.15	0.15
H4. Other actor	0.15	0.10	0.08	0.05	0.05

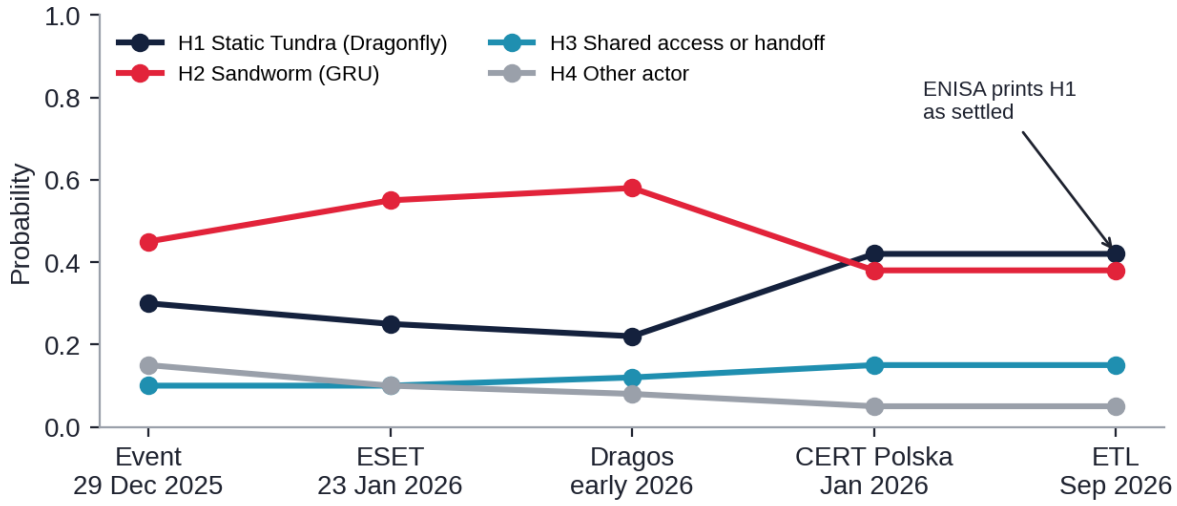

Figure 6 - Hypothesis Evolution Matrix for the Polish energy attack, December 2025 to September 2026

Lifecycle. H2 opened as the base-rate favorite for destructive grid attacks, strengthened on the ESET and Dragos releases, then weakened when CERT Polska, with direct incident access, pointed to Static Tundra and judged the similarity with Sandworm code generic. H1 revived and H3 gained, because two credible clusters with overlapping evidence fit a handoff model. The follow-up report of August 2026 widened the known scope ahead of ETL publication; ENISA reflects neither that report nor the competing assessments. **Result.** Russian state responsibility (H1 plus H2 plus H3) stands at 0.95: almost certain. Between the two named units, H1 holds about 0.52 of the combined weight: roughly even chance (45 to <55). ENISA printed H1 as settled at a point where the matrix shows a near-even contest. HET names the failure precisely: analytic inertia, a frozen snapshot of a moving hypothesis set.

2.6 Narrative Convergence Analysis (NCA)

Question. Whose account of the Collins Aerospace incident did ENISA adopt?

NCA overlays each actor's narrative in time order and marks convergence and divergence.

Date	Actor	Narrative	Assessment
19 Sep 2025	RTX (Collins parent)	Cyber-related disruption to MUSE check-in software	Initial, non-specific
22 Sep 2025	ENISA	Ransomware confirmed	Official position set
17 to 18 Oct 2025	Everest group	Claims the breach via FTP; says no ransomware was used and alleges an insurance-driven shutdown	Adversary narrative, divergent

Date	Actor	Narrative	Assessment
23 Oct 2025	Hudson Rock	Two incidents: ransomware, plus a separate Everest data theft via 2022 infostealer credentials	Convergent with ENISA; adds the second event (B2)
Sep 2026	ENISA (ETL table)	Everest gained FTP access; "airport shutdowns across Europe"	Convergence with the adversary; divergence from ENISA 2025
Sep 2026	ENISA (ETL transport chapter)	Ransomware incident	Consistent with ENISA 2025

Result. One document holds two ENISA narratives.

The table converged on the extortion group's framing, the chapter held the agency's original position, and nothing reconciles them. NCA flags adversary-narrative absorption: a criminal group's claim, including its self-serving denial of ransomware, entered an official record without a marker.

2.7 Perception Discrepancy Analysis (PDA)

Question. Where does the impact the report conveys diverge from verified impact? The Perception-Versus-Reality Matrix records the gap, its cause, and who benefits.

Topic	Perception conveyed	Verified reality	Gap cause	Beneficiary
Hacktivist DDoS	Largest threat category, 51.3 percent of entries	23.8 percent of assessed claims validated; outages temporary	Adversary manipulation, amplified by method	Pro-Russia hacktivist fronts
Hacktivist OT intrusions	124 claims in Q4 2025 alone	Verified disruption limited; most claims name no victim	Adversary manipulation	Same fronts
Collins Aerospace	Airport shutdowns across Europe	Manual check-in and boarding; no airport closed	Conflation error	Everest group
Public administration	Most targeted sector	Most claimed sector; real municipal ransomware load	Counting method	None; budgets misdirected
Ransomware geography	Germany most targeted at 26.5 percent	Leak-site refusals to pay, not attacks	Survivorship bias	None
FIMI reach	Thousands of channels, heavy X activity	Low organic engagement; effect unmeasured	Collection access bias	Russian and Chinese IMS

Result. In four of six rows the gap favors an adversary. The gaps are static until ENISA changes method, which makes them exploitable for twelve months. Two rows favor no one and still cost defenders: budgets follow the public administration headline, and the German figure invites a national response to a statistical artifact. PDA separates the rows by cause, so each gets the right fix. Adversary manipulation needs claim handling. The conflation error needs an editor. Survivorship and collection bias need method notes beside the charts.

2.8 Perspective Distortion Analysis (PDA-2)

Question. Which institutional perspectives shape how the report frames events? PDA-2 maps each actor's frame and classifies the distortion as ideological, organic, or deliberate.

Perspective	Frame applied in the ETL	Effect on the picture	Distortion type
ENISA as EU agency	Spyware operators left unnamed; vendors and victims named	EU member-state conduct escapes grading	Organic institutional

Perspective	Frame applied in the ETL	Effect on the picture	Distortion type
US cloud vendors (48 citations)	Actor names, telemetry, and taxonomies imported	Europe seen through customer telemetry of two firms	Organic commercial
EEAS collection	X at 88 percent of FIMI observables	Platform access defines the threat map	Organic collection
Pro-Russia hacktivist fronts	Claims timed to political events	Claim volume becomes sector ranking	Deliberate, adopted by method
Everest group	Denial of ransomware, blame on victim	Entered the Collins table	Deliberate, adopted by error

Result. No coordinated distortion appears.

The institutional frames are organic, while two deliberate adversary frames entered through ENISA's method and error, and PDA-2 separates them from the rest so each gets its own fix.

2.9 Cognitive Dissonance Mapping (CDM)

Question. Where does ENISA's stated method contradict its observed practice?

The Cognitive Dissonance Matrix pairs each statement with the corresponding action.

Stated position (ETL text)	Observed practice (ETL text)	Source grade	Pattern
Analysts curated the dataset to avoid inflating the threat	Unverified hacktivist claims counted as incidents	B1	Internal inconsistency
Hacktivist claims likely served an influence objective	Executive Summary led with those claims	B1	Internal inconsistency
Cyberespionage is the more impactful long-term threat	Rankings built on volume, where espionage is 6 percent	B1	Internal inconsistency
Top-five intrusion set ranking speaks to lack of stealth	Ranking published anyway	B1	Internal inconsistency
Ransomware confirmed at Collins (September 2025)	Everest FTP narrative printed in the table	B1	Internal inconsistency
No AI-generated content used	AI used in collection and processing, undisclosed	B1	Disclosure gap
Data breaches, fraud, and ransomware overlap	Totals summed without deduplication	B1	Internal inconsistency

Result. Seven contradictions, all visible inside one document.

The pattern is consistent across chapters, which points to process, not intent: separate drafting teams, no reconciliation pass. CDM rules out deliberate deception on the evidence available.

> **Trigger for alignment.** The Cybersecurity Act revision and ENISA Management Board scrutiny are the pressure points most likely to force reconciliation. Watch the next CTL methodology update for claim-handling language.

2.10 Causal Density Mapping (CDM-2)

Question. What actually produces the ETL ransomware country ranking?

CDM-2 lists contributing causes, maps influence between them, and finds the high-density nodes.

Cause	Influence	Mechanism and dependencies
C1. Economic size and number of firms	Strong	More targets; drives C5 and C3
C2. Victim refusal to pay	Strong	Only refusals reach a leak site; gates visibility of every other cause
C3. Affiliate targeting and language preference	Moderate	Shapes which countries affiliates work; feeds C1 effects
C4. Disclosure and regulatory pressure (GDPR, NIS2)	Moderate	Raises payment pressure (Qilin legal-threat feature) and public disclosure alike
C5. Sector mix, led by manufacturing	Moderate	Manufacturing is the top ransomware sector at 25.2 percent
C6. ENISA collection by leak-site monitoring	Strong	Gatekeeper: nothing enters the ranking without passing C2 and C6
C7. Law-enforcement disruption of brands	Weak	Shifts which brand claims, not which country is hit

Result. C2 and C6 are the high-density nodes.

Remove C6 and the ranking disappears; change C2 and the ranking reorders. The ranking is a joint product of attacker behavior, victim behavior, and ENISA's collection lens. Treating it as a map of attacks is a false correlation CDM-2 exposes in one pass.

2.11 Counterintelligence Deception Diagnostics (CIDD)

Question. How reliable are the adversary claimants whose output ENISA counted?

CIDD runs source validation, discrepancy history, communication analysis, and deception indicators on each.

Claimant	Consistency and discrepancy history	Deception indicators	CIDD verdict and ASA handling
NoName057(16)	23.8 percent of assessed claims validated by ENISA	Claims timed to political events; operation branding; retaliation framing	Systematic inflation. Source E; claims enter as adversary claims only
Z-Pentest Alliance and OT claimants	Most claims name no victim and no technique	Screenshots without provenance; escalating claim volume	Unverifiable by design. Source F; information 6
Everest group	Contradicted by ENISA, RTX filing, and Hudson Rock on ransomware	Self-serving blame on victim; leak site vanished after posting	Partly true on data theft, false on cause. Source E; information 4
Babuk2	ENISA itself assesses recycled and fabricated claims	Copycat branding of a defunct group	Fabricator. Source E; exclude from counts

Result. Every claimant ENISA counted carries a documented deception history, and ENISA documented two of those histories itself. CIDD turns a general criticism of claim counting into a per-source exclusion rule. Babuk2 shows the cost of skipping the step: ENISA labeled the group a fabricator in Chapter 3 and still counted its claims. Under CIDD, a source graded E stays out of every count, every chart, and every summary until a second independent source confirms the specific claim. The rule costs ENISA nothing in collection. Adversaries lose their free distribution.

2.12 Cyber Adversary Reflex Mapping (CARM)

Question. How does NoName057(16) react to disruption and exposure, and how will it react to the ETL itself? CARM maps observed triggers to reflexes, then forecasts.

Trigger	Type	Observed reflex (ETL data)	Reflex class
Telegram removals of 60+ groups, Q1 2025	Operational disruption	Alias changes and migration off the platform	Dispersal
Operation Eastwood, July 2025	Operational disruption	Surge from mid-July to mid-August; Germany became the main target	Retaliatory surge
Danish Ukraine aid package, November 2025	Political stimulus	Campaign against Danish transport and ministries	Punitive signaling
ETL 2026 publication	Exposure event	Forecast below	Validation seeking

Forecast. The next law-enforcement action against DDoSia infrastructure produces a retaliatory surge within weeks: likely (55 to <85). A pro-Russia channel citing ETL figures as proof of reach within twelve months: roughly even chance (45 to <55).

Counteraction. Publish the validated-claim ratio beside every hacktivist count. An adversary that needs perceived reach loses the payoff when the official record reports its failure rate first.

2.13 Adaptive Threat Calibration and Risk Indexing (ATCRI)

Question. What should the EU threat priority order be, measured by consequence instead of volume? ATCRI runs a paired comparison across eight threat categories, then a weighted impact score. Scoring follows the corrected ATCRI rule in the corpus: Weighted Score = 20 × (0.3 Likelihood + 0.3 Severity + 0.4 Strategic Impact), each factor rated 1 to 5 against the corpus anchors, range 20 to 100. Ties break by paired order.

Threat category	L	S	I	Score	Paired wins (of 7)	ETL volume position
State espionage via edge devices and identity	5	4	5	94	7	Small share
Destructive state operations on energy and infrastructure	3	5	5	88	6	One sentence
Ransomware and data extortion	5	4	4	86	5	Second
Supplier and third-party compromise cascades	4	4	4	80	4	Anecdotal
DPRK IT-worker placements	4	3	4	74	3	Insider share
Russian-led FIMI	5	2	4	74	2	Separate chapter
Hacktivist OT intrusion claims	3	2	3	54	1	Rising claims
Hacktivist DDoS	5	1	2	52	0	First

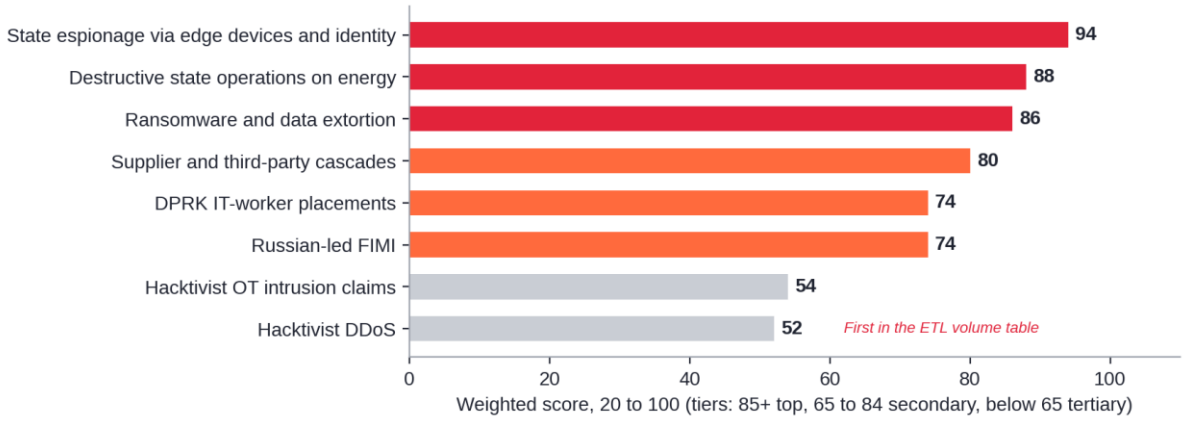

Figure 7 - Consequence ranking (ATCRI) against the ETL volume ranking

Result. The category ENISA's data puts first ranks last by consequence, while the category ENISA gives one sentence ranks second. DPRK placements and Russian-led FIMI tie at 74; DPRK takes the higher rank on paired order, having won the pair on direct access inside EU defense firms. Recalibration triggers: a verified hacktivist OT disruption raises that row's severity to 4 (score 66); a second destructive state operation in the Union raises its likelihood to 4 (score 94).

2.14 Domain Screening

Fourteen further techniques were run as screens. Each asks whether the report covers the ground the technique is built for.

Technique	Screen result	Gap exposed
Cyber Threat Convergence Analysis (CTCA)	ENISA asserts convergence of criminal, hacktivist, and state activity	No convergence risk scoring; Moonstone Sleet use of Qilin cited without a score
Hybrid Warfare Vulnerability Matrix (HWVM)	No cross-domain intersection mapping	Cables, GNSS jamming, and sabotage recruitment absent
Cognitive Warfare Impact Assessment (CWIA)	Engagement counted; sentiment shift unmeasured	No audience segmentation or effect measure
Influence Infrastructure Mapping (IIM)	EEAS maps Portal Kombat, Paperwall, and shared amplifiers	Partial credit; no weak-point or disruption simulation
Synthetic Influence Payload Dissection (SIPD)	AI content judged low quality by assertion	No AI-origin dissection method stated
Insider Threat Behavior Profiling (ITBP)	DPRK placements logged as a percentage	No baseline, anomaly, or risk-scoring model
Blockchain Exploitation Pathways Analysis (BEPA)	Drainers and DPRK theft discussed	Bybit theft absent; no laundering-pathway analysis
Recursive Malicious Code Attribution (RMCA)	Polish code overlap described as general by CERT Polska	No attribution confidence scoring applied
Adversary Threat Vector Analysis (ATVA)	Vectors known in 5.2 percent of cases	No adversary profiling behind vector claims
Disruptive Technology Threat Mapping (DTTM)	AI outlook without technology risk scoring	No capability-by-adversary matrix
Weaponized AI and Autonomous Conflict Scenarios (WAACS)	Human-out-of-the-loop mentioned once	No scenarios or signposts
Supply Chain Intelligence Mapping (SCIM)	Supplier incidents cited as examples	No dependency map, including EU reliance on CISA KEV and the CVE program

Technique	Screen result	Gap exposed
Economic Influence and Coercion Analysis (EICA)	Economic drivers absent	Sanctions, crypto markets, and state vulnerability law unaddressed
Adversarial Cognitive Simulation (ACS)	Adversary decision calculus absent	No model of why Russia pairs destructive attacks with hacktivist noise

3. Gaps and Remedies

Nineteen gaps, grouped by failure type. A remedy counts here only if it exists today on treadstone71.com or ships on a dated release.

3.1 Method gaps

Gap 1. Survivorship bias in the ransomware data

A victim appears on a leak site when negotiation fails. Victims who paid quietly never appear. ENISA's roughly 1,144 ransomware entries count refusals to pay, not attacks. Germany at 26.5 percent of ransomware claims means German victims refused more often, or German firms were listed more often, or some mix of the two. The report never asks. Treadstone 71 assesses as **highly likely (85 to <95 percent)** that the leak-site country and sector rankings misstate true victimization.

> **Treadstone 71 remedy.** Under the ASA Standard, each data stream receives a collection-bias grade before it enters a score. A leak-site listing enters as an adversary claim and caps the credibility grade. ASA Rule 2 (admission against interest) separates what an adversary says in its own disfavor from what it says to sell itself.

Gap 2. No normalization

Raw counts by member state appear with no denominator: no GDP, no firm count, no internet-exposed asset count. Germany leads because Germany is large. The ecological fallacy, applied across 27 countries.

> **Treadstone 71 remedy.** TAI publishes composite scores across 8 sub-indices and 4 tiers, so rank reflects weighted capability and intent, not raw volume. Treadstone 71 client work applies the same rule to victim-side analysis: rate per exposure unit, never raw count.

Gap 3. Admitted overlap, never deduplicated

ENISA states that data breaches, fraud, and ransomware are expected to overlap, then sums them anyway. One stolen dataset counts up to three times.

> **Treadstone 71 remedy.** ASA scoring runs one event, one record, with linked observables. Duplicates collapse before scoring. The CTI Program Build course on the Cyber Intelligence Training Center teaches the same intake rule.

Gap 4. No forecast accountability

ETL 2025 made forecasts. None are graded in ETL 2026. The outlook offers no scenarios, no signposts, no alternative hypotheses, and no dates. An agency that never scores its own predictions has no basis to claim calibration.

> **Treadstone 71 remedy.** TAI runs on crowd-forecast values with trigger zones set at plus or minus 5 points of each tier boundary, and the ASA Standard carries a re-grade rule. The 5 October 2026 release pairs the TAI Q3 refresh with the CWTR inaugural, putting prior calls under scrutiny on a published date.

3.2 Analytic gaps

Gap 5. No intent or capability model

ENISA names 52 state intrusion sets and ranks the top five by how many member states each touched. Its own text concedes the ranking mostly speaks to a lack of stealth. Mustang Panda and Salt Typhoon, the actors that matter most to maritime and telecommunications operators, fall outside the list. No capability score, no intent score, no trend line. A defender learns who was loud.

> **Treadstone 71 remedy.** TAI v2.1 scores 42 actors plus 7 Iranian-Axis annexes across 10 clusters. Canonical Tier 0 scores: China 89, Russia 85, DPRK 79, Iran 78. The free edition carries all four at three-tearline depth at treadstone71.com/tai, answering the question ENISA declined: which adversary matters most, and by how much.

Gap 6. No deception analysis of adversary claims

ENISA recognizes that NoName057(16) inflates. Yet no structured deception test runs anywhere in the report. Claims enter the dataset at face value and leave as statistics.

> **Treadstone 71 remedy.** Counterintelligence Deception Diagnostics and Cyber Adversary Reflex Mapping, each in the Treadstone 71 Advanced SATs Practitioner's Manual. CIDD grades every claimant on consistency, discrepancy history, and deception indicators before its output enters a count. CARM maps how the claimant reacts to takedowns and exposure, then forecasts the next reflex.

Gap 7. No counterintelligence lens

The word counterintelligence appears zero times in 101 pages.

DPRK IT workers inside EU defense firms are logged as an insider-threat percentage. That is a hostile placement operation. The questions that matter go unasked: what did the worker access, who vetted the hire, what collection requirement drove the target selection, and what else has the same recruiter touched?

> **Treadstone 71 remedy.** Cyber counterintelligence has been a founding Treadstone 71 discipline since 2002, taught through the online Cyber CI bundle with client-tailored workbooks. The method treats each placement as an operation with a tasking path, a handler, and a collection requirement, then works backward to the exposure.

Gap 8. No driver analysis

Geopolitics appears as a trigger for DDoS waves.

Economic, legal, and technological drivers never appear as analytic categories. China's vulnerability-disclosure regime, which routes zero-days to the state before vendors, goes unmentioned in a chapter about China-nexus zero-day exploitation. DPRK revenue generation appears, yet the February 2025 Bybit theft of roughly USD 1.5 billion, attributed by the FBI to DPRK and the largest cryptocurrency theft on record, does not.[12][13] ENISA cites a 2024 figure instead.

> **Treadstone 71 remedy.** STEMPLES Plus, developed by Treadstone 71, forces every assessment through social, technical, economic, military, political, legal, educational, and security drivers plus added factors before a judgment issues. The Cognitive Warfare Monitor tags every driver with STEMPLES Plus codes.

Gap 9. Cognitive warfare measured as content, not effect

The FIMI chapter counts incidents, channels, videos, and views. No section asks whether any audience changed a belief or a behavior. The word cognitive appears once. Views measure distribution. Effect requires baselines, target audience analysis, and measures of effectiveness kept separate from measures of performance.

> **Treadstone 71 remedy.** The Cognitive Warfare Monitor (treadstone71.com/cognitive-warfare-monitor, inaugural edition 12 October 2026) runs weekly narrative briefs with Admiralty-graded sources and Kent bands, rolls up monthly, and ties to TAI quarterly. Jeff Bardin's book The Mind Domain and the online cognitive warfare course teach effectiveness against performance, while the ASA F-Score asks the effect question ENISA never asks: what did the operation most likely achieve?

Gap 10. No alternative analysis

No hypothesis tracking, no Bayesian updating, and no check of the agency's statements against its own practice anywhere in the report, including the Polish attribution where two credible hypotheses existed on the public record.

[12] FBI Internet Crime Complaint Center, Alert I-022625-PSA, North Korea Responsible for $1.5 Billion Bybit Hack, 26 February 2025: https://www.ic3.gov/PSA/2025/PSA250226
[13] Chainalysis, 2025 Crypto Theft Reaches $3.4 Billion: https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2026/

> **Treadstone 71 remedy.** The Advanced SATs Practitioner's Manual puts Minimal Viable Hypothesis Testing, Dynamic Bayesian Narrative Analysis, Hypothesis Evolution Tracking, and Cognitive Dissonance Mapping ahead of publication. Applied here, DBNA pulled one of Treadstone 71's own judgments down a band before release.

3.3 Coverage gaps

Gap 11. The hybrid cyber-physical nexus

Absent: undersea cable incidents in the Baltic, GNSS jamming against aviation, and Telegram recruitment of disposable saboteurs. Sabotage appears only inside the FIMI chapter as a companion to narratives. The clandestine pipeline that turns cyber reconnaissance and online recruitment into physical sabotage is absent from a report that claims to cover threats to the Union.

> **Treadstone 71 remedy.** Clandestine cyber HUMINT, run under approved rules of engagement, works the recruitment channels directly. The Russia UAV intelligence product line tracks the cyber-to-kinetic seam through Russian-language firmware and channel analysis.

Gap 12. The United States policy shock

ENISA became a CVE Root in November 2025 and runs the European Vulnerability Database. The report never names the April 2025 CVE program funding crisis that made the two moves urgent. Nor does it mention reductions at CISA or the lapse of the US Cybersecurity Information Sharing Act of 2015 on 30 September 2025. The report still relies on the CISA Known Exploited Vulnerabilities catalogue for its exploited-vulnerability backbone and never assesses that dependency.

> **Treadstone 71 remedy.** The STEMPLES Plus political and legal driver sweep flags allied policy volatility as a threat driver in its own right. Partial remedy only: the dependency decision belongs to ENISA.

Gap 13. No impact measurement

No loss figures for 2025.

The only euro figure, EUR 4.2 billion in investment fraud, covers 2024. No downtime, no dwell time, no ransom payments, no victim counts.

> **Treadstone 71 remedy.** The ASA F-Score scores the most likely achieved endgame for each adversary operation, putting effect ahead of activity.

Gap 14. Mandatory data pushed to a footnote

NIS2 produced 1,954 reported events for 2025. Of 941 malicious events, about half list the root cause as unknown. That finding indicts NIS2 reporting quality across the Union, and it sits in a footnote while claim counts fill the main tables.

> **Treadstone 71 remedy.** None. NIS2 mandatory reporting sits outside Treadstone 71's reach. The fix is method: ENISA should move its best data to the center of its analysis.

Gap 15. Native-language collection

Citations run overwhelmingly to English-language Western vendor reporting. Iranian state-aligned hacktivist personas such as Handala and CyberAv3ngers never appear, despite the June 2025 Israel-Iran war sitting inside the reporting period. Persian, Arabic, and Russian primary sources appear only as raw Telegram links.

> **Treadstone 71 remedy.** Native-language source work in Farsi, Arabic, and Russian is core Treadstone 71 practice. The Russia UAV product line analyzed the 1001 drone firmware from Russian-language channels, and Treadstone 71 mapped the Persian-language worldwar3.ir threat network at the source.
>
> ENISA reads what vendors translate. Treadstone 71 reads what adversaries write.

Gap 16. EU institutions missing from their own picture

CERT-EU appears zero times. Threats against the Commission, the Parliament, and EU agencies stay in a separate stovepipe while the report claims to cover the Union.

> **Treadstone 71 remedy.** Partial only. Treadstone 71 fuses open, adversary-side, and client-side collection into one picture per engagement, without access to CERT-EU holdings.

3.4 Delivery gaps

Gap 17. Timeliness

Calendar 2025 published in September 2026, with six months of overlap with ETL 2025 and trends already described. Nine months of lag on a threat that moves weekly. The AI box reaches into 2026 selectively while the 2026 Middle East escalation stays out of period.

> **Treadstone 71 remedy.** Three cadences stacked: the Daily Adversary Brief at 06:00 (treadstone71.substack.com), the weekly Cognitive Warfare Monitor, and quarterly TAI releases.

Gap 18. No decision linkage and no defender view

No priority intelligence requirements, no audience-specific actions, no control-failure analysis, and no NIS2 transposition status. The word recommend appears twice in 101 pages. ENISA informs; it never tells a board what to do on Monday.

> **Treadstone 71 remedy.** The Treadstone 71 standard: if it does not change the decision, it is not intelligence. Every Treadstone 71 assessment opens with TL;DR, BLUF, Who, What, So What, Why Now, and Outlook, and ends on action. The Intelligence Program Build service (treadstone71.com/services/intelligence-program-build) starts from the client's decisions and works back to requirements and collection.

Gap 19. Analytic writing quality

"ENISA assess." "Highly likely increasingly." Estimative words stacked without time bounds, corrupted figure numbers, and a table that contradicts its own chapter. The text never passed an editor trained in intelligence prose.

> **Treadstone 71 remedy.** Analytic writing training, the Kent spectrum with half-open intervals, the expanded Admiralty grid, and a house standard applied to every deliverable before release.

4. So What: Who Cares

CISOs and boards will read public administration first and DDoS first, then fund scrubbing. The losses sit with ransomware, stolen identities, and compromised suppliers. Misallocation is **likely (55 to <85 percent)** wherever the ETL drives a risk register without a denominator check.

NIS2 competent authorities inherit a baseline that sidelines their own mandatory data. The root-cause gap in NIS2 reporting deserves the headline; it got a footnote.

Commission policy teams drafting the Cybersecurity Act revision will anchor on claim counts unless someone puts the denominators in front of them.

Insurers and underwriters pricing European cyber risk on sector rankings will price hacktivist marketing.

Consequence ranking. Adaptive Threat Calibration and Risk Indexing scores eight EU threat categories on likelihood, severity, and strategic impact. State espionage through edge devices and identity leads at 94. Destructive state operations against energy follow at 88, ransomware at 86. Hacktivist DDoS, first in ENISA's data, finishes last at 52.

Moscow wins twice. NoName057(16) gets its claims certified by an EU agency, and the most serious Russian destructive attack of the year reads as a one-line entry with a contested attribution presented as settled.

4.1 Crosswalk: Failure to Remedy

ENISA failure	Treadstone 71 remedy
Claims counted as incidents	ASA adversary-claim caps; CIDD per-claimant verdicts
Confidence fused with likelihood	Kent half-open bands; separate Admiralty axes
Percentages without n	Sample disclosure on every rate
Loud actors ranked first	TAI composite scores across 42 actors
Views counted as cognitive effect	Cognitive Warfare Monitor with effectiveness kept separate from performance
No counterintelligence lens	Cyber CI training and client workbooks
Missing economic and legal drivers	STEMPLES Plus driver sweep
Vendor-translated collection	Native-language adversary-side collection
Nine-month lag	Daily brief, weekly monitor, quarterly index
No forecast scoring	Crowd forecasts, trigger zones, re-grade rule
No decision linkage	Decision-first program build; action-ending products

5. Where Treadstone 71 Does Not Solve the Problem

Three limits, stated plainly. First, Treadstone 71 has no access to NIS2 mandatory reporting, Europol case data, CERT-EU holdings, or member-state classified holdings. ENISA's best data is data Treadstone 71 does not see, and the remedy there is method ENISA should adopt, not a product for sale.

Second, Treadstone 71 is also a commercial vendor, so the vendor-bias critique in Finding 5 applies to Treadstone 71 as well. The mitigation is a published, citable method that any reader audits (the ASA Standard is published under a DOI), graded sources on every claim, and grades applied to partner states as well as adversaries.

Third, Treadstone 71 is a founder-led firm. Continental-scale incident coverage sits outside its reach. The value lies in depth, adversary-side collection, and decision linkage, not breadth.

6. Evidence Grading

6.1 The report's core claims

Grades sit at the ASA entry anchor. Source and information axes are graded independently and never averaged.

Claim cluster	Source reliability	Information credibility	Basis
Sector and objective rankings	B: Usually reliable (ENISA as publisher)	4: Doubtful	Built on unverified hacktivist claims; 23.8 percent validation rate on the largest contributor
Vector percentages (60.4 and 70 percent)	B: Usually reliable	5: Improbable as generalized	True only for subsets of about 103 and 70 incidents
State-nexus narratives drawn from joint advisories	A/B: National CERTs and joint CSAs	2: Probably true	Consistent with multiple independent government sources
Collins Aerospace table entry	B: Usually reliable	5: Improbable as written	Contradicted by ENISA's own September 2025 statement and its own transport chapter
Polish energy attribution to DragonFly	B: Usually reliable	3: Possibly true	Matches CERT Polska; contested by ESET and Dragos; competing hypothesis omitted
AI outlook for 2026	B: Usually reliable	6: Truth cannot be judged	No time bound, no indicator, no test
FIMI incident counts (EEAS)	B: Usually reliable	3: Possibly true	Collection skewed toward X; 65 percent unattributed

6.2 External evidence used in the review

Item	Source reliability	Information credibility	Basis
CERT Polska energy-sector incident report (January 2026)	A: Completely reliable	1: Confirmed	National CERT with direct incident access; scale corroborated by ESET and Dragos
CERT Polska follow-up report (August 2026)	A: Completely reliable	1: Confirmed	Direct incident access; adds a second heat and power plant and the private APN vector
ESET and Dragos Sandworm attribution	B: Usually reliable	3: Possibly true	Medium and moderate confidence; CERT Polska calls the code overlap general
ENISA statement confirming Collins ransomware (22 September 2025)	B: Usually reliable	1: Confirmed	Consistent with the RTX SEC filing; ransomware family still contested
Hudson Rock two-incident analysis of Collins	B: Usually reliable	2: Probably true	Infostealer log evidence; consistent with the timeline
Everest claims on Collins	E: Unreliable	4: Doubtful	Adversary claim; leak site vanished after posting
FBI attribution of the Bybit theft to DPRK (February 2025)	A: Completely reliable	1: Confirmed	Official attribution corroborated by on-chain tracing firms

6.3 Treadstone 71 estimative judgments

Judgment	Band	Time bound
Sector and objective rankings reflect claim visibility more than compromise risk	Highly likely (85 to <95)	Reporting period 2025
The Collins table entry conflates two incidents	Highly likely (85 to <95)	September 2025
Leak-site rankings misstate true victimization	Highly likely (85 to <95)	Reporting period 2025
Headline figures appear stripped of denominators in vendor and national material	Likely (55 to <85)	By 23 October 2026
ETL 2027 continues to count claims as incidents	Likely (55 to <85)	Next ETL release
A pro-Russia hacktivist channel cites ETL 2026 figures	Roughly even chance (45 to <55)	By September 2027
Russian state responsibility for the Polish energy attack	Almost certain (95 to 99)	29 December 2025

6.4 Sources Consulted

- ENISA, ENISA Threat Landscape 2026, September 2026. ISBN 978-92-9204-807-5, DOI 10.2824/0806036.
- CERT Polska, energy-sector incident report on the 29 December 2025 attacks, January 2026 (cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/).
- CERT Polska, follow-up report on the December 2025 energy-sector incident, August 2026 (cert.pl/en/posts/2026/08/incident-follow-up-report-energy-sector-2025/).
- ESET Research, Sandworm attribution of the late-2025 attack on Poland's power grid, 23 January 2026 (welivesecurity.com).
- The Hacker News, "Poland attributes December cyber attacks," January 2026, reporting CERT Polska, ESET, and Dragos positions.
- Hudson Rock (infostealers.com), Collins Aerospace Hit Twice: 2022 Infostealer Infection Enabled a Separate Breach, 23 October 2025 (graded B2).
- Infosecurity Magazine and SecurityWeek, UK National Crime Agency arrest and contested ransomware family in the Collins Aerospace case, September 2025.
- BlackFog, timeline of the Collins Aerospace ransomware attack, including ENISA confirmation of 22 September 2025.
- Cyber Daily, Everest claim of the Collins Aerospace breach, 18 October 2025.
- FBI, public attribution of the Bybit theft to DPRK, February 2025.
- Treadstone 71, ASA Evidence Standard, Public Edition 1.0, DOI 10.5281/zenodo.22662242.
- Treadstone 71, Advanced SATs corpus (33 techniques), including the corrected ATCRI scoring rule.

7. Outlook and Conclusion

7.1 Fix Order for ETL 2027

- Separate verified incidents from adversary claims in every table and chart.
- Publish n beside every percentage, including the Executive Summary.
- Split confidence from likelihood; add almost certain; close the band overlaps at 60 and 90.
- Time-bound every forecast and attach signposts; grade the ETL 2026 forecasts in ETL 2027.
- Present competing attributions side by side with a band for each.
- Move NIS2 mandatory reporting to the analytic center and report the root-cause gap as a finding.
- Normalize member-state figures by exposure and deduplicate overlapping cybercrime entries.
- Disclose the AI tools used in collection and processing, with validation method and error rate.

7.2 Conclusion

ENISA built a census. Defenders need an assessment.

The findings and gaps above share one root: the report measures what adversaries and vendors publish, then skips the steps that turn counts into judgment. Claimant diagnostics, denominators, normalization, driver analysis, hypothesis tracking, and stated confidence each fix a named error, and each already runs in Treadstone 71 practice. The state-actor chapter, the ShinyHunters kill-chain box, and the DDoSia validation work deserve to survive into ETL 2027. Its quantitative spine does not.

The Advanced SATs added what the classic set lacked. DBNA put a number on the core finding and pulled Treadstone 71's own judgment down one band before release. HET showed the Polish attribution as a moving contest ENISA froze. CIDD and CARM turned a general complaint about claim counting into per-source exclusion rules and a counteraction that denies NoName057(16) its payoff. ATCRI and the ETL volume ranking agree on almost nothing: hacktivist DDoS leads the ETL volume table and scores 52 by consequence, the lowest of eight, while edge-device and identity espionage by states tops the index at 94.

Until ENISA separates claims from verified incidents, treat every ETL 2026 percentage as a claim count, and discount the sector ranking by the 76.2 percent of NoName057(16) claims ENISA itself failed to verify.



ABOUT TREADSTONE 71

Treadstone 71 is a veteran-owned cyber and strategic intelligence training and consulting firm, operating since 2002. The firm delivers adversary intelligence, cyber counterintelligence, cognitive warfare analysis, and structured analytic training to government and corporate clients. Its published methods include the ASA Evidence Standard and the Treadstone 71 Adversary Index. More information about Treadstone 71 and its work is available at treadstone71.com.

Treadstone 71 LLC
Half Moon Bay, California
United States